CANSO

GLOBAL NAVIGATION SATELLITE SYSTEM INTERFERENCE: JAMMING AND SPOOFING

SHAPING OUR FUTURE SKIES

canso.org

Acknowledgements

This document was prepared by the CANSO Operations Programme Communication, Navigation, and Surveillance workgroup (CNSWG), Airspace Optimisation Workgroup (AOWG) and the CANSO Safety Programme Safety Intelligence Workgroup (SIWG). CANSO would like to thank the following organisations, whose representatives have invaluably contributed to the document:

- ATNS South Africa
- Airways New Zealand
- Cyprus Department of Civil Aviation
- Fintraffic, Finland
- Nav Canada
- Skyguide, Switzerland
- US FAA
- Aireon
- Skykraft
- Tetratech
- Think Research
- Viasat

Executive Summary

Are we ready for the unexpected?

> In April 2024, under CAVOK conditions, an aircraft under Tower procedural control and operating at 1800 feet, completed its base turn, and turning to establish on the ILS with clearance to land, reported "going-around" in response to a ground proximity warning system (GPWS) alert.
>
> The aircraft initiated an uncoordinated climb to 6500 feet, without Air Traffic Control (ATC) clearance or warning (the published missed approach altitude was 2000 feet). A few seconds later, the aircraft indicated on mode S, selected level 060, overshooting its intended level by 500 feet, due to a high rate-of-climb.
>
> Fortunately, there were no aircraft operating above the landing aircraft, and it was released to surveillance approach control, vectored to final and landed safely.

The occurrence, above, constitutes a vertical deviation from ATC clearance. It is one of numerous safety hazards resulting from Global Navigation Satellite System (GNSS) interference events, thousands of which are occurring every day, around the world.

Beginning in late 2023, a rapid rise in intentional GNSS interference events began to cause significant disruption to aviation and air traffic operations, impacting airspace efficiency and introducing a safety risk. The aviation community has responded with investigations, analysis, safety and technical bulletins, workshops, and other initiatives by ICAO, States, Air Navigation Service Providers (ANSPs), IATA, standards bodies, equipment manufacturers and service suppliers.

In October 2024, CANSO presented a webinar: Intentional GNSS Jamming and Spoofing. This document, an outgrowth of that webinar, provides CANSO Members with urgent information on the rapid growth of GNSS interference events. It addresses how interference events may impact aircraft and air traffic operations, provides strategies for anticipating, monitoring and managing interference events to reduce the associated impacts and hazards, and it discusses considerations for future proofing aircraft and air traffic operations against GNSS interference. The document describes the role of spectrum management for resiliency against radio frequency interference (RFI) and it emphasises the role of safety intelligence systems to effectively monitor, detect, and mitigate GNSS threats.

CANSO's intent is to raise awareness among ANSPs and to support them in establishing effective strategies to mitigate potential safety hazards and impacts to airspace efficiency arising from GNSS interference.

The guidance provided in this document reflects the state of operations and technology implementation at publication. GNSS and other radio frequency interference is an evolving threat: one that requires CANSO, its ANSP members and the broader aviation community to remain vigilant.

Contents

1. Introduction

Beginning in August 2023, the aviation industry began to note a significant increase in incidents that result in disruption to GNSS signals. While civil aviation operators are not being directly targeted, they are being impacted, particularly as a result of flights over or near conflict zones. According to the September 6, 2024 Final Report of the GNSS Spoofing Workgroup, published by OPSGROUP, incidents of GNSS spoofing and jamming rose from an average of 300 incidents per day, globally, in January 2024, to more than 3,000 per day in August 2024.

GNSS signals are vulnerable to degradation because of their extremely low power. This may be naturally occurring, such as from atmospheric scintillation and solar effects. RFI may be unintentional, such as equipment malfunction, equipment operating near the GNSS frequency, or multipath (signal is reflected from surrounding objects). Finally, GNSS RFI may result from deliberate acts, such as intentional jamming or spoofing. This Intentional interference is the focus of this document.

Because GNSS interference incidents are so prevalent, with the potential for significant impacts to safety and efficiency, the aviation industry, ANSPs, States and ICAO have been working to establish policies, guidance, and tools to identify and mitigate the impacts from interference events. For example, ICAO Air Navigation Conference (ANC) 14 published recommendations for States and for ICAO regarding GNSS interference, and ICAO Assembly 42nd Session adopted resolution A42-8, Appendix C, Ensuring the resilience of ICAO Communication, Navigation, and Surveillance (CNS)/ Air Traffic Management (ATM) systems and services, which recognised the increased risk posed by escalating use of GNSS RFI, and urged a number of actions by States and ICAO to address the issues. A number of workshops have been conducted, reports and publications to aid industry in understanding and mitigating risks of GNSS interference have been published, tools have been developed to aid in identifying and monitoring interference events, and technical solutions are being pursued.

This paper specifically addresses GNSS jamming/ spoofing. Its purpose is to provide ANSPs with information to aid them in mitigating the risks of GNSS interference while maintaining a safe and efficient air traffic operation. The paper will discuss operational impacts of jamming and spoofing from the perspectives of both, pilot/operator and controller/ATM. It will address strategic and tactical ATM approaches to mitigating the impacts from interference events, and it will provide information on tools, guidance materials and other available resources.

GNSS Interference

Jamming

- Jamming is understood to be caused by signals that are not specifically designed to mislead, and merely cause a service interruption or quality degradation;
- Jamming can result in denial of GNSS navigation, positioning, timing and aircraft dependent functions;
- Jamming effects are generally detected by avionic systems and, often, alerts are provided to the flight crew. Primary jamming sources include military RFI and Personal Privacy Devices (PPD), which, while illegal to operate in many States, are inexpensive and readily available over the internet.

Spoofing

- Spoofing uses counterfeit signals designed to create misleading information. Because spoofing signals by design look like desired GNSS signals, they can cause problems to GNSS receivers at levels much weaker than the interference mask;
- 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. (ICAO Doc 9849, GNSS Manual);
- Spoofing events are not automatically detected by current avionics systems or ATM systems and no specific alert is provided to the flight crew or the ANSPs. With few exceptions, GNSS Spoofing is conducted by State actors as a result of or in preparation for conflict, and is not directly aimed at commercial air transport. However, aircraft that operate in the vicinity of conflict zones are being affected.

1. Introduction

Aviation systems are generally developed with the resiliency to overcome GNSS jamming. However, impacts to aviation from a spoofed GNSS signal may be severe and cascading, as GNSS is incorporated into a number of ATM ground systems and a large number of modern aircraft systems (e.g. FMS, Hybrid IRS, aircraft clock, TAWS, weather radar, CPDLC, ADS-B, ADS-C, among others). Further, the effects of GNSS interference may continue well after a flight is no longer in proximity to the area being targeted (as some aircraft systems are unable to fully recover), and it may impact, both, ATM efficiency and flight safety.

Conflict Zones or Geostrategic Competition

By their nature, conflict zones and geostrategic competition change over time. Recently, areas most impacted by GNSS interference have included: the southern and eastern Mediterranean and Middle East; the Black Sea; eastern Europe; the Baltic Sea; the Arctic; Pakistan and India, and; Myanmar.

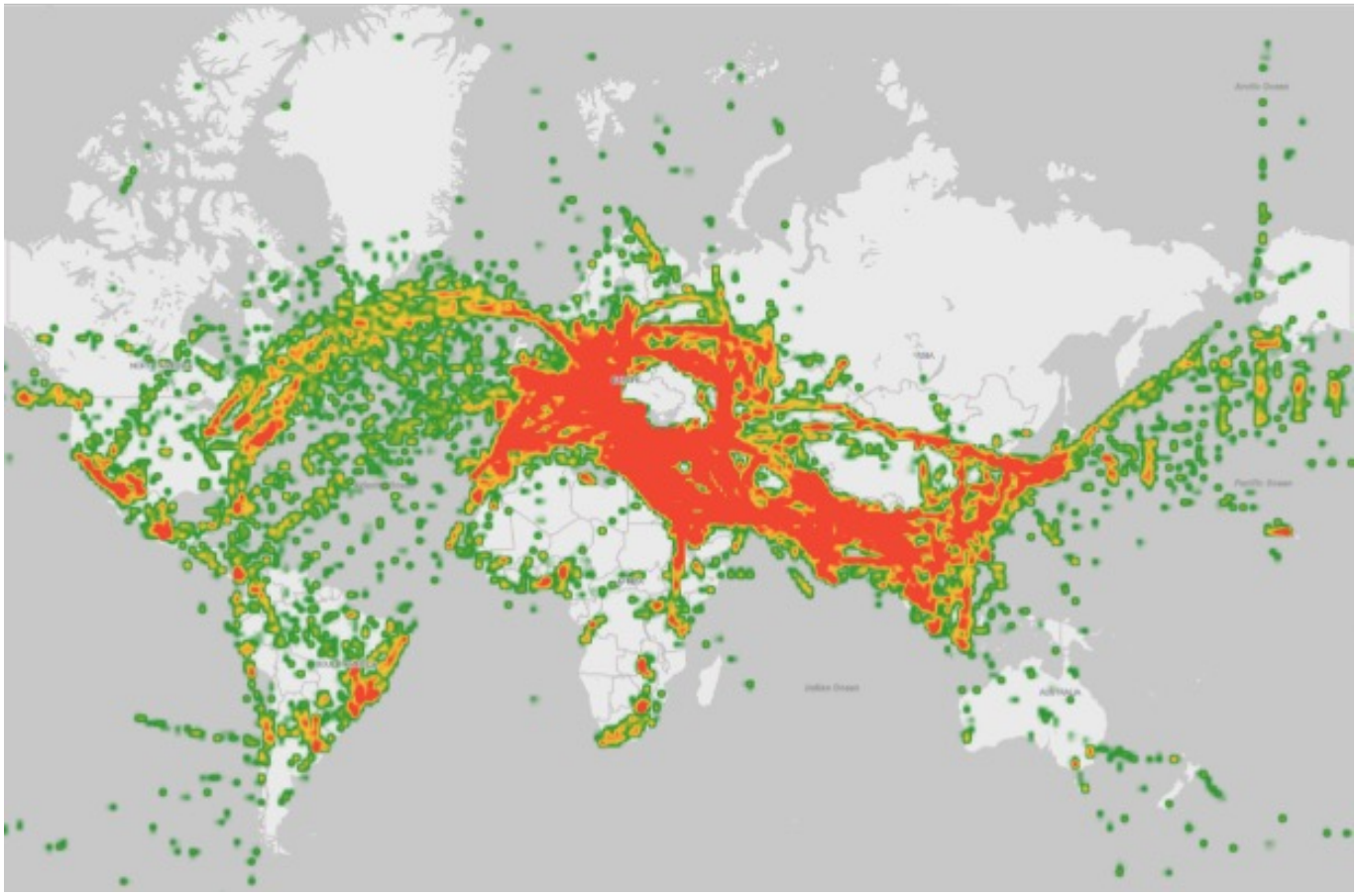


Figure 1: GNSS RFI recorded events depicting “hot spots,” Jan-Jun 2025 from IATA FDX

2. The Impact of GNSS RFI on Flight and Air Traffic Operations

While this document is oriented toward ANSPs, a holistic understanding of how GNSS interference impacts flight crews and aircraft operations, as well as air traffic controllers and airspace management is important, in order to raise awareness and to establish effective tactical and strategic mitigations.

This section begins with a discussion of human factors issues that affect flight crews and air traffic controllers. It is essential that air traffic controllers are aware of how pilots might be affected by GNSS interference events, to promote effective communication and teamwork between controllers and pilots, ultimately maintaining or improving safety. Just as important, understanding the human factors concerns faced by air traffic controllers, enables air traffic managers to prepare for interference events and effectively support the operation.

The discussion then moves to information on how systems may be affected by GNSS RFI and the consequential impacts for both aircraft operators and air traffic control. Finally, the section concludes with a summary of impacts reported by one de-identified FIR that operates in close proximity to a conflict zone.

1 Human Factors Related Safety and Workload Concerns

1.1 The Pilots View

Human factors concerns for pilot, from jamming and spoofing, include increased workload and risk associated with loss of trust in aircraft instruments or desensitisation to alerts. For example:

a) **Increased Workload:** A notable increase in workload may occur when pilots must deal with aircraft systems affected by jamming/spoofing, which may lead to fatigue, complacency, reduced reporting, and reduced awareness of non-interference related errors.

b) **Cognitive Dissonance:** When a pilot's beliefs or actions conflict, mental stress, physical impairment, and slower reaction times may result. For example, during the final approach, the pilot breaks out through the weather and is able to see the runway. However, the aircraft's location is different than what is indicated on the navigation display. In this example, the pilot will need to transition to visual cues that indicate actual aircraft position and ignore the position shown on the navigation display. It may be necessary to request radar vectors, if available. This conflicts with the pilot's mindset to "trust your instruments."

c) **Loss of Trust:** Multiple false alerts may cause pilots to question the legitimacy of the alerting system. For example, authentic Terrain Awareness and Warning System (TAWS) alerts may be ignored, because pilots have received multiple false warnings. The overall effect is that pilots lose trust in safety systems.

d) **Reduced Attention to Detail:** Spoofing causes a high number of Engine Indicating and Crew Alerting System (EICAS) warnings, which can lead to complacency and missing important warnings not related to spoofing.

e) **Normalisation of Risk:** Risk normalisation is the process by which dangerous or risky behaviors and practices become acceptable over time. As jamming/spoofing occur more often, there can be an acceptance of a higher risk tolerance at an organisational and even at a pilot level. As a person adapts to small changes and modified behaviors that were once a slight deviation from the norm, they may progress to where bigger deviations become acceptable. This can be accompanied by the hazardous attitude of "It worked before. Maybe we can push the envelope a little." The overall effect is a higher risk to flight safety.

f) **Reduced Situational Awareness:** Spoofing can cause a sudden shift in the aircraft's indicated position and decreased confidence in navigation capability.

g) **Pilot Disagreement and Conflict:** Without proper training and clear procedures to address jamming/spoofing, pilots may disagree on the best course of action. This conflict may have a negative impact on Crew Resource Management (CRM).

h) **Communication Challenges:** When data link communications are disabled, pilots may have to revert to all voice communication, including position reports at compulsory reporting points. This increases, both, pilot workload and the risk of misunderstandings and miscommunication, especially in high traffic conditions.

1.2 The Controller's View

Human factors and safety concerns for air traffic controllers include:

a) **Increased Workload:** Controllers may need to manage more aircraft manually/procedurally or may need to provide additional navigational support/ radar vectors, leading to higher stress levels and potential fatigue.

b) **Situational Awareness:** Without GNSS on ATM systems, maintaining an accurate picture of aircraft positions becomes more challenging, which can impair decision-making.

c) **Inconsistent flight crew response:** Flight crews may respond differently to similar types of events.

d) **Communication Challenges:** Key Controller Pilot Data Link Communication (CPDLC) benefits include reduction in communication errors and reduced workload. When CPDLC cannot be used, increased reliance on voice communication can lead to misunderstandings or miscommunication, especially under high traffic conditions. In cases where many operations are affected by CPDLC impacts, rostering may require adjustment to manage increased workload.

e) **Training and Proficiency:** Controllers may need to rely on outdated skills related to conventional navigation procedures that are rarely used, raising concerns about proficiency and confidence.

f) **Decision-Making:** The need for rapid and effective decision-making increases in emergency situations, which can be compromised under stress or time pressure.

g) **Error Management:** There is a potential for error as controllers juggle more variables due to increased complexity.

h) **Emotional Stress:** The pressure of ensuring safety during GNSS loss can lead to anxiety or frustration among controllers, affecting their performance.

i) Air traffic complexity may quickly increase creating traffic overload for the Air Traffic Control Officer (ATCO) in a sector, at an airport or more broadly.

j) Loss of trust in technologies, e.g., surveillance, data communications.

Addressing these concerns through training, effective communication protocols, and support systems is vital for maintaining safety and efficiency during loss of GNSS.

2 Technical and Operational Impacts

ATM/CNS is a complex system of systems. In addition to providing position and navigation information, GNSS is frequently used as a source of timing information within communication and radar systems and is also used for Automatic Dependent Surveillance (ADS) services. As ATM/CNS systems continue to become increasingly interconnected, the cascading effects from GNSS interference incidents could create greater vulnerabilities. The OPSGROUP: *GNSS Spoofing; Final Report of the GNSS Spoofing Workgroup*, published in September 2024, was a key source of information for this guidance document and, particularly, for the details on the technical impacts in this section.

2.1 Data Communications

a) **CPDLC:** The aircraft clock provides a timestamp to CPDLC downlinks, resulting in CPDLC messages being unavailable during jamming, as the timestamp will not be updated. Two distinct impacts to CPDLC have been observed after the aircraft clock time is altered by spoofing:

   When a discrepancy between the corrupted aircraft time or date and the correct time and date of the ground system is detected, the ground system may terminate the CPDLC connection with the message "ATC COMM TERMINATED." Downlinks will be unsuccessful after receiving this message. The system may continue to attempt logons, which may initially be accepted but promptly terminated again once another corrupted timestamp is received via downlink.

   Some corrupted timestamps can cause the uplink delay monitor to display the message header, "UPLINK DELAY EXCEEDED." Pilots can still respond to this message and continue to send and receive CPDLC messages as normal. Any issues with CPLDC equipment should be clarified and mitigated between ATC and the aircrew.

b) **ADS-C (Automatic Dependent Surveillance-Contract):** ADS-C uses a timestamp from the aircraft clock and will be unavailable during jamming.

   A metric within the ADS-C protocol is the Figure of Merit, or FOM. FOM is a statistically derived value on the reliability and accuracy of aircraft navigation data, which is interpreted by the air traffic control system in use. After having been spoofed or jammed, a common lingering symptom is low FOM, or low position confidence.

   This equates to the downgrading of the Required Navigation Performance (RNP) status of the flight and a disqualification from eligibility for performance-based reduced separation standards. As with CPDLC, the aircraft clock provides a timestamp for ADS-C reports. Incorrect time stamps on ADS-C reports can result in these being discarded by the air traffic system, which will also disqualify aircraft from utilising reduced separation minima.

Operational Impact

If the GNSS signal is jammed or spoofed, CPDLC and ADS-C are unavailable (jammed) or unreliable (spoofed). Failure to maintain connectivity, a low FOM or discarded ADS-C reports disqualifies an aircraft from Performance Based Communication and Surveillance (PBCS) reduced separation minima.

When this occurs, not only is the affected aircraft directly impacted, but aircraft in the vicinity may also be prevented from using optimal altitudes due to the increased longitudinal and lateral separation required. Additionally, in some FIRs with airspace that requires PBCS compliance, a controller may be required to descend or reroute downgraded aircraft out of optimal altitudes and/or around the most congested airspace, potentially reducing aircraft fuel efficiency and range and increasing exposure to adverse weather conditions.

In oceanic airspace, without CPDLC or ADS-C, High Frequency (HF) voice relay will be required to issue clearances and to receive position reports and clearance requests. ATC may find it more challenging to maintain accurate and timely position information and delivery of safety alerts and weather information. ATC should use all surveillance systems available, to include primary radar to establish precise position of an aircraft in this scenario.

2.2 Navigation

a) **GNSS Navigation:** GNSS interference can significantly impact the primary means of navigation and may require the use of other navigation aids (NAVAIDs). During jamming, GNSS may not be available, or suffer performance degradation, for departure, enroute, terminal, or approach GNSS-based navigation. This results in a loss of, or degraded, Ground Based Augmentation System (GBAS) and/or European Geostationary Navigation Overlay Service (EGNOS) European Geostationary Navigation Overlay Service (EGNOS) Receiver Integrity Monitoring Station (RIMS) performance, Area Navigation (RNAV) solution, and a probable loss of RNP capability. The pilot may need to revert to ground-based NAVAIDs (either for RNAV navigation or conventional procedures). During spoofing, GNSS may also not be available for navigation and may cause a "map shift" on the navigation display (e.g., moving map and electronic flight bag) showing a false position of the aircraft and may cause the pilots to lose situational awareness. Pilots may not be immediately aware of being spoofed as the aircraft subtly drifts or turns off course.

b) **Flight Management Systems (FMS) and other aircraft automation:** If the GNSS signal is jammed or spoofed, automatic tuning of NAVAIDs by the FMS is degraded or not available, and pilots may need to manually input waypoints and use traditional navigation methods to maintain accurate route adherence. There may also be unanticipated position-dependent flight management system effects (e.g., fuel computation system, runway overrun protection system, etc.) and loss of or misleading time and/or date dependent systems (e.g., clock, discarded CPDLC messages).

Operational Impact

If the GNSS signal is jammed or spoofed, pilots must navigate via conventional navaids and may require assistance. In cases where the pilot is unaware of being spoofed, there is a risk of airspace infringement and/or lateral or vertical deviation from ATC clearance.

It is important to note, however, that GNSS spoofing may also have unanticipated effects on use of Resilient Operational Network (RON)/Minimum Operational Network (MON). During GNSS disruptions, conventional terrestrial navigation infrastructure is often inadequate to support continuous PBN operations and positional awareness. To minimise impacts of GNSS disruptions, ANSPs can repurpose conventional navigation systems to establish a MON or RON.

There is a variation in how different States interpret the NAV MON Concept, which is compounded by the absence of an ICAO definition. For some, NAV MON is viewed as a means to maintain only the minimum level of service or the smallest necessary infrastructure to ensure aircraft can reach an airport and land. For others, it represents a means to ensuring the continuity of navigation services. Thus, there is a clear need for harmonisation and optimisation of navigation services, making use of existing infrastructure and resources.

To support GNSS reversion, conventional terrestrial navigation aids (NDB, VOR, DME, ILS) can be used in three ways:

1) as redundant aids to support PBN navigation specifications (esp RNAV 1, RNAV 5) and enable cross-check with GNSS

2) as contingency support to facilitate pilot positional awareness and/or

3) as already well established, as infrastructure for conventional Instrument Flight Procedures (IFP).

Most IFR aircraft are equipped with a VOR/ILS receiver that can be used for conventional navigation during GPS disruptions. Air carrier aircraft can revert to Distance Measuring Equipment (DME)/ DME (multiple DME) navigation to continue RNAV to the planned destination to fly a conventional precision approach procedure during GNSS disruptions. All other aircraft can revert from GNSS to VOR navigation to fly through the GPS disrupted area or land safely using a VOR/ILS approach. Without conventional NAVAIDs and non-GNSS RNAV or conventional procedures, pilots and ANSPs would rely on radar vectors.

While a MON or RON is a recommended approach to providing resilience to GNSS interference or loss, this may require training and frequent tests to confirm that crews are competent to operate with only the MON/RON, and that aircraft and ATC systems will allow use of the MON/RON even in the presence of spoofing. There is a long term trend for automation in software systems to increasingly rely on GNSS availability and accuracy, even in systems that are intended as resiliency measures against GNSS degradation.

2.3 Surveillance

a. Automatic Dependent Surveillance-Broadcast (ADS-B)

During jamming, the ADS-B transponder can no longer receive accurate positioning data from GNSS and may display a failure light. Since ADS-B relies on GNSS for position data, jamming can prevent aircraft from broadcasting their correct position or cause it to provide a degraded position (quality of service). If spoofed, ADS-B may broadcast inaccurate location data. To summarise:

- **ADS-B Out.** ADS-B depends on GNSS input to broadcast the aircraft position and does not take inputs from alternative navigation systems. Spoofing may result in the broadcast of a false ADS-B position. The Navigation Integrity Category (NIC), Navigation Accuracy Category (NAC), or Navigation Uncertainty Category (NUC) value may be an indication that ADS-B is unreliable or degraded.
- **ADS-B In.** During spoofing, ADS-B traffic may display false aircraft locations on the navigation display, as the result of incorrect ADS-B out data from other aircraft and/or traffic may be missing. Some systems with an alerting capability (e.g. ADS-B Traffic Advisory System (ATAS)) may give erroneous or missing alerts.

Operational Impact

If the GNSS signal is jammed or spoofed, ADS-B reports will be unavailable (jammed) or unreliable (spoofed). ATC would then need to revert to radar surveillance, Wide Area Multilateration (WAM), or position reports via Ultra High Frequency (UHF)/ Very High Frequency (VHF), or, in oceanic airspace, HF if ADS-C is not available. ATC may find it more challenging to maintain accurate and timely position information, which could raise separation concerns.

Note that certain impacts on aircraft systems may render an aircraft ineligible for RVSM altitudes. Coordinate with the impacted crew to verify, and if needed provide standard 2000' vertical separation with the impacted aircraft and other traffic or descend the crew below RVSM altitudes.

b. Multilateration (MLAT), Wide Area Multilateration (WAM), Surface Movement Guidance and Control System (SMGCS)

Most MLAT technologies depend on GNSS (GPS) time synchronisation for the computation of an aircraft position. The times of arrival of received signals at all ground stations must be accurately and precisely measured with respect to a common time base. Any error in synchronisation will directly translate into errors of the computation of an aircraft position or localisation process; therefore the synchronisation between sensors is a crucial capability of the system. GPS receivers – embedded into the WAM ground stations are used, that are optimised for outputting reference timing pulses.

Operational Impact

If the GNSS signal is jammed or spoofed, Multilateration position may be unavailable (jammed) or unreliable (spoofed). ATC would then need to revert to radar surveillance or position reports via UHF/VHF or interpolated tracks from last known position.

c. Radar

Some radar systems use GNSS (time stamping before sending radar data to the ATC automation system. When the radar GPS clock is impacted, the radar tracks become unavailable so, radar surveillance is lost. Where able, the ATC system interpolates tracks from the last known position.

d. Airborne Collision Avoidance System (ACAS)/ Traffic Collision Avoidance System (TCAS)

During or following jamming/spoofing, ATC may have to rely on witness accounts and updates, adjust evidence gathering, and ensure verifiable descriptions of aircraft incidents.

Operational Impact

The potential loss of traffic (Traffic Alert and Collision Avoidance System (TCAS)) alerts removes the last line of defense against mid-air collisions.

2.4 Safety Systems

a. TAWS

The TAWS look ahead feature utilises aircraft position in conjunction with terrain databases to provide advance warnings about obstacles. The aircraft position may become degraded with GNSS spoofing and interference, unlike the basic functions of TAWS, which only detect terrain directly below the aircraft. Database integrity monitoring ensures these databases remain accurate despite potential loading errors or equipment failures.

Spoofing has the potential to generate incorrect or misleading TAWS alerts. Erroneous alerts can inhibit valid TCAS advisories, increasing the risk of separation errors. Misleading TAWS warnings, such as a false "PULL UP" command during flight, may lead to dangerous, uncoordinated climbs, during which TAWS alerts take precedence over traffic alerts. Jamming can likewise produce spurious TAWS alerts, especially under high-power jamming conditions or when operating near terrain.

Operational Impact

During or following spoofing, false TAWS alerts can lead to unnecessary, uncoordinated escape maneuvers, resulting in possible vertical deviations and loss of separation. The levels that the aircraft are climbing to, in response to GPWS alerts, are often unknown, and the aircraft may be climbing at very high vertical speeds. Uncoordinated climbs at high velocity are considered the most serious ATC impact encountered.

Additionally, controllers need to be aware that false TAWS alerts may suppress legitimate TCAS advisories and alerts, potentially removing the last line of defense against mid-air collisions and creating a high cognitive workload for pilots.

Repeated false alerts could lead to risk of expectation bias and valid alerts being disregarded.

b. Airport Surface Tracking and Alerting

Surface surveillance and alerting systems, such as Airport Surface Detection Equipment (ASDE), use radar, multilateration, and satellite technology to track surface movements. The Runway Awareness and Advisory System (RAAS) uses the GNSS altitude from the look ahead feature of the TAWS database, potentially affecting advisory accuracy.
Alternate methods, such as ATC communication and navigation instruments, may be necessary to determine aircraft position without GNSS. Other Original Equipment Manufacturers (OEMs) also provide runway systems with varying capabilities and terminology.

Operational Impact

If the GNSS signal is jammed or spoofed, malfunctioning runway/surface detections systems could limit ATC's ability to track aircraft and vehicle movements on the ground, potentially compromising safety, and operational efficiency.

2.5 ATC Automation and Aircraft Specific Functions

a. Time-shift of Various Systems

Synchronisation: Many avionics systems and ground-based systems, including communication, surveillance (radar and ADS) and navigation equipment, use GNSS time synchronisation for accuracy.

Loss of GNSS may impact the precision of time-sensitive functions and lead to failures or degradation of ATM infrastructure and its associated systems and networks that rely on GNSS.

Operational Impact

If the GNSS signal is jammed or spoofed ATC may not have the normal complementary systems needed to manage aircraft sequencing and spacing.

b. Synthetic Vision Systems (SVS) and Head-Up Display (HUD)

Jamming and spoofing may degrade the accuracy and reliability of SVS, requiring pilots to rely on visual references for situational awareness. Spoofing makes the terrain information on the HUD unreliable and reduces situational awareness.

Operational Impact

If the GNSS signal is jammed or spoofed, a go-around or diversion may be necessary.

c. Weather Radar

Some commonly used weather radars use GPS position to assist with “Ground De-cluttering”. GPS information is taken from the TAWS, rather than directly from the GPS receiver. Crews report unusual weather radar behavior after spoofing, including inability to detect Cb cells (thunderstorms). Weather radar issues may also present due to RF interference around jamming or spoofing areas, rather than directly from GPS spoofing.

Operational Impact

During or following spoofing ATC may have to provide more frequent weather updates and adjust routes.

2.6 Administrative and Investigation

a. ATC Digital Audio Legal Recorder (DALR)

ATC facilities employ digital voice recording system for time synchronised voice recording of all pilot-controller communications during the last hour of every transmission. Such digital voice recording systems may depend on GNSS for their precision timing synchronisation operation. GNSS jamming or spoofing causes the DALR to use incorrect time data, leading to misinterpreted voice recordings, and synchronisation errors. These issues will cause the legal voice recordings to be unacceptable for any aircraft accident investigation and fact finding.

Operational Impact

During or following jamming/spoofing, ATC may have to rely on witness accounts and updates, adjust evidence gathering, and ensure verifiable descriptions of aircraft incidents.

2.7 Additional Challenges for ANSPs, Operators, and Regulators

- There is no global or regional process or criteria for determining when a GNSS RFI NOTAM or AIC (Aeronautical Information Circular) should be issued or when GNSS RFI is no longer a factor and a NOTAM may be cancelled;
- There is currently no NOTAM code for GNSS interference events for the category: CNS - GNSS Services (G). Because of this, GNSS RFI-related NOTAMs contain varying QCodes and inconsistent significations. IATA reported that eighteen (18) different QCodes are used worldwide, rendering filtering mechanisms ineffective.

Note—The ICAO Navigation Systems Panel (NSP) is currently developing QCodes for GNSS RFI NOTAMS and working to address the need for the guidance.

- There are no clear mandatory occurrence reporting requirements for GNSS jamming and spoofing events. Additionally, operator reporting procedures are not uniform, and not all occurrences are reported by flight crews - reporting is sometimes related to the severity of the effects of GPS interference;
- There is currently no standard phraseology to report and acknowledge interference occurrences or for *emergency climbs*;
- ANSPs, Operators, and Regulators operating near "hot zones" may need to manage thousands of occurrence reports via the current regulatory provisions and databases. This activity overloads aviation stakeholders, putting extreme demands on administrative resources.

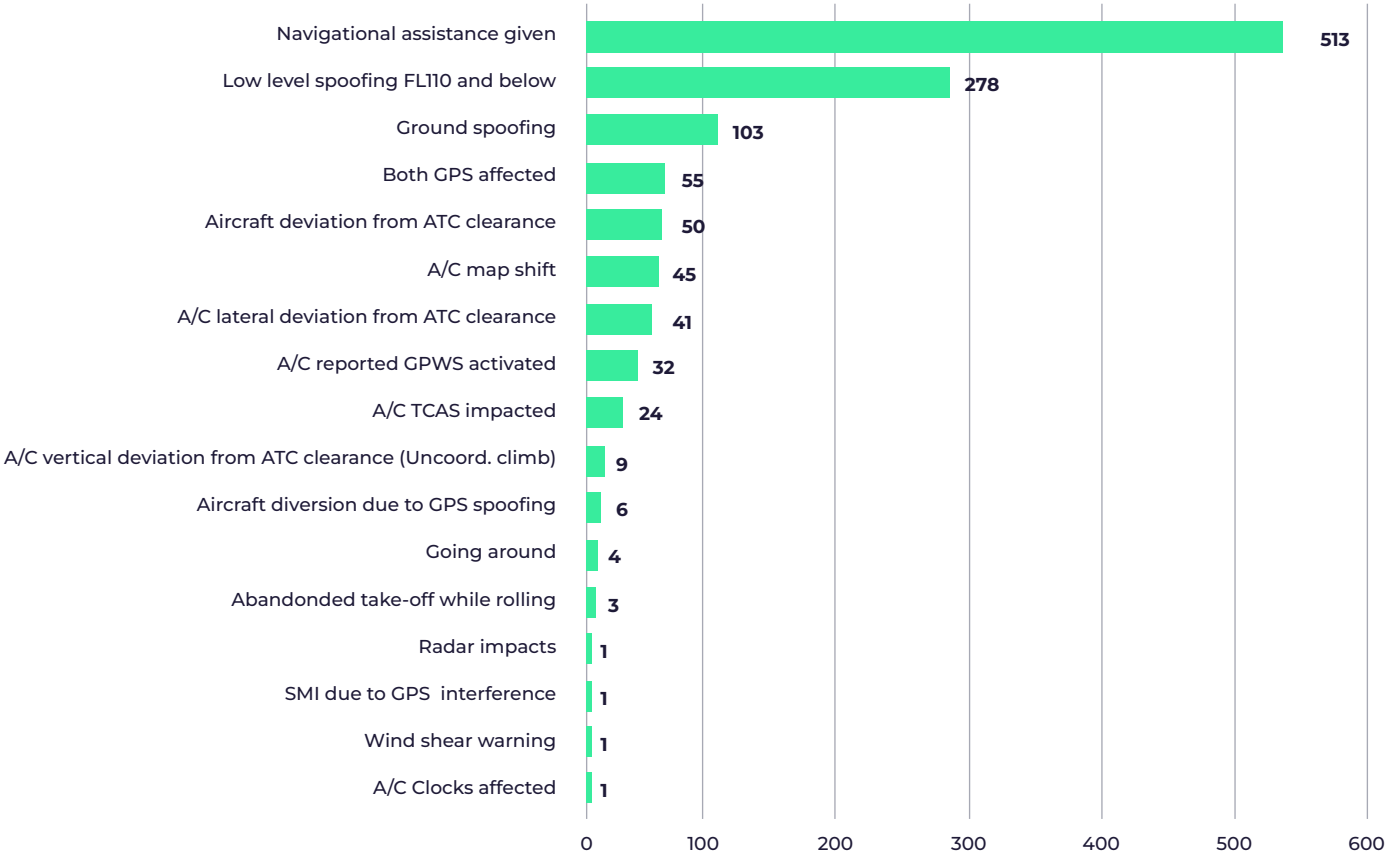
3 Summary Of Impacts To One FIR Operating Adjacent To A Conflict Zone

One impacted flight information region (FIR), which operates in close proximity to a conflict zone, provided the following summary of *GNSS Interference Occurrence Reports* filed by controllers, based on flight crew reports over the year 2024. Detailed information is provided in Attachment A from case studies of spoofing occurrences that resulted in vertical and lateral deviations from ATC clearances for aircraft on final, on approach, on departure and enroute; separation minima infringement, and; impact to radar systems.

In 2024, the impacted FIR reported a total of 2653 GNSS Jamming and Spoofing reports filed. Because only reported occurrences are included, and there are no clear reporting procedures, the actual numbers are likely higher.

- Of the 2653 occurrences reported, 799 were classified as GNSS spoofing, or a ratio of 3:7 spoofing to jamming events;
- 48 per cent of the spoofing occurrences have been classified as ground and low-level spoofing at or below Flight Level 110;
- 13 per cent of the spoofing occurrences have been classified as ground spoofing;
- 513 of the 2653 occurrences required radar vectors (navigational support) by ATC, due to inability to self-navigate;
- 381 of the 2653 occurrences were related to ground and low-Level jamming or spoofing at or below Flight Level 110;
- 50 of the 2653 occurrences were classified as *Aircraft Deviation from ATC Clearance;*
  - Of those 50 aircraft deviations, 41 were classified as *Aircraft Lateral Deviation from ATC Clearance* and nine as *Aircraft Vertical Deviation from ATC Clearance*;
  - The *Aircraft Vertical Deviation from ATC Clearance* occurrences have been defined as *Uncoordinated Climbs* or *Emergency Climbs*;
  - One of the Uncoordinated Climbs resulted in a separation minima infringement with another aircraft at Flight Level 380;
- 32 of the 2653 occurrences resulted in GPWS activation;
- 24 of the 2653 occurrences resulted in TCAS problems;
- Further impacts included abandoned take-offs during rolling, missed approaches, and one impact on radars.

Specific Impacts on Aircraft and ATC due to GPS Jamming or Spoofing for 2024



3. Mitigating the Effects of GNSS Interference

ICAO Air Navigation Conference 14 recommended that States ensure that effective GNSS RFI mitigation measures are implemented based on measures developed by ICAO and industry, including the need to maintain a sufficient network of conventional navigation aids to ensure operational safety and sufficient airspace capacity during times of GNSS interference. ICAO Doc 9849, GNSS Manual, Chapter 5, GNSS Vulnerability, and Appendix F, GNSS Radio Frequency Interference Mitigation Plan, as well as a number of State and Industry prepared technical and safety bulletins, reports, and information papers provide substantive information to aid ANSPs in mitigating operational impacts and safety risk associated with GNSS interference.

ATM approaches to mitigating the effects of GNSS interference include, both, tactical actions for managing and assisting affected aircraft and strategic approaches by ANSPs and regulators to minimise the risks of interference events and to maintain airspace efficiency and safety. Additional emphasis is provided on spectrum management practices, to ensure resilience to RFI and on the use of safety intelligence to support effective GNSS risk management.

1. Tactical and Strategic Mitigations

ATM tactical mitigations by ANSPs and ATCOs to deal with real time effects of impacted aircraft include:

- Provide relevant and timely information and GNSS RFI alerts to airspace users as appropriate, e.g., through ATIS, NOTAMs, AIC, AIP, etc;
- Ensure ATM personnel are made aware of GNSS issues via alerts, bulletins and briefings;
- Ensure that flights impacted by GNSS RFI are instructed (by NOTAM) to inform ATC so that ANSPs can plan route realignment and other mitigations for longer-term RFI issues;
- Where GNSS RFI results in increased air traffic complexity in a sector, at an airport, or more broadly, Traffic Management Initiatives (TMIs) should be initiated until airspace impacts are resolved.
- ATC personnel should be aware of potential for traffic overload, due to increased complexity in impacted airspace, and take action to maintain an appropriate level of safety, considering the level of impacts to the airspace;
- Ensuring clear and effective communication with pilots is critical, as both parties must adapt to the loss of navigation aids;
- ATCOs should be prepared to provide navigation assistance to aircraft, using radar vectoring (if available), as long as needed;
- ATCOs should monitor traffic for signs of GNSS interference to prevent any lateral or vertical deviation from ATC clearances;
- In areas affected by GNSS jamming/spoofing, promote the use of conventional navigation flight procedures;
- Introduce a quick GNSS reporting mechanism. For example, when pilots report RFI over the radio, ATCOs can record the event on a short ATC board template. Safety management should then, each day, monitor and analyse the GNSS reporting;
- Utilise frequent consultations and safety data sharing with local aviation stakeholders (competent authorities, ATM/ANS ANSP, CNS ANSP, local airlines);
- Ensure sufficient staffing for procedural ATC sectors/ units to handle increased workload associated with impacted operations.

a. **Strategic activities** have been identified for ANSPs and State Regulators to ensure safe and resilient operations:

i. Threat Assessment

- Conduct a national threat assessment to determine the likelihood and effects of GNSS vulnerabilities and preparedness to ensure operational continuity, and apply, as necessary, recognised and available mitigation methods;
- Conduct local GNSS safety surveys to ascertain the readiness of a facility and its personnel to tactically respond to and manage GNSS RFI incidents, with results and guidance disseminated.

ii. RON/MON

Retain specific ground-based navigation aids as part of a RON or MON to ensure operational safety and continuity during times of GNSS interference. CANSO has published **Guidelines for Implementing a MON: Using Conventional NAVAIDS for Contingency During a GNSS Outage**, as a source for considerations and best practices in conducting an operational analysis of contingency operations to mitigate potential GNSS RFI outages. Listed below are strategic considerations for MON or RON:

- When conventional navigation systems are used to mitigate impacts for air carrier aircraft, give priority to retention of DME in support of Inertial Navigation System (INS)/DME or DME/DME area navigation, and of instrument landing systems at selected runways;
- When conventional navigation systems are used to mitigate impacts for non DME/DME aircraft, retain VHF Omnidirectional Range (VOR) systems to provide a minimum en route capability in the FIR to ensure safe recovery during GNSS disruptions;
- Maintain a conventional enroute network in the FIR for redundancy to the RNAV route, direct route and free route network;
- Provide ATCO refresher training and frequent tests to confirm that crews are competent to operate with only the MON/RON, and that aircraft and ATC systems will allow use of the MON/RON even in the presence of spoofing.

iii. Conventional navigation procedures

Maintain conventional standard arrival and standard departure routes for redundancy to the RNP Standard Instrument Departures (SIDs) and Standard Terminal Arrival Routes (STARs);

- Maintain conventional instrument approach procedures for redundancy to the RNP instrument approach procedures;
- In high impact areas, ATC may consider authorising only conventional SIDs, STARs and instrument approach procedures;
- Allow for realisation of the full advantages of on-board mitigation techniques, particularly INS.

iv. Surveillance

- Ensure surveillance coverage is resilient to GNSS interference.

v. Contingency planning

- Enhance procedures for airspace contingency and reversion planning, so aircraft can navigate safely even if interference occurs, including in cases of large-scale jamming and/or spoofing events and planned RFI exercises.

vi. Monitoring, Alerting and Reporting

- Several monitoring tools are now available and are being developed. These tools should be utilised to better understand the prevalence of interference activity. Attachment B provides an overview of GNSS interference metrics that may be accessed through the Aireon Safety Dashboard, which is one toolset that is currently available;
- Use ADS-B provided aircraft GNSS satellite tracking information to identify areas where GNSS service is unavailable due to jamming;
- Improve air traffic system automation capabilities to verify aircraft position relative to planned track to alert controllers of potential GNSS spoofing;
- Report to ICAO cases of harmful interference to the GNSS that may have an impact on international civil aviation operations;
- Coordinate with the State spectrum regulator to establish GNSS RFI monitoring, notification, and mitigation processes;
- A simplified GNSS jamming and spoofing occurrence reporting mechanism would ease administrative workload, especially for heavily impacted FIRs.

vii. Training

- Include GNSS jamming and spoofing in ATCO training, and promote joint ATCO-pilot simulations with GNSS jamming and spoofing scenarios.
- Provide all ATM personnel with training based on real occurrence examples and lessons learnt.
- Provide ATCO refresher training on use of conventional navaids, where needed, to enable efficient fallback from GNSS/PBN procedures.

viii. Military cooperation

- Better utilise military ATM capabilities, including tactical air navigation networks and real-time airspace GNSS incident monitoring;
- Improve civil-military coordination, including the sharing of GNSS RFI event data and planned RFI exercises.

ix. Regulatory controls

- Develop and enforce a strong regulatory framework governing the use of global navigation satellite system repeaters, pseudolites, spoofers and jammers;
- Tighten controls (including possession, export and licensing restrictions) on jamming devices.

x. Industry and Regional Collaboration

- Publish standards and guidance material for the aviation community to address concerns, such as a lack of consistency in how flight crews report occurrences or respond to certain alerts, and the lack of phraseology for emergency climbs;
- Occurrence reporting standards and regulations should be enhanced and clarified;
- Collaborate on initiatives, presentations and safety data sharing with: ICAO; EASA; US FAA; Competent Authorities; Eurocontrol Safety Team, SAFOPS Group, EVAIR; CANSO; European Aviation Crisis Coordination Cell (EACCC); other ANSPs; Airlines; OpsGroup; Local and Regional events/workshops;
- Work through the ICAO Planning and Implementation Regional Groups (PIRGs) to develop regional or global navigation satellite system reporting mechanisms, as described in the GNSS Manual (Doc 9849);
- Work with industry to provide guidance on detecting GNSS jamming or spoofing and maintaining safe and efficient aircraft operation in case of global navigation satellite system anomalies;
- Develop standards to allow ADS-B to use DME/DME position information during GNSS jamming events;
- Develop standards to allow ADS-B aircraft to use own-ship-multilateration position for navigation purposes during GNSS disruptions to allow the aircraft to proceed safely to an airport;
- Establish standards for avionics manufacturers to verify aircraft position information from multiple sources to improve detection of GNSS spoofing.

Safety Intelligence to Monitor GNSS Interference Related Risk

ANSP safety performance is determined by ability to implement and maintain safety intelligence capability at a level that is sufficient to inform safety decision making and risk mitigation across operational and technical domains.

GNSS spoofing and jamming threats represent emerging risks to the safety of aviation operations. Understanding the sources, impacts, locations, and risk mitigations that an ANSP can implement is vital.

ANSP safety intelligence activities should be formally planned, structured, and executed to establish barriers that are effective in detecting, monitoring, and mitigating GNSS threats.

Surveillance data, separation standards, and reporting requirements provide the framework for risk mitigation activities.

a. Understand the environment and technical capability

ANSP surveillance capability varies widely. At its lowest level of maturity where data is wholly derived from primary surveillance radar, the risk does not exist. Where an ANSP's surveillance capability is wholly reliant upon GNSS-derived position data, the risk exposure is at its greatest extent. Understanding how surveillance data is derived is the starting point for an ANSP's GNSS risk management activity.

It is just as important for ANSPs to understand how communication applications, such as CPDLC, use GNSS-derived precision timing information.

b. Separation standards

Nation States define the requirements for separation of aircraft within controlled airspace. Separation standards are designed to conform with the provisions of ICAO Doc 4444 (Procedures for Air Traffic Management). Methods of achieving separation are varied and complex[1]. Understanding what these separation standards are and if they have been compromised by GNSS interference is a key aim of safety intelligence activity.

c. Minimum requirements

Reporting of GNSS interference events by pilots and air traffic controllers provides manual inputs to an ANSP's safety management system at the lowest level of capability. Manual reporting can be complemented by automatically derived data.

1 Loss of Separation | SKYbrary Aviation Safety

d. Risk mitigation

Risk mitigation is informed by data monitoring and analysis. These activities should be designed to provide a complete and accurate picture of the prevailing threats and performance of an ANSP's risk management barriers.

Using fields collected and derived from ADS-B messages can help identify position anomaly events related to GNSS interference. Examples of this include, the Position Integrity Category (PIC), an industry standard for measuring position quality that is also used as an indicator for interference and possible jamming from ADS-B data, and the Independent Position Check (IPC), an Aireon unique measure of possible spoofing through time difference of arrival (TDOA), only possible with its global satellite network and collection of ADS-B data. Further details of the application of these two fields appears in Attachment B.

The PIC provides the estimated error of the position broadcast by the aircraft and is represented as an integer value between 0 and 14, with each value mapped to a specific error in distance as depicted in the table below. Reports of fewer than seven is considered an incident.

PIC	Integrity Containment Bound
14	< 0.004 NM
13	< 0.013 NM
12	< 0.04 NM
11	< 0.1 NM
10	< 0.2 NM
9	< 0.3 NM
8	< 0.5 NM
7	< 0.6 NM
6	< 1.0 NM
5	< 2.0 NM
4	< 4.0 NM
3	< 8.0 NM
2	< 10.0 NM
1	< 20.0 NM
0	No integrity (or > 20.0 NM)

While the PIC value is useful, it is insufficient on its own to understand the full potential impact to the safety of navigation. Recognising this shortfall, Aireon, in collaboration with the CANSO Safety Intelligence Work Group, developed the IPC value. This calculation identifies offsets from aircraft-derived positions. This is performed through a Satellite Wide Area Multilateration (SWAM) application that uses TDOA measurements from simultaneous detection of ADS-B transmissions on multiple satellite payloads. This solution leverages traditional multilateration techniques used by terrestrial systems, but applied via satellite. This is possible due to both the Iridium constellation, with its significant overlapping satellite coverage, and the ability to accurately track the position and timing of each satellite (on the order of hundreds of nanoseconds), which is processed by Aireon[2].

Safety intelligence planning should provide mechanisms to detect, report, assess, mitigate, and monitor GNSS threats. ANSP preparedness and defensive activities include:

- Recognition that GNSS spoofing and jamming threats pose increasing risks to aviation safety;
- Assessing the maturity of an ANSP's surveillance capabilities to mitigate risk exposure;
- Safety intelligence activities that are structured and data-driven to detect, assess, and mitigate these threats;
- Delivery of safety intelligence insights that enhance and augment manual reports from pilots and air traffic controllers with objective data gained through automated sources, and
- Hotspot identification, trending, and barrier management performance analysis informed by data sources that underpin risk management activities.

2 Aireon White Paper | Space-based ADS-B for GNSS-independent position validation

The role of Spectrum Management in Mitigating Radio Frequency Interference

Managing GNSS signal spoofing and jamming through effective spectrum management is an essential foundational layer in a comprehensive defense strategy. This requires a shift from a passive to an active spectrum management paradigm by States and ANSPs, and is achieved by combining tactical, strategic and operational initiatives, such as: implementing regulatory protections, real-time monitoring, signal processing techniques and strengthening international cooperation to improve resilience and stability of GNSS signals. Effective spectrum management in aviation is necessary to ensure interference free and efficient operation of radio services (e.g. air/ground communications and radio navigation) resulting in reliable positioning, navigation and timing (PNT) services.

Following are some of the key strategic and operational approaches recommended for States and ANSPs to manage GNSS signal interference through spectrum management:

a. Continuous detection and monitoring of aviation spectrum

- This initiative is focused on creating a monitored and regulated electromagnetic environment. It involves deployment of GNSS signal interference detection and monitoring tools, such as the GNSS interference metric on the Aireon Safety Dashboard, to detect and locate interference sources. Employment of GNSS signal interference detection tools with spectrum analysing, AI-based anomaly detection and adaptive filtering capabilities are recommended to help identify areas with prevalent GNSS signal jamming and spoofing problems. Other related solutions can include deployment of terrestrial monitoring networks through a grid of stationary sensors around sensitive areas (i.e. aerodromes, GNSS stations, etc.) to monitor GNSS frequencies. The data received from these sensors, after the successful detection of anomalies and location of ground-based emitters, can be fused into a common operational picture for real-time alerts.

b. Regulatory and policy measures

- States should work with ANSPs and law enforcement agencies to enforce International Telecommunication Union (ITU) Radio regulations to promulgate anti-jamming/spoofing laws to prevent harmful GNSS signal interference, especially from adjacent bands. This can be achieved through enacting and enforcing laws with severe penalties for the operation of GNSS jammers and spoofers around sensitive areas (i.e. aerodromes, GNSS stations, etc.). A tactical solution can involve licensing and compliance where spectrum certification is granted for devices (i.e. 5G, non-ATM radars and IoT) operating near GNSS frequencies. Other operational initiatives can include public awareness programs to educate the public about the dangers and illegality of using personal “privacy” jammers. Through this initiative, ANSPs, operators and users will be required and encouraged to report GNSS signal interferences via national agencies.

c. Strengthening international cooperations

- States should work with ITU and coordinate with ICAO to harmonise GNSS spectrum protection by designating GNSS bands (e.g. GPS L1, Galileo E1, Glonass G1, GPS L5, Galileo E5, Glonass G2, Beidou, etc.) as protected spectrum with strict emission limits. This coordination must also involve establishment of cross-border protocols for addressing GNSS signal interferences from neighboring countries.

d. Technical mitigation techniques:

- States should work with aviation ecosystem stakeholders to consider promulgating frequency exclusion zones and buffer zones at/around aerodromes. Tactical mitigation strategies can also involve downward tilting of 5G antennae and limiting power of transmitters. This is necessary due to the fact that GNSS signal arriving at the antenna is much weaker than the unjammed noise seen by the receiver. Any nearby radio transmitter (i.e. cellphones, LTE, WiFi, broadcast radio, VHF radios) can easily overload the sensitive amplifier in the GNSS receiver. This can be considered as superficial GNSS jamming due to frequency spectrum environment within the proximity of the aerodrome. There is therefore a need to manage strong signals outside the GNSS frequency bands (e.g. 5G or cellular signals) from overloading the front-end amplifier, causing desensitisation or complete failure.
- Other technical initiatives can include filtering and shielding techniques that involve the use of bandpass filters to block out-of-band GNSS signal interferences. Manufacturers are encouraged to produce spectrum-compliant designs and develop GNSS systems with signal processing enhancements, including appropriate RF spectrum filtering and satellite signal tracking to improve resilience to GNSS signal interference. Manufacturers are also encouraged to develop jamming resistant GNSS receivers with multi-frequency, multi-constellation capabilities to mitigate narrowband jamming.

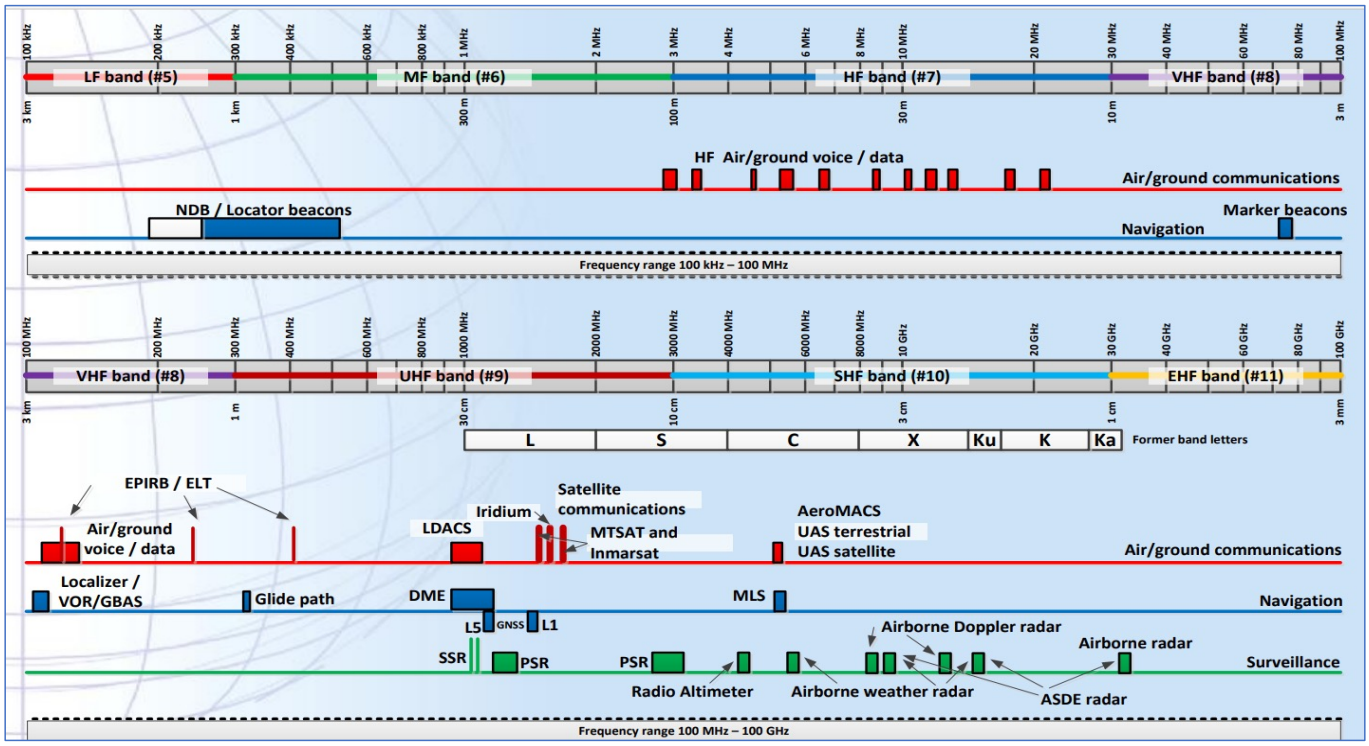


Figure 2: Spectrum Allocations to Aeronautical Services Utilised by Civil Aviation

The protection of radio frequency spectrum for civil aviation is a matter of safety and efficiency. It ensures that critical systems for CNS are free from some GNSS harmful interferences, allowing aircrafts to operate safely. The ITU as a specialised agency of the United Nations (UN), has designated the specific frequency bands, in Figure 2, as primary allocation for specific aviation services (e.g., aeronautical mobile service, aeronautical radionavigation service).

These allocations are made at World Radiocommunication Conferences (WRCs). This therefore implies that aviation ecosystem has primary allocation, meaning it has priority over other services in the above depicted bands. As such, States and ANSPs need to ensure that adjacent bands do not cause harmful interference to existing systems. In addition we should ensure that secondary services are not allocated in the GNSS spectrum.

4. Further Considerations

In addition to current and short-term mitigations, ICAO, States and industry are urgently exploring medium and long term technical solutions to increase resilience to or prevent GNSS RFI. A key concern is how to balance the need for quick, easy, cost-effective solutions at the GNSS sensor levels with longer-term, robust solutions at the CNS (air and ground) system level.

ICAO Assembly Resolution A42-8 and Industry signal agreement on key strategies to address the evolving threat from GNSS RFI, including:

- The need for ICAO to expedite efforts to standardise GNSS RFI related solutions, including complementary position, navigation and timing (C-PNT) and alternative PNT (A-PNT), signal authentication for GNSS core constellations and augmentation services;
- Support for a multi-faceted approach for mitigating GNSS RFI, including the development of real-time GNSS monitoring, detection, analysis and reporting systems;
- The need for a comprehensive review framework to ensure the overall resilience of CNS/ATM systems and services;
- The need to support States in planning and implementing the new concept for NAV RON.

These longer-term solutions must be supported by continued investment in near-term tools for ATM, policies, procedures and training to support air traffic operations, and continued vigilance to anticipate, identify and address emerging RFI threats.

5. Additional Guidance Material and References

The reference materials in this section were instrumental in producing this guidance document: CANSO recommends that ANSP members become familiar with these materials, and utilise them as appropriate to their specific operational needs. It is important to keep in mind that GNSS interference, and other forms of RFI, is an evolving threat. New materials continue to be developed and some of the materials in this section will be updated or superceded, requiring ANSPs to ensure they have the most recent information pertaining to their operation.

ICAO:

- ICAO Doc 9849, GNSS Manual, Chapter 5 and Appendix F
- Annex 10, Vol I, Radio Navigation Aids
- ICAO Fourteenth Air Navigation Conference (AN-CONF/14) – Conclusions
- ICAO Assembly 42nd Session, Working Paper 34, Global Navigation Satellite System (GNSS) Radio Frequency Interference (RFI)

State regulations:

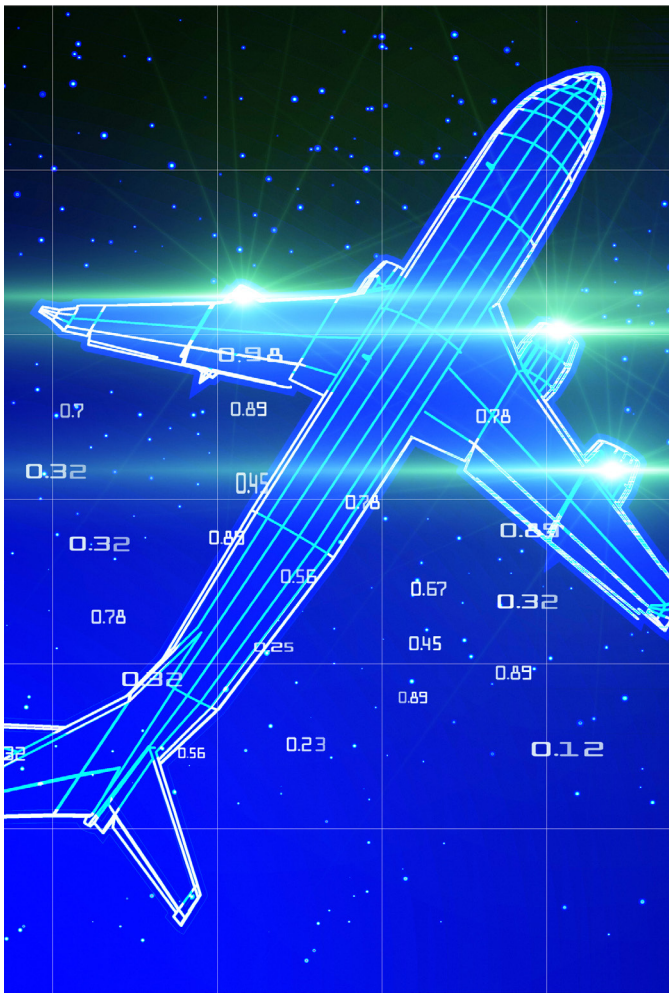
- Eu REG.2020/469 amending 2017/373 (from 27 January 2022)

Safety and technical information bulletins:

- ATA: 30 March 2023
- EASA: 2022-02R3, 05 July 2024
- FAA: SAFO 24002, 25 Jan 2024
- SINGAPORE: 2022-01 R3, 11 Jan 2024
- CAA UK: SN-2025/006, 30 Apr 2025

Papers/Reports:

- US Federal Aviation Administration, Flight Technologies and Procedures Division: Jamming and/or Spoofing; GNSS Interference Resource Guide 2026, Version 1.0, 4 Dec 2025. **GPS and GNSS Interference Resource Guide**
- CANSO: Guidelines for Implementing a Minimum Operational Network (MON), 14 March 2025
- OPSGROUP: GNSS Spoofing; Final Report of the GNSS Spoofing Workgroup, 6 Sep 2024. **GPS-WG-FinalReport_v2.4** (ops.group)
- IATA: Global Navigation Satellite System GNSS-Radio Frequency Interference Safety Risk Assessment, 4 Sep 2024, **Global Navigation Satellite System GNSS Radio Frequency Interference**
- Cyprus DCA Flyer on GNSS SPOOFING Ed.1 - September 2024 (Attachment C)



Attachment A: Air Traffic Control RFI Occurrence Case Studies

Sharing case studies of recorded occurrences related to GNSS RFI supports the need for training based on lessons learned and may serve as triggers to create objectives and scenarios for Air Traffic Controllers and Pilots simulator training. This section includes case studies of occurrences by an impacted FIR that operates in close proximity to a conflict zone, followed by a discussion of the downing of Azerbaijan Airlines Flight 8243.

I. Reported GNSS RFI occurrences from an FIR operating proximal to a conflict zone

1. Spoofing on Approach: Aircraft uncoordinated Climb (Vertical Deviation from ATC Clearance) on the ILS/VOR approach at International Airport 1 with published missed approach altitude 2000 feet

April 2024, under CAVOK conditions, aircraft under Tower procedural control, at 3000 feet, on the outbound leg of the ILS/VOR approach, reported "going-around" in response to GPWS Alert.

The aircraft initiated an uncoordinated climb, with 4700 feet vertical speed, without ATC clearance to 6500 feet due to reported GPWS alert. The mode S intended level has been overshot by 500 feet. The aircraft has been released to the Approach Surveillance Service, vectored to final and landed safely.

2. Spoofing on Approach: Aircraft uncoordinated Climb (Vertical Deviation from ATC Clearance) on the ILS/VOR approach at International Airport 2 with published missed approach altitude 2000 feet

Similarly to occurrence one, the aircraft initiated an uncoordinated climb, with 4600 feet vertical speed, without ATC clearance to 8000 feet due to reported GPWS alert. The mode S intended level has been overshot by 900 feet. The aircraft has been re-cleared for a conventional ILS/VOR approach and landed safely.

3. Spoofing on departure: Aircraft Lateral Deviation from ATC Clearance at International Airport 1

April 2024, under CAVOK conditions, aircraft under surveillance approach service, after take-off from international airport 1 turned to the right instead of left.

The ATC clearance was for a conventional Standard Instrument Departure to the east over water, but the aircraft after take-off turned to the right towards high terrain and opposite to other inbound aircraft. Conflict detected and resolved through vectoring by approach surveillance service.

4. Spoofing enroute: Separation Minima Infringement (SMI) in response to GPW at FL370

June 2024, early morning, weather not relevant, aircraft at FL370 responded to a GPW and initiated an uncoordinated climb without ATC clearance. At that moment there was an opposite direction traffic at FL380. The standard 1000 feet separation was lost. The Area Radar Control Centre, early detected the conflict through monitoring the mode C deviation and the Level Deviation safety net. ATC responded by providing essential traffic information to the aircraft which climbed up to FL374, before descending back to FL370.

5. Spoofing on Radars

August 2024. At one sector of the Area Radar Control Centre, all targets on the radar screen shifted from their current position to previous position for approximately five seconds. Two targets at the FIR boundary were lost. The CNS engineer's immediate assessment indicated that three of the five radars have been impacted due to the time synchronisation of the radars which were using the radar GNSS clocks. Technical mitigation solutions have been implemented immediately by deselecting the radars' GNSS antennas and using a combination of the radars' internal clock supported by manual synchronisation with another ground time reference system. The system manufacturer has been informed and involved. The mitigation is daily monitored to confirm the measures' effectiveness. It appears that, so far, these mitigations are working well.

II. Azerbaijan Airlines Flight 8243

Jamming and Spoofing

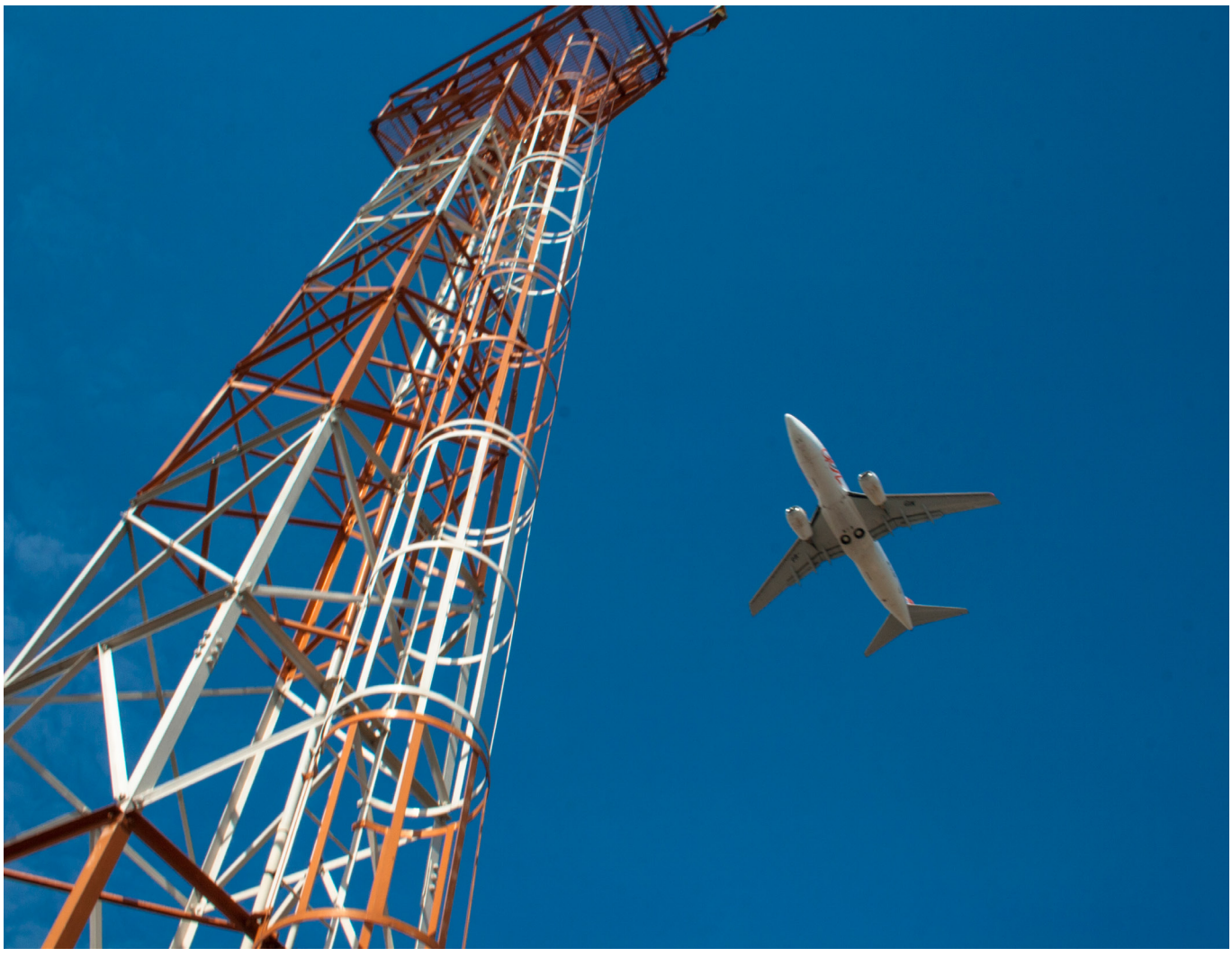
Azerbaijan Airlines Flight 8243, an Embraer 190, departed Baku, Azerbaijan on December 25, 2024. The flight was enroute to Grozny, Russia, where dense fog had been reported.

About 30 minutes after departure, the pilot reported loss of GPS; this was followed by its position being spoofed.

As AZAL8243 neared Grozny, the pilot, again, reported “lost both GPS,” and requested vectoring for an NDB approach. Soon after, a false TAWS alert was received, followed by a time shift that was captured by the FDR. AZAL8243 again requested and received vectors for an NDB approach. However, about 13 minutes later, at 04:53:55, the pilot reported “going around, non-stabilised approach,” and requested vectors for another approach.

The controller asked for confirmation that the flight was requesting an RNAV GNSS approach. The pilot reported “No GNSS approach, lost both GPS,” and the controller responded with “expect RNAV GNSS approach…” The pilot, repeated the loss of both GPS and requested vectors for the NDB approach. As the aircraft was being vectored and nearing the airport, additional communications reveal a discrepancy in altitudes displayed to the pilot and controller, quickly followed by AZAL8243 stating that it would divert to Baku. The controller cleared the aircraft to a waypoint, prompting AZAL8243 to again report “both GPS lost, requesting vectoring.” As it was departing the Grozny area, the aircraft was struck by a missile, which precipitated loss of control surfaces and flight systems.

AZAL8243 continued its flight across the Caspian Sea and was attempting an emergency landing to Aktau, Azerbaijan when, at 06:28, it crashed. The crash resulted in 38 fatalities and 29 survivors.



Attachment B: Aireon Monitoring Tools

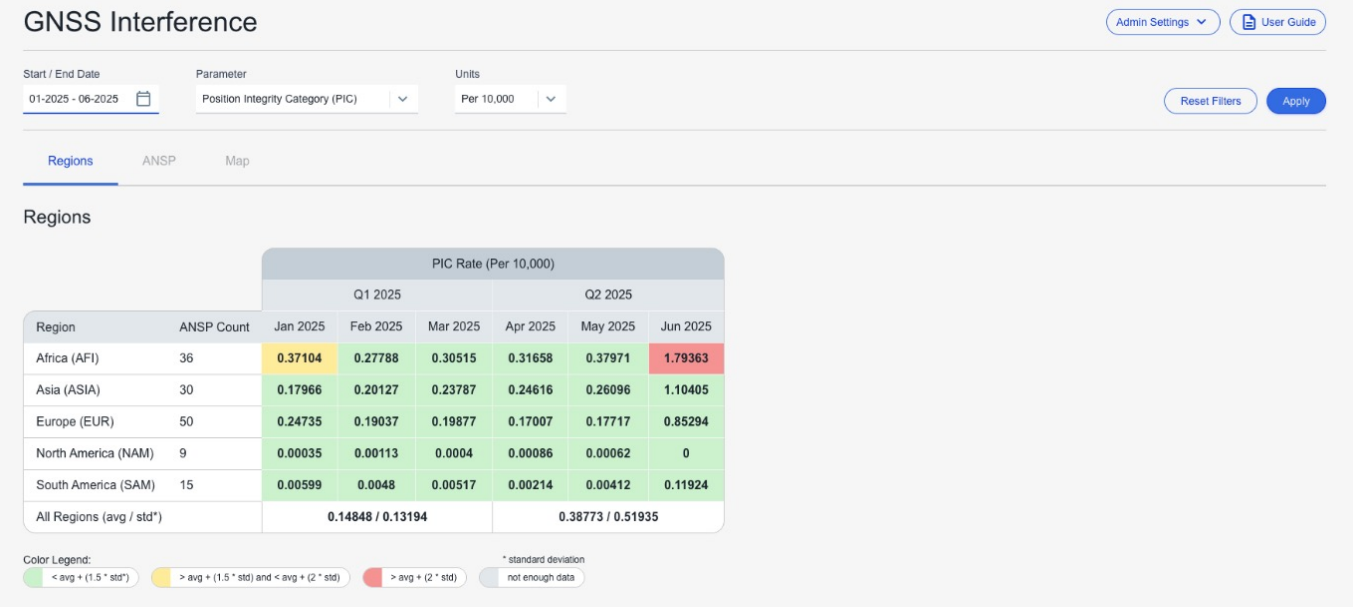
Aireon Safety Dashboard

Aireon customers with access to the GNSS Interference metric on the Aireon Safety Dashboard product are provided with a comprehensive view of the GNSS signals in their airspace, specifically targeting deliberate interference with global satellite navigation systems. This helps identify potential threats, but also empowers users to take proactive measures. Data is available in aggregate by month with a historical backlog dating back to 2023.

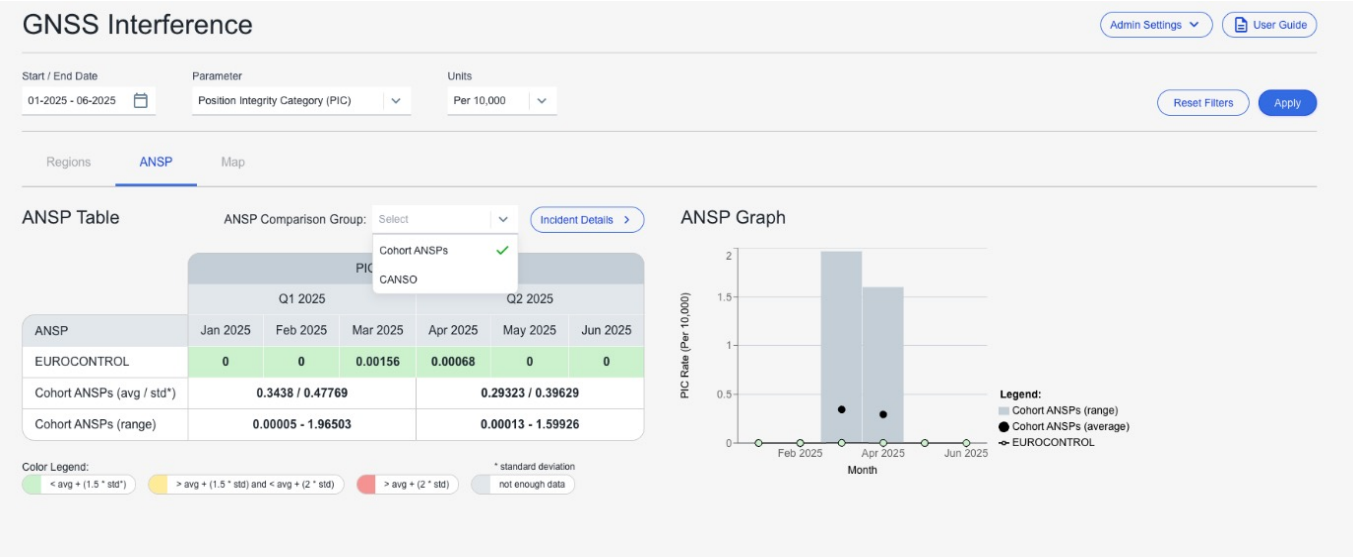
Key features of the GNSS Interference metric include:

- Trending of Position Integrity Category (PIC) values, an industry standard for measuring interference and possible jamming from Automatic Dependent Surveillance-Broadcast (ADS-B) data;
- Trending of Independent Position Check (IPC) values, an Aireon unique measure of possible spoofing through time difference of arrival (TDOA), only possible with Aireon's global satellite network and collection of ADS-B data;
- The summary view, depicted below, shows the most recent GNSS interference trends for the user's ANSP compared to its "cohort", or group of related ANSPs;

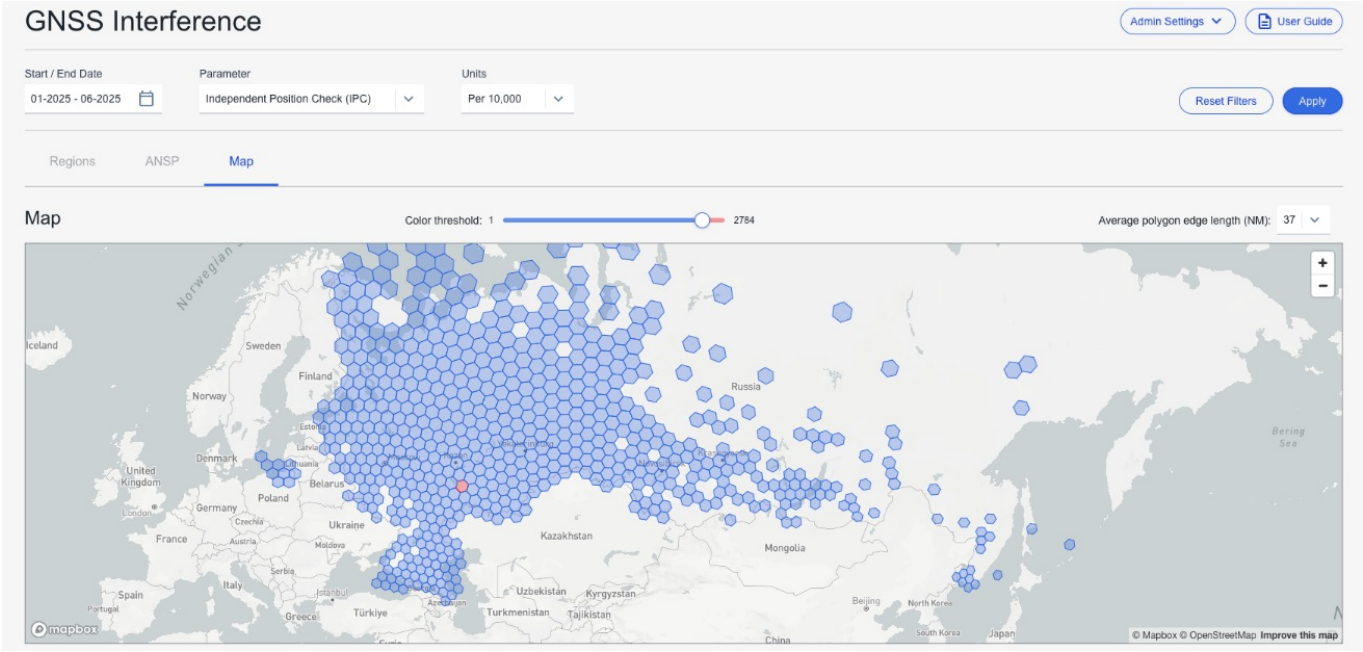
- The regional view depicted below, displays an aggregation for the global rate of GNSS interference for all ANSPs by region and month for either PIC or IPC value;



- The ANSP view displays PIC or IPC rates for the ANSP compared to the cohort of similar ANSPs or for all CANSO ANSP data. Incident details contain a list of all the backend incidents based on the selected parameter selections. Data range includes minimum and maximum rates for the selected ANSP group;

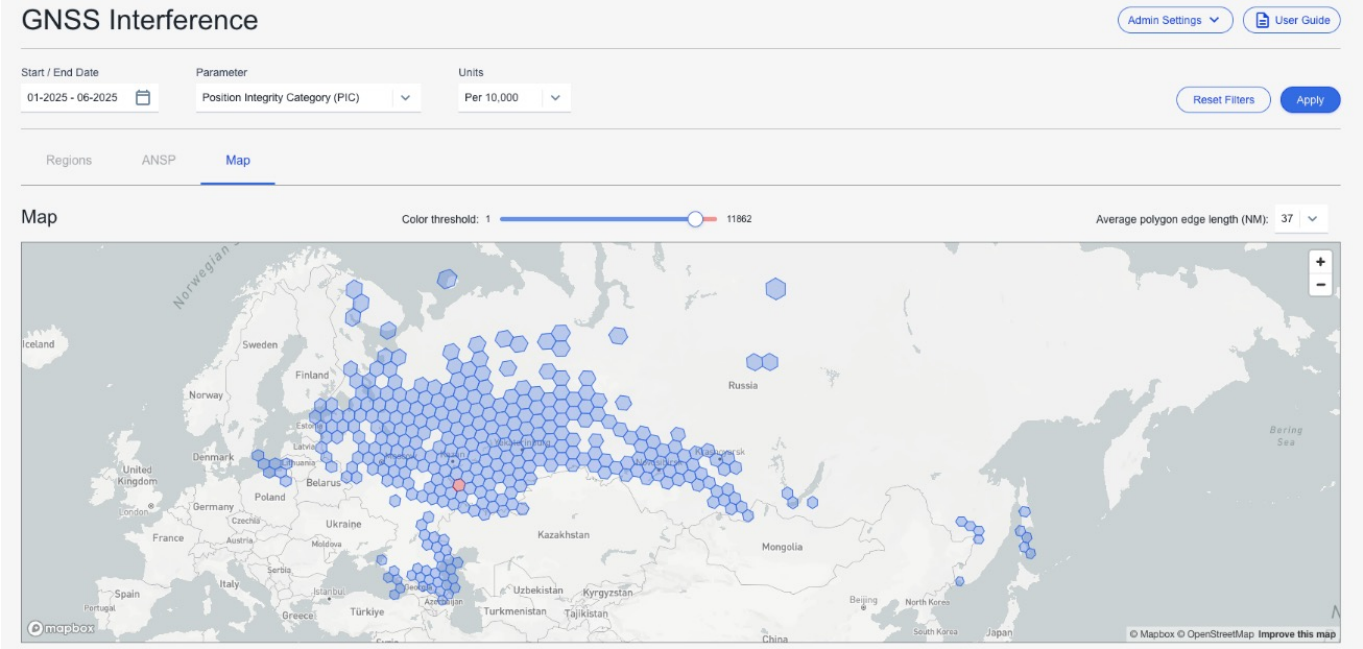


- The map views show heat maps of incident locations based on either PIC or IPC selection, matched with the underlying events detected by Aireon's network;



- The highlighted hexes show areas where there are high concentrations of identified GNSS interference incidents. A hex is identified where at least five targets were present and four per cent or more reported at least four messages with PIC less than seven;

- For IPC, a hex is identified when the IPC is flagged positive three times within 120 seconds or if a sudden, physically impossible jump in the trajectory occurs. Selecting each hex displays further details of the individual incident data as shown below. For every IPC incident, the data shows the highest PIC as a way of indicating whether the two parameters are in sync;



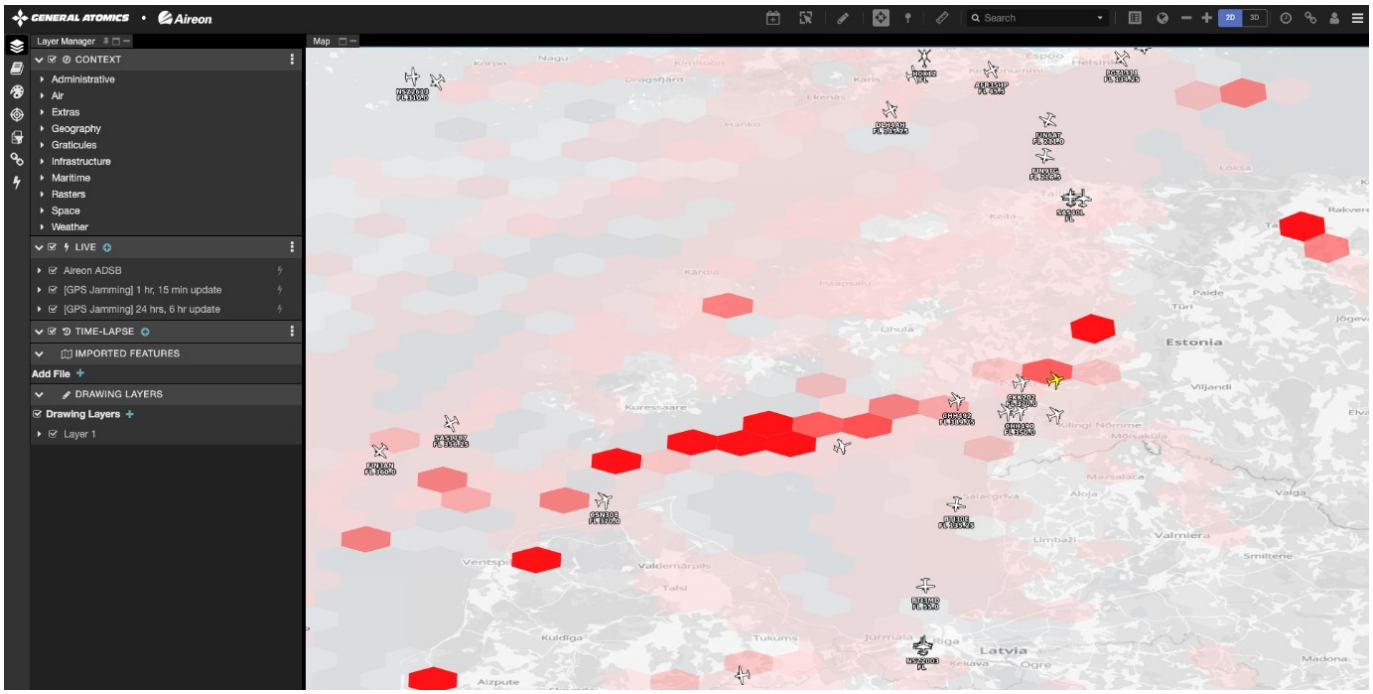
IPC Events: State ATM, Mar 2025 to Jun 2025

Filters | Download | Rows per page: 25 | Showing: 1-3 of 3

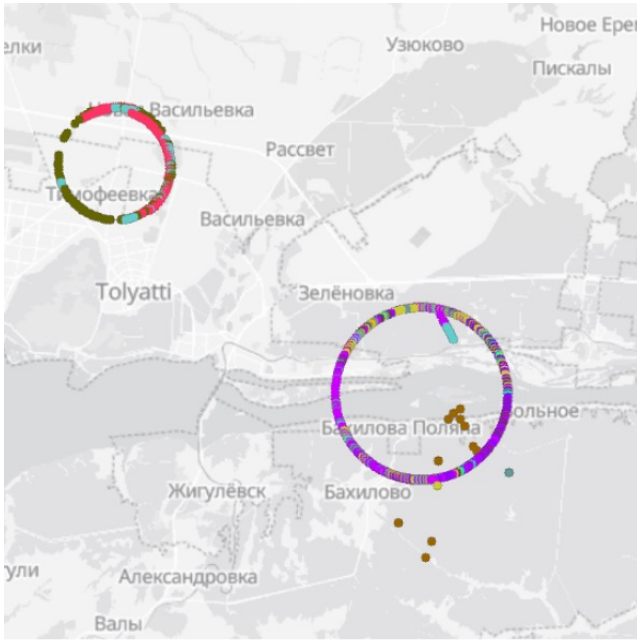
Time of Message Receipt (UTC)	Target Address	ACID	Latitude	Longitude	Altitude (FL)	Track Angle (deg)	Duration (secs)	Ground Speed (kts)	Highest PIC
2025-03-23 02:50:36	7813F9	CSN304	61.83999	63.79751	370	82.07	1536.92	551.07	8
2025-03-30 11:28:57	78149F	CSN607	61.73026	62.56449	360	294.99	162.47	473.29	6
2025-04-13 09:09:33	155C63	RWZ1506	61.47689	63.89353	350	42.32	1303.16	500.32	0

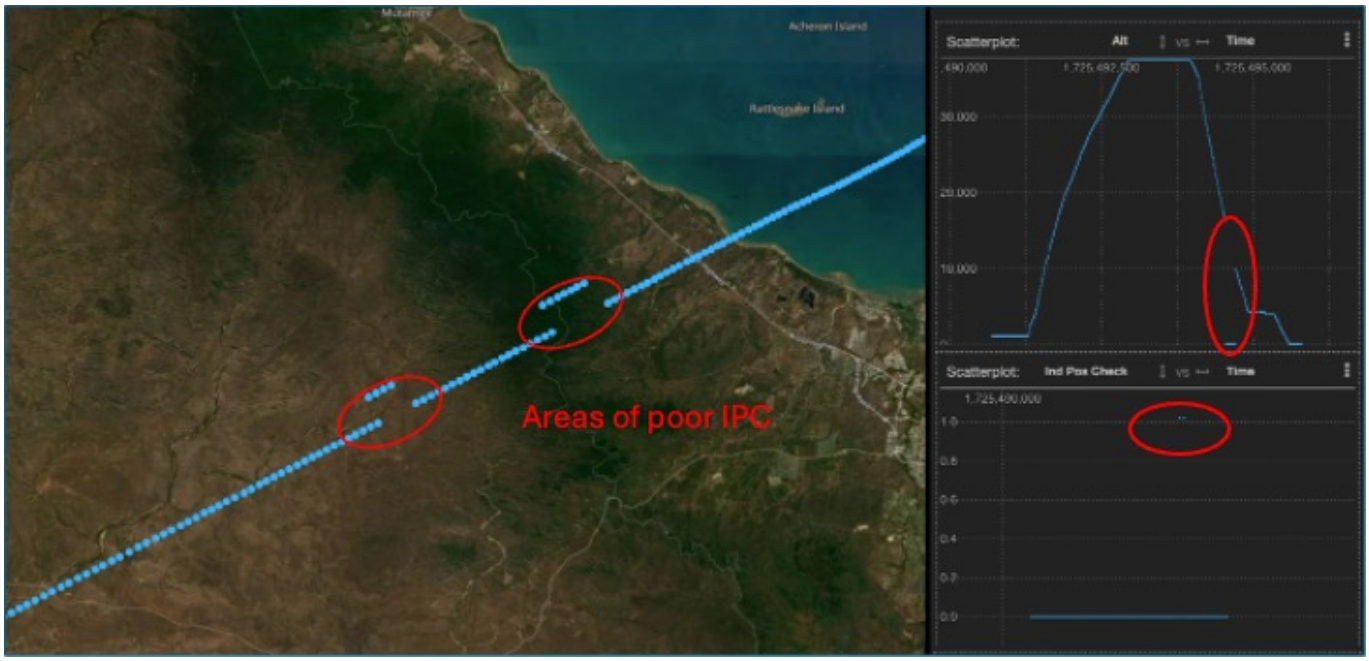
(H3 cell 8310e9fffffffff)

- For real-time analysis of GNSS interference events, the AireonVECTOR Monitor product provides ANSPs live perspective of jamming and spoofing events. AireonVECTOR leveraged Aireon's global, real-time ADS-B data to pinpoint the location of aircraft independent of the GNSS signal via a proprietary algorithm. Interference monitoring via a map visualisation is also available via AireonVECTOR Monitor to help with operational awareness. Visualisation of interference data is available for the previous rolling one-hour or 24-hour period for real time navigation and planning. The map view displays areas of high levels of GNSS interference linked to Aireon's network of ADS-B data. Live traffic can be merged in conjunction with the hotspots along with additional analytical tools to assist investigations, as indicated by the view below;



- The AireonVECTOR Monitor tool also allows users to replay events by providing time and position data. The images below show some historical examples of GNSS interference events based on poor PIC and/or IPC values and their associated flight paths.





Attachment C: The Cyprus' DCA Flyer on GNSS SPOOFING Ed.1 - September 2024

This single page Flyer promotes the executive mitigating actions already taken by the local airlines and the Cyprus ANSP which have proved to be effective and can even be considered as best industry practices.

GPS SPOOFING

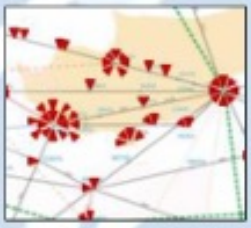
CYPRUS AVIATION COMMUNITY ADDRESSES NEW THREATS – Edition 1 - SEPTEMBER 2024

The geopolitical situation in the south-east Mediterranean warrants urgent measures to assure the safety of flights.

The Cyprus Civil Aviation Authority (DCAC) initiated an ongoing stakeholder consultation with the participation of local airline operators and the main air navigation service provider to share experiences and decide on the best possible measures to mitigate the impact of GPS spoofing[1]. The actions already taken by the airlines and the ANSP have proved to be effective and can even be considered as best industry practices.

These actions include:

From local airline operators:



- Incorporate GNSS Spoofing/Jamming scenarios in Ground and Simulator pilot training;
- Update company policies in accordance with recommendations from Aircraft Manufacturers and the latest EASA guidelines and SIBs;
- Pre-flight preparation: Airline Flight Operations Departments (OCCs) monitor daily active NOTAMS on GNSS Affected airports and airspaces and update operational procedures if and as needed;
- Apply supplementary operational procedures to limit the use of GPS prior to departures and before entering Nicosia FIR;
- Encourage pilots to submit AIRREPs to ATS Units.

From the local ANSP:

- Promote the use of conventional navigation flight procedures;
- Provide navigational assistance to aircraft (using radar vectoring);
- Improve ATCO response to abnormal situations through training and awareness campaigns;
- Issue spoofing warnings via NOTAMs, AIP and ATIS;
- Regularly consult with airspace users for safety data exchanges.

[1] Global Positioning System (GPS) allows aircraft to determine precisely their position using signals by satellites orbiting the Earth. By spoofing GPS signals, military actors can trick aircraft into following incorrect flight paths or even cause them to lose navigation altogether.

CYPRUS CIVIL AVIATION AUTHORITY PROMOTES COORDINATED ACTIONS AGAINST GPS SPOOFING

LOCAL AIRLINES TAKE ACTIVE SAFETY MITIGATION MEASURES

THE AIR NAVIGATION SERVICE PROVIDER REVERTS TO CONVENTIONAL NAVIGATION PROCEDURES

THE CIVIL AVIATION AUTHORITY COMMUNICATES BEST PRACTICES TO EUROCONTROL AND EASA

DEPARTMENT OF CIVIL AVIATION – MINISTRY OF TRANSPORT

27 Pindarou str.
Nicosia 1020
https://www.mcw.gov.cy/

2024

CANSO

canso.org