International Civil Aviation Organization
North American, Central American and Caribbean Office

INFORMATION PAPER

NACC/WG/09 — IP/04
17/09/24

Ninth North American, Central American and Caribbean Working Group Meeting (NACC/WG/09)
Mexico City, Mexico, 30 September to 04 October 2024

Agenda Item 4: Follow-up to the NACC/WG 2023-2024 work plan

MITIGATING GNSS JAMMING AND SPOOFING: ENHANCING AVIATION SAFETY AND RESILIENCE

(Presented by United States)

EXECUTIVE SUMMARY

This paper provides an analysis of Global navigation satellite system (GNSS) Radio Frequency Interference events (GNSS jamming and spoofing), which are significant threats to aviation safety and efficiency. The paper outlines observed symptoms, impacts on aircraft systems, and necessary mitigation and contingency measures. It emphasizes the importance of detection and reporting mechanisms, international observations, and collaborative decision-making processes to ensure aviation safety.

Strategic Objectives:	• Safety • Air Navigation Capacity and Efficiency
References:	• FAA SAFO 24002, *Recognizing and Mitigating Global Positioning System (GPS) / Global Navigation Satellite System (GNSS) Disruptions* • EASA SIB 2022-02R3, *Global Navigation Satellite System Outage and Alterations Leading to Communication / Navigation / Surveillance Degradation* • ICAO Doc 9849, GNSS Manual • OpsGroup GPS Spoofing Work Group Material • NAT TIG/17 and 18 Working and Information Papers

1. Introduction

1.1 The Global Navigation Satellite System (GNSS), made up of four main constellations in orbit--Global Positioning System (GPS), Galileo, GLONASS, and BeiDou, plays a critical role in modern aviation, providing essential services for position, navigation, and timing. However, the increasing prevalence of GNSS jamming and spoofing presents significant challenges to the safety and efficiency of air travel. These intentional interferences, whether through jamming or spoofing, can lead to severe operational disruptions, compromised system integrity, and increased risks for both flight crews and air traffic control (ATC) personnel.

1.2 This paper:

a) delves into the critical aspects of GNSS jamming and spoofing, exploring their definitions, effects, and the observed symptoms associated with these types of interference;
b) highlights the impact on aircraft systems, detailing the cascading failures that can occur from compromised GNSS receivers;
c) suggests mitigation and contingency measures that civil aviation authorities and air traffic management/air navigation service providers could implement to safeguard against these threats;
d) emphasizes the importance of detection and reporting mechanisms.

2. Discussion

Jamming and Spoofing

2.1 Jamming and spoofing are two distinct types of interference that disrupt Global Navigation Satellite System (GNSS) signals, but they differ significantly in their methods and impacts on aviation.

Jamming

2.2 Jamming involves the intentional broadcasting of radio frequency interference that overwhelms GNSS signals, preventing receivers from locking onto the satellites. This results in an immediate and noticeable loss of GNSS functionality, rendering the system ineffective or degraded for users in the affected area.

2.3 The FAA Aeronautical Information Manual Pilot/Controller Glossary defines jamming as: Emissions that do not mimic Global Navigation Satellite System (GNSS) signals (e.g., GPS and WAAS), but rather interfere with the civil receiver's ability to acquire and track GNSS signals. Jamming can result in denial of GNSS navigation, positioning, timing, and aircraft dependent functions.

2.4 When aircraft encounter jamming, the GNSS signal will be considered lost or invalid.

2.5 One of the many impacts of jamming can be the loss of GNSS-based navigation and timing services, which can compromise aircraft navigation and degrade overall situational awareness.

2.6 Flight crews typically become aware of jamming quickly because the systems fail to receive GNSS signals, leading to obvious operational disruptions.

Spoofing

2.7 Spoofing involves the broadcasting of counterfeit satellite signals designed to deceive GNSS receivers into computing incorrect position, navigation, and timing (PNT) data.

2.8 The FAA Aeronautical Information Manual Pilot/Controller Glossary defines spoofing as: Denotes emissions of GNSS–like signals that may be acquired and tracked in combination with or instead of the intended signals by civil receivers. The onset of spoofing effects can be instantaneous or delayed, and effects can persist after the spoofing has ended. Spoofing can result in false and potentially confusing, or hazardously misleading, position, navigation, and/or date/time information in addition to loss of GNSS use.

2.9 The effects of spoofing can be subtle and may not be immediately apparent to the flight crew, posing a higher safety risk.

2.10 It is important to note that these attacks are getting very sophisticated; they are jamming first, and then spoofing, destroying the so-called "warm data" in the GNSS receiver, so the system is unable to detect an illogical jump in position or time.

2.11 When aircraft encounter spoofing, the GNSS signal may be erroneous but will continue to look valid to the receivers. Therefore, bad data may be used by downstream systems without it being obvious to the flight crew.

2.12 Spoofing can lead to incoherent navigation position, abnormal differences between ground speed and true airspeed, and erroneous time and date displays. These false signals can cause various onboard systems to malfunction, resulting in misleading or corrupted data, which can compromise flight safety and require manual circuit resets (literally like the way you used to pull or change fuses in your car) which by regulation, can only be accomplished after landing. This creates the condition where the compromised avionics cannot be recovered in flight.

2.13 The deceptive nature of spoofing makes it a more challenging threat to address, necessitating sophisticated detection and response strategies to maintain the integrity of GNSS-dependent operations.

Mitigations and Contingency Measures

2.14 All aviation stakeholders, including Civil Aviation Authorities (CAA), Air Traffic Service Providers (ATSP), Airline Operators, Pilots, and Operational Aviation Equipment Manufacturers (OEM) need to work together to create mitigation and contingency procedures to effectively handle GNSS interference.

2.15 This work should be done internally by the States and should also include regional agreements and practices.

2.16 It is vital that neighbouring FIRs in a region develop agreements that support regional sharing of information on jamming and spoofing events in near real-time as much as practical. The information should include, at a minimum:

a) The time and location of the interference, if known;
b) The type of interference, if known; and,
c) Flight information on any aircraft that could have been affected by the interference event.

Operational Equipment Manufacturer (OEM)

2.17 Operational Equipment Manufacturers (OEMs) recognize the serious nature GNSS interference and its impact on safety of flight.

2.18 Information Paper (IP/10), presented by Boeing to the ICAO North Atlantic Technology and Interoperability Group (NAT TIG) meeting (Washington D.C., USA, 10 – 13 September 2024), provides information on known impacts of GNSS interference on Boeing aircraft. (complete information paper included as an **Appendix**).

2.19 GNSS interference events have been reported on all Boeing models. Being impacted by such an event is not always immediately apparent to flight crews. Known Flight Deck Effects (FDEs) can be used as signs of being exposed to GNSS interference, however these may not occur consistently. Some potential FDEs which crews may encounter during GNSS interference events can include (but are not limited to):

a) Incoherence in navigation position, such as GNSS/Flight Management Function (FMF) position disagree warnings.
b) Loss of SATCOM (if installed) may also occur for all models except the 737
c) Time/Date shift
d) Spurious EGPWS alerts
e) Loss of ADS-B or erroneous position data in ADS-B

2.20 Operators may be able to de-select GNSS input to the FMS prior to entering known areas of GNSS interference and re-enable when leaving. However, there is currently no ability to isolate the GNSS receiver from other aircraft systems (e.g., EGPWS, clock).

2.21 Aircraft avionics may recover after exiting the area of GNSS interference, however it is not guaranteed, as reports of recovery and non-recovery have both been received. The likelihood of recovery will vary based on the specific avionics installed as the same aircraft model may support multiple GNSS receiver configurations for installation.

2.22 Boeing is currently working with suppliers on avionics improvements which can make them more resilient to GNSS interference events as well as improving recovering procedures, and holds operator calls on a monthly basis to discuss the latest development in GNSS interference issues.

Civil Aviation Authorities (CAA)

2.23 As an integral part of mitigating and preventing GNSS interference, CAAs are encouraged to work collaboratively with their stakeholders to:

a) Establish contingency procedures with ATM/ANSPs.
b) Ensure non-GNSS navigation infrastructure (e.g., ILS, DME, VOR) is operational.
c) Issue NOTAMs to describe affected areas and limitations.
d) Develop policy to address the response and handling for aircraft impacted abroad who go on to transit the airspace under their jurisdiction.

Air Traffic Management/Air Navigation Services Provider (ATM/ANSP)

2.24 ATM and ANSPs, along with their respective CAAs should work collaboratively among themselves and along with their stakeholders, neighbouring FIRs, and region(s) to:

a) Collect and share information on GNSS degradations.
b) Assess impact on CNS systems and ensure resilient surveillance coverage.
c) Provide appropriate contingency procedures for GNSS interference.

Detection and Reporting

2.25 Timely detection and reporting of GNSS interference events is crucial to ensure successful mitigation efforts. An easily accessible reporting platform should be maintained by the CAA and/or the ANSP to facilitate event reporting, integration with reports provided by other CAAs and/or ANSPs. EXAMPLE: the FAA's Report a GPS Anomaly website.

2.26 States should be encouraged to develop their own reporting methods and capabilities and then, further, work with other States in their region(s) to create and maintain a space where the reports, along with other information, are easily accessible.

Flight Crew and Air Traffic Control (ATC) Facility Concerns

2.27 Flight crews have stressed, among other things, concerns about losing trust in aircraft systems due to spoofing and the importance of clear guidance and information on handling GNSS disruptions.

2.28 ATC facilities expressed the need for a clear path to collaborative decision-making for resuming operations post-GNSS interference events as well as their roles in describing affected areas, aircraft types impacted, and signs of spoofing.

3. Conclusion

3.1 The growing prevalence of GNSS jamming and spoofing represents a significant threat to aviation safety and operational efficiency. The immediate and noticeable effects of jamming, contrasted with the insidious and hard-to-detect nature of spoofing, underscore the need for comprehensive and proactive mitigation strategies.

3.2 In conclusion, the increasing frequency and sophistication of GNSS interferences call for a concerted effort to ensure the continued safety and reliability of air travel. By adopting comprehensive response strategies and fostering collaborative decision-making processes, aviation stakeholders can effectively address these emerging threats and safeguard the integrity of GNSS-dependent operations. This paper serves as a resource for aviation stakeholders, offering insights and recommendations to navigate the challenges posed by GNSS jamming and spoofing, thereby enhancing the overall safety and resilience of the global aviation system.

— — — — — — — — — — — —

NAT TIG/18 – IP/10
29/08/2024

European and North Atlantic Office

NORTH ATLANTIC TECHNOLOGY AND INTEROPERABILITY GROUP

(NAT TIG)

EIGHTEENTH MEETING

(Washington DC, USA, 10-13 September 2024)

Agenda Item 2: Data Link performance monitoring and analysis, including trials and operations. Reports by States, industry and DLMA

d) Other issues

GNSS INTERFERENCE IMPACT ON BOEING AIRCRAFT

(Presented by Boeing)

SUMMARY

This Information Paper provides input on known impacts of GNSS RFI on Boeing aircraft.

1. Introduction

1.1 There has been an increase in reported Global Navigation Satellite System (GNSS) interference events affecting commercial aircraft. Such events have a direct impact on multiple aircraft functions including datalink. As datalink is utilized for both communication and surveillance in reduced separation areas, there is growing concern around the risk incurred by degraded avionic functions when exposed to such events.

2. Discussion

Background

2.1 GNSS Radio Frequency Interference (RFI) events can occur due to jamming or spoofing of GPS signals. In incidents of jamming, the GPS frequency band can be manipulated to prevent receivers from decoding GPS signals. In spoofing incidents, GPS-like signals can be made to look valid and consistent but with erroneous information.

2.2 When an aircraft encounters jamming, the GPS signal will be considered lost or invalid. In these instances, the aircraft will revert to using normal backup systems as available and provide any associated indications to the flight crew. When an aircraft encounters spoofing, the GPS signal may be erroneous but will continue to look valid to the receivers. Therefore, that data may be used by downstream systems without it being obvious to the flight crew.

Detection

2.3 GNSS RFI events have been reported on all Boeing models. Being impacted by such an event is not always immediately apparent to flight crews. Known Flight Deck Effects (FDEs) can be used as signs of being exposed to RFI, however these may not occur consistently. Some potential FDEs which crews may encounter during RFI events can include (but are not limited to):

- Incoherence in navigation position, such as GNSS/Flight Management Function (FMF) position disagree warnings.

- Loss of SATCOM (if installed) may also occur for all models except the 737

- Time/Date shift

- Spurious EGPWS alerts

- Loss of ADS-B or erroneous position data in ADS-B

2.4 The FDEs encountered will vary based on the aircraft model, avionics configuration and the type of interference experienced. For the most up to date known FDEs due to GNSS RFI on Boeing aircraft, operators should refer to their applicable Fleet Operations Technical Bulletin (FOTB) and Flight Crew Operating Manual (FCOM).

Major Model	Most Recent Published FOTB	Released Month	FTD Maintenance Document
737*	737 23-01R1 737-24-01 (hybrid)	Dec 2023 Mar 2024	737NG-FTD-34-23002 737MAX-FTD-34-23001 MT 34-064
747	747 23-80	Dec 2023	737NG-FTD-34-23002 737MAX-FTD-34-23001 MT 34-064
757	757-23-99	Dec 2023	757-FTD-34-23001
767	767-23-102	Dec 2023	767-FTD-34-23002 MT 34-080
777	777-62	Dec 2023	777- FTD-34-23002 MT 34-051R1
787	787-27	Nov 2023	787-FTD-34-23001

Table 1: FOTB and FTD numbers per model.

Datalink Impact

2.5 GNSS RFI can impact datalink operations, primarily due to potential for erroneous time/date, position and loss of navigational accuracy.

2.6 In the ATN environment this may result in inability to logon to an ATC center as well as inability to exchange messages due to the ground system and aircraft date/time being out of sync.

2.7 In the FANS-1/A+ environment, logon and use of CPDLC and ADS-C will continue to work. However, the 4D position exchanged with the ground may be erroneous. On Boeing aircraft, there is currently no method to manually select a different source for time. If GPS signal is valid (although erroneous), the FMF will continue to include it in downlinks. In the event of an erroneous GPS position, the FMF will detect such jumps and revert to using another source for position such as radio updating. Manual and automatic reversion to alternate navigation modes will be reflected in the value of FOM

2.8 Inaccurate position may also impact SATCOM availability as certain SATCOM avionics use position for antenna steering. This may result in loss of SATCOM for all or part of the NAT crossing.

Recovery

2.9 Operators, per their discretion and after conducting a risk assessment can choose to disable GPS updating when entering known areas of RFI and re-enable when leaving. Further considerations of when to do such procedures and potential risks to address are detailed in the applicable Flight Operations Technical Bulletin (FOTB), which operators can obtain from Boeing.

2.10 Aircraft avionics may recover after exiting the area of RFI, however it is not guaranteed as reports of recovery and non recovery have both been received. The likelihood of recovery will vary based on the specific avionics installed as the same aircraft model may support multiple GPS receiver configurations for installation. Therefore operators should contact Boeing to understand the impacts specific to each of their installed configurations.

2.11 Boeing has provided on-ground maintenance actions to perform after experiencing RFI events. These are available for all operators in their associated maintenance document.

Next Steps

2.12 Boeing is currently working with suppliers on avionics improvements which can make them more resilient to RFI events as well as improving recovering procedures. The availability of these updated avionics will vary by model and operators should contact Boeing for latest updates.

2.13 Boeing holds operator calls on a monthly basis to discuss the latest development in RFI issues. Additionally Boeing encourages operators to submit service requests to Boeing to ensure that any new RFI symptoms are properly captures and evaluated.

3. Action by the Meeting

3.1 The NAT TIG is invited to note the information provided.

— END —