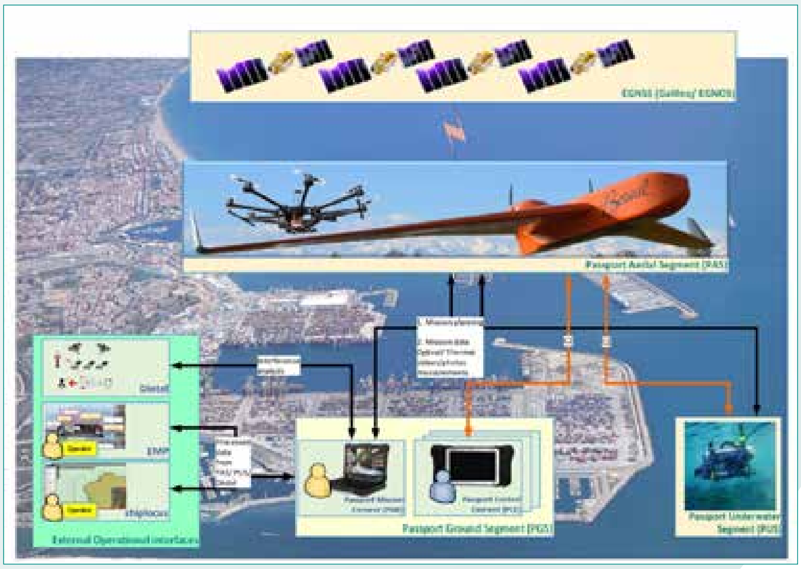
PASSport: a sample of heterogeneous fleet of drones powered by Galileo OSNMA service

by A. R. Martín, I. Armengol, M. López, H. Llorca, M. Nisi, M. Lopez

Ports and National Authorities around the world assuming its role as critical infrastructure have the commitment to establish, update and maintain a security plan. The issue of security in maritime ports is a well-known complex problem due to the particular characteristics of these facilities. They consist of large wide areas with many entry points, usually very transited and operating 24 hours per day, every day.


EGNSS (Galileo/ EGNOS)
Passport Aerial Segment (PAS)
Passport Ground Segment (PGS)
Passport Underwater Segment (PUS)
External Operational interfaces

These features lead to certain vulnerabilities and threats whose risks may be mitigated by implementing innovative surveillance actions. Besides these widely known dangers, over the past two decades, new risks have emerged with the development of new technologies, such as jamming and spoofing of GNSS signals that in practice represents the Denial-of-Service (DDoS). These might lead to failures or disruptions in the daily operations of the port, degrading its services and/or infrastructures. In particular, signal jamming consists of interfering GNSS receivers with higher-power signals on the GNSS frequency bands at user level, or with unintentional interferences due to space weather or other nearby radiating equipment. Jamming techniques can be followed by spoofing attacks, whose goal is to deceive receivers with GNSS-like signals that contain wrong observable data.

These problems have been identified by the European Commission and the need of improving security and safety in port areas has been portrayed in the directive 2005/65/CE. As part of the important search of solutions, PASSport (Operational Platform managing a fleet of semi-autonomous drones exploiting GNSS High Accuracy and Authentication to improve Security & Safety in port areas) is an EUSPA funded project that responds to the needs expressed by port authorities, harbour master and border control authorities by extending situational awareness to improve safety and security in port areas.

The surveiilance solution

The proposed surveillance solution of the project combines both aerial and underwater drones with a network of RFI monitoring stations. The use of this fleet of drones is intended to provide innovation and operational support to the recognition, management and analysis of safety and security aspects of daily operations, with particular attention to pollution monitoring, support to e-navigation, protection of critical infrastructures and against non-cooperative small craft approaching port areas, and underwater threats monitoring. Particularly, the drones combine state of the art technologies to collect on field data in real time, which allows surveillance with an extended situational awareness by covering larger areas. So far, operational surveillance activities to guarantee security and safety are dealing with static sensors, and the data collected cannot automatically trigger dedicated operational procedures. With PASSport vision, this limitation is overcome by proposing a holistic surveillance solution. The solution will be connected with already deployed operational platforms and exploit the innovation brought by drones assisted with E-GNSS technology.

Drone fleet and GNSS hybridisation

The above-mentioned drone fleet integrates, among other sensors, the use of GNSS receivers for a secure, safe and accurate guidance, navigation, and control (GNC). GNSS technologies are widely used for many purposes in drone navigation systems, as they are integrated in most, if not all, conventional autopilots. However, accuracy and security of this technology can be compromised in certain demanding areas, such as port infrastructures due to multipath, or if subjected to certain interferences, either intentional or not, and this is the reason why hybridisation with other sensors is usually contemplated in a risk assessment. In any case, even with hybridised configurations, a diminished GNSS performance may lead to a potential degradation of the drone navigation system.

Open Service – Navigation Message Authentication (OSNMA)

Taking this into consideration, the integration and exploitation of new GNSS services oriented to improving accuracy and security is not only justified but also necessary.

In terms of accuracy, a PPP algorithm in post-processing is considered, as it is a widely mature positioning technique. This positioning method uses single or dual-frequency code and carrier phase measurements for centimetric accuracy applications. On the other hand, in terms of security, navigation with Galileo's newcomer Open Service – Navigation Message Authentication (OSNMA) is used. OSNMA is a data authentication function for Galileo that provides receivers with the assurance that the received Galileo navigation message is coming from the system itself and has not been modified. The use of this service in the PASSport solution helps in the avoidance of some of the aforementioned threats in port context. In terms of safety an integrity (as IBPL) approach is considered to provide protection levels (PLs). The described capabilities in terms of accuracy, integrity, and security will be introduced in an evolution of GMV's GNSS receiver MAGIC User Terminal, which will be embarked onboard the aerial drones. For the monitoring backbone, GMV's srx-10i (also known as DINTEL) will provide a cost-effective, dual-band, simultaneous monitoring of GNSS bands. Monitoring stations will augment on-ground the decision-making process of port area operators by providing alert mechanisms and automated report functionalities on the presence of RFI threads.

The purpose of this paper, in this context, is to assess the functionalities of PPP, OSNMA and RFI monitoring in terms of robustness against spoofing attacks and accuracy of positioning obtained with authenticated navigation messages compared to non-authenticated navigation results. These functionalities are validated with results obtained from different flight campaigns using real Signal-in-Space (SiS). These campaigns are performed in different European ports such as Kolobrzeg, Valencia, Le Havre, Hamburg and Ravenna.

KEYWORDS
Ports; OSNMA; GNSS; Galileo; Drone fleet

ABSTRACT
PASSport is an Operational Platform managing a fleet of semi-autonomous drones exploiting GNSS High Accuracy and Authentication to improve Security & Safety in port areas. EUSPA funded the project that responds to the needs expressed by port authorities, harbour master and border control authorities by extending situational awareness to improve safety and security in port areas.

AUTHOR
A. R. Martín,
I. Armengol,
M. López, H.
Llorca, GMV;

M. Nisi,
marco.nisi@grupposistematica.it
SISTEMATICA S.p.A;

M. Lopez, EUSPA

NOTE
More information available on paper presented at ION GNSS+ 2023
Session B2: Marine Applications, and Search and Rescue
https://www.ion.org/gnss/sessions.cfm?sessionID=1566