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.