International Civil Aviation Organization

WORKING PAPER

AN-Conf/14-WP/163
22/7/24
(Information Paper)
English and Spanish only[1]

FOURTHEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

Agenda Item 2: Timely and safe use of new technologies
2.2: Addressing safety risks related to evolving aviation technologies

MITIGATIONS OF GNSS VULNERABILITIES IN EUROPE – ACTIVITIES AND EXAMPLES

(Presented by Spain)

EXECUTIVE SUMMARY

This information paper is aligned with the discussion developed in the working papers "Planning for GNSS contingencies" and "Aviation safety and security concerns regarding interference to the Global Navigation Satellite System (GNSS)" (AN-Conf/14-WP/61 and AN-Conf/14-WP/63 refer, respectively), and tries to give a wider view about GNSS vulnerabilities, one of the main drivers justifying the elaboration of both working papers. Moreover, this information paper includes a description of some mitigation actions taken generally in Europe and particularly in Spain.

The use of GNSS in all phases of the flights has increased recently worldwide, thanks to being the main navigation sensor that supports the performance-based navigation (PBN) concept. Moreover, the benefits that brings to aviation makes logical the massive deployment of its use. However, as any other system, it has some inherent vulnerabilities that could potentially impact the aviation that are needed to be minimized and mitigated. Regarding these vulnerabilities, all the aviation actors worldwide are working to set barriers and mitigation actions to guarantee the safety and continuity of the air operations when facing GNSS outages and degradations. At European level, GNSS contingencies have been addressed by different European institutions, spreading recommendations and best practices to minimize their impact. Furthermore, at national level, there are several States that are working to define the contingency scenarios and to foster the deployment of the needed systems, on the one hand, to detect the GNSS degradation in order to trigger the contingency scenarios without any major safety concerns and, on the other hand, to assure a reasonable continuity of the operations.

1. INTRODUCTION

1.1 Despite of the fact that GNSS has been used from a long time in all flight phases and particularly in en route phase, nowadays, its use is increasing as a primary navigation method, being the main enabler of the PBN concept, which represents the future of the air navigation. Moreover, GNSS core constellations combined with their augmentation systems are the only sensor capable of supporting all flight phases, making it a key player in the development of aviation worldwide.

[1] English and Spanish versions provided by Spain.

1.2 Furthermore, the use of GNSS is going beyond the provision of navigation position for aircraft, being used by other on board and ground communications, navigation, and surveillance (CNS) systems for providing alternative communication (controller-pilot data link communications (CPDLC)) and surveillance (automatic dependent surveillance – broadcast (ADS-B)) services that tend to complement the use of the legacy systems.

1.3 For navigation, the GNSS core constellations, along with their frequencies and the augmentation systems, that are permitted for civil aviation are specified in the ICAO Annex 10 — *Aeronautical Telecommunications*, Volume I — *Radio Navigation Aids*. GNSS core constellations included in the Standards and Recommended Practices (SARPs) are Global Positioning System (GPS) (L1, L5), Global Navigation Satellite System (GLONASS) (L1, L3), Galileo (E1, E5) and BeiDou Navigation Satellite System (BDS) (B1I, B1C, B2a). The augmentation systems listed in that document are aircraft-based augmentation system (ABAS), satellite-based augmentation system (SBAS), ground-based augmentation system (GBAS) and ground-based regional augmentation system (GRAS) for each of the core constellations. Even if all these elements are listed, it should be the responsibility of each State to approve the use of each system in the airspace under their responsibility.

1.4 Although the possibility of the use of these systems in the air navigation exists, it is still needed that all the involved stakeholders share the same maturity level for its effective use, accompanying, among others, the development of the GNSS systems, the equipment of the aircraft, the adaptation of the air traffic management (ATM)/air traffic services (ATS) and the crew's certification.

1.5 However, despite the multiple benefits that the use of GNSS can bring to the aviation community, it is not exempted of some vulnerabilities due to the nature of their satellite signals and their widespread use, which carries associated risks for CNS/ANS services that are not present in other positioning/navigation ground-based navaids whose sole purpose is to provide signals for air navigation services. Also, the fact that they are global signals means that there may be a common cause of failure, and any outage on them could have an impact on a large airspace area.

1.6 GNSS signals received on Earth are very weak due to the long distance that the transmitted signal must travel from satellite orbit to reception. This makes these signals vulnerable and easy to be interfered by RF disturbances (whether intentional or unintentional), both in the receiving environment and on their way from the satellite to the receiver. This could cause severe degradations in the reception of GNSS signals, including complete loss of position and time solution. The main threats to GNSS are space weather, radio frequency interference (RFI), cyberattacks and constellation failures. The most likely ones are the first two, both developed in this paper.

1.7 Consequently, nowadays the aviation community is working on the one hand, to set barriers to avoid the effects of the hazards associated to loss and disturbances on GNSS signals, (e.g., developing dual-frequency multi-constellation systems). On the other hand, to implement mitigations measures to minimize the impact they could have on the aviation community (e.g., developing a harmonized planning for GNSS contingency as is set in the European working paper AN-Conf/14-WP/61, "Planning for GNSS contingencies").

1.8 In this regard, different European institutions, amongst them, the European Commission, the European Union Aviation Safety Agency (EASA) and European Organisation for the Safety of Air Navigation (EUROCONTROL), are addressing the GNSS contingencies.

2. EUROPEAN REGULATORY FRAMEWORK

2.1 From a regulatory standpoint, the objective of a high uniform level of civil aviation safety in the European Union and the main requirements to achieve that goal are set, for all relevant actors, by the EASA Basic Regulation, i.e. *Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency.*

2.2 The main European Regulation addressing the safety impact of GNSS contingencies in civil aviation is, for the moment, *Commission Implementing Regulation (EU) 2018/1048 of 18 July 2018 laying down airspace usage requirements and operating procedures concerning performance-based navigation (PBN)*. PBN contingencies are defined as situations where, for unexpected reasons beyond their control, GNSS or other methods used for performance-based navigation are no longer available, making it impossible for them to provide their services in accordance with the PBN requirements laid down in the Regulation.

2.3 Since GNSS is the main navigation system supporting PBN – the only one, for some applications – a PBN contingency amounts in practice to a GNSS contingency focused on-air navigation. Should such an event occur, the air navigation services provider (ANSP) shall take measures for the continued, safe provision of their services through other means – for example, retaining a network of conventional navigation aids and related surveillance and communications infrastructure. *Annex II of EASA Decision 2018/013/R (Guidance Material to Commission Implementing Regulation (EU) 2018/1048)* provides supplementary guidance on GNSS contingencies and the establishment of such an infrastructure.

2.4 From the perspective of safety risks, EASA defines safety portfolios in Volume III of the European Plan for Aviation Safety (EPAS) 2024, which contains several Safety Issues (SI), i.e. safety deficiencies related to one or more hazards. Once a Safety Issue is identified and captured within a portfolio, it is subject to a technical safety assessment providing potential mitigating actions.

2.5 Several Safety Issues are related to GNSS contingencies:

2.5.1 GNSS signal manipulation leading to navigation or surveillance degradation (SI-5501A) addresses the disturbance or alteration of GNSS signals near conflict zones. The contents of its associated mitigation measure, EASA Safety Information Bulletin (SIB) 2022-02R3 (*Global Navigation Satellite System Outage and Alterations Leading to Navigation/Surveillance Degradation*) are developed in the following sections.

2.5.2 Space weather effects on aviation (SI-5102) acknowledges the impact of such events on GNSS, especially on the performance of un-augmented GNSS in the region close to the magnetic equator. As before, the contents of its associated mitigation measures, EASA SIBs 2012-09R1 *Effects of Space Weather on Aviation* and 2012-10R1 *Single Event Effects on Aircraft Systems caused by Atmospheric Radiation,* are developed in the following sections.

2.6 Finally, the high-level views of EUROCONTROL on the issues derived from GNSS interference have been posed through EUROCONTROL Think Paper #9 (dated 1 March 2021)[2]. It presents a number of recommendations for policymakers in order to safeguard the reliability of GNSS for aviation and maintain safety at the highest possible level. The current relevance of GNSS for efficient air navigation is described, as well as the increasing trend of GNSS vulnerability, which reduces safety and operational

[2] https://www.eurocontrol.int/publication/eurocontrol-think-paper-9-radio-frequency-interference-satellite-navigation-active

efficiency. GNSS RFI events require additional awareness and actions at State level to ensure that aviation can continue to operate safely.

3. MAIN GNSS VULNERABILITIES

3.1 The main types of ground disturbance that can affect the normal operation of satellite-based navigation systems are the emission of signals of enough power to degrade or completely inhibit the GNSS reception (jamming), and the replacement of true GNSS signals by false ones (spoofing). These phenomena can be caused either intentionally or unintentionally.

3.2 The disturbances due to space weather impact the signals when getting through the different layers of the Earth's atmosphere. The main contribution to the disruption of the signals is the interaction with the ionosphere, whose behavior is directly linked to the solar activity.

3.3 The functioning of GNSS normally relies on navigation signals transmitted from core constellation satellites in medium Earth orbit (MEO). The received power of these signals at the antenna output of a user receiver is typically extremely small, from approximately -165 up to -150 decibel watt (dBW), which makes them inherently vulnerable to RFI caused by the emissions of other radio systems. This interference could be unintentional in nature, such as from malfunctioning or spurious emission from a transmitter in the vicinity of the GNSS receiver, or intentional, i.e. by deliberate use of jamming or spoofing equipment, whether with low (e.g. personal privacy devices) or high radiated power (e.g. military grade).

3.4 The most frequent examples of such interference reports are caused by so called personal privacy devices, which are essentially low power GNSS jammers used to locally disable the operation of GNSS receivers. Although the use of personal privacy devices is illegal they can be easily acquired on the Internet at low cost (e.g. ~10 USD for a jammer with 100 milliwatts (mW) of transmitter power, which is enough to degrade performance or disrupt GNSS receivers in a range of 10-100 m or even more). In the last decade, spoofers have also become available on the Internet (e.g. ~100 USD for a software defined radio that can be used as a spoofer).

3.5 Wide-area GNSS RFI events are reported by users more often, due to electronic warfare or "security measures", supposedly performed by military or paramilitary forces around the world. Therefore, the pure unintentional RFI has become a lesser threat for GNSS compared to the intentional RFI (whether collateral or targeted).

3.6 RFI can impact either aircraft themselves or ground-based critical infrastructure that use GNSS to augment the performance of the positioning solution (e.g. European Geostationary Navigation Overlay Service Ranging and Integrity Monitoring Station (EGNOS RIMS) and GBAS) or to synchronize systems (e.g. a radar station or any other ATM/ANS ground infrastructure that use GNSS time for synchronization).

4. USER'S DEMANDS AGAINST GNSS DEGRADATIONS IMPACTING AVIATION

4.1 For some time on, in the aviation community has risen the concern about the impact of the GNSS degradation. Different initiatives have been started to warn the community about the problematic, detailing the impact on each user of the GNSS degradation and trying to find common and harmonized solutions to them.

4.2 Recently, at European level, two workshops have been performed seeking these objectives. The ICAO European and Middle East (EUR/MID) Radio Nav Symposium that took place in Antalya, Türkiye, between 6 to 8 February 2024 and the EASA-International Air Transport Association (IATA) Workshop on Positioning, Navigation and Timing (PNT) Resilience on 25 January 2024 in Cologne, Germany. In both meetings, the message launched by the users was the same.

4.3 From the commercial aircraft operators' point of view, there has been an increased attention on the necessity of developing reporting and coordinating protocols between pilots and ground control for events management. This is deemed necessary regarding the recurrent effects detected on board due to GNSS events, which can leave pilots with no navigation information whatsoever, or create false alerts from the safety nets that, if not checked with external reference, cannot be properly assessed for acting, which could lead to incidents or accidents.

4.4 Commercial aircraft operators believe as well in the necessity of providing crews with detailed instructions from equipment manufacturers regarding the proper way of managing the systems during GNSS events, and in the retention of sufficient non GNSS-dependent CNS means for ensuring continuity of services. They also are keen on collaboration in order to gain common knowledge about GNSS vulnerabilities, regarding both their nature and the recurrent affected areas to avoid.

4.5 From ANSP point of view, there exists the necessity for a thorough knowledge of how GNSS events can affect both the performance of users and the performance of their own services network. It is important that ANSP personnel clearly know how to provide assistance for what the users need and take preventive measures as far as possible. Over reliance on GNSS for support of CNS services can bring to common mode failures that may render scenarios operationally unmanageable, so appropriate measures should be taken for avoiding such scenario. At the same time, operational actors need to improve their awareness regarding GNSS unavailability and degradations, so that contingency situations can be managed as effectively as possible.

5. EUROPEAN ACTIVITIES REGARDING GNSS CONTINGENCY

5.1 As mentioned before, EASA, as a mitigation action against the increasing number of GNSS RFI impacting the airspace users near conflict zones, published and updated a Safety Information Bulletin with two main objectives. The first one is to describe what, and which, is the impact on civil aviation of the RFI, listing the more affected zones. The second one is to make some recommendations in order to implement mitigating measures to: civil aviation authorities, ATM/ANS providers, air operators, and aircraft and equipment manufacturers. This information is shown in detailed in the appendix.

5.2 As an initiative at network level, EUROCONTROL's Operational Excellence Programme, managed by the Network Directors of Operations and the Network Directors of Technology working groups, and reporting to the Network Manager Board, seeks to ensure the coordination for the implementation of operational and technical evolutions, enhanced operational and technical concepts, covering, among several other areas, the harmonised implementation of new operational concepts for addressing GNSS reversion strategy and evolutions of CNS infrastructure and technologies for an improvement in resiliency.

5.3 For each of the considered areas, the Operational Excellence Programme developed dedicated work stream topics, in which the Network Manager and relevant stakeholders (ANSPs, aerodrome operators, airlines, etc.) discussed and proposed operational and technical evolutions, which are recognised as beneficial for further improvement of the network and local performance.

5.4 In these work streams are addressed, on the one hand on network resilience and infrastructure risks, focusing on GNSS threat assessment, identifying the different threat types, regarding their nature and the typical effect on aviation to provide users with tools for the safety assessment of events. Besides, work was made for developing guidelines for coordination between the civil and the military regarding interference emissions exercises and testing.

5.5 On the other hand, the development of a strategy for the continued safe management of air traffic in the event of a GNSS outage. This “GNSS reversion strategy” pursues presenting a harmonized approach to the matter that users could use as a framework for reference for their strategies development.

5.6 Finally, it is considered worth to mention that during the last years several tools and means have been developed for users with a lack of appropriate own resources that can be of use for the assessment of operational scenarios, navigation systems monitoring and identification and addressing of GNSS threats.

5.7 At the European level, several states and institutions are already integrating GNSS monitoring systems based on different technologies and information such as, GNSS receiver networks, ADS-B data and spectrum analysis, among others, which seek to survey both the correct functioning of GNSS services used in their airspace and the interferences that may affect the most critical phases of flights when using GNSS sensors as the primary means of navigation.

5.8 Apart from the unplanned or unexpected RFI events, there are planned events that many States perform as part of electronic warfare military exercises or other national security uses. These exercises could impact civil aviation, and therefore a diligent coordination with the ANSP should be considered. In some cases, the impact of the RFI could reach more than one State, and an international coordination is needed. For this practice, the EUROCONTROL GRIT coordination tool, currently under development, is expected to be very useful.

6. SPANISH ACTIVITIES REGARDING GNSS CONTINGENCY

6.1 The GNSS monitorization in those scenarios where their dependence has increased considerably is becoming almost essential in order to activate the necessary mechanisms to maintain the safety, efficiency and continuity of air navigation operations.

6.2 In the case of Spain, ENAIRE, the main air navigation and CNS service provider, operates a network of GNSS receivers in those airports with Required Navigation Performance approach (RNP APCH) maneuvers, which evaluates GNSS performance and reports the behavior of these systems (RECNET system), being able to take mitigating actions in case of service degradation. Likewise, in those high-density scenarios, interference detection and localization systems (DYLEMA system) are being deployed, enabling coordination procedures, on the one hand, with air traffic control officers to inform them of possible interference in their environment and thus increase the situational awareness of controllers, and on the other hand, with the agents of the national spectrum agency in charge of the correct use of the radioelectric spectrum.

6.3 As mentioned, ENAIRE is operating a ground based RFI detection and localization system around Madrid airport called DYLEMA. It consists of 10 RFI monitoring stations and a GNSS monitoring centre operated 24/7. From this centre, ENAIRE reports RFI events to the Spanish National Spectrum Agency, in a collaborative agreement between them, and to ATCOs to augment their situational awareness. In case any pilot reports a GNSS malfunctioning onboard, the air traffic controllers could immediately take mitigation actions. The immediate action is not taken with the only input of DYLEMA since most of the RFI events do not impact the aircraft, but the ground area around the jammer or spoofer (low power devices). Similar RFI detection and localization systems will be deployed in other main Spanish terminal control areas in the next years (e.g. Palma de Mallorca airport in 2024).

6.4 As examples of the outcomes of both GNSS monitoring systems, thanks to the RECNET system, it has been possible to detect the degradations of the European SBAS system, EGNOS, services in the Canary Islands, due to the solar peak. This has made it possible to act accordingly. In the case of DYLEMA, and average of 10 interferences each month have been detected since the start of the operation, and the detection and localization processes have been activated, although without being necessary the coordination with the ATCOs.

7. CONCLUSION

7.1 GNSS systems have uncountable benefits that bring the aviation community an increasing level of safety and efficiency while trying to meet the challenges of the future of the air operations and lead it to the next generation of ATM/ANS provision.

7.2 However, like any technology, it presents a series of vulnerabilities that must be known and studied in order to minimize their impact on the airspace users.

7.3 This paper aims to showcase these vulnerabilities and to disseminate to the aviation community the mitigation measures being carried out in Europe in general, and in Spain in particular, so that more harmonized practices may be established for reference of all users in other parts of the world.

7.4 Amongst the mitigations defined in the above-mentioned activities, there are:

a) foster the implementation of policies to ensure the definition of a national GNSS contingency strategy, establishing the basic principles regarding the adoption of measures deemed necessary and the availability of the means to carry them out;

b) planification, in accordance with the related national policies, of the disposition of the necessary CNS means for sustaining an adequate level of operations during GNSS contingency scenarios, supporting non-GNSS based instrumental procedures compatible with the nominal PBN airspace concept and direct assistance by ATS personnel if needed;

c) direct coordination with operational agents for the definition of specific procedures and action protocols to address GNSS contingency related operational scenarios, regarding reversion to non-GNSS-based operations, traffic diversion management, identification and assistance of affected traffic, etc; and

d) deployment and operation of GNSS monitoring systems based on different technologies, to be able to trigger the predefined contingency measures as soon as possible, guaranteeing the highest safety level of air navigation operations.

— — — — — — — —

APPENDIX

European Union Aviation Safety Agency

Safety Information Bulletin

Operations – ATM/ANS – Airworthiness

SIB No.: 2022-02R3

Issued: 05 July 2024

Subject: **Global Navigation Satellite System Outage and Alterations Leading to Communication / Navigation / Surveillance Degradation**

Revision:

This SIB revises EASA SIB 2022-02R2 dated 06 November 2023.

Applicability:

Competent Authorities (CA), Air Traffic Management/Air Navigation Service Providers (ATM/ANS providers), air operators, aircraft and equipment manufacturers, organisations involved in the design or production of ATM/ANS equipment.

Description:

Since February 2022, there has been an increase in jamming and/or spoofing of Global Navigation Satellite Systems (GNSS). EASA has analysed recent data from the Network of Analysts and open sources and has concluded that GNSS jamming and/or spoofing has shown further increase in the severity of its impact, as well as an overall growth of intensity and sophistication of these events. This issue particularly affects the geographical areas surrounding conflict zones, but it is also encountered in the south and eastern Mediterranean, Black Sea, Middle East, Baltic Sea, and Arctic area.

The list of affected flight information (FIR) regions is published on the EASA website at https://www.easa.europa.eu/GNSS.

Jamming is an intentional radio frequency interference (RFI) with GNSS signals. This interference prevents receivers from locking onto satellites signals and has the main effect of rendering the GNSS system ineffective or degraded for users in the jammed area.

Spoofing involves broadcasting counterfeit satellite signals to deceive GNSS receivers, causing them to compute incorrect position, navigation, and timing (PNT) data.

There are no specific flight crew alerts that would indicate which kind of interference is being experienced – jamming or spoofing. Nevertheless, the effects of jamming are typically immediate and noticeable by the flight crew, as systems fail to receive GNSS signals. This should allow for quick recognition of the problem and reaction with mitigation measures. On the other hand, detection of spoofing is more difficult and not immediate for the flight crew, thus posing more safety risk than jamming. Depending on aircraft-system integration, various side effects of jamming have been observed which could be attributed to spoofing and vice-versa. For the purposes of this safety information bulletin, jamming and spoofing are discussed as suspected causes, regardless of their actual cause.

The following non-exhaustive list provides observed symptoms of suspected GNSS spoofing:
- Incoherence in navigation position, such as GNSS/FMS position disagree alerts;
- Abnormal differences between Ground Speed and True Airspeed;
- Time and date shift;
- Spurious Terrain Awareness and Warning System (TAWS) alerts;
- Potential deviation of hybrid position (IRS/GNSS).

The effects of GNSS jamming and/or spoofing have been observed by crews in various phases of flight, in some cases leading to re-routing or diversions, to ensure safe continuation of flight, and triggering spurious TAWS alerts. Under the present conditions, it is not possible to predict GNSS interference or its effects. The magnitude of the issues generated by these interferences depends upon the extent of the area concerned, on the duration, on the traffic density, on the phase of flight, and on how dependent the aircraft systems are on GNSS signals.

The following non-exhaustive list provides examples of issues that a degradation of GNSS signal (including Satellite Based Augmentation Systems (SBAS) and Ground Based Augmentation Systems (GBAS)) could generate:

- Temporary or non-recoverable failure or degradation of PNT information provided by GNSS, possibly resulting in:
    - Loss of or misleading TAWS (e.g., spurious PULL UP alerts triggered by predictive TAWS during cruise, descent, approach, and landing phase that in some cases resulted in high vertical rate uncoordinated climbs, note that traffic alerts are deprioritised over TAWS PULL UP alerts);
    - Loss of Airborne Collision Avoidance System (ACAS);
    - Loss of or misleading surveillance function (e.g., corrupted Automatic Dependent Surveillance-Broadcast (ADS-B);
    - Loss of or misleading information on a Synthetic Vision Systems (SVS), weather uplink functions, predictive wind shear, and other surface functionalities;
    - Inconsistent flight guidance possibly resulting in route divergence, uncommanded turns, and deviations from the ATC clearances or instructions received, which could potentially lead to airspace infringements, loss of traffic separation, insufficient terrain/obstacle clearance, etc.;
    - Inconsistent, or potentially misleading aircraft position, GNSS altitude, and calculated ground or wind speed on the navigation display or on the Electronic Flight Bag (EFB);
    - Inconsistent, or potentially misleading aircraft position and/or GNSS altitude, later in the flight after having exited the affected area, e.g., during approach;
    - Loss or misleading time and/or date dependent systems (e.g., clock, fuel computation system, flight management system, discarded Controller Pilot Data Link Communication (CPDLC) messages).
- Inability to use GNSS for navigation, including waypoint navigation;
- Inability to use GNSS for navigation after exiting the affected area or for the remainder of the flight;

- Inability to maintain GNSS based Area Navigation (RNAV) and/or Required Navigation Performance (RNP).

Repeated or widespread disruptions of the GNSS signals can lead to increased workload of both flight crews and air traffic controllers that can cause cognitive overload or confusion and increase the risk for errors.
The combination of two or more of the issues listed above may have cumulative adverse effects on flight safety.
GNSS Jamming and Spoofing also can affect ground-based systems, especially when they use GNSS as their only source for timing.

This SIB is revised to list new issues observed and update recommendations, as a result of analysis of recently reported occurrences of jamming and spoofing.

EASA is continuously monitoring and assessing the situation, however, at this time, the safety concern described in this SIB is not considered to be an unsafe condition, that would warrant Safety Directive (SD) action under Commission Regulation (EU) 965/2012, Annex II, ARO.GEN.135(c), nor under Commission Regulation (EU) 2017/373, Annex II, point ATM/ANS.AR.A.030, or Airworthiness Directive (AD) action under Regulation (EU) 748/2012, Part 21.A.3B.

Recommendation(s):
To address the identified issues EASA recommends the implementation of the following mitigating measures. These measures are to be considered for the flight information regions published on EASA website and should be extended to any other area where GNSS jamming and/or spoofing is identified. Some recommendations for aircraft operators are now separated for jamming as compared with spoofing, due to the specificities of the two different cases.

CAs should:
- Ensure that contingency procedures are established in coordination with ATM/ANS providers and airspace users, and that existing non-GNSS based navigation infrastructure, particularly Instrument Landing Systems (ILS), Distance Measuring Equipment (DME) stations and Very High Frequency Omnidirectional Range (VOR) stations are made available and kept operational as required;
- Implement appropriate and proactive mitigating measures as a matter of high priority, including the issuance of NOTAMs, e.g., describing affected areas and related limitations;
- Facilitate the establishment by ATM/ANS service providers of a process to collect information on GNSS degradations, in coordination with the relevant national regulatory authorities for telecommunications, and promptly notify the related outcomes to air operators and to other airspace users;
- Consider measures at national level, by involving appropriate and competent entities, to avoid the proliferation, circulation and operation of unauthorized transmitters that cause or have the potential to cause harmful interference to GNSS signals;

- When applicable, encourage civil-military coordination prior to testing or use of GNSS disturbance systems[1];
- Ensure that contents of this SIB are duly considered by air operators, ATM/ANS providers, aircraft and equipment manufacturers, and organisations involved in the design or production of ATM/ANS equipment.

ATM/ANS providers should:

- Establish a process to collect information on GNSS degradations, in coordination with the relevant CAs, national regulatory authorities for telecommunications, and promptly notify the related outcomes to air operators and to other airspace users;
- Assess the impact of loss or anomalies of GNSS-based timing on CNS systems;
- Adhere to the procedures on the provision of information to airspace users as appropriate, e.g., through ATIS, issuing NOTAMs, AIP, etc.;
- Consider keeping a ground navigation infrastructure operational such as ILS, DME, and/or VOR in support of conventional and performance-based navigation procedures;
- Make sure that the surveillance coverage is resilient to GNSS interference;
- For areas, where surveillance remains exclusively based on ADS-B, ensure that appropriate contingency procedures are available, when GNSS jamming or spoofing is detected;
- In areas affected by GNSS jamming and/or spoofing promote the use of conventional navigation flight procedures or performance-based flight procedures using VOR/DME;
- Be prepared to provide navigation assistance to aircraft (using radar vectoring) as long as needed;
- Ensure that the communications coverage and performance meet the needs for radar vectoring provision in case of GNSS jamming or spoofing;
- Ensure that contingency plans include procedures to be followed in case of large-scale GNSS short-term and long-term jamming and/or spoofing events;
- Consider implementing local GNSS RFI detection and GNSS status monitoring systems in addition to network-level capabilities, as needed;
- Reinforce the monitoring of the traffic closely to prevent any deviation from ATC clearances (e.g., navigation track and altitude);
- Assess whether sector capacities and applicable separation minima remain appropriate;
- Ensure that GNSS jamming or spoofing topic is included in the ATCO training, highlighting the identified operational scenarios to recognise, react in a timely manner to different jamming and spoofing cases.

Air operators should:

- Ensure that flight crews are aware, trained and prepared to recognise and adequately respond to an encounter of GNSS interferences during flight;
- Ensure that flight crews are aware of the importance of prompt reporting by means of a special air-report (AIREP) to air traffic services of any observed interruption, degradation or anomalous performance of GNSS equipment or related avionics (e.g., map shifts, suspected GNSS spoofing, lost or misleading position, time anomalies, etc., including their duration);

[1] Refer to EUROCONTROL "Guidelines on a Process for Civil and Military GNSS Interference Testing" for further guidance.

- Evaluate different possible scenarios based on the type of operations in order to provide the flight crew with timely information to increase awareness of jamming and spoofing;
- Ensure that GNSS jamming or spoofing topic is included in the flight crew ground recurrent training and training of other relevant operations personnel, especially when operating in the mentioned areas, highlighting the identified operational scenarios to recognise, react in a timely manner to different jamming and spoofing cases;
- Assess operational risks and limitations linked to the loss of on-board GNSS capability, including any on-board systems requiring inputs from a reliable GNSS signal, e.g., impact on TAWS;
- Maintain contact with aircraft or equipment manufacturers for instructions and guidance on how to operate and maintain their products, when exposed to jamming or spoofing, and implement the recommendations in the standard operating and maintenance procedures;
- Ensure that any system used as a backup to GNSS is not inoperative according to the Minimum Equipment List, before commencing a flight into known affected areas, with the exception of one flight if necessary to reach a station, where the repair can be done;
- Ensure that systems, used as a backup for an inoperative system according to the Minimum Equipment List, are not reliant on GNSS, before commencing a flight into affected areas, with the exception of one flight if necessary to reach a station where the repair can be done;
- Ensure, whenever possible (e.g., airspaces that are not oceanic or remote), in the flight planning for flights into affected areas, the availability of alternative non-GNSS based procedures for the whole flight, regardless of the type of operation. This should be complemented with information regarding the ability to receive radar vectoring in the airspaces to be transited;
- If subject to Flight Data Monitoring (FDM) requirements and necessary data are available, use FDM programme to identify and assess GNSS jamming and spoofing events.

GNSS jamming specific recommendations for Air operators:

- Ensure that flight crews and relevant flight operations personnel:
  - are aware of possible GNSS jamming;
  - verify the aircraft position by non-GNSS means, when flights are operated in proximity to the affected areas;
  - check that the navigation aids essential to the operation for the intended route and approach are available;
  - remain prepared to revert to a non-GNSS procedure where appropriate; and
  - report (AIREP) any observed irregularities to air traffic services.

GNSS spoofing specific recommendations for Air operators:

- Ensure that flight crews and relevant flight operations personnel:
  - are aware of possible GNSS spoofing;
  - when possible monitor aircraft position using non-GNSS navaids and all available automatic navigation accuracy calculations, including the Estimated Position Uncertainty (EPU) figure;
  - monitor the GNSS time versus non-GNSS time sources;
  - closely monitor the ATC frequencies in the vicinity of spoofing area;
  - apply the manufacturer's instructions and guidance for the aircraft type on detecting and dealing with suspected spoofing;

- report (AIREP) to air traffic services any observed irregularities.

Aircraft and equipment manufacturers, should:

- Assess the effects of jamming and spoofing on their products considering cumulative effects of multiple systems being affected simultaneously;
- Support Air operators, by providing guidance on how to detect suspected GNSS spoofing events, when using their products;
- Provide instructions and guidance to Air operators on how to operate and maintain their products, when affected by GNSS jamming and spoofing, and implement the recommendations in the standard operating and maintenance procedures.

Organisations involved in the design or production of ATM/ANS equipment, should:

- Assess the effects of jamming and spoofing on their products considering cumulative effects of multiple systems being affected simultaneously;
- Support ATM/ANS providers, by providing guidance on how to detect suspected GNSS spoofing events, when using their products;
- Provide instructions and guidance to ATM/ANS providers on how to operate and maintain their products, when affected by GNSS jamming and spoofing, and implement the recommendations in the standard operating and maintenance procedures.

All parties concerned are reminded of their obligations to report any event impacting safety according to Regulation (EU) No. 376/2014.
Air operators are also reminded to report the suspected GNSS spoofing and higher risk jamming occurrences to aircraft manufacturers and support their investigations by providing relevant information in compliance with point ORO.GEN.160 (b) of Regulation (EU) No 965/2012.

Contact:
For further information contact the EASA Safety Information Section, Certification Directorate, E-mail: ADs@easa.europa.eu.

— END —