	Aeronautical Services Advisory Memorandum (ASAM) Focal Point: Gen	ASAM No: 050 Issue 1 Date 20/10/2025
Title	**Global Navigation Satellite System (GNSS) Interference**	

1. Introduction

This ASAM is issued to inform pilots, air traffic controllers (ATCOs), airlines, air navigation service providers (ANSPs), and competent authorities/States about the increasing occurrence and impact of Global Navigation Satellite System (GNSS) interference, including both jamming and spoofing.

This notice aims to raise awareness of the potential safety risks and to outline recommended actions to mitigate these risks. This information is for guidance only and recommendations are not mandatory. As of June 2025, EASA and IATA have shifted focus from containment to resilience, emphasizing proactive measures and coordinated strategies to address GNSS interference.

Since February 2022, there has been a notable increase in reports of GNSS jamming and/or spoofing events affecting civil aviation operations globally. Analysis of recent data indicates a further increase in the severity of the impact, as well as an overall growth in the intensity and sophistication of these events. These issues particularly affect geographical areas surrounding conflict zones. Areas impacting Civil Aviation both directly and indirectly are known to be in the south and eastern Mediterranean, Black Sea, Middle East, Baltic Sea, and Arctic area. A list of affected Flight Information Regions (FIRs) is published on the EASA Website.

GNSS Jamming is an intentional radio frequency interference (RFI) with GNSS signals. This interference prevents receivers from locking onto satellite signals, rendering the GNSS system ineffective or degraded for users in the jammed area.

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

Detection of spoofing is more difficult and not immediate for the flight crew, thus posing a potentially higher safety risk than jamming.

The scale and effects of the current wave of spoofing are unprecedented, with a significant increase observed since September 2023. By August 2024, approximately 1500 flights per day were experiencing spoofing.

Current and historical GNSS Interference status is accessible from Eurocontrol AUGUR system.

2. Impacts on Aircraft Systems and Operations

GNSS interference, whether jamming or spoofing, can lead to a temporary or non-recoverable failure or degradation of PNT (Position, Navigation & Timing) information provided by GNSS. This can result in a wide range of issues during various phases of flight:

- **Navigation Issues:** Incoherence in navigation position, such as GNSS/FMS position disagree alerts. Inability to use GNSS for navigation, including waypoint navigation, or to maintain GNSS-based Area Navigation (RNAV) and/or Required Navigation Performance (RNP). Potential deviation of hybrid position (IRS/GNSS). Inconsistent flight guidance possibly resulting in route divergence, un-commanded turns, and deviations from ATC clearances. Inability to use hybrid GNSS inertial systems for navigation.

- **Surveillance Issues:**
  - Loss of or misleading surveillance function (e.g., corrupted Automatic Dependent Surveillance-Broadcast (ADS-B) and ADS-C). Inaccurate aircraft position on the navigation display (e.g., moving map and Electronic Flight Bag (EFB)). Loss of ADS-B IN (ATSAW) function.
  - Partial loss of conventional primary and secondary surveillance service in ATC, due to spoofed GNSS time stamp causing an aircraft plot/track to be 'rejected as stale' by Surveillance Data Processing System (SDPS).

- **Alerting System Issues:** Spurious Terrain Awareness and Warning System (TAWS) alerts (including PULL UP alerts). Unreliable triggering of TAWS/GPWS/EGPWS. Loss of or misleading information on Synthetic Vision Systems (SVS). Runway Awareness and Advisory System (RAAS) and Runway Overrun Protection Systems (ROPS) may be unavailable or give false warnings.

- **Timing and Data Link Issues:** Time and date shifts, potentially affecting time-dependent systems (e.g., clock, fuel computation system, flight management system, discarded Controller Pilot Data Link Communication (CPDLC) messages). Loss of CPDLC and ADS-C.

- **Other System Impacts:** Abnormal differences between Ground Speed and True Airspeed. Inconsistent, or potentially misleading aircraft position, GNSS altitude, and calculated ground or wind speed on the navigation display or EFB. Unanticipated effects on the use of conventional navigation aids (e.g., inability to auto-tune). Unanticipated position-dependent flight management system effects (e.g., insufficient fuel indication). Potential impact on weather radar. Loss of Ka SATCOM. Internet/Wi-Fi may not work correctly.

Repeated or widespread disruptions of GNSS signals can lead to increased workload for both flight crews and air traffic controllers, potentially causing cognitive overload or confusion and increasing the risk of errors. The combination of multiple issues can have cumulative adverse effects on flight safety.

GNSS jamming and spoofing can also affect ground-based systems, especially those using GNSS for timing.

3. Safety Concerns

The impact of GNSS Spoofing on flight safety, aircraft operation and handling, and ATC operations is extremely significant. Key overall safety concerns include:

- **Risk of complacency** due to the increasing frequency of events.
- **GNSS Complexity** in aircraft systems, creating a chain of complexity making safety and risk assessment challenging.
- **Lack of technical information** available to flight crew.
- Crew being **forced to accept degraded aircraft** systems during flight.
- **Potential for worsening of the situation** with evolving spoofing tactics.
- **Emergencies now carry higher risk** due to degraded systems and increased workload.
- Risk related to **contaminated GNSS Receivers** even after apparent recovery, potentially affecting RNP operations.
- **False EGPWS alerts** leading to startle effects, lowered trust in the system, and potentially dangerous manoeuvres, including go-arounds at unusual altitudes and separation minima infringements with proximate traffic.
- **Lateral deviation** of aircraft during spoofing without ATC clearance.
- **Increase in ATC workload** due to the need for radar vectoring and managing affected aircraft.

4. Recommendations

To address the identified issues, the following is recommended:

4.1. Air Traffic Management/Air Navigation Service Providers (ATM/ANS providers):

- Establish a process to collect information on GNSS degradations, in coordination with the National Frequency Manager and ComReg, and promptly notify the related outcomes to air operators and 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. This includes adopting standardised phraseology and NOTAM coding (e.g., Q codes) for GNSS interference reporting, as recommended by EASA and IATA.
- Consider keeping ground navigation infrastructure operational such as ILS, DME, and/or VOR in support of conventional and performance-based navigation procedures.
- Make sure that 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 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 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 ATCO/ATSEP training, highlighting the identified operational scenarios to recognise and react in a timely manner to different jamming and spoofing cases.
- Circulate awareness to Approach and Enroute controllers to anticipate GPWS responses in/at previously uncommon locations and altitudes.
- Introduce specific phraseology for GPWS response manoeuvres.
- Clarify the altitude to climb to after a GPWS response.
- Notify adjacent ANSPs of aircraft impacted by GNSS interference to ensure proper coordination and separation, especially in the ICAO NAT region.

4.2. Organisations involved in the design or production of ATM/ANS equipment:

- 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.

5. Reporting

All parties concerned are reminded of their obligations to report any event impacting safety according to Regulation (EU) No. 376/2014. Operators should report suspected GNSS RFI events to regional (e.g., ANSPs) and international organizations (e.g., EUROCONTROL's EVAIR). Within the ICAO NAT region, early notification of GNSS interference to ATC is crucial.

6. Conclusion

The increasing threat of GNSS interference poses significant risks to aviation safety and operational efficiency. It is crucial for all stakeholders to be aware of these risks and to implement the recommended mitigation measures. Enhanced collaboration, communication, and proactive measures are essential to safeguard against the risks posed by GNSS jamming and spoofing. Continuous monitoring and assessment of the situation are necessary to adapt to this evolving threat.

No further text on this page

7. References

- European Union Aviation Safety Agency (EASA) Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation
  SIB 2022-02 | EASA
- Federal Aviation Administration (FAA) Safety Alert for Operators (SAFO) 24002
  SAFO 24002
- AIRBUS Safety First #29 safety_first_29.pdf
- International Civil Aviation Organisation (ICAO) NAT OPS Bulletin 2025_001
  NAT OPS Bulletin 2025_001.pdf
- OPS Group GPS Spoofing Final Report GPS Spoofing: Final Report published by WorkGroup – International Ops 2025 – OPSGROUP
- EASA and IATA Comprehensive Plan to Mitigate GNSS Interference (June 2025)
  https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-and-iata-outline-comprehensive-plan-mitigate-gnss

8. Further Information

Requests for further information on the contents of this notice should be addressed to ansdinfo@iaa.ie.

End