

Advisory Wire

REFERENCE AW000-34-0027

ATA: 34-55

EFFECTIVITY: All Challenger
All Global

**SUBJECT: Global Navigation Satellite
System Spoofing**

1. REFERENCES:

- 1.1. Bombardier Flight Operation Notifications (FON) manual: AVNC-008 for Challenger series and AVNC-047 for Global series; GNSS Spoofing causing FMS incorrect position.
- 1.2. Full Throttle Blog - November 2023 - [Global Navigation Satellite System Spoofing](#)
- 1.3. EASA (European Union Aviation Safety Agency) Safety Information Bulletin (SIB) No. [2022-02R2](#)
- 1.4. Collins Aerospace Service Information Letter, SIL GPS-4000S-22-1, CPN:523-0834272, NVM Clearing Procedure

References 1.1, 1.2 and 1.4 are available on the Bombardier Customer portal. The FONs are located within the technical publication flight manuals section.

2. INTRODUCTION:

This Advisory Wire (AW) is to inform operators of a condition related to Global Navigation Satellite System (GNSS) spoofing and associated maintenance actions, as well as the FONs (Ref. 1.1) available to the flight crew for operational aspect and guidance.

3. DESCRIPTION:

Since September 2023, there has been an increase in reports on GNSS spoofing impacting industry wide as well as Bombardier operators. The reported events indicated that the GNSS Latitude/ Longitude versus actual aircraft position was incorrect suggesting that the GNSS receiver was 'spoofed' resulting in an erroneous position. This was also broadcasted in a Bombardier article and EASA Safety Information Bulletin (Ref. 1.2 and 1.3)

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 GNSS position as valid. Crew is alerted with Flight Deck Effects (FDE) and different message(s), indicating that the GNSS position is suspect.

The FONs (Ref. 1.1) were published providing flight crew guidance to identify spoofing and provide work around procedures.

So far, cases have been reported in several different Flight Information Regions (FIR) in the Middle East, Eastern Europe, and Russia near the Baltic Sea.

- UM688 airway, approximately 100-120 nm from SISIN waypoint
- Bagdad FIR, Iraq and Tehran FIR, Iran and their border
- Tbilisi, Georgia
- Yerevan, Armenia
- Baku FIR, Azerbaijan
- Istanbul and Ankara FIR, Turkey. Major part of Turkey and towered Black Sea
- Sofia FIR, Bulgaria
- Bucarest South FIR, Romania
- Nicosia and Larnaka FIR, Cyprus
- Cairo FIR, Egypt and Red Sea
- Tel Aviv FIR, Israel
- Beirut, Libanon
- Tripoli, Libya
- Amman FIR, Jordan
- Kuwait FIR
- Helsinki, Finland
- Kaliningrad, Russia near Baltic sea
- Riga, Latvia
- Vilnius, Lithuania
- Warsaw, Poland

Note that this list is not exhaustive and other FIRs regions may also be affected by similar activity.

The behavior of the GNSS when the aircraft is out of the spoofing area, will depend on the specific type of spoofing attack that the GNSS is exposed. In general, there are three (3) scenarios that can occur when the aircraft is out of the spoofing region.

1. GNSS goes back to normal operation by itself without any reset.
2. GNSS requires a power cycle post flight with clear view sky of satellites constellation to return to normal operation.
3. GNSS is inoperative with a software lock condition, remaining in acquisition mode or showing wrong date. For this scenario, the following options can be initiated, to recover normal operation:
 - a) Open the affected GNSS circuit breaker(s), including any clock power back up like on Global 7500.
 - b) Perform manual entry of correct date and time to the avionics suite.
 - c) Power up the GNSS, ensuring clear view sky of satellites constellation.
 - d) If still inoperative, for Collins Aerospace, GPS-4000S Part Number (PN) 822-2189-101 or later only, perform a field reset in accordance with the SIL (Ref. 1.4).

Note: For PN 822-2189-101 the SIL (Ref. 1.4) was design to fabricate a full breakout panel cable assembly. However, the breakout panel cable may be simplified: the ARINC 600 rack, BNC connectors and the ARINC 429 transmitter/receiver could be ignored. It is possible to manufacture a simpler harness with jumpers (Middle plug MP-7D, 4D and 7C) and supply power to the GNSS via the aircraft connector (MP-15A and ground MP-15C) or a 28V power supply per SIL (Ref. 1.4) Figure 1, sheet 2.

- e) If all the above failed, the affected GNSS will require replacement to perform a software reset at the supplier repair facility to return to normal operation.

The scenario 3, where the GNSS software lock condition would require a software reset, can only be avoided if the GNSS is deselected and powered off prior to entering an area with a particular spoofing type that would generate such GNSS fault condition.

Based on recent reports regarding spoofing attacks, most of the time the GNSS returns to normal operation once the aircraft exited the spoofing area. Only in few cases so far, the Collins Aerospace GNSS required a software reset. And for aircraft equipped Honeywell GNSS, no case of software lock condition was reported so far.

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 Certificate (STC). Operators should be familiar with their GNSS installation and interface with the FMS for navigation, where these may potentially be affected by spoofing as well.

4. ACTION:

Maintenance personnel and dispatcher should be aware of the information and guidance in this AW and familiar with the published FONs (Ref. 1.1).

No corrective action at this time would prevent GNSS spoofing since this condition is confirmed to be related to external sources. The associated aircraft systems are responding per design.

To support our operators who have experienced recent spoofing events in locations other than those specified or with FDE not reported in the FONs (Ref. 1.1), Bombardier would appreciate feedback. After the flight, these FONs indicates that flight crew should report to maintenance and the recorded observations and pictures can be provided your Bombardier local Field Service Representative (FSR)/Customer Response Center (CRC).

If the condition experienced is in accordance with the FONs (Ref. 1.1), feedback is optional.

As reminder, operator should also be familiar on previous FONs AVNC-005 for Challenger series and AVNC-030 for Global series; GNSS Outage due to Signal Degradation or Jamming with Associated FDE.

Should you have any query pertaining to this AW or require additional information, please contact your FSR or the CRC.