Civil Aviation Authority of Singapore

Safety Information Bulletin

CAAS SIB No. 2022-01 R2

Issued 22 Dec 2023

Subject Global Navigation Satellite System (GNSS) Outage and Alterations Leading to Navigation / Surveillance Degradation

Ref. Publication(s) EASA SIB 2022-02 dated 6 Nov 2023, Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation

Purpose This SIB advises AOC holders on the possible GNSS outages or disturbances near geographical areas surrounding the conflict zones, including the south and eastern Mediterranean and Black Sea, Baltic Sea, and Arctic area. GNSS disturbances have also been reported in the Yangon FIR.

This SIB is revised to update the reporting requirements for AOC holders and operating crew. All AOC Holders are reminded of their obligation to immediately report any event encountered impacting safety and to report the suspected GNSS alterations and higher risk jamming occurrences to CAAS.

Applicability All Singapore AOC holders operating to destinations, or overflying airspace near the aforementioned geographical areas.

Cancellation This SIB supersedes the previous SIB dated 13 May 2022 on this subject.

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 conflict zones and geographical areas highlighted above.

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 affected 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 SIB, jamming and spoofing are described as suspected causes, regardless of their actual cause.

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

1. The Black Sea area
   - FIR Istanbul, FIR Ankara.
   - Eastern part of FIR Bucur Esti, FIR Sofia.
   - FIR Tbilisi, FIR Yerevan, FIR Baku.

2. The south and eastern Mediterranean area, and the Middle East
   - FIR Nicosia, FIR Beirut, FIR Damascus, FIR Tel-Aviv, FIR Amman, FIR Cairo
   - FIR Baghdad, north-western part of FIR Tehran.
   - Northern part of FIR Tripoli.

3. The Baltic Sea area (FIRs surrounding FIR Kaliningrad)
   - Western part of FIR Vilnius, north-eastern part of FIR Warszawa, FIR Riga.

4. Arctic area
   - Northern part of FIR Helsinki, northern part of FIR Polaris.

5. Asia area
   - Yangon FIR

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 are on GNSS signals.

The following, non-exhaustive, list provides examples of issues that a degradation of GNSS signal could generate:

1. Temporary or non-recoverable failure or degradation of position, navigation, and timing (PNT) information provided by GNSS resulting in:

    - Inconsistent flight guidance resulting in route deviations, uncommand 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.

2. Inability to use GNSS for navigation, including waypoint navigation.

3. Inability to conduct or maintain GNSS based Area Navigation (RNAV) and/or required Navigation Performance (RNP) operations.

Recommendation

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. AOC holders should **consider** the following measures:

- Ensure that flight crew 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 scenarios based on the type of operations, 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 dependable 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 that 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 Flight Data Management (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 or spoofing **specific recommendations** for AOC holders:

- Ensure that flight crew and relevant flight operations personnel are aware of possible GNSS jamming or spoofing.
  - Verify and monitor 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.
  - Monitor the GNSS time versus non-GNSS time sources.
  - Closely monitor the ATC Frequencies in the vicinity of the area.
  - Apply the manufacturer's instructions for the aircraft type on dealing with suspected spoofing and report to air traffic services any observed irregularities. The non-exhaustive list of examples of instructions could be such as:

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

Contact(s) For further information contact the respective POIs.