Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

NOTA DE INFORMACIÓN

NACC/WG/09 — NI/04
17/09/24

Novena Reunión del Grupo de Trabajo de Norteamérica, Centroamérica y Caribe (NACC/WG/09)
Ciudad de México, México, 30 de septiembre al 04 de octubre de 2024

Cuestión 4 del Orden del Día: **Seguimiento al plan de trabajo 2023-2024 del NACC/WG**

MITIGACIÓN DEL JAMMING Y SPOOFING DE GNSS: MEJORANDO LA SEGURIDAD Y RESILIENCIA EN LA AVIACIÓN

(Presentado por los Estados Unidos)

RESUMEN EJECUTIVO	
Este documento proporciona un análisis de los eventos de interferencia de radiofrecuencia del Sistema mundial de navegación por satélite (GNSS) (interferencias y suplantación de identidad de GNSS), los cuales son amenazas significativas para la seguridad y eficiencia de la aviación. El documento describe los síntomas observados, los impactos en los sistemas de las aeronaves y las medidas de mitigación y contingencia necesarias. Se enfatiza la importancia de los mecanismos de detección y reporte, observaciones internacionales, y procesos de toma de decisiones colaborativos para garantizar la seguridad operacional.	
Objetivos Estratégicos:	• Seguridad Operacional • Capacidad y eficiencia de la navegación aérea
Referencias:	• FAA SAFO 24002, *Reconocimiento y mitigación de interrupciones del sistema de posicionamiento global (GPS)/sistema mundial de navegación por satélite (GNSS)* • EASA SIB 2022-02R3, *Interrupciones y alteraciones del sistema global de navegación por satélite que provocan degradación de las comunicaciones, la navegación y la vigilancia* • ICAO Doc 9849, Manual del GNSS • Material del grupo de trabajo sobre suplantación de GPS de OpsGroup • Documentos de trabajo e información NAT TIG/17 y 18

1. Introducción

1.1 El Sistema Mundial de Navegación por Satélite (GNSS), compuesto por cuatro constelaciones principales en órbita: Sistema de Posicionamiento Global (GPS), Galileo, GLONASS y BeiDou, juega un papel crítico en la aviación moderna, proporcionando servicios esenciales de posicionamiento, navegación y sincronización. Sin embargo, la creciente prevalencia de interferencias y suplantación de identidad (jamming y spoofing) de GNSS presenta desafíos significativos para la seguridad y eficiencia del transporte aéreo. Estas interferencias intencionales, ya sea mediante jamming o spoofing,

pueden provocar graves interrupciones operativas, comprometer la integridad del sistema y aumentar los riesgos tanto para las tripulaciones de vuelo como para el personal de control de tránsito aéreo (ATC).

1.2 Este documento:

a) Profundiza en los aspectos críticos del jamming y spoofing de GNSS, explorando sus definiciones, efectos y los síntomas observados asociados con estos tipos de interferencia;
b) Resalta el impacto en los sistemas de las aeronaves, detallando las fallas en cascada que pueden ocurrir por receptores de GNSS comprometidos;
c) Sugiere medidas de mitigación y contingencia que las autoridades de aviación civil y los proveedores de servicios de gestión del tráfico aéreo/navegación aérea podrían implementar para protegerse contra estas amenazas;
d) Enfatiza la importancia de los mecanismos de detección y reporte.

2. Discusión

Jamming y Spoofing

2.1 El jamming y el spoofing son dos tipos distintos de interferencia que interrumpen las señales del Sistema Global de Navegación por Satélite (GNSS), pero difieren significativamente en sus métodos e impactos en la aviación.

Jamming

2.2 El jamming implica la transmisión intencional de interferencia de radiofrecuencia que sobrecarga las señales de GNSS, impidiendo que los receptores se conecten a los satélites. Esto resulta en una pérdida inmediata y notable de la funcionalidad de GNSS, volviendo el sistema ineficaz o degradado para los usuarios en el área afectada.

2.3 El Glosario de Piloto/Controlador del Manual de Información Aeronáutica de la FAA define el jamming como: emisiones que no imitan las señales del Sistema Global de Navegación por Satélite (GNSS) (ej. GPS y WAAS), sino que interfieren con la capacidad del receptor civil para adquirir y rastrear señales de GNSS. El jamming puede resultar en la negación de la navegación GNSS, posicionamiento, sincronización y funciones dependientes de la aeronave.

2.4 Cuando las aeronaves encuentran jamming, la señal de GNSS se considera perdida o inválida.

2.5 Uno de los muchos impactos del jamming puede ser la pérdida de servicios de navegación y sincronización basados en GNSS, lo que puede comprometer la navegación de la aeronave y degradar la conciencia situacional general.

2.6 Las tripulaciones de vuelo en general se dan cuenta rápidamente del jamming porque los sistemas dejan de recibir señales de GNSS, lo que conduce a interrupciones operativas evidentes.

Spoofing

2.7 El spoofing implica la transmisión de señales satelitales falsas diseñadas para engañar a los receptores GNSS haciéndolos calcular datos incorrectos de posición, navegación y sincronización (PNT).
2.8 El Glosario de Piloto/Controlador del Manual de Información Aeronáutica de la FAA define el spoofing como: emisiones de señales similares a GNSS que pueden ser adquiridas y rastreadas en combinación con o en lugar de las señales deseadas por los receptores civiles. Los efectos del spoofing pueden ser instantáneos o retardados, y los efectos pueden persistir después de que el spoofing haya terminado. El spoofing puede resultar en información falsa y potencialmente confusa, o peligrosamente engañosa, de posición, navegación, y/o fecha/hora, además de la pérdida del uso de GNSS.

2.9 Los efectos del spoofing pueden ser sutiles y no ser inmediatamente aparentes para la tripulación, lo que representa un mayor riesgo para la seguridad.

2.10 Es importante señalar que estos ataques están volviéndose muy sofisticados; primero realizan jamming y luego spoofing, destruyendo los llamados “datos cálidos” en el receptor GNSS, lo que hace que el sistema sea incapaz de detectar un salto ilógico en posición o tiempo.

2.11 Cuando las aeronaves encuentran spoofing, la señal GNSS puede ser errónea, pero seguirá pareciendo válida para los receptores. Por lo tanto, los datos incorrectos pueden ser utilizados por los sistemas descendentes sin que sea obvio para la tripulación.

2.12 El spoofing puede llevar a posiciones de navegación incoherentes, diferencias anormales entre la velocidad en tierra y la velocidad aérea verdadera, y pantallas de tiempo y fecha erróneas. Estas señales falsas pueden causar que varios sistemas a bordo funcionen mal, lo que resulta en datos engañosos o corruptos, que pueden comprometer la seguridad del vuelo y requerir reinicios manuales de los circuitos (literalmente como cuando solías cambiar fusibles en tu coche) que, según regulación, solo se pueden realizar después de aterrizar. Esto crea la condición en la que los sistemas aviónicos comprometidos no pueden ser recuperados en vuelo.

2.13 La naturaleza engañosa del spoofing lo convierte en una amenaza más desafiante de abordar, lo que requiere estrategias de detección y respuesta sofisticadas para mantener la integridad de las operaciones dependientes de GNSS.

Mitigaciones y Medidas de Contingencia

2.14 Todos los actores de la aviación, incluidas las Autoridades de Aviación Civil (CAA), los Proveedores de Servicios de Tráfico Aéreo (ATSP), los Operadores Aéreos, los Pilotos y los Fabricantes de Equipos Operacionales (OEM) necesitan trabajar juntos para crear procedimientos de mitigación y contingencia para manejar eficazmente la interferencia de GNSS.

2.15 Este trabajo no solo debe realizarse internamente por los Estados, sino que también debe incluir acuerdos y prácticas regionales.

2.16 Es vital que las FIR vecinas en una región desarrollen acuerdos que apoyen el intercambio regional de información sobre eventos de jamming y spoofing en tiempo casi real en la medida de lo posible. La información debe incluir, como mínimo:

a) La hora y ubicación de la interferencia, si se conoce;
b) El tipo de interferencia, si se conoce; y
c) Información de vuelo de cualquier aeronave que podría haber sido afectada por el evento de interferencia.

Fabricante de Equipos Operacionales (OEM)

2.17 Los Fabricantes de Equipos Operacionales (OEM) reconocen la seria naturaleza de la interferencia GNSS y su impacto en la seguridad del vuelo.

2.18 La Nota de información (NI/10), presentada por Boeing en la reunión del Grupo de Tecnología e Interoperabilidad del Atlántico Norte de la OACI (NAT TIG) (Washington D.C., EE. UU., 10-13 de septiembre de 2024), proporciona información sobre los impactos conocidos de la interferencia de GNSS en las aeronaves Boeing. (se incluye el documento de información completo como un **Apéndice**, únicamente en inglés).

2.19 Se han reportado eventos de interferencia de GNSS en todos los modelos de Boeing. El ser afectado por tal evento no siempre es inmediatamente aparente para las tripulaciones. Los Efectos Conocidos en la Cabina de Vuelo (FDE) pueden ser utilizados como señales de exposición a interferencia GNSS, aunque estos no ocurren de manera consistente. Algunos posibles FDE que las tripulaciones pueden encontrar durante eventos de interferencia GNSS incluyen (pero no se limitan a):

a) Incoherencia en la posición de navegación, como advertencias de desacuerdo en la posición GNSS/Función de Gestión de Vuelo (FMF).
b) Pérdida de SATCOM (si está instalado) también puede ocurrir para todos los modelos excepto el 737
c) Desplazamiento de tiempo/fecha
d) Alertas espurias del EGPWS
e) Pérdida de ADS-B o datos de posición erróneos en ADS-B

2.20 Los operadores pueden desactivar la entrada de GNSS en el FMS antes de ingresar a áreas conocidas de interferencia GNSS y volver a activarla al salir. Sin embargo, actualmente no hay forma de aislar el receptor GNSS de otros sistemas de la aeronave (ej. EGPWS, reloj).

2.21 Los sistemas aviónicos de las aeronaves pueden recuperarse después de salir del área de interferencia GNSS, sin embargo, no está garantizado, ya que se han recibido informes tanto de recuperación como de no recuperación. La probabilidad de recuperación variará según los aviónicos específicos instalados, ya que el mismo modelo de aeronave puede admitir múltiples configuraciones de receptores GNSS para la instalación.

2.22 Boeing está trabajando actualmente con proveedores en mejoras de aviónica que pueden hacer que sean más resistentes a los eventos de interferencia GNSS, así como mejorar los procedimientos de recuperación, y realiza llamadas mensuales con los operadores para discutir los últimos desarrollos en los problemas de interferencia GNSS.

Autoridades de Aviación Civil (CAA)

2.23 Como parte integral de la mitigación y prevención de la interferencia GNSS, se anima a las CAA a trabajar en colaboración con sus partes interesadas para:

a) Establecer procedimientos de contingencia con ATM/ANSP.
b) Asegurarse de que la infraestructura de navegación no GNSS (ej. ILS, DME, VOR) esté operativa.
c) Emitir NOTAMs para describir las áreas afectadas y las limitaciones.
d) Desarrollar políticas para abordar la respuesta y el manejo de aeronaves afectadas en el extranjero que luego transiten el espacio aéreo bajo su jurisdicción.

Gestión del Tránsito Aéreo/Proveedores de Servicios de Navegación Aérea (ATM/ANSP)

2.24 Los ATM y ANSP, junto con sus respectivas CAA, deben trabajar en colaboración entre ellos y junto con sus partes interesadas, FIR vecinas y la(s) región(es) para:

a) Recopilar y compartir información sobre las degradaciones de GNSS.
b) Evaluar el impacto en los sistemas CNS y garantizar una cobertura de vigilancia resiliente.
c) Proporcionar procedimientos de contingencia adecuados para la interferencia GNSS.

Detección y Reporte

2.25 La detección y reporte oportunos de eventos de interferencia de GNSS es crucial para asegurar esfuerzos exitosos de mitigación. Una plataforma de reporte de fácil acceso debe ser mantenida por la CAA y/o el ANSP para facilitar el reporte de eventos, la integración con reportes proporcionados por otras CAAs y/o ANSPs. **EJEMPLO**: el sitio web de la FAA para Reportar una Anomalía de GPS.

2.26 Se debe alentar a los Estados a desarrollar sus propios métodos y capacidades de reporte y luego, además, trabajar con otros Estados en su(s) región(es) para crear y mantener un espacio donde los reportes, junto con otra información, sean fácilmente accesibles.

Preocupaciones de la Tripulación de Vuelo y las Instalaciones de Control de Tránsito Aéreo (ATC)

2.27 Las tripulaciones de vuelo han manifestado, entre otras cosas, preocupaciones sobre la pérdida de confianza en los sistemas de las aeronaves debido al spoofing y la importancia de una orientación clara e información sobre cómo manejar las disrupciones de GNSS.

2.28 Las instalaciones de ATC expresaron la necesidad de un camino claro hacia la toma de decisiones colaborativa para reanudar las operaciones después de los eventos de interferencia de GNSS, así como sus roles en la descripción de las áreas afectadas, los tipos de aeronaves impactadas y las señales de spoofing.

3. Conclusión

3.1 La creciente prevalencia del jamming y spoofing de GNSS representa una amenaza significativa para la seguridad y la eficiencia operativa de la aviación. Los efectos inmediatos y notables del jamming, contrastados con la naturaleza insidiosa y difícil de detectar del spoofing, subrayan la necesidad de estrategias de mitigación proactivas y completas.

3.2 En conclusión, la creciente frecuencia y sofisticación de las interferencias de GNSS requieren un esfuerzo concertado para garantizar la seguridad y confiabilidad continuas del transporte aéreo. Adoptando estrategias de respuesta integrales y fomentando procesos de toma de decisiones colaborativos, los actores de la aviación pueden abordar efectivamente estas amenazas emergentes y salvaguardar la integridad de las operaciones dependientes de GNSS. Este documento sirve como un recurso para los actores de la aviación, ofreciendo perspectivas y recomendaciones para navegar los desafíos planteados por el jamming y spoofing de GNSS, mejorando así la seguridad y la resiliencia general del sistema de aviación global.

— — — — — — — — — — —

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 —