The GNSS Operative Monitoring Equipment (GNOME)

An SDR-Based Solution for Integrity Assurance

Vincenzo Pellegrini, Fabio Principe, Andrea Tomei, Massimo Mori, Marco Natali, Riccardo Cioni
EM Framework Design Laboratory
Ingegneria Dei Sistemi S.p.A.
Pisa, Italy
{v.pellegrini, f.principe, a.tomei, m.mori, m.natali, r.cioni}@idscorporation.com

Abstract — **The *GNSS operative monitoring equipment* (GNOME) system is a distributed network of remote sentinels aimed at monitoring integrity, reliability and spoofing/interference-immunity of GNSS signals. The key features of this system directly come from the ICAO recommendations and standards which highly advise continuous control of the GNSS performance and integrity, both in the signal and in the navigation domains. The GNOME system design finds a key enabler in the *software-defined radio* signal-processing paradigm, which provides the necessary *flexibility* to perform all of the real-time analyses required to obtain the full picture of GNSS infrastructure status. In observance of ICAO recommendations, recording and playback capabilities for both instantaneous analysis reports and raw signal dumps is provided along with suitable playback and navigation tools which support quick localization of critical or abnormal events.**

Keywords — **GNSS, GPS, SBAS, SDR, interferences, integrity, anti-spoofing, multipath.**

I. INTRODUCTION

SATELLITE positioning systems represent a very attractive technology to provide accurate and reliable navigation services for the civil aviation community. This is due to a number of enablers which are continuously improving the performance of GNSS. These enablers include both *Ground* (GBAS) and *Satellite-Based* (SBAS) augmentation systems, foreseen modernization of existing systems, such as GPS and GLONASS, and new constellations still in the deployment phase (Galileo and Compass), [1] and [2].

Compared to conventional radio navigation aids for aviation, satellite-based systems are less expensive and, if correctly managed, controlled, and protected by possible threats, could provide several benefits. These include global coverage and improved performance in terms of *required navigation performance* (RNP) parameters, i.e., accuracy, integrity, availability, and continuity, [3].

As a result, civil aviation organizations and *air navigation service providers* (ANSPs) are currently investigating all the aspects related to the deployment of new GNSS-based approach procedures. The aim is to enhance airspace capacity and operations' efficiency, while improving safety and reducing environmental impact. Besides feasibility assessment and procedure design, these investigations must consider all the issues related to both ground and flight validations: verification of compliance with ICAO recommendations [3], GNSS infrastructure performance and anomaly control.

In this context, the Italian authorities have been leading a number of experimental projects with the objective of achieving standardization of GNSS-based procedures as well as of subsequently integrating them within conventional operations. In the framework of these projects, IDS S.p.A. has played a relevant role in the development of verification methods that support the validation of GNSS-based procedures ([4]-[6]), by means of:

- design of GNSS approach procedures,
- implementation of EM models and software simulations,
- on-site validation of GNSS performance through extensive measurement campaigns.

Concerning this last point, the need to cover ICAO recommendations and requirements ([3] and [7]-[9]) relating to:

- GBAS site selection procedures (essential step to correctly install a GBAS system),
- flight inspection campaigns (needed to validate GNSS procedures),
- continuous monitoring of GNSS signals (in order to monitor compliance with ICAO requirements),
- legal recording capabilities,
- direction finding of interferers,
- anti-spoofing mechanisms,

led IDS to design and develop what was called a *GNSS operative monitoring equipment*, i.e. the GNOME system.

GNOME is firstly a network of *remote sentinels* each of which continuously monitors GNSS signals and provides timely alerts in case of detected anomalies.

II. ICAO GUIDELINES AND RECOMMENDATIONS

The usage of GNSS systems in the field of civil air-navigation is primarily focused on maintaining those safety conditions which shall preserve the security of passengers during any flight procedure and landing operation. To this purpose, the ICAO has defined specific standards and recommendations ([1], [3], and [7]-[9]) which shall discipline design and implementation of every GNSS-based procedure in order to guarantee *safety-of-life* (SoL) service performances. Such service level is characterized by means of pre-determined thresholds for *position accuracy*, *service availability*, *integrity*, and *continuity*, as summarized in Tab. I (extracted from [3]).

TABLE I. SOL SERVICE PERFORMANCE REQUIREMENTS, [3].

Typical operation	Accuracy horizontal 95% (Notes 1 and 3)	Accuracy vertical 95% (Notes 1 and 3)	Integrity (Note 2)	Time-to-alert (Note 3)	Continuity (Note 4)	Availability (Note 5)
En-route	3.7 km (2.0 NM) (Note 6)	N/A	$1 - 1 \times 10^{-7}$/h	5 min	$1 - 1 \times 10^{-4}$/h to $1 - 1 \times 10^{-8}$/h	0.99 to 0.99999
En-route, Terminal	0.74 km (0.4 NM)	N/A	$1 - 1 \times 10^{-7}$/h	15 s	$1 - 1 \times 10^{-4}$/h to $1 - 1 \times 10^{-8}$/h	0.99 to 0.99999
Initial approach, Intermediate approach, Non-precision approach (NPA), Departure	220 m (720 ft)	N/A	$1 - 1 \times 10^{-7}$/h	10 s	$1 - 1 \times 10^{-4}$/h to $1 - 1 \times 10^{-8}$/h	0.99 to 0.99999
Approach operations with vertical guidance (APV-I)	16.0 m (52 ft)	20 m (66 ft)	$1 - 2 \times 10^{-7}$ per approach	10 s	$1 - 8 \times 10^{-6}$ in any 15 s	0.99 to 0.99999
Approach operations with vertical guidance (APV-II)	16.0 m (52 ft)	8.0 m (26 ft)	$1 - 2 \times 10^{-7}$ per approach	6 s	$1 - 8 \times 10^{-6}$ in any 15 s	0.99 to 0.99999
Category I precision approach (Note 8)	16.0 m (52 ft)	6.0 m to 4.0 m (20 ft to 13 ft) (Note 7)	$1 - 2 \times 10^{-7}$ per approach	6 s	$1 - 8 \times 10^{-6}$ in any 15 s	0.99 to 0.99999

Theory and field experience show that these metrics are strongly constrained by site orography, interference, multipath reflections, etc. Consequently, real-time monitoring of such quantities requires site-specific instruments and analyses as well as dedicated computational resources. A GNSS monitoring infrastructure is thus much better suited on ad-hoc ground receivers than on certified on-board navigation systems, as well documented by [10] and practically verified by several performance and validation campaigns ([5], [11], [12], and [13]). Furthermore, the need of local GNSS monitoring systems is clearly inferable by the following ICAO recommendations.

"**Recommendation**. A State that approves GNSS-based operations should ensure that GNSS data relevant to those operations are recorded."

"*Note*. These recorded data are primarily intended for use in accident and incident investigations. They may also support periodic confirmation that accuracy, integrity, continuity and availability are maintained within the limits required for the operations approved."

Extracted from Chap. 2, Par. 2.1.4.2 of [3]

"In order to be able to conduct post-incident/accident investigations, it is necessary to record GNSS information both for the augmentation system and for the appropriate GNSS core system constellation used for the operation. The parameters to be recorded are dependent on the type of operation, augmentation system and core elements used. All parameters available to users within a given service area should be recorded at representative locations in the service area."

Extracted from Att. D, Par. 11.1 of [3]

"Reliance on GNSS will require States to re-examine their respective capabilities to detect, localize and identify interference sources in order to minimize potential service disruption in their flight information regions. This examination may result in planning efforts to investigate [...] ground-based systems for detecting and localizing potential sources of interferences (RFI) to the GNSS signals."
"In order to indentify and mitigate GNSS interference, a suite of systems may be required. Current technology provides RFI direction finding (DF) and localization capabilities […]."

Extracted from Att. 3, Par. 4.2 and 4.3 of [14]

"At airports with high traffic that rely on GNSS as the navigation means for approach, it may be desirable to deploy a permanent interference monitoring station. In this way a timely notification of the interference threat can be forwarded to the authorities of each State that are concerned with GNSS integrity."

Extracted from Att. 3, Par. 4.9 of [14]

Furthermore, the following specifications, that come from ICAO statements, remarks other important features that should characterize a monitoring station of GNSS signals.

Ground technical personnel and any other public surveillance authority concerned with GNSS integrity shall be provided with information on the operational status of the GNSS service essential for approach, landing and take-off at the aerodrome(s) with which they are concerned, on a timely basis consistent with the use of the service(s) involved.

Derived from Chap. 2, Par. 2.3 of [3]

For GBAS site selection and, more in general, for any GNSS ground validation activity, ICAO recommends site survey campaigns aimed to characterize the local GNSS scenario.

Derived from [3], [8], and [14]

The aforementioned citations and specifications are only a few extracts that highlight the attention ICAO reserves for the control and monitoring activities being essential to preserve the integrity of GNSS signals.

It is also worth noting that ICAO clearly delineates the basic capabilities that shall characterize GNSS monitors. Specifically, these features are briefly listed below.

- *Real-time monitoring of the GNSS integrity* to provide timely alert in case of detected anomalies.
- *Post incident/accident investigation*, yielding data logging and review capabilities.
- *GNSS ground validation campaigns*, aimed at characterizing GNSS site performance (e.g., for GBAS and RIMS siting).

III. GNOME System

The previous section contextualizes and motivates, through a brief overview of the main ICAO indications, the importance of the monitoring activities on the GNSS signals both to have a real-time check of its integrity and to provide effective support to the public authorities in case of post incident/accident investigations. These needs, including the necessity to have a system able to measure the GNSS performance during ground validation campaigns, can be satisfied by a single, carefully designed, system.

On these bases and with the perspective of satisfying the ICAO requirements, IDS has developed the *GNOME-sentinel* whose main features and capabilities are outlined in the Sect. III.A. Furthermore, the sentinel can be considered as the data-entry point of a more ambitious system constituted by a network of remote sensors (GNOME-sentinels) connected to a common collector, named *Central Monitoring Facility* (GNOME-CMF), which operates both as the controller of the sentinel segment and as the interface to the user segment. The entire infrastructure falls under the name of GNOME-system and Sect. III.B provides an overview of its architecture.

A. System Capabilities

1) Real-time monitoring of the GNSS integrity.

The requirement to have a real-time monitoring of the GNSS integrity, of course, comes from the need to provide timely alerts in case of detected anomalies. Therefore, the following features are considered essential to have a complete analysis of the GNSS signals, a monitoring of its frequencies, and a check of its performance.

- Monitoring of GPS and SBAS signals: a real-time analysis of CNR (carrier-to-noise ratio), code correlations, pseudorange residuals, etc.
- Real-time detection and classification of possible interfering signals.
- Direction finding in order to indentify the direction from which an interfering signal comes from, [12].
- Anti-spoofing mechanisms.
- Monitoring of the navigation domain metrics.
- Fine multipath estimation by means of a *maximum likelihood estimator* (MLE) algorithm.

2) Post incident/accident investigation.

To cover this feature, it is essential to provide a set of tools which allow authorities to investigate the achieved GNSS performance during the occurred anomaly or accident. For such sense reason, the sentinel is provided with the following functions.

- *Legal recording* of the GNSS data and performance to permit post investigation analysis.
- *Play-back capability* to review and navigate the measured GNSS data.
- *Signal re-injection* in order to re-feed an arbitrary GNSS receiver with the purpose of replicating its behavior during the occurred anomaly or accident.

3) GNSS ground validation campaigns.

What characterizes this need wrt the previous ones is the necessity for the deployed system to satisfy the following requirements.

1. It shall be *a portable system*, easy to be installed.
2. It shall be provided with a set of tools to process a large amount of data and produce long-term statistics.

For such reason, the first prototype of the GNOME sentinel has been designed to provide a very compact, rack-mount solution (see Fig. 1) and features an ad-hoc statistical analysis tool able to characterize site performances in terms of position accuracy, service availability, integrity and continuity consistently with the ICAO recommendations [3].

B. Architectural Overview

An effective real-time monitoring, which aims to protect the GNSS integrity in SoL-service applications, requires a distributed ground infrastructure that is able to maintain the control of the entire region of interest. Indeed, typical operational scenarios, such as airports, are essentially very wide regions where the characteristics of sites can be sensibly different from each other (e.g., in term of orography, satellite visibility, presence of interferences, etc.), thus making the presence of multiple coordinated monitoring systems a necessity.

Fig. 2 shows the overall architecture of the GNOME system. Specifically, its structure is constituted by the main three segments, briefly described below.

Figure 1. Picture of the GNOME-sentinel prototype.

- The *sentinel segment* includes the entire ensemble of sentinels that are placed on-site. This segment is to be regarded as the core of the GNOME system, as it provides all needed measurements and data being necessary to have a complete real-time analysis of the GNSS performance. More details on the sentinel architecture are provided in Sect. IV.
- The *central monitoring facility segment* is the interface between the sentinel and the user segments. Roughly speaking, this unit works as a common collector of the sentinel reports and possible alarms which are immediately forwarded towards the user segment. This unit is also able to store data provided by each sentinel in a local data-base for a later investigation and processing. Furthermore, the system leverages on the presence of a centralized data collection point in order to perform localization of interference sources through specific *triangulation techniques* based on the analysis of data received from each sentinel.
- The *user segment* includes the entire ensemble of users enabled to access to the GNOME services.

Concerning this last point and in order to protect the system from non-expert personnel, it is worth noting that users are provided with following different privilege classes.

- *Advanced users* have full access to all CMF and sentinel functionalities and capabilities. Thus, they can be considered administrators of the GNOME system.
- *Standard users* can access to all data provided by sentinels through interaction with the CMF unit.
- *Operative users* have full access to a synthesis of the key results that are of interest for operational uses (such as, service integrity for landing approaches, presence of interfering signals, etc.). Furthermore, a *low-latency channel*, through a low-bit-rate link, is available for these clients, in order to provide them an immediate access to possible synthetic alarms produced by sentinels in case of detected anomalies.

IV. GNOME SENTINEL: AN SDR-BASED DESIGN

A. Design Overview and Major Implementation Choices

Although an initial demonstrator of the GNOME concept had been developed in the past and was fielded in the aforementioned test campaigns (Sect. I) to verify candidate positions for GNSS signal acquisition stations, a major technology upgrade was definitely needed in order to support all of the required capabilities. Indeed, the previous HW-based solution was limited in terms of supported signal analyses as well as too expensive and complex to manage for being used in a network. In order to cover all the mentioned capabilities and, simultaneously, to reduce the implementation costs without

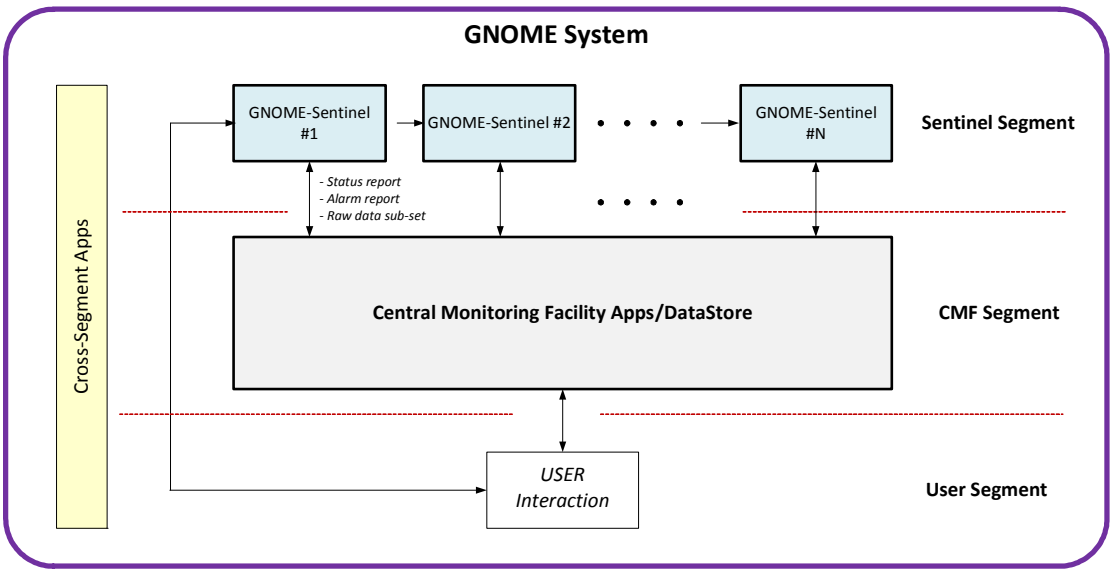

Figure 2. GNOME system architectural overview.

compromising on performance, an SDR kernel has been chosen as the core of the GNOME sentinels. The SDR paradigm offers large advantages in terms of configurability/upgradability and reduces the use of hardware components that typically raise costs and make the system less flexible.

Also, performing signal analysis within the software domain opens up extremely interesting possibilities for investigating the integrity of signals that it would not be practical to pursue by means of hardware implementation, due to the imbalance between hardware development costs and number of deployable systems. In fact, the SDR-based GNOME sentinel implements *digital signal processing* algorithms covering multipath estimation, interference detection, classification and direction finding as well as spoofing attempt detection. This kernel is sided by a state-of-the-art, dedicated receiver that helps tracking all satellites and extracting conventional performance metrics for navigation signals (such as SNR, DOP, correlation residuals, positional deviation etc.). All the data collected by the dedicated receiver as well as that obtained from the real-time, SDR-based PHY-layer signal analysis are assembled into a live report which is both stored into the *on-board repository* and sent to a *remote display & control* interface located at the CMF site. Transmission rates of such reports can be both static and automatically tuned, depending on the contingently available network capacity. A high-level architectural overview of the sentinel is provided in Fig. 3.

Last, but still worth to be mentioned, is the fact that resorting to an SDR-based approach leaves the system somehow open for the implementation of add-on algorithms into the sentinels even after deployment, via just a simple remote software upgrade. Therefore, covering specific analysis needs that could arise from *unexpected integrity anomalies* being detected on the field (and thus not foreseeable at the time of initial design) becomes a natively supported feature of the overall GNOME system.

B. Real-Time and Virtual-Time Analysis

Being intended as both a real-time integrity monitoring infrastructure and a virtual-time performance and anomaly investigation tool, the GNOME system comprises three main user-land applications, namely:

- the *real-time inspector (RTI),* aimed at live, continuous visualization of performance analyses and integrity alarms;
- the *virtual-time inspector (VTI),* conceived as an instrument to play back the live data flow generated by deployed sentinels and stored within the system repository. Playback can either happen at normal or accelerated/reduced speed, upon user request;
- the *statistical inspector (StI),* designed for extraction of long-term performance metrics and statistics from large (24h to several months) observation data sets.

The RTI software component is completely independent and segregated from the GNOME sentinel application which feeds it with the data to display. Such software-architecture feature aims at guaranteeing continuity and stability of the

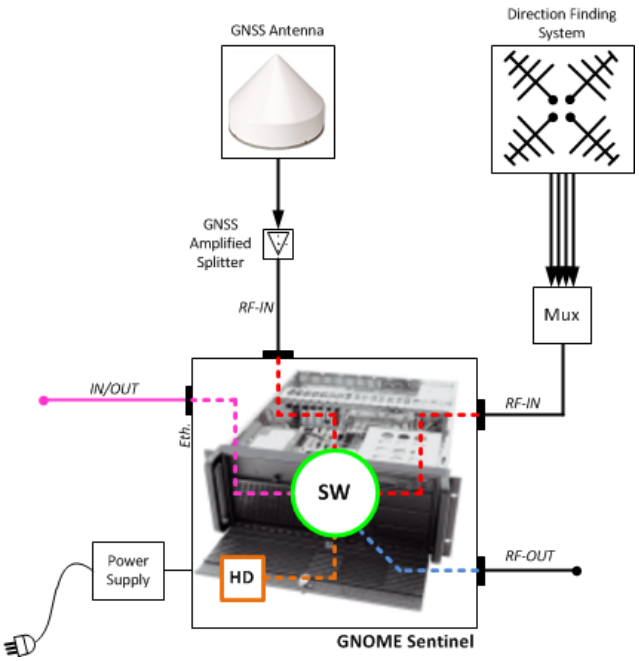

Figure 3. GNOME sentinel architectural overview.

GNSS status analysis and logging regardless of user-segment behavior or possible anomalies. The RTI can thus be connected and disconnected at will from the real-time data flow and can be used either locally, on the deployed sentinel, or remotely at the user or CMF sites.

The VTI application is particularly useful for agencies in charge of GNSS infrastructure patrolling and maintenance and spectrum regulators as long as it re-displays all of the analyses carried-out by the live version of the system in a "media player - like" fashion. For such reason, VTI supports all sorts of "post incident/accident" investigations that ICAO recommends should be carried out in the presence of abnormal events affecting the GNSS infrastructure. The VTI application is provided with all the data navigation tools the user would expect within any media-player-type device, which were specifically tailored to navigate a large repository such as that generated by multiple sentinels continuously submitting their analysis reports (see Fig. 4).

One of such navigation functions which allow quick identification of anomalies within a set of stored reports is worth a specific mention. Called "auto-pause", a quick search feature is offered as a playback option through which the user can accelerate data presentation and review a full day of live analysis within as little as ten minutes time, while having the VTI application pausing on any pre-selected combination of anomalies.

Finally, the StI is a well suited instrument for siting campaigns and for all GNSS analysis applications wherever long observations are required.

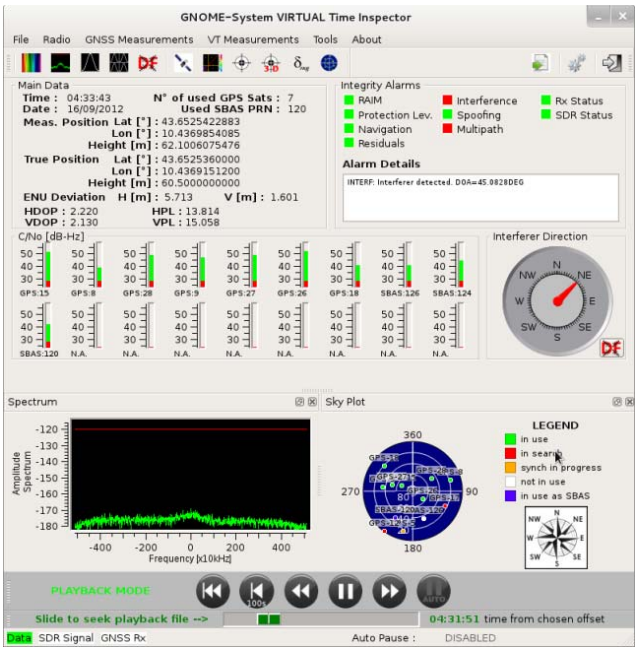

Figure 4. Virtual-time inspector screenshot.

C. *PHY-Layer Signal Analysis*

Both the RTI and the VTI tool encompass a wide variety of signal analyses which give the advanced GNSS infrastructure user direct access to the full GNSS stack from the navigation domain metrics down to the PHY-layer signals.

GNOME sentinels log and provide live presentation of all standard GNSS infrastructure status indicators that one would expect from a pro-grade GNSS receiver (see Fig. 4), such as:

- per-satellite SNRs and skyplot,
- DOP,
- correlation residuals,
- positional deviation,
- satellite visibility maps,
- RAIM,
- Stanford Diagrams.

Still, in the event of an anomaly, whether a degradation of performance, an interference phenomenon (accidental or deliberate); or a spoofing attempt, real-time integrity analysis of GNSS signals carried out at the PHY-layer provides a much greater visibility of the undergoing processes. Thus, by actually *"watching the live signal"*, both automatic anomaly detection/classification algorithms and human users are given a lot more chances to track and solve abnormal events by understanding and removing their causes.

The most relevant signal analysis functions performed by the GNOME sentinel application are briefly presented in the following.

1) *2D spectral analysis and presentation.*

In order to evaluate spectral integrity both automatically and through user interaction, the GNOME sentinel SDR provides analysis and presentation of the real-time-captured 8 MHz spectrum slice (centered at GPS L1) within a two-dimensional time/frequency domain. Graphical presentation of such data to the user is provided via a real-time 3D waterfall plot as depicted in Fig. 5. Automatic spectrum integrity control algorithms check compliance with ICAO interference thresholds, morphological consistency with ground-based received signal models and reference power levels as well as time-domain behavior of spectral coefficients exceeding some pre-defined attention level.

2) *Per-satellite correlation function analysis.*

Received signal integrity and quality monitoring is also achieved by continued observation of highly oversampled correlation functions being measured for every visible satellite (see Fig. 6). Besides providing instantaneous indication of satellites presence and signal strength, such oversampled functions allow both visualization and quantitative estimation of the instantaneous distortions that might affect each satellite.

The type and intensity of such distortion serves as the basis for multipath estimation and is a crucial indicator for detecting spoofing attempts. Future processing additions could also exploit such fine-grained time-domain knowledge of the satellites' correlation functions in order to estimate the contingent intensity of major atmospheric events such as scintillation (as suggested in [15]-[17]).

3) *Multipath estimation.*

Based on the above-described real-time extraction of the satellites' correlation function, a maximum likelihood fitting is performed upon sufficiently averaged oversampled correlation measures, which minimizes the distance between them and a local multipath model.

Depending on the computational capacity of the deployed

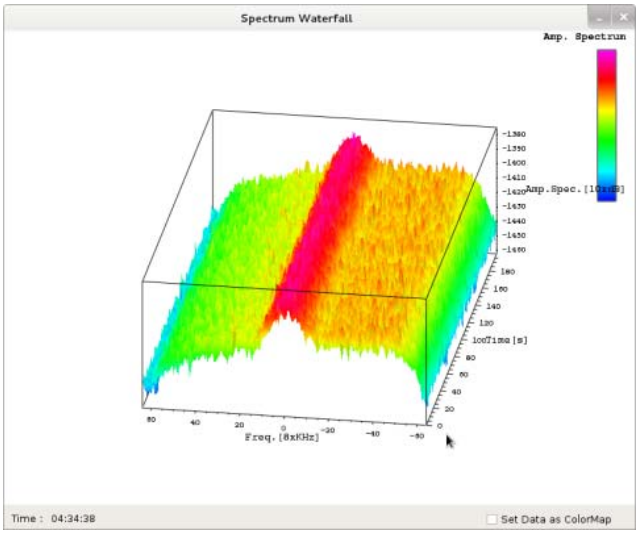

Figure 5. Real-time 3D spectrum waterfall plot.

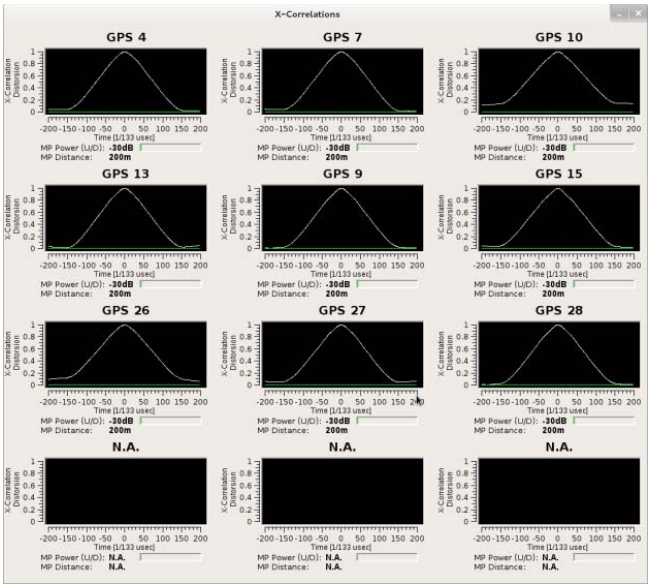

Figure 6. Per-satellite oversampled correlations.

GNOME sentinel version, the local multipath model can feature two or more rays.

4) Anti-spoofing protection.

By cross-checking the received power level, the morphological consistency of the received spectrum (wrt ground-based received signal models) and, most importantly, the outcome of per-satellite correlation function analysis, the likelihood of an ongoing spoofing attempt is continuously evaluated. An alarm notification is then issued whenever major inconsistencies are detected within the above mentioned quantities. Actually, such monitored quantities, especially when jointly watched, provide a good synopsis of the most descriptive spoofing detection analyses as suggested in [18].

5) Signature-based interferer classification.

Designed to serve not just as an infrastructure monitoring instrument but also as a signal debugging and anomaly removal tool, the GNOME system has been provided with interferer classification and direction finding units. A two-dimensional (time and frequency domain) signature is extracted from any abnormal signal received at the sentinel site and correlated with pre-stored models of typical interferers. Such comparison provides an automatic indication on the possible nature of the detected interferer. The signature database includes models for AM, NFM, WFM transmissions, digital and analogue TV broadcasts, GSM, UMTS, LTE signals and some types of radar pulses. Also, thanks both to the SDR-based implementation paradigm and to the signature extraction strategy, training the system to recognize and classify new and unforeseen emissions is pretty straightforward.

6) Signature-based interferer direction finding.

Using the signature extraction strategy along with a direction finding system (based on multiple co-located antennas) also allows dissecting the whole spectral picture of the interference event understanding what contributions came from which directions. Such interference recognition and direction finding subsystem feeds a dedicated interface section where data presentation happens in compliance with user-defined filtering. Specifically, selection filters can be applied on both the direction of arrival and the interferer signature.

V. Conclusions and Future Developments

The GNOME system work presented within this paper in the form of the achieved and described pre-production prototype proves both the viability and the convenience of an SDR approach to GNSS signal integrity monitoring.

SDR-based, real-time analyses carried out directly at the PHY-layer have shown their premium usefulness in investigating, understanding and ultimately solving anomalies and troubles that might occasionally affect critical GNSS infrastructures, both for casual and intentional causes.

What is currently implemented with a sound maturity and refinement level for GPS signals can be extended in the near-future to include support for Galileo and other GNSS constellations.

Furthermore a flexible and low-cost real-time processing architecture has been developed which can host additional signal analyses covering interesting phenomena (such as scintillation) or other contingent needs which might arise on the field.

List of acronyms

AM	Amplitude Modulation
ANSP	Air Navigation Service Provider
CMF	Central Monitoring Facility
CNR	Carrier-to-Noise Ratio
DOP	Dilution of Precision
GBAS	Ground-Based Augmentation System
GLONASS	Global Navigation Satellite System
GNOME	GNSS Operative Monitoring Equipment
GNOME-CMF	GNOME-Central Monitoring Facility
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile telecom.
ICAO	International Civil Aviation Organization
IDS	Ingegneria Dei Sistemi
LTE	Long Term Evolution
MLE	Maximum Likelihood Estimator
NFM	Narrow-band Frequency Modulation
OSI	Open System Interconnect
PHY	PHYsical (OSI Layer)
RAIM:	Receiver Autonomous Integrity Monitoring

RIMS	Ranging and Integrity Monitoring Stations
RTI	Real-Time Inspector
SBAS	Satellite-Based Augmentation System
SDR	Software-Defined Radio
SNR	Signal to Noise Ratio
SoL	Safety-of-Life
StI	Statistical Inspector
UMTS	Universal Mobile Telecom. System
VTI	Virtual-Time Inspector
WFM	Wide-band Frequency Modulation
wrt	with respect to

AKNOWLEDGMENTS

The authors wish to acknowledge Enrico Cocca, Matteo Batisti, Kevin Dell'Omodarme and Antonio Sarri for their precious support during the development and implementation of the GNOME sentinel prototype.

REFERENCES

[1] E. D. Kaplan and C. J. Hegarty, Understanding GPS – Principles and Applications, 2nd ed., Artech House Inc., Norwood, MA 02062, 2006.

[2] C. J. Hegarty and E. Chatre, "Evolution of the global navigation satellite system (GNSS)," Proc. of the IEEE, vol. 96, no. 12, Dec., 2008.

[3] ICAO, International Standards and Recommended Practices – Annex 10 to the Convention on International Civil Aviation Aeronautical Telecommunications – Volume I Radio Navigation Aids, 6th ed., July 2006.

[4] Ingegneria Dei Sistemi S.p.A. website: http://www.idscorporation.com/.

[5] G. Del Duca, R. Perago, V. Paciucci, G. Di Bitonto, and F. Principe, "Verification of GNSS applications at italian regional airports," Proc. of ENC-GNSS 2009, Naples (Italy), May 3-6, 2009.

[6] A. Italiano, F. Principe, R. Cioni, and R. Perago, "Multipath and interference modelling in complex GNSS scenario," Proc. of EuCAP 2010, Barcelona (Spain), April 12-16, 2010.

[7] SC-159, Assessment of RF Interference Relevant to the GNSS, RTCA DO-235B, Washington DC 2036, March 13, 2006.

[8] EUROCAE, Minimum Operational Performance Specification for Global Navigation Satellite GBAS Ground Equipment to Support Cat. I Operations, ED-114, Sept. 2003.

[9] SC-159, MOPSs for GPS/WAAS Airborne Equipment, RTCA DO-229D, Washington DC 2036, Dec. 13, 2006.

[10] B. A. Renfro, and *et al*. "Challenges in the development of GNSS monitoring receivers – Historical lessons learned," Proc. of the 2008 National Technical Meeting of the ION, San Diego, CA, Jan. 28-30, 2008.

[11] W. Dunkel and F. Butsch, "GNSS monitoring and information systems at Frankfurt airport," Proc. of the 13th ITM of the Satellite Division of the ION (ION GPS 2000), Salt Lake City, UT, Sept. 19-22, 2000.

[12] K. Gromov, and *et al*. "Interference direction finding for aviation applications of GPS," Proc. of the ION GPS 1999, Nashville, TN, Sept. 14-17 , 1999.

[13] S. Pullen and G. Xingxin Gao, "GNSS jamming in the name of privacy - Potential threat of GPS aviation," Inside GNSS, March/April, 2012.

[14] ICAO Doc. 8071, Manual on Testing of Radio Navigation Aids, vol. 2, 5th Ed., 2007.

[15] T. L. Beach and P. M. Kintner, "Development and use of a GPS ionospheric scintillation monitor," IEEE Trans. on Geoscience and Remote Sensing, vol. 39, no. 5, May, 2001.

[16] A. J. Van Dierendonck, J. Klobuchar, and Q. Hua, "Ionospheric scintillation monitoring using commercial single frequency C/A code receivers," Proc. ION GPS-93, Arlington, VA, Sept., 1993.

[17] S. Peng and Y. Morton, "A USRP2-based multi-constellation and multi-frequency GNSS software receiver for ionosphere scintillation studies," Proc. of the ION GNSS 2011, Portland, OR, Sept. 20-23, 2010.

[18] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," International Journal of Navigation and Observation, vol. 2012, art. ID 127072, 16 pages, 2012.