ALERTA de SEGURIDAD

DIRECCIÓN DE SEGURIDAD OPERACIONAL

SMS – 020 - 2025

TEMA: **NUEVAS AMENAZAS CIBERNETICAS EN AVIACION: JAMMING Y SPOOFING DE LAS SEÑALES GNSS**

DESTINATARIO:

TODO EL PERSONAL DE TALLERES, TÉCNICOS, INSPECTORES, CERTIFICADORES, ALMACÉN AERONÁUTICO Y PERSONAL CLAVE DE LA OMA HTC.

LINK DE VALIDACIÓN DE LECTURA

(Favor ingresar y diligenciar el link)

https://forms.gle/dk4UajVcsaXjwBJH9

Código SMS:	**GSMS-F-007**
Versión:	**No.: 06**
Vigencia:	**Marzo 2025**
Fecha:	05/03/2025

Helistar TECHNICAL CENTER

NUEVAS AMENAZAS CIBERNETICAS EN AVIACION: JAMMING Y SPOOFING DE LAS SEÑALES GNSS

Contexto:

El jamming y el spoofing de señales GPS representan serios riesgos para la aviación debido a su impacto en la navegación, comunicación y seguridad operacional de aviones y helicópteros. Estos ataques pueden comprometer la precisión de la posición, el guiado de aproximaciones y la gestión del tráfico aéreo, lo que aumenta el riesgo de incidentes y accidentes.

Aunque en la mayoría de los casos se identifica el error humano como la causa raíz predominante, los accidentes aéreos suelen ser el resultado de una combinación de factores.

1. JAMMING GPS

El jamming consiste en la interferencia deliberada en las señales GPS mediante transmisores de alta potencia que bloquean la recepción de la señal en los receptores de aeronaves. Esto puede generar los siguientes problemas:

- **Pérdida de la navegación basada en GPS:** Los sistemas GNSS (Global Navigation Satellite System) son fundamentales para la navegación de área (RNAV) y los procedimientos de aproximación con navegación basada en performance (RNP). Si el GPS es inutilizado, la aeronave puede perder su capacidad de navegación precisa, obligando a los pilotos a depender de métodos tradicionales como VOR/DME o incluso navegación visual.

- **Impacto en sistemas de aviónica:** En aeronaves modernas, el GPS es clave para el sistema de gestión de vuelo (FMS) y sistemas como ADS-B (Automatic Dependent Surveillance-Broadcast), que depende de una ubicación precisa para la gestión del tráfico aéreo. El jamming puede causar la pérdida de información precisa de posición para los controladores de tráfico aéreo.

ALERTA de SEGURIDAD

DIRECCIÓN DE SEGURIDAD OPERACIONAL

SMS – 020 - 2025

NUEVAS AMENAZAS CIBERNETICAS EN AVIACION: JAMMING Y SPOOFING DE LAS SEÑALES GNSS

- **Interrupción de sistemas de seguridad:** Algunas aeronaves utilizan el GPS para sistemas de alerta de tráfico y evitación de colisiones (TCAS), así como para sistemas de aterrizaje asistido. Un ataque de jamming puede reducir la eficacia de estos sistemas.

- **Afectación en helicópteros:** Los helicópteros, especialmente aquellos en misiones de búsqueda y rescate o evacuación médica (MEDEVAC), dependen del GPS para operaciones en condiciones de baja visibilidad. Un bloqueo de señal puede poner en peligro la misión y la seguridad de la tripulación.

2. SPOOFING GPS:

El spoofing es un ataque más sofisticado en el que un transmisor emite señales falsas de GPS para engañar al receptor de la aeronave, haciéndole creer que está en una ubicación diferente. Esto puede causar:

- **Desviaciones de ruta no detectadas:** Si una aeronave recibe señales falsas de GPS, su sistema de navegación puede indicar posiciones erróneas sin que la tripulación lo note de inmediato. Esto podría llevar a desviaciones de rutas aerovías, aumentando el riesgo de colisión o ingreso en espacio aéreo restringido.
- **Problemas en aproximaciones y aterrizajes:** Durante una aproximación instrumental basada en GPS (LPV, RNP), un ataque de spoofing podría hacer que la aeronave siga una trayectoria falsa, llevándola fuera de la senda correcta de aproximación.
- **Interferencia en UAVs y aeronaves no tripuladas:** Muchos drones y aeronaves autónomas dependen completamente del GPS para su navegación. Un ataque de spoofing podría desorientarlos, hacerlos aterrizar en áreas no previstas o incluso ser secuestrados mediante una manipulación de coordenadas.
- **Confusión en la gestión del tráfico aéreo:** Si varias aeronaves reciben señales erróneas de GPS, los controladores podrían recibir información de posición falsa a través de sistemas como ADS-B, dificultando la gestión del espacio aéreo y aumentando el riesgo de conflictos de tráfico.ADSB (Automatic Dependent Surveillance–Broadcast)

Los anteriores entre otros equipos mandatorios refuerzan la seguridad en las operaciones IFR.

MEDIDAS DE MITIGACIÓN

Para reducir el impacto de estos ataques, las aeronaves y operadores pueden aplicar varias estrategias:

- **Uso de sistemas alternativos de navegación:** Integrar redundancias con sistemas inerciales (IRS), radioayudas terrestres (VOR, DME, ILS) y referencias visuales cuando sea posible.

- **Sensores de detección de interferencias:** Algunas aeronaves están equipadas con detectores de interferencias GNSS que alertan a la tripulación sobre anomalías en la señal.

- **Filtrado de señales y autenticación:** Se están desarrollando técnicas de autenticación de señales satelitales para prevenir el spoofing, verificando la procedencia de la señal.

- **Protocolos de entrenamiento para pilotos:** Familiarizar a los pilotos con los síntomas de interferencia GPS y entrenarlos en procedimientos de recuperación ante pérdida de navegación por GPS.

ALERTA de SEGURIDAD

DIRECCIÓN DE SEGURIDAD OPERACIONAL

SMS – 020 - 2025

NUEVAS AMENAZAS CIBERNETICAS EN AVIACION: JAMMING Y SPOOFING DE LAS SEÑALES GNSS

Desde el punto de vista de mantenimiento aeronáutico, la prevención del jamming y spoofing en las señales GPS implica una combinación de inspección de equipos, actualización de software, implementación de tecnologías de mitigación y entrenamiento del personal. A continuación, se detallan las acciones clave que pueden tomarse para minimizar los riesgos:

MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE NAVEGACIÓN

a) Inspección y calibración de receptores GPS

- Verificar periódicamente la sensibilidad y precisión de los receptores GPS instalados en la aeronave.
- Asegurar que los receptores estén correctamente blindados contra interferencias electromagnéticas (EMI).
- Realizar pruebas de recepción en condiciones controladas para detectar posibles anomalías en la señal.

b) Revisión de antenas y cableado

- Inspeccionar las antenas GPS en busca de desgaste, corrosión o daños físicos que puedan afectar la recepción de la señal.
- Asegurar que el cableado de RF esté correctamente conectado y que las conexiones a tierra sean óptimas para minimizar la susceptibilidad a interferencias.
- Verificar la correcta fijación y alineación de las antenas en la estructura de la aeronave.

c) Pruebas funcionales de sistemas de navegación y aviónica

- Realizar pruebas de navegación redundante utilizando sistemas alternativos (INS, VOR/DME, ILS) para verificar la confiabilidad del GPS.
- Comparar la precisión de la señal GPS con otros sistemas de navegación a bordo y verificar la coherencia de los datos.
- Usar simuladores de señal GPS en mantenimientos programados para evaluar la respuesta del receptor ante posibles ataques de spoofing.

CAPACITACIÓN DEL PERSONAL DE MANTENIMIENTO

a) Entrenamiento en detección de interferencias GPS

- Capacitar al personal técnico para reconocer los síntomas de jamming (pérdida intermitente o total de señal) y spoofing (desplazamiento erróneo de la posición sin pérdida de señal).
- Proporcionar formación en el uso de herramientas de monitoreo de señal GPS y espectro de radiofrecuencia.

b) Simulaciones de ataque y respuesta

- Implementar simulaciones en talleres de mantenimiento para evaluar la respuesta de los sistemas de navegación ante interferencias deliberadas.
- Instruir a los técnicos en el uso de procedimientos alternativos de navegación en caso de pérdida de GPS.

Conclusión: Desde la perspectiva del mantenimiento, la clave para prevenir los efectos del jamming y spoofing en GPS radica en la inspección regular de equipos, la actualización tecnológica, la vigilancia del entorno electromagnético y la capacitación del personal. Estas acciones garantizan la integridad de los sistemas de navegación y también mejoran la seguridad y fiabilidad de las operaciones aéreas.

"MANTENIMIENTO PRECISO, NAVEGACIÓN SEGURA: ¡PROTEGE EL GNSS DEL JAMMING Y SPOOFING!"