DEVELOPMENT OF A GNSS MONITORING NETWORK WITHIN THE MEDITERRANEAN AREA FOR AIR NAVIGATION APPLICATIONS - BLUEGNSS PROJECT -

Fabio Principe, Giuseppe Di Bitonto, Andrea Tomei, Vincenzo Pellegrini, Giovanni Morelli

IDS Ingegneria Dei Sistemi S.p.A. – https://www.idscorporation.com
Via Enrica Calabresi, 24, 56121 Pisa (Italy)
Email: {f.principe, g.dibitonto, a.tomei, v.pellegrini, g.morelli}@idscorporation.com

ABSTRACT

The main objective of BLUEGNSS project is the harmonization of PBN approach operations among the BLUE-MED FAB States. This is the first time in Europe that a RNP approach implementation project has been coordinated at FAB level. According to the ICAO recommendations, a key enabler to reach this purpose is the development of a regional GNSS monitoring network able to produce periodic reports on GNSS performance within the area of interest. Such activity has been therefore carried out in the framework of the BLUEGNSS project and has led to the results illustrated within this paper.

I. INTRODUCTION

BLUEGNSS was one of the Horizon 2020-Galileo-2015-1 projects selected for co-financing by GSA (grant agreement nr. 687198) whose declared purpose was the promotion of *European GNSS* (E-GNSS) adoption for air navigation operations within the BLUE-MED Functional Airspace Block (FAB). The consortium, led by ENAV, was composed of four Air Navigation Service Providers (ANSPs) belonging to BLUE-MED FAB – i.e. DCAC, HCAA and MATS – and IDS Ingegneria Dei Sistemi S.p.A., as the industrial partner.

According to main ICAO recommendations [1]-[3], its key tasks are summarized in the following list.

1. Design of RNP approaches with all 3 minima (LPV, LNAV/VNAV, LNAV) to be flown on pre-selected airports within States involved in the project.
2. Publish previous procedures on national AIPs in order to permit their usage and to prove the consequent benefits in terms of accessibility, safety, operational and economic aspects.
3. Train procedure designers for the development and review of RNP approach procedures.
4. Disseminate an E-GNSS culture among BLUE-MED partners.
5. Design and implement a **regional E-GNSS monitoring network** provided with data recording capabilities in order to support the validation of RNP approaches and introduce Galileo, as future air navigation enabler.

The 5th point is the object of the present paper. Its outline is structured as follows. Sec. II provides a brief overview of the GNSS monitoring concept recommended by ICAO within Doc-9849, [3]. This is an important starting-point for delineating the operative role covered by GNSS monitoring networks within the air navigation field. A quite detailed overview on the BLUEGNSS monitoring network is reported in Sec. III. Many aspects concerning the installation activity are illustrated in Sec. IV and conclusions with the achieved results are presented in Sec. V.

II. GNSS MONITORING CONCEPT

According to the following statement extracted from Sect. 7.8 of ICAO GNSS manual [3]:

> 7.8.1.1 – *Annex 10, Volume I, 2.1.4.2 recommends that a State that approves GNSS-based operations should monitor and record relevant GNSS data to support accident and incident investigations. This data can also be used periodically to verify GNSS performance. It should be noted that this verification of GNSS performance is not intended to support a real-time notification process.*

the *GNSS monitoring concept* covers the following use cases.

- **GNSS performance assessment** is a periodic, off-line activity aiming at demonstrating the *signal-in-space* (SiS) conformance to ICAO Annex 10 relevant requirements, [2]-[3].
- **GNSS operational status monitoring** provides real-time information to technical staff and ATC services on the current operational status of GNSS services. **RF interference (RFI) monitoring** is typically part of this activity and aims at surveilling the GNSS spectrum and providing timely warnings in case of potentially critical RFIs.
- **GNSS data recording** is a legal recording service of GNSS data for post-incident/accident investigations.

In the framework of the BLUEGNSS project, such a concept has become one of the leading targets that paved the way to the deployment of an innovative, *multi-source monitoring network* able to: (*i*) assess and record GNSS performance, measurements and data, and (*ii*) analyze and report any detected RF interference (RFI) within the GNSS spectrum.

The next section provides more details on network components and its architectural design.

III. BLUEGNSS MONITORING NETWORK: ARCHITECTURAL DESIGN AND MAIN ELEMENTS

III.1. BLUEGNSS Monitoring Network: General Overview

The BLUEGNSS monitoring network has been designed to carry out the *performance assessment* of GPS, GPS/EGNOS and Galileo systems within the BLUE-MED area, in compliance with the ICAO guidelines (see Sect. II and [3]). Its architectural design dips the roots in the *GNOME System* concept, whose overall schematic is shown in Fig. 1, [4]. This picture shows three segments whose roles are briefly illustrated below.

i. The *sentinel segment* identifies a network of GNSS monitoring stations installed within the area of interest. Such stations have the important role of characterizing the local GNSS scenario by measuring ad-hoc metrics, which can be used for real-time monitoring, performance assessment, or post-accident investigation activities.

ii. The *central monitoring facility (CMF) segment* is the interface between sentinel and user segments. Specifically, it gathers data coming from the sentinel segment and processes it in order to produce periodic performance reports or detect possible anomalies that might compromise the GNSS positioning service. In this last case timely warnings are emitted towards the authorized personnel.

iii. The *user segment* indicates the entire ensemble of users enabled to accede to GNOME services, see also [4].

The same concept has been used to implement the BLUEGNSS network. Indeed, according to the schematic shown in Fig. 2, the CMF unit is fed by a set of *heterogeneous remote sources*, which provide the central node (i.e. the CMF) with all needed data to compute the KPIs for:

- a *global GNSS performance assessment* within the BLUE-MED area;
- a *local GNSS performance assessment* for each monitoring site (which hosts a GNOME sentinel).

More in detail, Fig. 2 shows that the sentinel segment is composed of four dedicated monitoring stations (i.e. *GNOME sentinels*, see Sect. III.2) and other five servers belonging to already existing GNSS network: i.e. EDAS, IGS/MGEX, EUREF, NavCen, and EGSC (see also Sect. III.3). Such choice is motivated by the need to develop a flexible and easy configurable network that is able to integrate and process data, coming from many monitoring stations, even if it belongs to external, independent networks. This architectural solution has the obvious advantage of reducing the need for new infrastructures to monitor the GNSS performance within the BLUE-MED FAB, thus saving significant costs.

Fig. 2 also highlights the main CMF functions of data gathering, processing, and storage. Specifically, the activity of data processing leads to the computation of specific KPIs (in compliance with ICAO guidelines, see [2]-[3]) that are collected within periodic reports (daily and monthly). Such reports are then uploaded to the BLUE-MED portal where they can be browsed by authorized personnel.

Further details on each element composing the BLUEGNSS network are provided in the next sections.

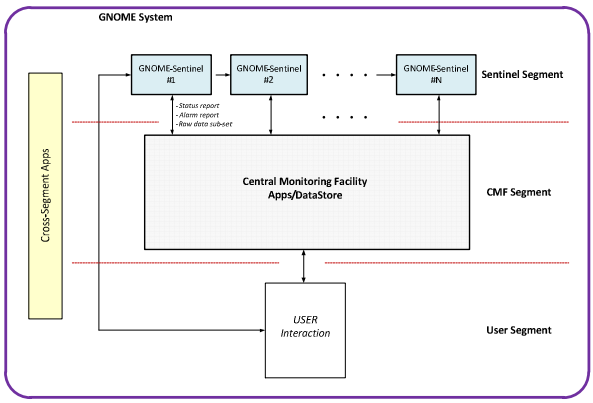


Fig. 1 – GNOME system architectural concept

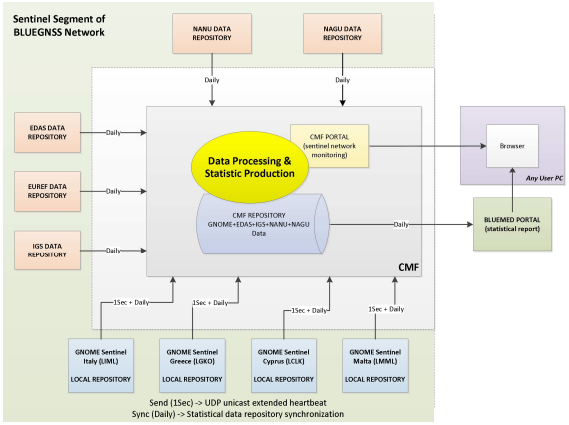


Fig. 2 – BLUEGNSS monitoring network with a detailed view on the main CMF functions

III.2. GNSS Operative Monitoring Equipment (GNOME) Sentinels

GNOME sentinels, [4], are very versatile and highly-configurable GNSS monitoring stations, designed and developed by IDS. They are conceived to assess the integrity of GNSS signals, monitor their performance and record measurements and data. Currently, the 4 GNOME sentinels belonging to the BLUEGNSS network are installed within the following airports: **Kos airport** (Greece), **Luqa airport** (Malta), **Larnaka airport** (Cyprus), and **Milan/Linate airport** (Italy). Fig. 3 contains a map representing the BLUE-MED FAB (green region) in which the 4 GNOME sentinels are geographically located.

A simplified architectural schematic of a GNOME sentinel is presented in Fig. 4 (see also [4]). This picture shows an amplified GNSS multiband antenna which receives any GNSS signal. This transducer feeds the *RF-Navigation unit*, which is made up of the following 2 modules.

- A state-of-the-art *GNSS receiver* which tracks positioning signals and processes them, in order to measure some standard metrics in the NAV-domain (e.g., position, protection levels, SNRs, pseudoranges, DOPs, etc.) that are subsequently sent to the *processing unit*.

- A *widely tunable front-end* that receives, down-converts and digitalizes the incoming RF signals. Such streams of digital samples are then sent to the *processing unit*.

Furthermore, the *RF-Navigation unit* is also provided with a *Rb-clock* (rubidium clock) which aims at reducing the internal clock noise of the above mentioned devices.

For the sake of simplicity, the *processing unit* (PU) can be viewed as a general purpose computer that receives: (*i*) navigation data (from GNSS receiver) via Ethernet, and (*ii*) I/Q digital samples (from the front-end) via USB. Such unit hosts a SDR (*software-defined radio*) kernel, which is tasked with: real-time processing of I/Q samples, handling and monitoring the sentinel status, generating statistics, storing data, and providing suitable interface to the CMF. Therefore, this software module is considered the real core of a GNOME sentinel.

It is worth noting that GNOME sentinels are designed according to the GNSS monitoring concept recommended by ICAO (see Sect. II and [2]-[3]). Indeed, they are able to accomplish the following tasks, [4]: (*i*) real-time monitoring of the GNSS integrity to provide timely alert in case of detected anomalies, (*ii*) post incident/accident investigation, yielding data logging and review capabilities, and (*iii*) performance assessment and ground validation campaigns (e.g., for GBAS and RIMS siting). More details are available in [4].

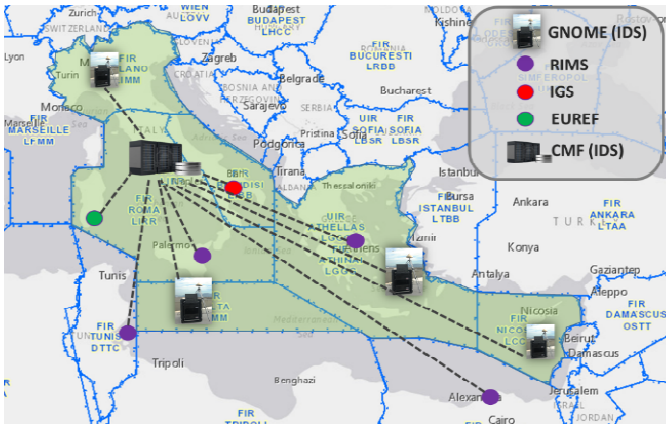


Fig. 3 – BLUE-MED FAB (green area) with the monitoring stations belonging to the BLUEGNSS network

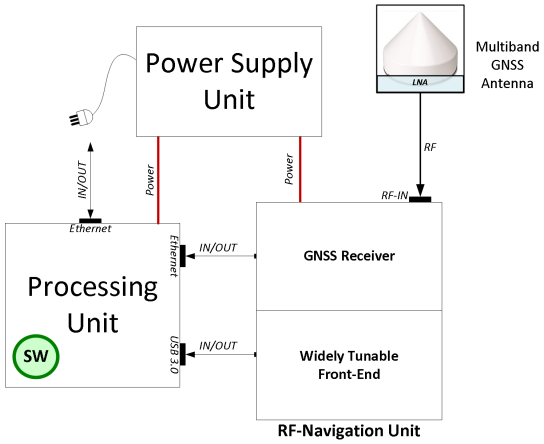


Fig. 4 – A simplified architecture that shows the three units composing a GNOME sentinel

III.3. External Resources Integrated with the BLUEGNSS Monitoring Network

As stated in Sect. III.1, the BLUEGNSS network has been designed to also process data and measurements provided by already existing monitoring networks. Such networks are listed below.

- *EDAS network* provides GNSS performance and analysis coming from EGNOS RIMS, [5]. Its monitoring stations are included within the BLUEGNSS network in order to increase the grid of monitoring points.
- *IGS-MGEX network* offers many services (such as, precise ephemerides, iono and clock corrections, etc.) and GNSS performance analysis, [6], that are used by the CMF for (*i*) computing some global metrics within the BLUE-MED FAB (such as GPS URE and Galileo SISE, see [2] and [4]) and (*ii*) increasing the number of monitoring points in the Mediterranean area.
- *EUREF network* provides some geodesy services and GNSS performance analysis, [7]. Its stations are mainly used to increase the number of monitoring points within the Mediterranean area.
- *US Navigation Center (NavCen) server* gives access to GPS NANUs, almanacs, and currently operational advisories. Specifically, NANUs are used to assess the GPS continuity, [8].
- *European GNSS Service Center (EGSC) server* provides Galileo NAGUs, almanacs, etc. Specifically, NAGUs are used to assess the Galileo continuity, [9].

Fig. 3 provides a view of the BLUE-MED FAB with the stations of EDAS, IGS-MGEX and EUREF that are currently included within the BLUEGNSS network.

III.4. Details on Network Architecture

A TCP/IP network allows the communication between the CMF and the sentinel segment. A schematic picture of network topology is presented in Fig. 5. It shows a TCP/IP star-network that connects GNOME sentinels and EDAS, IGS/MGEX, EUREF, NavCen, and EGSC servers to the CMF unit.

A more detailed view on network architecture is provided in Fig. 6. This picture sketches a dedicated VPN (Virtual Private Network) implemented in order to satisfy all project needs and its strict security policy requirements. Specifically, such VPN network contains only BLUEGNSS hosts and no other host is permitted. Furthermore, a wide set of public GNSS services (e.g. EDAS, IGS/MGEX, EUREF, NavCen, etc.) are reached via severe firewall policies.

More in detail, the CMF server has two network interfaces: (*i*) the *inner interface* only reaches the BLUEGNSS hosts located on the VPN, and (*ii*) the *outer one* strictly connected to only the previously mentioned public servers on fixed and pre-selected IP-addresses (via *https* and *ftps* protocols).

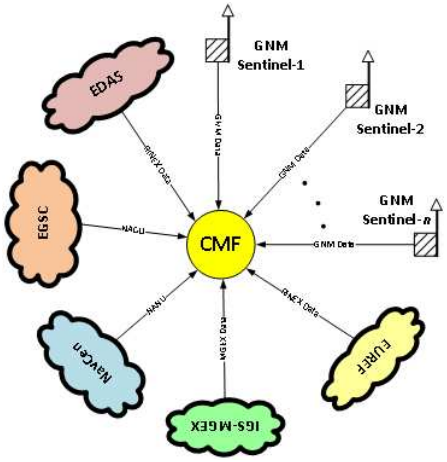


Fig. 5 – BLUEGNSS network topology

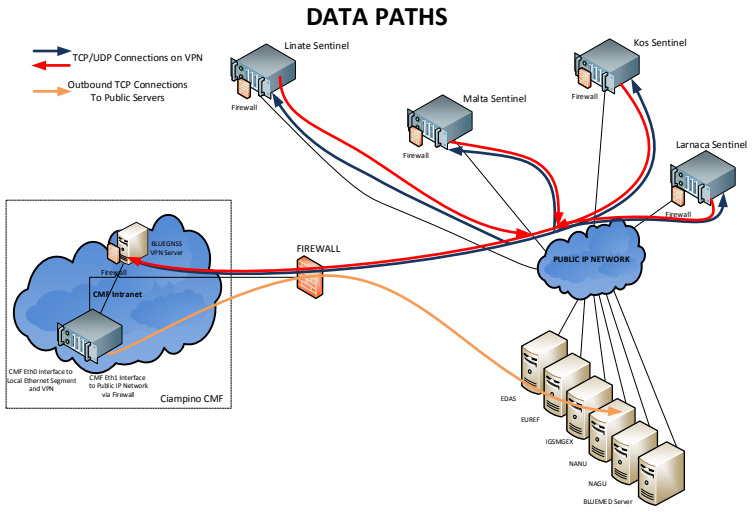


Fig. 6 – Detailed view on network architecture

IV. GNOME SENTINEL AND CENTRAL MONITORING FACILITY INSTALLATIONS

IV.1. Details on GNOME Sentinel Installations

IV.1.A. Site Requirements

A correct selection of candidate sites to host GNOME sentinels is the first important step to guarantee a correct monitoring of GNSS signals. Indeed, the presence of large obstacles (i.e., man-made obstacles, such as, hangars, shelters or other infrastructure, and site orography) as well as the presence of RF emitters close to the GNSS antenna can sensibly compromise the reception of positioning signals, and consequently affect the measurements of those KPIs used to characterize the GNSS performance. Therefore, the following two recommendations typically lead the activity of site selection (similar requirements are indicated in [10] for EGNOS RIMS installations).

- **REC-1**. Candidate sites shall be provided with a horizon as much as possible free from obstacles, at least above 5° elevation.
- **REC-2**. Candidate sites shall be provided with spectrum as much as possible free from interfering signals within the GNSS bands.

Moreover, the presence of existing infrastructures and assets (e.g., TCP/IP network, UPS, racks and storage, cable ducts, air conditioning, site accessibility, etc.) is another important aspect to be taken into account in order to guarantee the full operability of the monitoring station to be installed, [10].

The list of sites selected to host GNOME sentinels are: Linate airport (Italy), Kos airport (Greece), Luqa airport (Malta), and Larnaka airport (Cyprus). A dedicated survey activity was carried out within each airport in order to select the best hosting site in compliance with the previously mentioned guidelines.

IV.1.B. GNOME Sentinel Installation

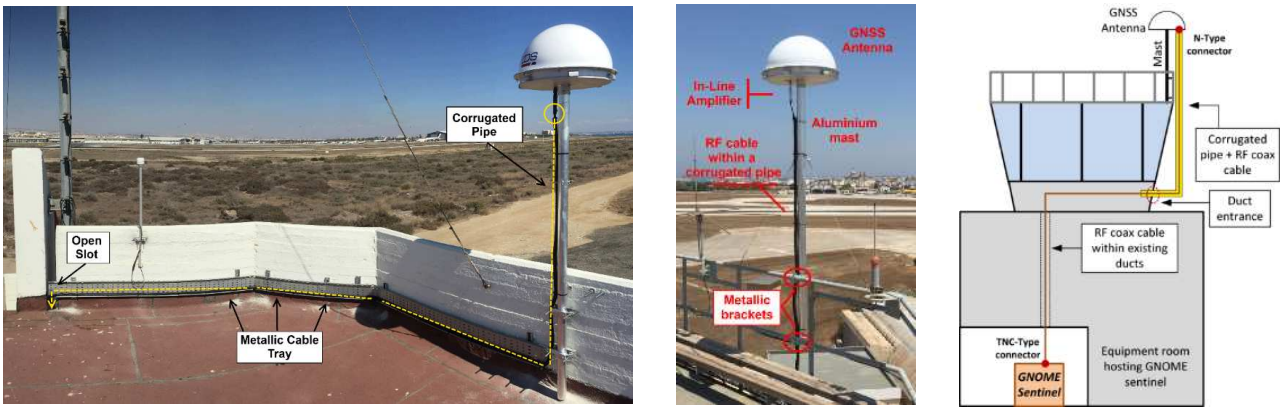
The typical GNOME sentinel installation, carried out in the framework of the BLUEGNSS project, is made up of a GNSS choke-ring antenna followed by a RF chain, that is composed of: (*i*) an in-line amplifier (connected to the antenna port) and (*ii*) a coaxial cable (RF cable), whose length is generally about 30 mt. Furthermore, a corrugated pipe was also used to protect the coaxial cable against weathering and direct solar exposure.

A pair of pictures showing examples of GNSS antenna installations compose Fig. 7. Choke-ring antennas were chosen in order to mitigate the detrimental effects that multipath might have on the required GNSS monitoring activity.

GNOME sentinel chassis (*Power Supply Unit*, *Processing Unit*, and *RF Unit*) are placed within dedicated racks, which are generally hosted in pre-selected equipment rooms that are provided with air-conditioning systems and internet connections. The physical specifications of GNOME sentinels are listed in Tab. 1.

Fig. 8 shows an operative GNOME sentinel installed within an equipment room. The main connections are listed below.

- The PSU powers the other 2 units with two independent lines, respectively: 12 Vdc and 24 Vdc.
- The RFU is fed by the GNSS antenna via a coaxial cable and powered by the PSU. Simply speaking, this unit can be considered the front-end that receives RF signals and digitalizes them for the next processing carried out by the PU, see Sect. III.2.
- The PU is fed by the RFU and powered by the PSU. In compliance with the analysis reported in Sect. III.2, this unit is considered the sentinel core, as it is devoted to: processing all acquired measurements and computing the consequent metrics, sending data and diagnostics to the CMF, and checking the overall sentinel status.



(*a*) *Installation of the GNSS antenna on the roof of a shelter placed within the airport of Larnaka*

(*b*) *Installation of the GNSS antenna on the tower of Malta airport (with a sketch of the coax-cable path)*

Fig. 7 – Two examples of GNSS antenna installation

Tab. 1 – Physical specifications of GNOME sentinels used within BLUEGNSS project

Rackmount chassis	*Power Supply Unit* (PSU)	19” – 2U (88H × 483W × 350L mm)
	Processing Unit (PU)	19” – 3U (133H × 483W × 350L mm)
	RF Unit (RFU)	19” – 3U (133H × 483W × 350L mm)
Voltage and frequency		220÷240 V, 50 Hz
Max absorption		400 W
Typical operating temperature		0÷40°C
Operating humidity (motherboard)		5÷90%

(*a*) *GNOME sentinel front view (real operative context)*

(*b*) *GNOME sentinel back view (real operative context)*

Fig. 8 – Typical installation of GNOME sentinel equipment

IV.2. Details on CMF Installation

The CMF is a server unit whose physical characteristics are summarized in Tab. 2. In this case, no RF stage is present and no antenna is installed. Therefore, its installation just requires an equipment room, provided with: an air conditioning system, a free rack, a TCP/IP connection and an uninterruptible power supply (UPS) system.

According to these requirements, the CMF was installed at the airport of Ciampino, within the ENAV/ACC (Area Control Center) facility. A picture is shown in Fig. 9. Once the installation was completed, the CMF was switched on and configured to operate within the BLUEGNSS VPN network in compliance with analyses illustrated in Sect. III.4 (see also the schematic of Fig. 6). At the end of the above described activities the CMF server was successfully commissioned.

Tab. 2 – CMF physical characteristics

Rackmount chassis size	19” – 1U (43H × 435W × 608L mm)
Voltage and frequency	220-240 V, 50 Hz
Max absorption	600 W
Typical operating temperature	10÷50°C
Operating humidity	≤ 80%

(*a*) *Front view of CMF*

(*b*) *Rear view of CMF*

Fig. 9 – CMF server installation within ENAV/ACC facility

V. CONCLUSIONS AND ACHIEVED TARGETS

BLUEGNSS has been the first project of its kind to be coordinated at FAB level and having the ambitious target of providing European States with those elements and tools, which are needed for supporting the harmonization and standardization process of PBN procedures. The service of permanent GNSS monitoring is one of the key ingredients that, combined with the other essential activities of procedure design-&-validation, safety analysis and personnel training, permits to sustain this evolution process involving the air navigation field.

The GNSS monitoring network developed in the framework of BLUEGNSS has been successfully validated and now is fully operative as shown in Fig. 10 (proved by the green status of LIVE and REPO LEDs).

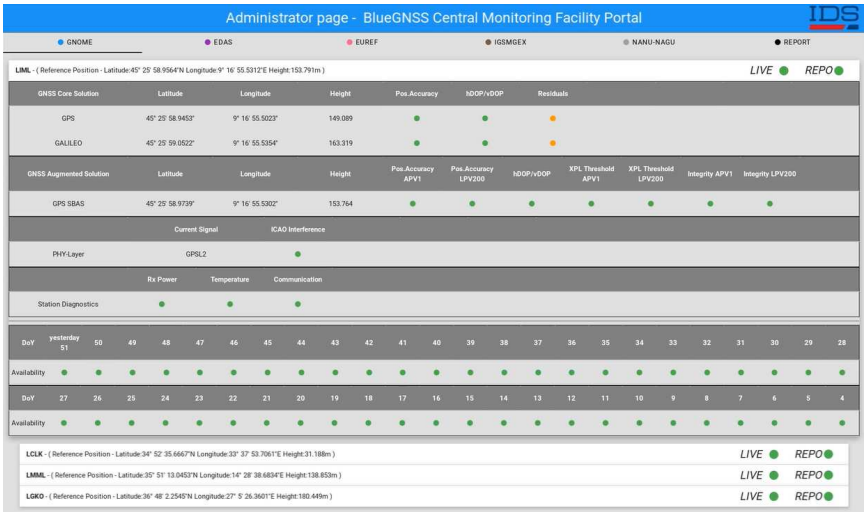


Fig. 10 – A screenshot of CMF portal showing statuses of the GNOME sentinels from the BLUEGNSS network: LIVE LEDs report current conditions of sentinels, REPO LEDs indicate the update status of the CMF repository

The activity of performance assessment is now on-going and the consequent reports, containing the recommended ICAO metrics, [2]-[3], are periodically produced and published on the BLUE-MED website, http://www.bluemed.aero.

The Italian reports were used as *Performance Assessment Reference* by the Italian CAA (ENAC). This important result allowed approval of GPS-based procedures without any additional mitigation (ENAC letter of 16th March 2018, nr. ENAC-VDG-16/03/2018-0028476-P).

Finally, the GNOME sentinels of Kos and Larnaka allowed the detection of some interference events that were also confirmed by Pilot reports on GPS loss in Nicosia FIR within the period between March and April 2018.

ACKNOWLEDGMENTS

The authors wish to thank the entire team of DCAC, HCAA, MATS, ENAV, IDS, and GSA for their precious support during each phase of BLUEGNSS project.

REFERENCES

[1] ICAO DOC 9613, *Performance-based navigation (PBN) manual*, 4th Ed., 2013.
[2] ICAO, Annex 10 Vol.1 Amend. 89 (13 Nov. 2014), *Aeronautical telecommunications – Radio navigation aids*, 6th Ed., 2006.
[3] ICAO Doc 9849, *Global Navigation Satellite System (GNSS) manual*, 3rd Ed., 2017.
[4] V. Pellegrini, F. Principe, A. Tomei, M. Mori, M. Natali, and R. Cioni, "The GNSS Operative Monitoring Equipment (GNOME): an SDR-Based Solution for Integrity Assurance," in Proc. NAVITEC 2012, ESTEC Noordwijk (The Netherlands), December 5-7, 2012.
[5] EDAS, webpage: https://www.egnos-portal.eu/discover-egnos/about-egnos/what-edas.
[6] IGS-MGEX, webpage: http://mgex.igs.org/.
[7] EUREF, webpage: http://www.epncb.oma.be/.
[8] U.S. Coast Guard Navigation Center, webpage: https://www.navcen.uscg.gov.
[9] European GNSS Service Center, webpage: https://www.gsc-europa.eu/system-status/nagu-information.
[10] ESA, *EGNOS v3 Phase C/D – EGNOS v3 sites implementation requirements document*, GNSS-EV3-REQ-ESA-X-0017, Issue 2.0, Jen. 25, 2016.