Info Tech

Edizione 12.2023 pubblicazione del Dipartimento Tecnico ANPAC dt@anpac.it

14 novembre 2023

(English text at the bottom)

EASA SIB - GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) OUTAGE AND ALTERATIONS

Gentili Colleghi,
Dal febbraio 2022 è stato riscontrato un significativo incremento dei casi di jamming e/o spoofing del Global Navigation Satellite Systems (GNSS).

Tale circostanza, opportunamente analizzata da EASA, non è considerata una condizione pericolosa, tale da giustificare, ai sensi del Regolamento della Commissione EU, la pubblicazione di una Safety Directive (SD), tuttavia EASA ha ritenuto di pubblicare un Safety information Bulletin (SIB) dedicato.

Sebbene il jamming o lo spoofing del GNSS possano essere riscontrati in qualsiasi area del mondo, il bollettino EASA riporta nel dettaglio le regioni in cui tali episodi si sono verificati più frequentemente e fornisce una lista non esaustiva delle problematiche che un degrado del segnale GNSS potrebbe generare.

Il Bollettino riporta inoltre raccomandazioni e misure di mitigazione rivolte alle Autorità dell'Aviazione Civile, ai fornitori di ATM/ANS e agli Operatori Aerei, fornendo infine un'analisi delle differenti problematiche tre jamming e spoofing.

Di seguito la pubblicazione EASA.
Buona lettura

ANPAC – Dipartimento Tecnico
dt@anpac.it

English Version

EASA SIB - GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) OUTAGE AND ALTERATIONS

Dear Colleagues,

Since February 2022, there has been an increase in jamming and/or spoofing of Global Navigation Satellite Systems (GNSS).

EASA has analysed recent datas from the Network of Analysts and open sources and has concluded that GNSS jamming and/or spoofing is not considered to be an unsafe condition, that would warrant Safety Directive (SD) action under Commission Regulation, however EASA has decided to publish a dedicated Safety information Bulletin (SIB).

Although GNSS jamming or spoofing can be encountered anywhere in the world, the EASA Bulletin indicates a list of the mainly affected flight information regions (FIR) and provide a non-exhaustive list of examples of issues that a degradation of GNSS signal could generate.

The Bulletin also shows recommendations and mitigating measures to Civil Aviation Authorities, ATM/ANS providers and Air Operators, finally providing an analysis of the different problems between jamming and spoofing.

Here below the EASA publication.
Enjoy the reading

ANPAC – Dipartimento Tecnico
dt@anpac.it

Safety Information Bulletin

Operations – ATM/ANS - Airworthiness

SIB No.: 2022-02R2

Issued: 06 November 2023

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

Revision:

This SIB revises EASA SIB 2022-02R1 dated 17 February 2023.

Ref. Publications:

None.

Applicability:

Competent Aviation Authorities (CAAs), Air Traffic Management/Air Navigation Service Providers (ATM/ANS providers), air operators, aircraft and equipment manufacturers.

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 is also encountered in the south and eastern Mediterranean and Black Sea, and present in Baltic Sea and Arctic area.

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 data (PNT).

Detection of jamming or spoofing as well as distinguishing which type of interference is being experienced is difficult, as there are generally no specific flight crew alerts for interference. Depending on aircraft 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 examples of symptoms of suspected GNSS spoofing:

- Incoherence in navigation position, such as GNSS/FMS position disagree warnings;
- Abnormal differences between Ground speed and True airspeed;

- Time shift;
- Problems with INS/IRS.

Although GNSS jamming or spoofing can be encountered anywhere in the world, the mainly affected flight information regions (FIR) are:

- The Black Sea area:
  - FIR Istanbul LTBB, FIR Ankara LTAA
  - Eastern part of FIR Bucuresti LRBB, FIR Sofia LBSR
  - FIR Tbilisi UGGG, FIR Yerevan UDDD, FIR Baku UBBA
- The south and eastern Mediterranean area, and the Middle East:
  - FIR Nicosia LCCC, FIR Beirut OLBB, FIR Damascus OSTT, FIR Tel-Aviv LLLL, FIR Amman OJAC, north-eastern part of FIR Cairo HECC
  - FIR Baghdad ORBB, north-western part of FIR Tehran OIIX
  - Northern part of FIR Tripoli HLLL
- The Baltic Sea area (FIRs surrounding FIR Kaliningrad UMKK):
  - Western part of FIR Vilnius EYVL, north-eastern part of FIR Warszawa EPWW, south-western part of FIR Riga EVRR
- Arctic area:
  - Northern part of FIR Helsinki EFIN, northern part of FIR Polaris ENOR

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 also triggering false Terrain Awareness and Warning System (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 phase of flight, and how dependant the aircraft systems on GNSS signals are.

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:
  - Inconsistent flight guidance possibly resulting in route deviations, uncommanded turns, and potential airspace infringements;
  - Loss or misleading surveillance system (e.g. corrupted Automatic Dependent Surveillance-Broadcast (ADS-B), TAWS (e.g., false PULL UP alert triggered by TAWS during cruising phase), wind shear, terrain and other surface functionalities);
  - Loss or misleading time dependent systems (e.g. clock, fuel computation system, flight management system);
  - Inconsistent, potentially misleading aircraft position, and ground or wind speed on the navigation display.
- Inability to use GNSS for navigation, including waypoint navigation;
- Inability to conduct or maintain GNSS based Area Navigation (RNAV) and/or required Navigation Performance (RNP) operations.

This SIB is revised to extend its applicability to aircraft and equipment manufacturers and address the cases of spoofing. This SIB is revised in its entirety, and no revision bars are used.

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 aforementioned flight information regions 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.

CAAs should:

- Ensure that contingency procedures are established in coordination with ATM/ANS providers and airspace users, and that essential conventional navigation infrastructure, particularly Instrument Landing Systems, are retained and fully operational;
- 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 (as appropriate and determined at State level);
- Facilitate the establishment by ATM/ANS service providers of a process to collect information on GNSS degradations, in coordination with the relevant National Telecommunications Authorities, and promptly notify the related outcomes to air operators and to other airspace users;
- Initiate discussion at a national level to restrict the usage of GNSS jammers;
- Confirm that contents of this SIB are duly considered by air operators, including helicopter operators, ATM/ANS providers, and aircraft and equipment manufacturers.

ATM/ANS providers should:

- Establish a process to collect information on GNSS degradations, in coordination with the relevant CAAs, National Telecommunications Authorities, 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;
- Issue NOTAMs to provide relevant information to airspace users (as appropriate and determined at State level);
- Provide reliable surveillance coverage that is resilient to GNSS interference, as well as maintain essential conventional navigation infrastructure operational (Instrument Landing Systems, Distance Measuring Equipment (DME), Very High Frequency omnidirectional range (VOR)) in support of conventional navigation procedures;
- Ensure that their contingency plans include procedures to be followed in case of large-scale GNSS jamming and/or spoofing events;
- Monitor the traffic closely to prevent any deviation from the flight track/route;

Air operators, including helicopter operators, should:

- Ensure that flight crews are aware of and trained on 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, position and duration of the GNSS interference);
- 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 outage or spoofing topic is included in the flight crew ground recurrent training, highlighting the identified operational scenarios to recognize, 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;
- Ensure that operational limitations introduced by the dispatch of aircraft with inoperative radio navigation systems in accordance with the Minimum Equipment List, are considered before operating an aircraft in the affected areas;
- Ensure, in the flight planning and execution phase, the availability of alternative conventional arrival and approach procedures (e.g. an aerodrome in the affected area with only GNSS, including augmentation, approach procedures should not be considered as destination or alternate);
- If subject to FDM requirements and necessary data are available, use FDM programme to identify and assess GNSS spoofing events;
- Concerning spoofing: contact aircraft or equipment manufacturers for instructions on how to deal with spoofing cases of their products and implement the recommendations in the Standard Operating Procedures.

GNSS jamming specific recommendations for Air operators, including helicopter operators:

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

GNSS spoofing specific recommendations for Air operators, including helicopter operators:

- Ensure that flight crews and relevant flight operations personnel:
  - are aware of possible GNSS spoofing;
  - continuously monitor aircraft position using non-GNSS navaids and all available automatic navigation accuracy calculations, including the Estimated Position Uncertainty (EPU) figures;
  - 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 for the aircraft type on dealing with suspected spoofing, non-exhaustive list of examples of possible instructions could be such as:

1. being ready to select HDG mode and manually adjust the flight course.
2. being ready to ask for verification vector from ATC as long as needed.
3. being ready to crosscheck with and switch to alternate PNT such as IRS and/or available ground facilities (Multi-DME and VOR/DME).
4. being ready to exclude the GNSS signals within affected area.
5. being ready to disable automatic INS/IRS updating.

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

Aircraft and equipment manufacturers, should:

- support Air operators, by providing instructions to follow on how to deal with suspected GNSS spoofing events, when using their products.

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 alterations and higher risk jamming occurrences to aircraft manufacturers and support their investigations by providing relevant information according to Regulation (EU) No 965/2012, ORO.GEN.160 (b).

Contact(s):

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