

Nov 1, 2023

# Global Navigation Satellite System spoofing

**Effectivity:** *Challenger* and *Global* aircraft

**ATA:** 34-55

By: Stephane Beauchamp – Avionics, Technical Services

In our last [article](#) on Global Navigation Satellite System Spoofing (GNSS), we discussed the EASA (European Union Aviation Safety Agency) Safety Information Bulletin (SIB) No. 2022-02 Revision 1, specifically on the effects of Global Navigation Satellite Systems (GNSS) jamming and/or possible spoofing, which has intensified in geographical areas surrounding conflict zones and other areas.

GNSS jamming and/or possible spoofing were observed by aircraft in various phases of flight, in certain cases leading to re-routing or even to destination changes due to the inability to perform a safe landing procedure.

Since this last article, we have received increasing reports on GNSS spoofing impacting aircraft industry-wide, as well as for Bombardier operators. The reported events indicate that the GNSS latitude/longitude versus actual aircraft position was incorrect, suggesting that the GNSS receiver was ‘spoofed’ resulting in an erroneous position.

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Contrary to GNSS signal jamming, where the data is

rendered invalid, the FMS will continue to use the spoofed GNSS position as valid. The crew is alerted with Flight Deck Effects (FDE) and different message(s), indicating that the GNSS position is suspect.

Recent cases so far have been experienced in Iraq along the Iranian border. It should also be noted that other regions are also affected by a similar condition. Based on the reports received so far in the Middle East airspace, the GNSS returned to normal operation once the aircraft exited the spoofing area, and the GNSS sensors were re-enabled for use via the Flight Management System (FMS).

Therefore, operators are encouraged to observe the following measures to mitigate the threat of spoofing:

- Plan to avoid airspaces known for an active military presence with contested airspace or conflict.
- Review enroute NOTAMS for the planned flight.
- Consult websites listed below for affected regions and review reports.

If spoofing is suspected:

- Follow the applicable loss of navigation guidance from the FMS Operating Guide for the associated message(s).
- If all navigation information is suspect, ask Air Traffic Control (ATC) for vectors reverting to traditional navigation methods until a reliable navigation source is restored. Deselect the affected GNSS sensors used in position determination.
- For any phase of flight other than enroute, refrain from using any RNAV type of procedures/approaches and revert to ILS/LOC or other non GNSS-based approach procedure.
- Refer to Bombardier Flight Operation Notification (FON) manual: AVNC-008 for *Challenger* series and AVNC-047 for *Global* series; FMS Incorrect Position due to GNSS Spoofing.

- Reminder on previous FON: AVNC-005 for *Challenger* series and AVNC-030 for *Global* series; GNSS Outage due to Signal Degradation or Jamming with Associated FDE.

Note: FON manuals are located within the technical publication flight manuals section.

Older aircraft were not initially equipped with GNSS at time of delivery; however, over time, GNSS became increasingly popular and was offered via different Supplemental Type Certificates (STCs). Operators should be familiar with their GNSS installation and interface with the FMS for navigation, where these may be potentially affected by spoofing as well.

Due to the nature of the issue, there is no corrective action that would prevent GNSS spoofing at this time, since this condition is related to external sources.

Spoofing may be sporadic and is often not formally revealed to the aviation community by the governing authorities of applicable countries. Usually, reports originate from outside countries or from aircraft operating in that area. Regardless of NOTAM availability, operators are reminded to remain vigilant, especially in regions with known military conflict or confrontation. This can occur even if an advisory is issued indicating a safe route.

It is good practice for operators to report any suspected GNSS events to regional aeronautical navigation service providers and ATC to enable the publication of NOTAMs. In addition, some websites allow the reporting of spoofing events for the benefit of all airspace users; for example, the FAA GPS reports and Safe Airspace Conflict Zone and Risk Database.

Below are some links which should be part of preflight planning:

- FAA GPS reports: [https://www.faa.gov/air\\_traffic/nas/gps\\_reports/](https://www.faa.gov/air_traffic/nas/gps_reports/)
- Safe Airspace Conflict Zone and Risk Database: <https://safeairspace.net/about/>
- Conflict Zone Information Bulletins (CZIBs):

<https://www.easa.europa.eu/domains/air-operations/czibs>

- FAA official U.S. government information about the Global Positioning System (GPS) and related
- topics: <https://www.gps.gov/support/user/>
- US Navigation Center: [Home | Navigation Center \(uscg.gov\)](#)
- NOTAMs for applicable countries/regions, such as the FAA site: <https://notams.aim.faa.gov/notamSearch/nsapp.html#/>

For details on SIB No. 2022-02R1, refer to <https://ad.easa.europa.eu/ad/2022-02R1>.