EDF-2021-SPACE-D: Resilient space-based PNT and SATCOM

EDF-2021-SPACE-D-SNGS: Space and ground-based NAVWAR surveillance

This call aims at improving space-based PNT resilience in contested environments through the mapping and analysis of threats. It will complement the on-going EDIDP project on Galileo PRS receivers and contribute to reinforce Galileo as a credible European solution for defence applications.

This call aims also at accompanying the development of European technologies and products for interoperable and resilient military satellite communications.

Proposals are invited against any of the following topics

- **EDF-2021-SPACE-D-SNGS:** Space and ground-based NAVWAR surveillance;

Budget

The Union is considering a contribution of up to EUR 50 000 000 to support proposals addressing any of the abovementioned topics and their associated specific challenge, scope, targeted activities and main functional requirements.

Several actions, addressing different topics, may be funded under this call.

The Commission will pay particular attention to existing and on-going developments within the Union to avoid unnecessary duplication.

Specific challenge

Navigation Warfare (NAVWAR) concept appeared in PNT[1] landscape more than twenty years ago. During those past decades, the PNT defence community mainly focused on acquisition and toughening GNSS (Global Satellite Navigation Satellite System) user segment, improving inertial sensors, and exploring alternate PNT capabilities (*e.g.* vision- based navigation).

Further work is nevertheless required to achieve PNT superiority in joint operations/missions. Indeed, NAVWAR entails more than resilient GNSS-based equipment or GNSS-free sensors. It also consists in knowing and dealing with the threat (*e.g.* on performing a spectrum and spatial surveillance). Some R&T initiatives allowed identifying some promising tools and technologies, but PNT sensors in use today mainly supports resiliency aspects of NAVWAR, and so do not fully provide a full-spectrum capability.

PNT sensors need to be resilient, but also to deliver information for NAVWAR surveillance and NAVWAR offensive measures. Galileo PRS[2] receivers themselves should contribute to the full-spectrum NAVWAR capability, becoming part of a NAVWAR sensor network, leveraged by associated C2 systems. Therefore for the targeted NAVWAR capability, a wide range of sensors including mobile applications (*e.g.* smart architectures, hand-held PRS receivers) and space-based surveillance needs to be available, in conjunction with Galileo PRS signal and

[1] Positioning, Navigation and Timing.
[2] Public Regulated Service.

service, in order to support a comprehensive NAVWAR situational awareness picture and NAVWAR offensive measures.

To face this challenge and preserve Europe sovereignty, this call topic aims at building an EU NAVWAR capability gathering efforts and federating means of the Member States. Such an EU NAVWAR capability will contribute to the unlimited and uninterrupted access to the Galileo PRS worldwide (Decision 1104/2011/EU), on EU Member States territory and abroad during operations or missions.

Scope

The proposals must aim at developing a comprehensive EU NAVWAR capability, relying on space-based and ground-based surveillance, and complementing current European efforts to strengthen the future Galileo PRS service resilience for military applications and the development of the user segment used by the forces of the EU Member States. To this end, the proposals must address the NAVWAR overall system, including a modular NAVWAR information-management system, networked with NAVWAR subsystems and NAVWAR PRS sensors. The objective is to achieve overall global capability dealing simultaneously with resilience, surveillance, and offensive measures. Different NAVWAR PRS sensors, along with common interfaces, must be determined and combined in various use cases as NAVWAR subsystems (integration environments) to create a NAVWAR network. They must include Galileo as PNT source and Galileo PRS as a PNT service. The interfaces with other communities and stakeholders must be specified as part of the proof of concept.

The proposals must address the following crucial development strands:

1. Support, via a space-based and ground-based NAVWAR surveillance system, the nominal performances of GNSS/PRS receivers in a contested and hostile electromagnetic environment;
    - Allowing localization, identification and characterization of main threats, and monitoring of GNSS signals;
    - Including the federation of NAVWAR operational centres (used by the Member States based on a NAVWAR information-management system for data exploitation and C2 of the network of NAVWAR sensors/subsystems (space and ground)), that will support the implementation of the overall NAVWAR capability (including PRS);
    - Including interfaces with other communities in order to exchange NAVWAR situational awareness picture and recommended offesnsive measures;
    - including common standards for NAVWAR surveillance interoperability among EU Member States;
2. Develop a modular PRS mobile receiver concept[3] able to contribute to the network of NAVWAR sensors/subsystems, and possibly benefit from the overall capability; functional requirements related to data content and delivery aspects, must in particular properly identify typical performance features[4] that must be made available to the user segment through a secondary channel or in a server-based GNSS service approach;

[3] Able to meet the integration in different hosts with a minimum SWaP-C (Size, Weight and Power and Cost) feature for a wide range of mobile user-segment applications in a military cross-domain framework.
[4] Performance requirements must be set for specific performance features in the trade-off engineering process.

- This must include a risk reduction phase for maturation of miniaturized, modular, and SWaP-C optimized mobile PRS technologies and analysis regarding availability by EU vendors;

3. Implement anti-jamming and anti-spoofing technologies in secure innovative architectures to support PNT superiority.

All aforementioned workstrands must take into account on-going EU funded initiatives, in particular Galileo 2nd generation, and complement the on-going EDIDP GEODE developments/designs with modular miniaturized form factor PRS technologies, in particular for small platforms or mobile use cases.

The proposals must provide an efficient answer to the following operational concerns:

- Regarding NAVWAR surveillance:
  - Detect illegitimate activities (*e.g.* jamming, spoofing) in GNSS frequency bands distinguishing between intentional or unintentional sources;
  - Provide RF and content analysis of detected signals;
  - Geolocate and track sources of malicious activities;
  - Deliver a NAVWAR situational awareness picture;
  - Support EU GNSS and Galileo signal-in-space monitoring;
- Regarding Offensive measures:
  - Provide analysis tools for the recommendation of offensive NAVWAR measures
- Regarding system architecture:
  - Identify the added-value of a NAVWAR sensor network;
  - Establish the role of Galileo PRS equipment in the overall NAVWAR capability;
  - Provide a perspective on offensive capabilities accessible via PRS equipment;
  - Provide, via the PNT sensors, information on the Quality of Service of PRS and OS[5] signals;
  - Provide options for the exchange of the NAVWAR situational awareness picture between NAVWAR centres and to electronic warfare (EW), Cyber or other communities.

Targeted activities

The proposals must cover the following activities as referred in article 10.3 of the EDF Regulation:

- Studies, such as feasibility studies to explore the feasibility of new or improved technologies, products, processes, services and solutions;
- The design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such design has been developed which may include partial tests for risk reduction in an industrial or representative environment;

[5] Operating Systems

- The development of a model of a defence product, tangible or intangible component or technology, which can demonstrate the element's performance in an operational environment (system prototype);
- The testing of product, tangible or intangible component or technology. In particular the proposals must address the following tasks:

- General Considerations:

- Definition and description of the general EU NAVWAR concept and gathering of user requirements;
- Functional and performance analysis of typical scenarios (to be defined) to allow the detection and localization of jammers and spoofers, based on both system-scale and sensing payloads simulations;
- Identification of various EU NAVWAR system architectures depending on KPIs[6] coming from user requirements (*e.g.* RF sensitivity, localization accuracy, refresh rate of information...);
- Studies regarding standardization and interoperability recommendations;

- NAVWAR Sensors:

- Design, prototyping and evaluation of various types of sensing payloads (including PRS);
- Study and design of a PRS mobile receiver, including study, prototyping and testing of identified technological hard points able to support, and possibly benefit from, the overall NAVWAR capability as part of the network of NAVWAR sensors/subsystems for dedicated military applications and use cases (dismounted, hand held, wearable or miniaturized integration, etc.);
- Study and implementation (proof of concept) of NAVWAR capabilities into PRS receivers;

- NAVWAR subsystems:

- In-orbit demonstration of (a portion of) the space-based NAVWAR surveillance capability;
- Study and implementation (proof of concept) of a common interface for various types of PNT/PRS-based NAVWAR subsystems in order to support the communication with the NAVWAR information-management system;
- Study, design and development (proof of concept) of integration environments for a network-based recognised picture of the NAVWAR situation for mobile applications (smart architectures, mobile radios) including housing, antennas, electronics and GUI;

- NAVWAR Overall system

- Study, design and development (proof of concept) of the federation of NAVWAR operational centers, including algorthms prototyping and implementation of the NAVWAR information management syste, to demonstrate NAVWAR situational awareness (elaboration and and update of a NAVWAR recognised picture);

[6] Key Performance Indicators

- Study and implementation of a PoC for a common interface and analysis tool for the NAVWAR information-management system to:
  - Manage the network of NAVWAR sensors/subsystems;
  - Recommend NAVWAR offensives measures (including at PNT sources level);
  - Interface with electronic warfare (EW), Cyber, Competent PRS Authority (CPA) and other communities (NAVWAR measures and exchange).
- Comprehensive demonstration of a situational awareness picture that rely on a NAVWAR sensors/subsystems grid network composed of mobile, ground and space equipment including Galileo PRS receivers.

Functional requirements

NAVWAR sensors:

- The modular miniaturized and SWaP-C optimized PRS receiver concept, including study, prototyping and testing of identified technological hard points, should support the integration in different hosts (NAVWAR subsystems). Solutions should support standard interface (including ICD[7]) or implement an Open Systems Modular Architecture for integration in different environments;
- The security architecture (proof of concept) should support smart architecture or server-based solutions for a wide range of mobile applications (encompassing high mobility domains).

NAVWAR subsystems:

- The sensing payload should cover all current GNSS frequency bands (Galileo, GPS, Glonass, Beidou...);
- The satellite system should allow to cover every region, worldwide, at least once every 2 days;
- The ground control segment of the satellites should implement an interface with the NAVWAR information-management system that supports data distribution to the analysis tool;
- The GUI for each component in charge of displaying NAVWAR information should be user-friendly;
- Peripheral technology developed for the mobile use cases should be able to support the contribution to a network of NAVWAR sensors/subsystems;
- In order to enable the NAVWAR sensors/subsystem network, all considered solutions mobile and satellites, should be able to identify jamming and spoofing events and then transmit (at least by defining an ICD) the data for further analysis by the NAVWAR information-management system;
- The mobile solutions should cover Galileo PRS on both frequencies and all GNSS open signals frequencies;
- The mobile PNT solution may also encompass integrated non-GNSS and/or non RF technology using sensor fusion algorithms and artificial intelligence;
- A small passive antenna-technology addressing relevant operational environmental conditions may be developed;

[7] Interface Control Document.

- The solutions should encompass a software defined approach and show compliance and interoperability with standardized PRS receivers already developed, able to be upgraded during their operative life through continuously updated libraries.

NAVWAR overall system:

- The system should geolocate and track, with an average accuracy better than 5 km, RF signals emitting at least 10 W power in GNSS frequency bands;
- The system should include all tools (*e.g.* graphical, algorithms...) in order to understand the NAVWAR picture on any area of interest. Especially, the system should handle chronological events to apprehend the evolution of the NAVWAR picture (including standardization of a recognised picture of the NAVWAR situation);
- An analysis tool should be developed to allow performance analysis of Galileo PRS and other GNSS signals to detect jamming and spoofing based on the data provided by the network of NAVWAR sensors/subsystems;
- The NAVWAR information-management system should implement a modular concept that includes common interfaces for the exchange of :
    - information with the network of NAVWAR sensors/subsystems;
    - Recommendations and tasking for NAVWAR offensives measures (including PNT sources);
    - Recommendations for NAVWAR resilience categories towards the mission planner;
    - information with EW, cyber and other communities;
    - information with CPAs internal systems;

- A common ICD (*e.g.* messages) for the system should be defined to address the whole network of NAVWAR sensors/subsystems and the NAVWAR overall capability (resilience, surveillance and offensive measures);
- The system should include a function to store raw data and refined data.
- The system should be able to provide a standardized NAVWAR analysis to the user who requests it, through a predefined and automated process that will make available *added-value information* to the PRS user segment via space and/or terrestrial communication links. *Added-value information* could be for example (not exhaustive list):
    - Availability of required accuracy (probability that PVT[8] data is provided with a certain level of accuracy);
    - EMI[9] localization accuracy (error of location measurement of an interfering signal);
    - GNSS-denied accuracy (error in PVT data when there is a loss of GNSS signal reception).

Innovative solutions should consequently be envisaged (study, design, proof of concept) to exploit “smart” or “server-based” PRS service architecture[10] able to make the aforementioned added-value information available to the end user.

[8] Position, Velocity and Time.

[9] Electro Magnetic Interference.

[10] Respectively with specific PRS crypto technology - or without any - built into the receiver to implement security functions.

The system should implement specific training functions in order to allow exercises without impacting the operation of the system.

Organisation:

- A risk-assessment taking into account all end-to-end data flows addressing relevant operational environments and identifying residual risks should be established;
- A concept to address the full NAVWAR capability (resilience, surveillance and offensive measures) should be established with the support of the Ministries of Defence of the participating Member States.

Expected impact

- Strengthen EU military resilience regarding NAVWAR offensive actions;
- Contribute to the autonomy of the European defence industry and to the security and defence interests of the Union;
- Provide essential technologies for EU defence interoperability;
- Contribute to Galileo services (especially PRS) monitoring and assist relevant spectrum monitoring agencies.