



DECIMOCUARTA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, Canadá, 26 de agosto - 6 de septiembre de 2024

Cuestión 2: Utilización oportuna y segura de nuevas tecnologías

2.2: Riesgos de seguridad operacional relacionados con las tecnologías de aviación en evolución

MITIGACIÓN DE LAS VULNERABILIDADES DEL GNSS EN EUROPA – ACTIVIDADES Y EJEMPLOS

(Nota presentada por España)

RESUMEN

Esta nota de información sigue la línea del debate desarrollada en las notas de estudio “Planificación contra contingencias GNSS” y “Cuestiones de seguridad operacional y seguridad física en relación con las interferencias en el Sistema Global de Navegación por Satélite (GNSS)” (véase AN-Conf/14-WP/61 y AN-Conf/14-WP/63), y trata de dar una visión más amplia de las vulnerabilidades del GNSS, uno de los principales motivos que justifican la elaboración de ambas notas de estudio. Asimismo, esta nota de información incluye información sobre algunas de las medidas de mitigación que se están llevando a cabo a nivel europeo y en España.

Recientemente, se ha ido incrementando el uso del GNSS en todas las fases de los vuelos a nivel global, debido a que es el principal sensor de navegación que soporta el concepto de navegación basada en la performance (PBN). Además, los beneficios que aporta a la aviación hacen que el despliegue masivo de su uso resulte lógico. Sin embargo, como cualquier otro sistema, tiene vulnerabilidades inherentes que podrían llegar a afectar a la aviación y que es necesario minimizar y mitigar. En lo que respecta a estas vulnerabilidades, los actores de la aviación de todas partes del mundo trabajan para establecer barreras y acciones de mitigación que garanticen la seguridad operacional y la continuidad de las operaciones aéreas en caso de interrupciones y degradaciones del GNSS. A nivel europeo, diversas instituciones han abordado las contingencias GNSS, difundiendo recomendaciones y mejores prácticas para minimizar su impacto. Asimismo, a nivel nacional, hay varios Estados trabajando para definir los escenarios de contingencia y fomentar el despliegue de los sistemas necesarios para, por un lado, detectar la degradación del GNSS y poner en marcha los escenarios de contingencia sin problemas de seguridad operacional graves y, por otro lado, garantizar una continuidad razonable de las operaciones.

¹ Las versiones en español e inglés fueron proporcionadas por España.

1. INTRODUCCIÓN

1.1 Pese a que el GNSS lleva mucho tiempo siendo utilizado en todas las fases de vuelo y, en particular, en la fase de ruta, en la actualidad su uso está aumentando como principal método de navegación, siendo el mayor habilitador del concepto PBN, que representa el futuro de la navegación aérea. Además, las constelaciones principales de satélites del GNSS combinadas con sus sistemas de aumentación constituyen el único sensor compatible con todas las fases del vuelo, lo que lo convierte en un actor clave en el desarrollo de la aviación mundial.

1.2 Además, el uso del GNSS va más allá de proporcionar la posición de navegación para las aeronaves, ya que otros sistemas de comunicaciones, navegación y vigilancia (CNS) en tierra y a bordo lo emplean para proporcionar servicios de comunicación [comunicaciones por enlace de datos controlador-piloto (CPDLC)] y vigilancia [vigilancia dependiente automática – radiodifusión (ADS-B)] alternativos que suelen complementar el uso de los sistemas tradicionales.

1.3 Para la navegación, las constelaciones principales de satélites del GNSS, sus frecuencias y los sistemas de aumentación permitidos en aviación civil se especifican en el Anexo 10 — *Telecomunicaciones aeronáuticas*, Volumen I — *Radioayudas para la navegación* de la OACI. Las constelaciones principales de satélites del GNSS que se incluyen en las Normas y Métodos recomendados (SARPS) son Sistema de Posicionamiento Global (GPS) (L1, L5), Sistema orbital mundial de navegación por satélite (GLONASS) (L1, L3), Galileo (E1, E5) y Sistema de navegación por satélite BeiDou (BDS) (B1I, B1C, B2a). Los sistemas de aumentación enumerados en dicho documento son sistemas de aumentación basado en la aeronave (ABAS), sistema de intensificación basado en satélite (SBAS), sistema de aumentación basado en tierra (GBAS) y sistema regional de aumentación basado en tierra (GRAS) para cada una de las constelaciones principales. Aunque se enumeren todos estos elementos, debería ser responsabilidad de cada Estado aprobar el uso de cada sistema en el espacio aéreo bajo su responsabilidad.

1.4 Aunque exista la posibilidad de uso de estos sistemas en navegación aérea, sigue siendo necesario que todas las partes interesadas implicadas tengan el mismo nivel de madurez para su uso efectivo, acompañando, entre otros, al desarrollo de los sistemas GNSS, el equipamiento embarcado, la adaptación de los servicios de gestión del tránsito aéreo (ATM)/ servicios de tránsito aéreo (ATS) y la certificación de la tripulación.

1.5 Sin embargo, pese a los múltiples beneficios que el empleo del GNSS puede aportar a la comunidad aeronáutica, no está exento de algunos puntos débiles debido a la naturaleza de sus señales satelitales y de su uso tan generalizado, lo que lleva aparejados riesgos para los servicios CNS/ANS que no se encuentran en otras ayudas terrestres de posicionamiento/navegación cuyo único objetivo es proporcionar señales para los servicios de navegación aérea. De igual manera, el hecho de que sean señales globales implica que podría haber una causa de fallo común, y cualquier interrupción que se produzca en ellas podría afectar a una amplia zona del espacio aéreo.

1.6 Las señales GNSS recibidas en la Tierra son muy débiles debido a la larga distancia que debe recorrer la señal transmitida desde la órbita del satélite hasta la recepción. Esto hace que estas señales sean vulnerables y fácilmente interferibles por perturbaciones de radiofrecuencia (ya sean intencionadas o no), tanto en el entorno de recepción como durante el trayecto desde el satélite hasta el receptor. Esto podría provocar graves degradaciones en la recepción de las señales GNSS, incluida la pérdida completa de la solución de posición y tiempo. Las principales amenazas para el GNSS son la meteorología espacial (RFI), la Interferencia de Radiofrecuencia (RFI), los ciberataques y los fallos de constelación. De ellas, las dos primeras son las más probables, y ambas se desarrollan en este documento.

1.7 Por tanto, hoy en día, la comunidad aeronáutica está trabajando, por un lado, en establecer barreras para evitar los efectos de los riesgos asociados a las pérdidas y perturbaciones en las señales GNSS (por ejemplo, desarrollando sistemas de doble frecuencia y multiconstelación); y, por otro lado, en aplicar medidas de mitigación para minimizar el impacto que puedan tener en la comunidad aeronáutica (por ejemplo, desarrollando una planificación armonizada para contingencias GNSS, como se establece en la nota de estudio europea AN-Conf/14-WP/61, “Planificación contra contingencias GNSS”).

1.8 En este sentido, diversas instituciones europeas, entre ellas, la Comisión Europea, la Agencia de la Unión Europea de Seguridad Aérea (EASA) y Organización Europea para la Seguridad de la Navegación Aérea (EUROCONTROL), están abordando las contingencias GNSS.

2. MARCO REGULADOR EUROPEO

2.1 Desde el punto de vista normativo, el objetivo de un nivel alto de uniformidad de la seguridad operacional de la aviación civil en la Unión Europea y los principales requisitos para cumplir dicho objetivo se establecen en el Reglamento Base de EASA.

2.2 Por el momento, el principal Reglamento europeo que trata el impacto de las contingencias GNSS en la seguridad operacional de la aviación civil es el *Reglamento de Ejecución (UE) 2018/1048 de la Comisión de 18 de julio de 2018 por el que se establecen los requisitos de utilización del espacio aéreo y los procedimientos operativos en relación con la navegación basada en la performance (PBN)*. Las contingencias PBN se definen como las situaciones en las que, por razones imprevistas y ajenas a su control, el GNSS u otros métodos empleados para la navegación basada en la performance dejan de estar disponibles, lo que les impide prestar servicios de conformidad con los requisitos PBN establecidos en el Reglamento.

2.3 Dado que el GNSS es el principal sistema de navegación que soporta la PBN (en el caso de algunas aplicaciones, el único) una contingencia PBN equivale en la práctica a una contingencia GNSS centrada en la navegación aérea. En caso de producirse un evento de este tipo, los proveedores de servicios de navegación aérea (ANSP) deberán tomar medidas para la prestación continuada y segura de sus servicios por otros medios, por ejemplo, manteniendo una red de ayudas a la navegación convencionales, así como la infraestructura de vigilancia y comunicaciones asociada a las mismas. El *Anexo II de la Decisión de EASA 2018/013/R (Material orientativo para el Reglamento de Ejecución (UE) 2018/1048)* proporciona orientación complementaria respecto a las contingencias GNSS y el establecimiento de dichas infraestructuras.

2.4 Desde el punto de vista de los riesgos para la seguridad operacional, EASA define las carteras de seguridad operacional en el Volumen III del Plan europeo de seguridad operacional para la aviación (EPAS) 2024, que contiene diversos “Safety Issues” (SI), es decir, deficiencias en la seguridad relacionadas con uno o más riesgos. Cuando se identifica un SI y se recoge en una cartera, se somete a una evaluación técnica de seguridad operacional en la que se ofrecen posibles medidas de mitigación.

2.5 Existen varios Safety Issues relacionados con las contingencias GNSS:

2.5.1 Manipulación de la señal GNSS que conduce a la degradación de la navegación o la vigilancia (SI-5501A) aborda la perturbación o alteración de las señales GNSS cerca de zonas de conflicto. El contenido de sus respectivas medidas de mitigación, el Boletín de información de Seguridad Operacional (SIB) de EASA 2022-02R3 (*Interrupciones y alteraciones del sistema global de navegación por satélite que provocan una degradación de la navegación/vigilancia*) se desarrolla en las siguientes secciones.

2.5.2 Efectos de la Meteorología espacial en la aviación (SI-5102) reconoce el impacto de dichos eventos en el GNSS, concretamente en las prestaciones de GNSS sin aumentaciones en la región cercana al ecuador magnético. Al igual que en el anterior, el contenido de sus respectivas medidas de mitigación, los Boletines de EASA 2012-09R1 *Efectos de la meteorología espacial en la aviación* y 2012-10R1 *Efectos de un único evento en los sistemas de las aeronaves causados por la radiación atmosférica*, se desarrolla en las siguientes secciones.

2.6 Por último, las posiciones de alto nivel de EUROCONTROL respecto a las cuestiones derivadas de las interferencias del GNSS se han planteado a través del "Think Paper" de EUROCONTROL N° 9 (con fecha de 1 de marzo de 2021)². Presenta diversas recomendaciones para los legisladores con el fin de garantizar la fiabilidad del GNSS para la aviación y mantener la seguridad operacional al mayor nivel posible. Se describe la relevancia actual del GNSS para una navegación aérea eficiente, así como la tendencia creciente de la vulnerabilidad del GNSS, que reduce la seguridad operacional y la eficiencia operativa. Los eventos de interferencia de radiofrecuencia (RFI) en el GNSS requieren una mayor concienciación y más acciones a nivel estatal para asegurar que la aviación pueda seguir operando con seguridad.

3. PRINCIPALES VULNERABILIDADES DEL GNSS

3.1 Los principales tipos de perturbaciones terrestres que pueden afectar al funcionamiento habitual de los sistemas de navegación por satélite son la emisión de señales con la potencia suficiente para degradar o inhibir por completo la recepción del GNSS (jamming) y la sustitución de las señales reales del GNSS por otras falsas (spoofing). Estos fenómenos se pueden producir de forma intencionada o no intencionada.

3.2 Las perturbaciones debido a la meteorología espacial afectan a las señales a medida que atraviesan las diferentes capas atmosféricas de la Tierra. La principal causa de perturbación de las señales es la interacción con la ionosfera, cuyo comportamiento está directamente relacionado con la actividad solar.

3.3 El funcionamiento del GNSS generalmente se basa en las señales de navegación transmitidas desde los satélites de las constelaciones principales en órbita terrestre media (MEO). La potencia recibida de estas señales en la salida de la antena de un receptor de usuario suele ser extremadamente pequeña, de aproximadamente -165 a -150 decibel watt (dBW), lo que las hace intrínsecamente vulnerables a las interferencias de radiofrecuencia (RFI) causadas por las emisiones de otros sistemas de radio. Estas interferencias pueden ser no intencionadas, como por ejemplo por un mal funcionamiento o una emisión espuria de un transmisor en las proximidades del receptor GNSS, o intencionadas, es decir, por el uso deliberado de equipos de jamming y spoofing, ya sea de baja potencia radiada (por ejemplo, dispositivos de privacidad personal) o alta (por ejemplo, de uso militar).

3.4 Los ejemplos más habituales de este tipo de avisos de interferencia provienen de los dispositivos de privacidad personal, que son inhibidores GNSS de baja potencia empleados para bloquear de forma local el funcionamiento de los receptores GNSS. Aunque el uso de dispositivos de privacidad personal es ilegal, son fáciles de adquirir por Internet a un precio bajo (por ejemplo, en el orden de los 9 euros por un "jammer" de 100 milliwatts (mW) de potencia de transmisión, suficiente para degradar las prestaciones o interrumpir el funcionamiento de los receptores GNSS en un rango de 10-100 m o más). En la última década, los "spoofers" también se han puesto a la venta en Internet (por ejemplo, en el orden de los 93 euros por un equipo radioeléctrico definido por software que se puede emplear como suplantador).

² <https://www.eurocontrol.int/publication/eurocontrol-think-paper-9-radio-frequency-interference-satellite-navigation-active>

3.5 Los usuarios informan con más frecuencia de eventos de interferencia de radiofrecuencia (RFI) en el GNSS de gran alcance, debido a guerra electrónica (EW ‘Electronic Warfare’) o ‘medidas de seguridad, supuestamente realizadas por fuerzas militares o paramilitares de todo el mundo. Por tanto, la RFI puramente no intencionada se ha vuelto una amenaza menor para el GNSS en comparación con la RFI intencionada (tanto la colateral como la intencionalmente específica).

3.6 La RFI puede afectar tanto a las propias aeronaves como a las infraestructuras terrestres esenciales que emplean el GNSS para aumentar el rendimiento de la solución de posicionamiento (por ejemplo, Servicio europeo de complemento geoestacionario de navegación (EGNOS RIMS y GBAS) o para la sincronización de sistemas (por ejemplo, una estación de radar o cualquier otra infraestructura ATM/ANS terrestre que use la fuente de tiempo GNSS para la sincronización).

4. DEMANDAS DE LOS USUARIOS CONTRA LA DEGRADACIÓN DEL GNSS Y SU IMPACTO EN LA AVIACIÓN

4.1 Desde hace un tiempo, en la comunidad aeronáutica ha surgido una preocupación por el impacto de la degradación del GNSS. Se han puesto en marcha distintas iniciativas para alertar a la comunidad de esta problemática, detallando el impacto que tiene la degradación del GNSS en cada usuario y tratando de encontrar soluciones comunes y armonizadas.

4.2 Recientemente, a nivel europeo, se han llevado a cabo dos talleres con estos objetivos. El simposio en Europa y Oriente Medio (EUR/MID) de Radionavegación de la OACI que tuvo lugar en Antalya, Turquía, del 6 al 8 de febrero de 2024, y el taller de EASA-Asociación del Transporte Aéreo Internacional (IATA) sobre resiliencia en el posicionamiento, la navegación y la temporización (PNT) el 25 de enero de 2024 en Cologne, Alemania. En ambas reuniones, los usuarios lanzaron el mismo mensaje.

4.3 Desde el punto de vista de los operadores de aeronaves comerciales, se ha prestado cada vez más atención a la necesidad de desarrollar protocolos de notificación y coordinación entre los pilotos y el control terrestre para la gestión de estos eventos. Esto se considera necesario teniendo en cuenta los efectos recurrentes detectados a bordo debido a eventos GNSS, que pueden dejar a los pilotos sin ningún tipo de información de navegación, o crear falsas alertas de las redes de seguridad que, de no comprobarse con una referencia externa, no se pueden evaluar adecuadamente para actuar, lo que podría derivar en incidentes o accidentes.

4.4 Los pilotos de aeronaves comerciales también creen en la necesidad de proporcionar a las tripulaciones instrucciones detalladas de los fabricantes de los equipos sobre la forma adecuada de gestionar los sistemas durante los eventos GNSS, y en la conservación de suficientes medios CNS que no dependan del GNSS para garantizar la continuidad de los servicios. También están a favor de la colaboración para adquirir un conocimiento común de las vulnerabilidades del GNSS, tanto de su naturaleza como de las áreas a evitar que se ven afectadas recurrentemente.

4.5 En el caso de los ANSP, hay necesidad de un conocimiento detallado sobre cómo pueden afectar los eventos GNSS tanto al rendimiento de los usuarios como al rendimiento de su propia red de servicios. Es importante que el personal de los ANSP sepa claramente cómo proporcionar asistencia en base a lo que los usuarios necesiten y tomar todas las medidas preventivas que sean posibles. Dependiendo excesivamente del GNSS para los servicios CNS puede provocar fallos de causa común que pueden hacer que los escenarios sean incontrolables desde el punto de vista operativo, por lo que se deberían tomar las medidas adecuadas para evitar esta posibilidad. Al mismo tiempo, los agentes operativos deben ser más conscientes de la indisponibilidad y degradación del GNSS para gestionar las situaciones de contingencia de la manera más eficaz posible.

5. ACTIVIDADES EUROPEAS EN MATERIA DE CONTINGENCIAS GNSS

5.1 Como se ha mencionado anteriormente, EASA, como medida de mitigación frente al creciente número de RFI del GNSS que afectan a los usuarios del espacio aéreo cerca de zonas de conflicto, ha publicado y actualizado un Boletín de Información de Seguridad Operacional con dos objetivos principales. El primero es describir en qué consiste y cuál es el impacto de las interferencias de radiofrecuencia (RFI) en la aviación civil, enumerando las zonas más afectadas. El segundo es hacer algunas recomendaciones para aplicar medidas de mitigación a: autoridades de aviación civil, proveedores ATM/ANS, operadores aéreos y fabricantes de aeronaves y equipos. En el apéndice se detalla esta información.

5.2 Como iniciativa a nivel de red, el "Operational Excellence Programme" (OEP) de EUROCONTROL, gestionado por los grupos de trabajo Network Directors of Operations y Network Directors of Technology, y subordinado al Network Manager Board, pretende garantizar la coordinación para la aplicación de evoluciones operativas y técnicas, así como conceptos operativos y técnicos mejorados, que abarcan, entre otras áreas, la aplicación armonizada de nuevos conceptos operativos para abordar la estrategia de reversión GNSS y las evoluciones de la infraestructura y tecnologías CNS para mejorar la resiliencia.

5.3 Para cada una de las áreas en cuestión, el Plan de evolución operacional desarrolló líneas de trabajo específicas, en las que la gestión de red y las partes interesadas (ANSP, operadores de aeródromo, aerolíneas, etc.) debatieron y propusieron evoluciones operativas y técnicas, que se consideran beneficiosas para una mejora adicional de la red y del rendimiento local.

5.4 En estas líneas de trabajo se abordan, por un lado, la resiliencia de la red y los riesgos para la infraestructura, haciendo hincapié en la evaluación de las amenazas GNSS, identificando los diferentes tipos de amenazas, en relación con su naturaleza y el efecto típico que tienen en la aviación, para proporcionar a los usuarios herramientas para la evaluación de la seguridad operacional de los eventos. Aparte, se ha trabajado en el desarrollo de directrices para la coordinación entre los ámbitos civil y militar en relación con los ejercicios y pruebas de emisiones de interferencias.

5.5 Por otro lado, se aborda el desarrollo de una estrategia para la gestión segura y continuada del tráfico aéreo en caso de interrupción del GNSS. Esta "estrategia de reversión GNSS" tiene por objetivo ofrecer un enfoque armonizado que los usuarios puedan utilizar como marco de referencia para desarrollar sus estrategias.

5.6 Por último, durante los últimos años, se han desarrollado diversas herramientas y medios para los usuarios que carecen de recursos propios adecuados y que pueden resultar útiles para la evaluación de escenarios operativos, la monitorización de sistemas de navegación y la identificación y resolución de las amenazas GNSS.

5.7 A nivel europeo, varios Estados e instituciones ya están integrando sistemas de monitorización GNSS basados en diferentes tecnologías y tipos de información, como redes de receptores GNSS, datos ADS-B y análisis del espectro, entre otros, que supervisan tanto el correcto funcionamiento de los servicios GNSS utilizados en su espacio aéreo como las interferencias que puedan afectar a las fases más críticas de los vuelos que utilizan el sensor GNSS como medio principal de navegación.

5.8 Además de los eventos RFI sobrevenidos o no planificados, hay eventos planificados que muchos Estados realizan como parte de sus ejercicios militares de guerra electrónica o con otros usos para la seguridad nacional. Dichos ejercicios podrían afectar a la aviación civil, por lo que se debería considerar establecer una coordinación efectiva con el ANSP. En algunos casos, el impacto de la RFI podría afectar a más de un Estado, por lo que es necesaria una coordinación internacional. Para ello, se espera que la herramienta de coordinación GRIT de EUROCONTROL, actualmente en fase de desarrollo, resulte de gran utilidad.

6. ACTIVIDADES ESPAÑOLAS EN MATERIA DE CONTINGENCIA GNSS

6.1 La monitorización del GNSS en los escenarios en los que su dependencia ha aumentado considerablemente se vuelve casi esencial para activar los mecanismos necesarios para mantener la seguridad, eficiencia y continuidad de las operaciones de navegación aérea.

6.2 En lo que respecta a España, ENAIRE, el principal proveedor de servicios de navegación aérea y CNS, opera una red de receptores GNSS en los aeropuertos con maniobras de aproximación con performance de navegación requerida (RNP APCH), que evalúa las prestaciones del GNSS e informa acerca del comportamiento de estos sistemas (sistema RECNET), permitiendo llevar a cabo acciones mitigadoras en caso de degradación del servicio. Asimismo, en los escenarios de alta densidad, se están desplegando sistemas de detección y localización de interferencias (sistema DYLEMA), haciendo posible la ejecución de procedimientos de coordinación, por un lado, con los controladores de tránsito aéreo para informarles acerca de posibles interferencias en su entorno y aumentar así el conocimiento situacional de los controladores, y por otro, con los agentes de la agencia nacional a cargo del correcto uso del espectro radioeléctrico.

6.3 Como se ha mencionado previamente, ENAIRE está operando un sistema terrestre de detección y localización de RFI alrededor del aeropuerto de Madrid llamado DYLEMA. Consta de 10 estaciones de monitorización RFI y un centro de monitorización GNSS que está en funcionamiento en todo momento, 24 horas al día y 7 días a la semana. Desde este centro, ENAIRE informa de los eventos RFI a la Agencia nacional del espectro en España, en un acuerdo de colaboración entre ambas, y a los ATCO para aumentar su conocimiento de la situación. En caso de que algún piloto avise de un mal funcionamiento del GNSS a bordo, los controladores de tránsito aéreo podrían tomar medidas de mitigación de forma inmediata. La acción inmediata no se lleva a cabo solo con la información proporcionada por DYLEMA, ya que la mayoría de los eventos RFI no afectan a la aeronave, sino a la zona terrestre alrededor del dispositivo inhibidor o suplantador (dispositivos de baja potencia). En los próximos años se desplegarán sistemas similares de detección y localización de RFI en otros de las principales áreas de control terminal españoles (por ejemplo, el aeropuerto de Palma de Mallorca en 2024).

6.4 Como ejemplos de los resultados de ambos sistemas de monitorización GNSS, gracias al sistema RECNET, se han podido detectar las degradaciones de los servicios del sistema SBAS europeo, EGNOS, en las Islas Canarias, debido al pico solar. Esto ha permitido actuar en consecuencia. En lo que respecta a DYLEMA, se han detectado una media de 10 interferencias al mes desde el inicio de la operación, y se han activado los procesos de detección y localización, aunque sin que haya sido necesaria una coordinación con los ATCO.

7. CONCLUSIÓN

7.1 Los sistemas GNSS presentan innumerables ventajas que proporcionan a la comunidad aeronáutica un nivel cada vez mayor de seguridad operacional y eficiencia, al tiempo que intentan abordar los retos del futuro de las operaciones aéreas y llevarnos hacia la próxima generación de prestación de servicios ATM/ANS.

7.2 Sin embargo, como cualquier tipo de tecnología, presenta una serie de vulnerabilidades que se deben conocer y estudiar para poder minimizar su impacto en los usuarios del espacio aéreo.

7.3 Este documento pretende poner de manifiesto dichas vulnerabilidades y difundir entre la comunidad aeronáutica las medidas de mitigación que se están llevando a cabo en Europa en general, y en España en particular, para que se puedan establecer prácticas más armonizadas como referencia para todos los usuarios de otras partes del mundo.

7.4 Las siguientes son algunas de las mitigaciones definidas en las actividades que se han mencionado previamente:

- a) fomentar la aplicación de políticas que garanticen la definición de una estrategia nacional de contingencia GNSS, estableciendo los principios básicos relativos a la adopción de las medidas que se consideren necesarias y la disponibilidad de los medios para llevarlas a cabo;
- b) la planificación, de acuerdo con las políticas nacionales correspondientes, de la disposición de los medios CNS necesarios para mantener un nivel adecuado de operaciones durante los escenarios de contingencia GNSS, apoyando procedimientos instrumentales no dependientes del GNSS compatibles con el concepto nominal de espacio aéreo PBN y la asistencia directa del personal ATS en caso de necesidad;
- c) la coordinación directa con agentes operativos para definir procedimientos y protocolos de actuación específicos para abordar los escenarios operativos de contingencias GNSS, teniendo en cuenta la reversión a operaciones no dependientes del GNSS, la gestión de los desvíos del tráfico, la identificación y asistencia al tráfico afectado, etc.; y
- d) El despliegue y la operación de sistemas de monitorización GNSS basados en diversas tecnologías, para poder llevar a cabo las medidas de contingencia preestablecidas lo antes posible, garantizando el mayor nivel de seguridad en las operaciones de navegación aérea.

— — — — —

APÉNDICE

EASA SIB No.: 2022-02R3



Safety Information Bulletin Operations – ATM/ANS – Airworthiness

SIB No.: 2022-02R3

Issued: 05 July 2024

Subject: Global Navigation Satellite System Outage and Alterations
Leading to Communication / Navigation / Surveillance
Degradation

Revision:

This SIB revises EASA SIB 2022-02R2 dated 06 November 2023.

Applicability:

Competent Authorities (CA), Air Traffic Management/Air Navigation Service Providers (ATM/ANS providers), air operators, aircraft and equipment manufacturers, organisations involved in the design or production of ATM/ANS equipment.

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 geographical areas surrounding conflict zones, but it is also encountered in the south and eastern Mediterranean, Black Sea, Middle East, Baltic Sea, and Arctic area.

The list of affected flight information (FIR) regions is published on the EASA website at <https://www.easa.europa.eu/GNSS>.

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 jammed area.

Spoofing involves broadcasting counterfeit satellite signals to deceive GNSS receivers, causing them to compute incorrect position, navigation, and timing (PNT) data.

There are no specific flight crew alerts that would indicate which kind of interference is being experienced – jamming or spoofing. Nevertheless, the effects of jamming are typically immediate and noticeable by the flight crew, as systems fail to receive GNSS signals. This should allow for quick recognition of the problem and reaction with mitigation measures. On the other hand, detection of spoofing is more difficult and not immediate for the flight crew, thus posing more safety risk than jamming. Depending on aircraft-system integration, various side effects of jamming have been observed which could be attributed to spoofing and vice-versa. For the

This is information only. Recommendations are not mandatory.



An Agency of the European Union

TE.CAP.00117-008 © European Union Aviation Safety Agency. All rights reserved. ISO9001 Certified.
Proprietary document. Copies are not controlled. Confirm revision status through the EASA-Internet/Intranet.

Page 1 of 6

purposes of this safety information bulletin, jamming and spoofing are discussed as suspected causes, regardless of their actual cause.

The following non-exhaustive list provides observed symptoms of suspected GNSS spoofing:

- Incoherence in navigation position, such as GNSS/FMS position disagree alerts;
- Abnormal differences between Ground Speed and True Airspeed;
- Time and date shift;
- Spurious Terrain Awareness and Warning System (TAWS) alerts;
- Potential deviation of hybrid position (IRS/GNSS).

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 triggering spurious 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 traffic density, on the phase of flight, and on how dependent the aircraft systems are on GNSS signals.

The following non-exhaustive list provides examples of issues that a degradation of GNSS signal (including Satellite Based Augmentation Systems (SBAS) and Ground Based Augmentation Systems (GBAS)) could generate:

- Temporary or non-recoverable failure or degradation of PNT information provided by GNSS, possibly resulting in:
 - Loss of or misleading TAWS (e.g., spurious PULL UP alerts triggered by predictive TAWS during cruise, descent, approach, and landing phase that in some cases resulted in high vertical rate uncoordinated climbs, note that traffic alerts are deprioritised over TAWS PULL UP alerts);
 - Loss of Airborne Collision Avoidance System (ACAS);
 - Loss of or misleading surveillance function (e.g., corrupted Automatic Dependent Surveillance-Broadcast (ADS-B));
 - Loss of or misleading information on a Synthetic Vision Systems (SVS), weather uplink functions, predictive wind shear, and other surface functionalities;
 - Inconsistent flight guidance possibly resulting in route divergence, uncommanded turns, and deviations from the ATC clearances or instructions received, which could potentially lead to airspace infringements, loss of traffic separation, insufficient terrain/obstacle clearance, etc.;
 - Inconsistent, or potentially misleading aircraft position, GNSS altitude, and calculated ground or wind speed on the navigation display or on the Electronic Flight Bag (EFB);
 - Inconsistent, or potentially misleading aircraft position and/or GNSS altitude, later in the flight after having exited the affected area, e.g., during approach;
 - Loss or misleading time and/or date dependent systems (e.g., clock, fuel computation system, flight management system, discarded Controller Pilot Data Link Communication (CPDLC) messages).
- Inability to use GNSS for navigation, including waypoint navigation;
- Inability to use GNSS for navigation after exiting the affected area or for the remainder of the flight;

This is information only. Recommendations are not mandatory.



An agency of the European Union

TE.CAP.00117-008 © European Union Aviation Safety Agency. All rights reserved. ISO9001 Certified.
Proprietary document. Copies are not controlled. Confirm revision status through the EASA-Internet/Intranet.

Page 2 of 6

EASA SIB No.: 2022-02R3

- Inability to maintain GNSS based Area Navigation (RNAV) and/or Required Navigation Performance (RNP).

Repeated or widespread disruptions of the GNSS signals can lead to increased workload of both flight crews and air traffic controllers that can cause cognitive overload or confusion and increase the risk for errors.

The combination of two or more of the issues listed above may have cumulative adverse effects on flight safety.

GNSS Jamming and Spoofing also can affect ground-based systems, especially when they use GNSS as their only source for timing.

This SIB is revised to list new issues observed and update recommendations, as a result of analysis of recently reported occurrences of jamming and spoofing.

EASA is continuously monitoring and assessing the situation, however, at this time, the safety concern described in this SIB is not considered to be an unsafe condition, that would warrant Safety Directive (SD) action under Commission Regulation (EU) [965/2012](#), Annex II, ARO.GEN.135(c), nor under Commission Regulation (EU) [2017/373](#), Annex II, point ATM/ANS.AR.A.030, or Airworthiness Directive (AD) action under Regulation (EU) [748/2012](#), Part 21.A.3B.

Recommendation(s):

To address the identified issues EASA recommends the implementation of the following mitigating measures. These measures are to be considered for the flight information regions published on [EASA website](#) and should be extended to any other area where GNSS jamming and/or spoofing is identified. Some recommendations for aircraft operators are now separated for jamming as compared with spoofing, due to the specificities of the two different cases.

CAs should:

- Ensure that contingency procedures are established in coordination with ATM/ANS providers and airspace users, and that existing non-GNSS based navigation infrastructure, particularly Instrument Landing Systems (ILS), Distance Measuring Equipment (DME) stations and Very High Frequency Omnidirectional Range (VOR) stations are made available and kept operational as required;
- Implement appropriate and proactive mitigating measures as a matter of high priority, including the issuance of NOTAMs, e.g., describing affected areas and related limitations;
- Facilitate the establishment by ATM/ANS service providers of a process to collect information on GNSS degradations, in coordination with the relevant national regulatory authorities for telecommunications, and promptly notify the related outcomes to air operators and to other airspace users;
- Consider measures at national level, by involving appropriate and competent entities, to avoid the proliferation, circulation and operation of unauthorized transmitters that cause or have the potential to cause harmful interference to GNSS signals;

This is information only. Recommendations are not mandatory.



An agency of the European Union

TE.CAP.00117-008 © European Union Aviation Safety Agency. All rights reserved. ISO9001 Certified.
Proprietary document. Copies are not controlled. Confirm revision status through the EASA-Internet/Intranet.

Page 3 of 6

- When applicable, encourage civil-military coordination prior to testing or use of GNSS disturbance systems¹;
- Ensure that contents of this SIB are duly considered by air operators, ATM/ANS providers, aircraft and equipment manufacturers, and organisations involved in the design or production of ATM/ANS equipment.

ATM/ANS providers should:

- Establish a process to collect information on GNSS degradations, in coordination with the relevant CAs, national regulatory authorities for telecommunications, and promptly notify the related outcomes to air operators and to other airspace users;
- Assess the impact of loss or anomalies of GNSS-based timing on CNS systems;
- Adhere to the procedures on the provision of information to airspace users as appropriate, e.g., through ATIS, issuing NOTAMs, AIP, etc.;
- Consider keeping a ground navigation infrastructure operational such as ILS, DME, and/or VOR in support of conventional and performance-based navigation procedures;
- Make sure that the surveillance coverage is resilient to GNSS interference;
- For areas, where surveillance remains exclusively based on ADS-B, ensure that appropriate contingency procedures are available, when GNSS jamming or spoofing is detected;
- In areas affected by GNSS jamming and/or spoofing promote the use of conventional navigation flight procedures or performance-based flight procedures using VOR/DME;
- Be prepared to provide navigation assistance to aircraft (using radar vectoring) as long as needed;
- Ensure that the communications coverage and performance meet the needs for radar vectoring provision in case of GNSS jamming or spoofing;
- Ensure that contingency plans include procedures to be followed in case of large-scale GNSS short-term and long-term jamming and/or spoofing events;
- Consider implementing local GNSS RFI detection and GNSS status monitoring systems in addition to network-level capabilities, as needed;
- Reinforce the monitoring of the traffic closely to prevent any deviation from ATC clearances (e.g., navigation track and altitude);
- Assess whether sector capacities and applicable separation minima remain appropriate;
- Ensure that GNSS jamming or spoofing topic is included in the ATCO training, highlighting the identified operational scenarios to recognise, react in a timely manner to different jamming and spoofing cases.

Air operators should:

- Ensure that flight crews are aware, trained and prepared to recognise and adequately respond to an encounter of GNSS interferences during flight;
- Ensure that flight crews are aware of 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, lost or misleading position, time anomalies, etc., including their duration);

¹ Refer to EUROCONTROL “Guidelines on a Process for Civil and Military GNSS Interference Testing” for further guidance.



EASA SIB No.: 2022-02R3

- Evaluate different possible scenarios based on the type of operations in order to provide the flight crew with timely information to increase awareness of jamming and spoofing;
- Ensure that GNSS jamming or spoofing topic is included in the flight crew ground recurrent training and training of other relevant operations personnel, especially when operating in the mentioned areas, highlighting the identified operational scenarios to recognise, 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 reliable GNSS signal, e.g., impact on TAWS;
- Maintain contact with aircraft or equipment manufacturers for instructions and guidance on how to operate and maintain their products, when exposed to jamming or spoofing, and implement the recommendations in the standard operating and maintenance procedures;
- Ensure that any system used as a backup to GNSS is not inoperative according to the Minimum Equipment List, before commencing a flight into known affected areas, with the exception of one flight if necessary to reach a station, where the repair can be done;
- Ensure that systems, used as a backup for an inoperative system according to the Minimum Equipment List, are not reliant on GNSS, before commencing a flight into affected areas, with the exception of one flight if necessary to reach a station where the repair can be done;
- Ensure, whenever possible (e.g., airspaces that are not oceanic or remote), in the flight planning for flights into affected areas, the availability of alternative non-GNSS based procedures for the whole flight, regardless of the type of operation. This should be complemented with information regarding the ability to receive radar vectoring in the airspaces to be transited;
- If subject to Flight Data Monitoring (FDM) requirements and necessary data are available, use FDM programme to identify and assess GNSS jamming and spoofing events.

GNSS jamming specific recommendations for Air operators:

- Ensure that flight crews and relevant flight operations personnel:
 - are aware of possible GNSS jamming;
 - verify the aircraft position by non-GNSS means, when flights are operated in proximity to the affected areas;
 - check that the navigation aids essential to the operation for the intended route and approach are available;
 - remain prepared to revert to a non-GNSS procedure where appropriate; and
 - report (AIREP) any observed irregularities to air traffic services.

GNSS spoofing specific recommendations for Air operators:

- Ensure that flight crews and relevant flight operations personnel:
 - are aware of possible GNSS spoofing;
 - when possible monitor aircraft position using non-GNSS nav aids and all available automatic navigation accuracy calculations, including the Estimated Position Uncertainty (EPU) figure;
 - monitor the GNSS time versus non-GNSS time sources;
 - closely monitor the ATC frequencies in the vicinity of spoofing area;
 - apply the manufacturer's instructions and guidance for the aircraft type on detecting and dealing with suspected spoofing;

This is information only. Recommendations are not mandatory.



An agency of the European Union

TE.CAP.00117-008 © European Union Aviation Safety Agency. All rights reserved. ISO9001 Certified.
Proprietary document. Copies are not controlled. Confirm revision status through the EASA-Internet/Intranet.

Page 5 of 6

- report (AIREP) to air traffic services any observed irregularities.

Aircraft and equipment manufacturers, should:

- Assess the effects of jamming and spoofing on their products considering cumulative effects of multiple systems being affected simultaneously;
- Support Air operators, by providing guidance on how to detect suspected GNSS spoofing events, when using their products;
- Provide instructions and guidance to Air operators on how to operate and maintain their products, when affected by GNSS jamming and spoofing, and implement the recommendations in the standard operating and maintenance procedures.

Organisations involved in the design or production of ATM/ANS equipment, should:

- Assess the effects of jamming and spoofing on their products considering cumulative effects of multiple systems being affected simultaneously;
- Support ATM/ANS providers, by providing guidance on how to detect suspected GNSS spoofing events, when using their products;
- Provide instructions and guidance to ATM/ANS providers on how to operate and maintain their products, when affected by GNSS jamming and spoofing, and implement the recommendations in the standard operating and maintenance procedures.

All parties concerned are reminded of their obligations to report any event impacting safety according to Regulation (EU) No. [376/2014](#).

Air operators are also reminded to report the suspected GNSS spoofing and higher risk jamming occurrences to aircraft manufacturers and support their investigations by providing relevant information in compliance with point ORO.GEN.160 (b) of Regulation (EU) No [965/2012](#).

Contact:

For further information contact the EASA Safety Information Section, Certification Directorate,
E-mail: ADs@easa.europa.eu.