FRONTIER SI

GNSS SPOOFING DETECTION IN AVIATION USING ADS-B DATA

PNT LABS WHITE PAPER

PNTLabs

April 2026

Contents

Acronyms

Acronym	Full Form
ADS-B	Automatic Dependent Surveillance-Broadcast
ADS-C	Automatic Dependent Surveillance-Contract
AGL	Above Ground Level
ANSP	Air Navigation Service Provider
ATC	Air Traffic Control
ATM	Air Traffic management
CANSO	
CPDLC	Controller-Pilot Data Link Communications
EGPWS	Enhanced Ground Proximity Warning System
ES	Extended Squitter
EW	Electronic Warfare
FIR	Flight Information Region
FMS	Flight Management System
FTC	Field Type Code
ICAO	International Civil Aviation Organization
IPC	Independent Position Check
IPV	Independent Position Validation
IRS	Inertial Reference System
LPV	Localiser Performance with Vertical guidance
MSL	Mean Sea Level
NACp	Navigation Accuracy Category for Position
NIC	Navigation Integrity Category
NM	Nautical Mile
PIC	Position Integrity Category
PNT	Positioning Navigation and Timing
RAIM	Receiver Autonomous Integrity Monitoring
RNP	Required Navigation Performance
RTCA	Radio Technical Commission for Aeronautics
SBAS	Satellite Based Augmentation System
SWAM	Satellite Wide Area Multilateration
TAWS	Terrain Awareness & Warning System
TCAS	Traffic Collision Avoidance System
TDOA	Time Difference of Arrival
TIS-B	Traffic Information Services-Broadcast
WAM	Wide Area Multilateration

1. Introduction

Over the past two years, civil aviation has witnessed an unprecedented rise in GNSS spoofing incidents, posing a serious threat to flight safety, air traffic management, and the broader integrity of aviation's Positioning, Navigation and Timing (PNT) ecosystem. Unlike traditional jamming, which simply denies or blocks GNSS signals, spoofing deceives receivers by transmitting counterfeit satellite signals that appear authentic. This causes aircraft systems to compute false position, altitude, and timing information, which is a far more insidious form of interference, and it is also one that is hard to detect.

Spoofing began to impact civil aviation on a wide scale in late 2023, and its scope expanded dramatically through 2024. According to the *OPSGROUP GPS Spoofing Workgroup Report*, which compiled data and analysis from over 950 industry experts and nearly 2,000 flight crew surveys, more than 41,000 flights were spoofed between July and August 2024, averaging 1,500 spoofed flights per day (OPSGROUP, 2024). The study found that spoofing activity increased fivefold during the year, concentrated in regions surrounding active geopolitical conflict zones, particularly the Eastern Mediterranean, Black Sea, Russia and the Baltic region, as well as India-Pakistan border. These signals, often generated by military electronic warfare (EW) systems designed to disrupt drones or precision-guided munitions, have unintentionally compromised the integrity of civil aircraft navigation systems operating thousands of miles away.

The OPSGROUP report concluded that the impact on flight safety is *extremely significant*, affecting more than a dozen aircraft systems reliant on GNSS data. These include the Flight Management System (FMS), Inertial Reference System (IRS), Enhanced Ground Proximity Warning System (EGPWS), Automatic Dependent Surveillance-Broadcast (ADS-B) and (Automatic Dependent Surveillance-Contract) ADS-C surveillance, Controller-Pilot Data Link Communications (CPDLC), and even cockpit clocks. Spoofing-induced map shifts have led to aircraft tracking off-course, incorrect runway alignment, and false terrain alerts from EGPWS, in some cases prompting go-arounds or level busts near busy airspace. Particularly concerning is the possibility of a *contaminated GNSS receiver* that continues to output plausible, but false data even after leaving a spoofing zone. This poses major implications for RNP-based navigation, EGPWS integrity, and post-event flight safety.

Flight crew feedback collected by OPSGROUP highlighted widespread confusion, inconsistent procedures, and a lack of official technical guidance. Many operators still treat spoofing as a form of jamming, unaware that post-spoofing contamination may persist for hours or until a hard receiver reset. Crews also reported high workload, false alerts, and growing spoofing fatigue. Notably, 70% of surveyed pilots rated their concern for flight safety as very high or extreme, and 91% as moderate or higher (OPSGROUP, 2024). A subsequent paper, *GNSS Interference: Jamming and Spoofing* published in 2026 by the Civil Air Navigation Services Organisation (CANSO) provided the challenges experienced by air traffic controllers during GNSS interference incidents, including increased workload, lack of situational awareness, and challenging decision making (CANSO, 2026).

While these papers represent the most comprehensive community-driven studies to date, their focus is largely operational and targeted at improving awareness and training. However, there remains a pressing need for complementary technical and systems-level analysis, particularly in the context of air traffic surveillance data and space-based detection methods.

This white paper builds upon these findings by exploring ADS-B-based detection of GNSS spoofing at scale. It profiles Aireon's global space-based ADS-B service, operating through the Iridium satellite constellation, providing real-time position and other derived information for aircraft worldwide. This unique dataset enables the detection and characterisation of GNSS interference signatures independent of ground infrastructure. By analysing anomalies in aircraft position broadcasts, velocity vectors, and timing consistency, it is possible to identify regions of GNSS disruption and spoofing with high temporal and spatial resolution.

The objective of this paper is threefold:

- Summarise the technical mechanisms and operational impacts of GNSS spoofing in aviation, as evidenced by recent global data
- Demonstrate how space-based ADS-B analytics can augment situational awareness and detection of spoofing events
- Propose data-driven pathways for interference monitoring, airspace management, and future resilience in aviation navigation systems.

2. PNT Labs – Capability and Role

PNT Labs is FrontierSI's independent testing and evaluation capability, established to assess the performance, resilience, and operational suitability of Positioning, Navigation and Timing (PNT) technologies. It provides a controlled and repeatable environment to evaluate systems under both nominal and degraded conditions, with a particular focus on real-world applicability across critical sectors.

The capability spans a combination of laboratory, field, and simulated environments. Laboratory testing enables controlled experimentation, including the introduction of interference such as jamming and spoofing within licensed facilities. Field-based environments extend this capability into operational contexts, including rail, maritime, and aviation domains, where system performance can be assessed under realistic dynamics, geometries, and signal conditions. In parallel, simulation environments support the evaluation of emerging concepts, including Low Earth Orbit (LEO) PNT and hybrid PNT architectures, under scalable and configurable scenarios.

PNT Labs is technology-agnostic and supports the testing of a broad range of systems. These include conventional GNSS and augmentation services, alternative PNT sources including LEO-based services and signals of opportunity, and timing distribution solutions. Of particular relevance is the ability to assess system behaviour under GNSS disruption, enabling comparative analysis of resilience strategies, fallback mechanisms, and multi-sensor fusion approaches.

The role of PNT Labs within this work is two-fold. First, it provides the experimental foundation for validating performance claims and assumptions presented in this paper. Second, it enables the systematic comparison of technologies and approaches under consistent test conditions, supporting evidence-based decision-making for infrastructure, policy, and operational adoption.

By bridging controlled testing and real-world deployment, PNT Labs aims to accelerate the maturation of resilient PNT solutions and support their transition into operational use.

3. ADS-B Background

ADS-B has become one of the cornerstones of modern air traffic surveillance and situational awareness. It enables aircraft to broadcast their position, velocity, and other flight parameters directly to ground stations and nearby aircraft, forming the foundation of performance-based surveillance in both domestic and oceanic airspace. The *Automatic* aspect reflects that the broadcast occurs continuously without pilot input, *Dependent* refers to its reliance on the aircraft's onboard navigation systems, primarily GNSS, to determine position and time.

ADS-B operates on 1090 MHz Extended Squitter (1090ES) for international use, in compliance with International Civil Aviation Organization (ICAO) Annex 10 (ICAO, 2018) and Radio Technical Commission for Aeronautics (RTCA) Document (DO)-260B/ED-102A (RTCA, 2009) standards[1]. Aircraft equipped with a compliant transponder automatically transmit a data packet containing latitude, longitude, altitude, velocity, identification, and integrity information roughly twice per second. Ground receivers and other aircraft with ADS-B capability use this information for real-time Air Traffic Service (ATS) surveillance including separation assurance, conflict detection, and enhanced situational awareness. The technology underpins surveillance in radar-limited regions and has become a regulatory requirement across many jurisdictions including the United States, Europe, and Australia.

Because ADS-B derives its positional data from onboard GNSS, its integrity is inherently tied to the quality of that navigation source. A corrupted or *spoofed* GNSS solution can therefore propagate directly into the aircraft's ADS-B broadcast, resulting in the transmission of a false position that may appear entirely valid to air traffic controllers and nearby aircraft. The OPSGROUP report highlighted several such occurrences, where spoofed aircraft appeared displaced by tens or even hundreds of nautical miles, sometimes into different Flight Information Regions (FIRs) altogether (OPSGROUP, 2024). In severe cases, multiple aircraft in the same airspace simultaneously broadcast identical falsified coordinates, creating confusion for both pilots and air traffic control.

[1] A subsequent RTCA DO-260C/ED-102B was published in December 2020, however, DO-260B/ED-102 remains the minimum standard.

The dependence of ADS-B on a single, externally derived PNT source presents a dual challenge. The first challenge is an operational one, since a spoofed position can mislead surveillance systems, however, the same ADS-B data can be used to detect and quantify interference when properly analysed. By examining inconsistencies between reported aircraft states, such as position discontinuities, impossible velocities, or divergence from inertial reference trajectories, spoofing events can be inferred retrospectively or even in near-real time. This makes ADS-B a valuable sensor network for detecting and characterising spoofing on a global scale.

The international aviation community has therefore placed increasing emphasis on ADS-B data quality monitoring and integrity metrics such as Navigation Accuracy Category for Position (NACp) and Navigation Integrity Category (NIC). These parameters, transmitted as part of the ADS-B message set, provide a measure of how accurate and reliable the aircraft's positional solution is expected to be. However, under spoofing conditions, these integrity flags can remain nominal because the aircraft's receiver perceives the counterfeit GNSS signal as genuine. As a result, traditional ADS-B integrity indicators cannot alone reveal spoofing, underscoring the importance of complementary analytics capable of identifying systemic anomalies in the data.

This paper leverages ADS-B's global reach and high-frequency positional updates as the primary dataset for spoofing detection. A key enabler of this work is Aireon, the space-based ADS-B surveillance provider that hosts ADS-B receivers on the Iridium satellite constellation. When combined with Aireon's global, space-based coverage, ADS-B provides continuous and uniform visibility across all flight regions (Aireon, 2025). This orbital vantage point enables GNSS interference to be mapped globally and correlated across multiple aircraft and timeframes, independent of local receiver networks. Such analysis forms the foundation for Aireon's interference detection service, which aims to provide real-time alerts and statistical insights into the geographic and temporal patterns of GNSS disruption worldwide.

4. Aireon Air Traffic Management Service

Aireon operates a global space-based ADS-B service, providing real-time aircraft surveillance and PNT integrity insights from Low Earth Orbit. Using ADS-B receivers hosted on the 66 operational satellites of the Iridium NEXT constellation, Aireon delivers continuous, uniform coverage of all flight regions including oceanic, polar and remote continental airspace (Iridium, 2024). This capability is foundational to detecting and characterising GNSS interference at scale.

4.1 Space-Based ADS-B: System Architecture and Data Characteristics

Each Iridium NEXT satellite carries an ADS-B receiver tuned to 1090 MHz Extended Squitter (1090ES), fully compliant with ICAO Annex 10 and RTCA DO-260B/DO-260C standards (ICAO, 2018; RTCA, 2009; RTCA, 2020). As aircraft broadcast ADS-B messages approximately twice per second, these are collected by multiple satellites, forwarded through Iridium's cross-linked LEO network, and delivered to Aireon's ground segment with low latency. This architecture is shown in Figure 1 below (Garcia et al., 2025).

This multi-satellite reception geometry allows Aireon to observe the following:

- Redundant reception of each ADS-B message from multiple orbital vantage points
- High temporal resolution, enabling fine-grained detection of discontinuities
- Global consistency, independent of national ground infrastructure
- Independent validation opportunities, through Time Difference of Arrival (TDOA) and Doppler measurements

The space-based view is especially important during GNSS interference events. Where ground receivers may lose coverage due to terrain masking or RF noise, Aireon's orbital perspective persists unaffected. This allows continuous surveillance even in contested or remote regions, making space-based ADS-B one of the most sensitive civilian datasets for monitoring GNSS integrity worldwide (Garcia et al., 2025).

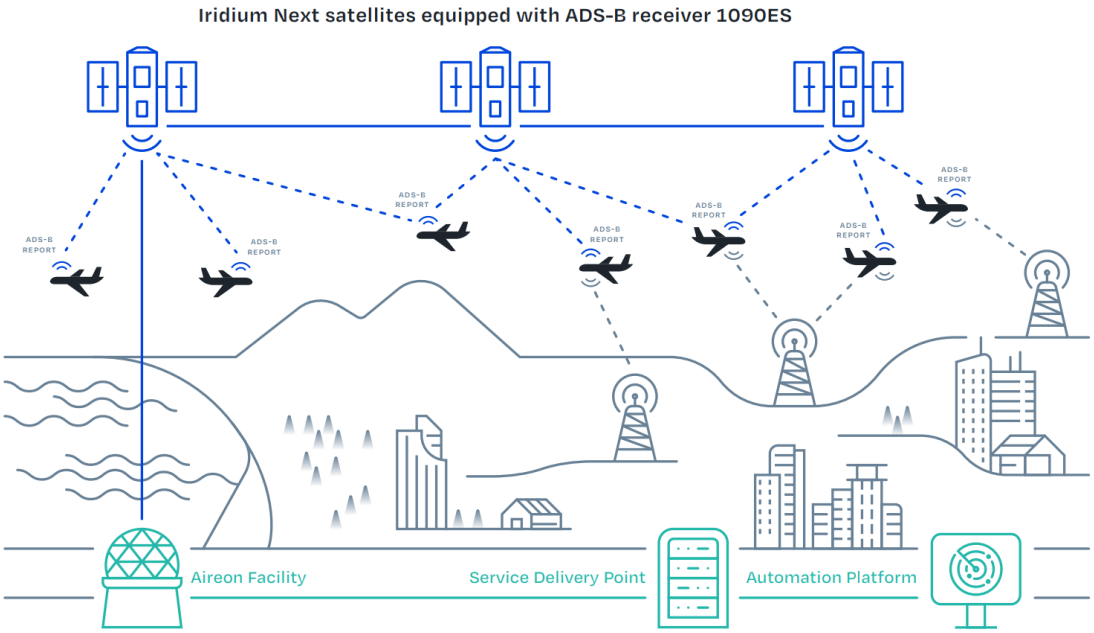


Figure 1. Architecture of Aireon ADS-B Service.

4.2 Interference Detection and Classification

ADS-B Version 2 messages include a rich set of indicators that describe the quality, accuracy, and integrity of the aircraft's navigation solution. These parameters are generated by the aircraft's onboard GNSS and avionics systems and provide essential insight into how reliable the reported position is at any given moment. Collectively, they form the basis for detecting abnormal behaviour caused by GNSS interference, spoofing, or satellite faults.

Key ADS-B integrity and accuracy indicators are summarised in Table 1 below.

ADS-B Indicator	Description
Navigation Integrity Category (NIC)	Reflects the integrity and associated horizontal containment radius of the position
Navigation Accuracy Category for Position (NACp)	Describes the expected horizontal position accuracy
Navigation Accuracy Category for Velocity (NACv)	Describes velocity accuracy
Source Integrity Level (SIL)	Indicates the probability of the position containing an undetected error
System Design Assurance (SDA)	Reflects the likelihood of avionics design errors affecting integrity
Position Integrity Category (PIC)	An Aireon-derived metric that combines multiple ADS-B integrity indicators to summarise overall GNSS quality and integrity
Independent Position Check (IPC)	An Aireon-derived position check of ADS-B reported position against position computed from Iridium satellites

Table 1. ADS-B integrity and accuracy indicators.

These indicators vary depending on receiver performance, GNSS availability, RAIM/SBAS status, and the presence of external interference. When GNSS is functioning normally, aircraft report high NIC, NACp, SIL, and PIC values, corresponding to small containment radii and reliable navigation. Under jamming, spoofing, or satellite degradation, these parameters typically degrade, reflecting increasing uncertainty in the aircraft's position.

Aireon's global ADS-B dataset shows that sustained reductions across multiple parameters are strong population-level indicators of underlying GNSS disruption (Garcia et al., 2025). Some of these concepts are described in more detail below.

4.2.1 Navigation Integrity Category (NIC)

NIC is defined in RTCA DO-260B/ED-102A as a code that indicates the *horizontal containment radius* within which the aircraft's true position is expected to be, with 95% confidence. Higher NIC values correspond to smaller containment radii and therefore better position integrity. Below is the standardised relationship between NIC and the associated containment radius:

NIC Value	Horizontal Containment Radius	Interpretation
0	> 20 NM (or unknown)	Position integrity not reliable
1	< 20 NM	Poor integrity
2	< 8 NM	Low integrity
3	< 4 NM	En route surveillance level
4	< 2 NM	Better than en route
5	< 1 NM	Terminal manoeuvring area
6	< 0.6 NM	Precision surveillance
7	< 0.2 NM	High accuracy (≈ 370 m)
8	< 75 m	GNSS with RAIM/SBAS nominal mode
9	< 25 m	Highest integrity level (SBAS LPV-equivalent)

Table 2. NIC value classification (RTCA, 2009).

Under normal GNSS performance, most commercial aircraft broadcast NIC values of 8 or 9. Sharp reductions (e.g., to NIC 4-6) strongly correlate with GNSS interference.

4.2.2 Position Integrity Category (PIC)

PIC is an Aireon-derived parameter that summarises the overall GNSS integrity state, combining ADS-B integrity indicators such as NIC, NACp, and SIL. In Aireon's dataset, PIC is used as a simplified integrity metric representing the effective GNSS quality integrity bound.

Unlike NIC, PIC is not directly defined in RTCA DO-260B, but instead, generated algorithmically by Aireon for supporting large-scale anomaly detection. However, PIC maintains the same fundamental interpretation, namely lower PIC values imply larger uncertainty in the position and decreased GNSS integrity. Although designed as a positioning quality indicator, PIC can be used to measure or detect GNSS interference, specifically jamming from ADS-B data. Table 3 shows the PIC Value designations and their containment radius.

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

Table 3. PIC value classification.

Aireon's anomaly model flags PIC < 7 as an incident for interference and possible jamming, especially when observed across multiple flights or covering extended geographic regions.

4.2.3 Independent Position Check (IPC)

As part of the ADS-B offering, Aireon developed the Independent Position Validation (IPV) algorithm, a GNSS-independent capability based on multilateration and TDOA measurements computing the aircraft's position and trajectory based solely on measurements from the Iridium NEXT satellites (Dolan & Garcia, 2019; Dolan et. al., 2023). When multiple satellites receive the same ADS-B message, the differences in signal arrival time and Doppler shift enable a multilateration solution that is

completely independent of the aircraft onboard GNSS receiver. This produces a reference track that acts as a truth position source that does not rely on GNSS.

If the aircraft's reported ADS-B position deviates from the reference track by more than three nautical miles, Aireon flags the event with the IPC flag, a binary validity flag indicated that the aircraft's onboard navigation solution is likely compromised (Garcia et al., 2025). Unlike NIC or PIC, which describe integrity bounds provided by the aircraft's own GNSS avionics, IPC is an external cross-check derived from Aireon's space-based ADS-B system. The IPC measurement is a critical pillar of Aireon's interference detection system and addresses identification of the growing threat of GNSS spoofing, which can pass integrity bound checks, but still pose a risk to GNSS. The IPC values are described in Table 4 below.

IPC Value	Result	Interpretation
0	Pass	The ADS-B-reported aircraft position is consistent with Aireon's independent TDOA-derived track. This is considered normal and healthy.
1	Fail	The ADS-B-reported position deviates beyond a certain threshold (e.g., > 3 NM) from Aireon's independent track. This correlates strongly with spoofing attacks.

Table 4. IPC value classification.

4.3 GNSS Interference Signatures in ADS-B Data

Understanding how GNSS interference manifests in ADS-B data is essential for detecting spoofing and related navigation anomalies at scale. Although ADS-B integrity indicators such as NIC, NACp and SIL provide important information about the aircraft's internal assessment of navigation quality, they often remain nominal during spoofing events, because the onboard receiver believes the counterfeit GNSS signals are genuine. As a result, the most reliable indicators of interference are not always the standard integrity fields, but rather behavioural signatures visible in the ADS-B data stream itself. These signatures reflect underlying inconsistencies between the aircraft's reported state and physically plausible flight behaviour. By analysing these anomalies across multiple aircraft and timeframes, it becomes possible to identify, classify, and geolocate GNSS interference with high confidence, even when traditional integrity parameters appear normal (Aireon, 2024). These signatures are described in detail in this section.

4.3.1 Duplicate Address Conditions

Under normal circumstances, each aircraft is assigned a unique 24-bit ICAO Mode S address that is transmitted in every ADS-B message. A duplicate address condition occurs when two aircraft appear to be broadcasting the same address simultaneously. While this can happen due to misconfiguration on the ground, Aireon's observations show that duplicate address events are increasingly triggered by GNSS interference.

During spoofing or severe GNSS corruption, an aircraft may begin broadcasting two spatially inconsistent positions within a short time window. When these conflicting positions exceed the positional consistency checks used by space-based surveillance systems, the target may be interpreted as two aircraft sharing the same ICAO address, even though only one aircraft exists. This phenomenon has been widely observed in regions experiencing spoofing activity, particularly around the Eastern Mediterranean and Black Sea (Garcia et al., 2025).

4.3.2 Field Type Code 0 (FTC0)

Under normal conditions, ADS-B airborne position messages use Type Codes 9-18 to indicate that valid latitude and longitude information is available, and the message includes the aircraft's encoded position coordinates (RTCA, 2020). FTC0 represents "no position information available" and is intended solely for use during initial receiver acquisition, before the GNSS solution is valid.

Under GNSS interference, however, aircraft navigation systems may lose the ability to compute a credible position while airborne. When this occurs, the ADS-B transponder reverts to FTC0, resulting in spurious gaps in the surveillance track. Unlike normal link drop-outs or 1090 MHz congestion, FTC0 is a definitive indicator that the avionics have rejected their own position solution and elected to broadcast "unknown position" instead. These mid-air FTC0 occurrences are rare under normal operations and therefore serve as a high-confidence signature of severe GNSS denial, jamming, or sudden spoofing loss-of-lock transitions.

4.3.3 Track Discontinuities

Track discontinuities occur when reported ADS-B positions exhibit instantaneous spatial jumps that are inconsistent with physical aircraft motion. These may range from minor deviations of a few nautical miles to extreme displacements of hundreds of miles within a single update interval. Because ADS-B provides high-frequency updates (typically twice per second), even modest discontinuities represent fundamental violations of kinematic feasibility.

These jumps often arise when a spoofed GNSS solution transitions between counterfeit satellite ensembles, causing the receiver to snap to a new synthetic location. Such discontinuities frequently align with periods of reduced NIC/PIC and increased IPC flags (Garcia et al., 2025).

Importantly, track discontinuities are a spoofing-dominant signature rather than jamming-dominant. This typically degrades, but does not misplace position. Spoofing, by contrast, produces spatially coherent, but incorrect trajectories that can abruptly collapse when the counterfeit geometry shifts. Thus, large discontinuities, especially when repeated, are highly indicative of synthetic GNSS manipulation.

4.3.4 Improbable Dynamics (Velocity / Turn Rate Anomalies)

A spoofed position solution may produce trajectories that appear continuous, yet violate basic aerodynamic or performance constraints. Examples may include ground speeds far below what is physically possible for an aircraft in cruise flight, abrupt turns with bank angles impossible for large commercial aircraft, circular patterns at high altitude and ground speeds inconsistent with wind fields or flight plan estimates.

These improbable dynamics occur because the spoofed trajectory is generated without regard to aircraft performance envelopes. The receiver, fooled by synthetic signals, computes a position solution that is mathematically plausible from a satellite geometry standpoint, but physically impossible for the airframe.

Such anomalies are particularly dangerous because they can contaminate downstream avionics including EGPWS, TCAS, and FMS calculations, creating genuinely unsafe aircraft states. Flights spoofed into circular patterns often report grossly incorrect velocities, sometimes as low as 60 knots at cruise altitude (Garcia et al., 2025). These improbable kinematics form one of the strongest indicators of maliciously generated GNSS signals.

5. Case Studies

In this section we profile several examples of GNSS spoofing detected through Aireon's ADS-B data. While spoofing is frequently associated with known conflict zones, all the events examined here occurred outside these traditional hotspots and illustrate a range of distinct GNSS interference signatures. Aireon provided FrontierSI with the relevant ADS-B data, which was analysed to produce the results presented below.

The first case study in Peru demonstrates operational impacts and highlights the potential risk of spoofing. The subsequent events, observed within Australian airspace, underline a key point of this paper - GNSS spoofing can occur anywhere, at any time, and well beyond regions typically considered high-risk.

5.1 GNSS Spoofing– Runway Misalignment Lima, Peru August 2024

In this event, the aircraft shows signatures of GNSS spoofing during the final approach into Lima Jorge Chávez International Airport (LIM) to runway 16L, with spoofing beginning at approximately 1300 feet above Mean Sea Level (MSL). Aireon's ADS-B data shows two distinct spoofing episodes during the descent, each causing the aircraft's GNSS-derived position to shift laterally from the true approach path.

Figure 2 shows that during both spoofing instances, the aircraft's reported position aligned with runway 16R, a parallel runway, not in use at the time. Full replay of the aircraft's actual position shows the aircraft remained aligned with 13L throughout the incident, however, presents the risk of unintentionally landing on a closed runway or taxiway as a result of map shift and loss of situational awareness, if not recognised.

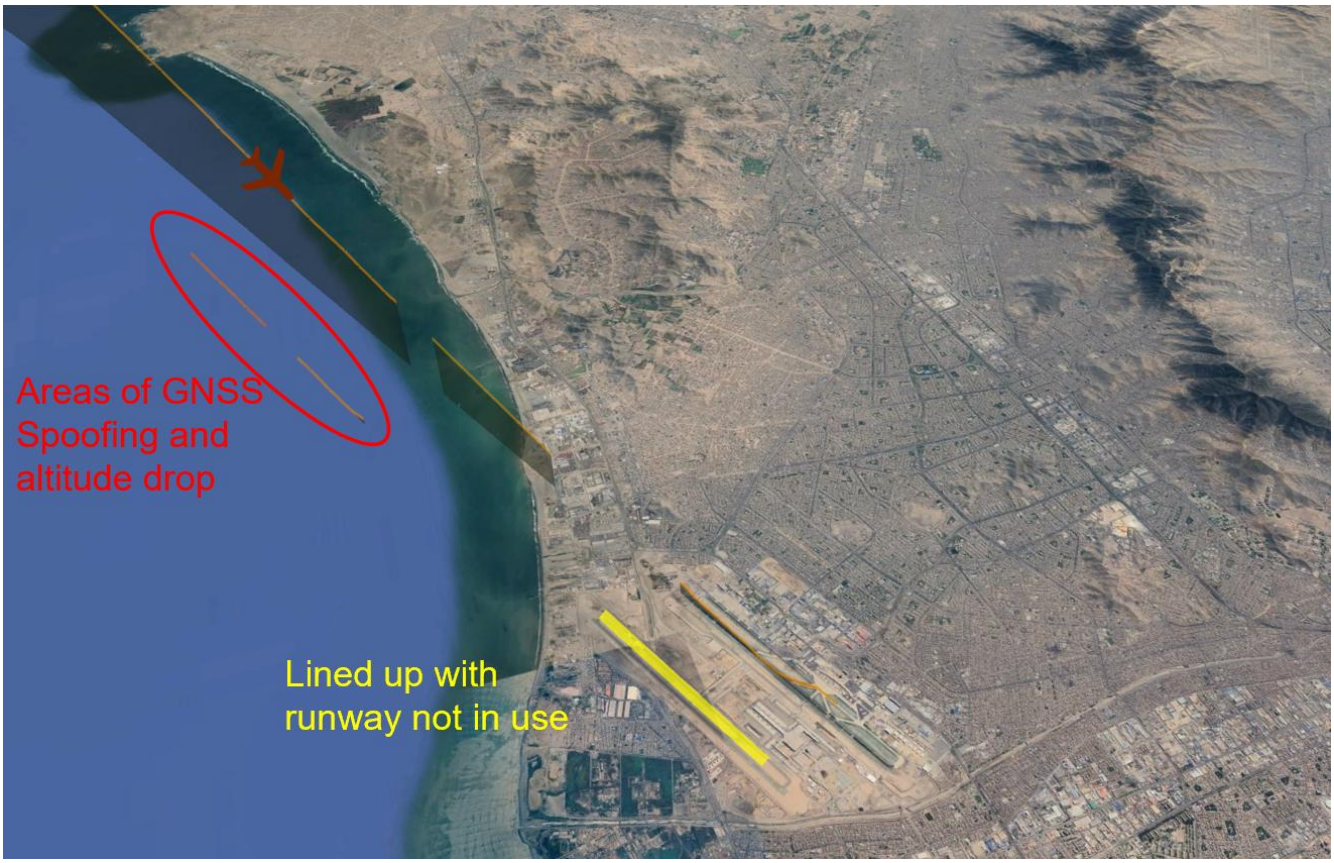


Figure 2. Map of the Lima landing showing the spoofed positions of the aircraft during the approach.

Figure 3 (left) shows the IPC values of 1 at two occasions during the approach, which indicates that the ADS-B-reported position was flagged by Aireon's IPC check, exceeding the allowable deviation threshold. Aireon's ADS-B data further indicates geometric altitude dropouts during the interference periods a result of compromised GNSS, resulting in temporary gaps or erroneous values in the broadcast data. The right panel of Figure 3 shows the geometrics altitude profile, where brief altitude dropouts occur at the same time as the IPC=1 period. Such disruptions are significant because systems including GPWS rely on stable and accurate GNSS inputs for terrain calculations and alerting logic.

Although the Lima aerodrome is at sea level, the aircraft's low proximity to the ground (<1000 feet MSL) during the GNSS incident in conjunction with the surrounding mountainous terrain around Lima increases sensitivity to corrupted position or altitude inputs during approach. Any degradation of GNSS-derived data in this phase of flight can affect the reliability of downstream avionics and impact situational awareness for both the flight crew and ATC.

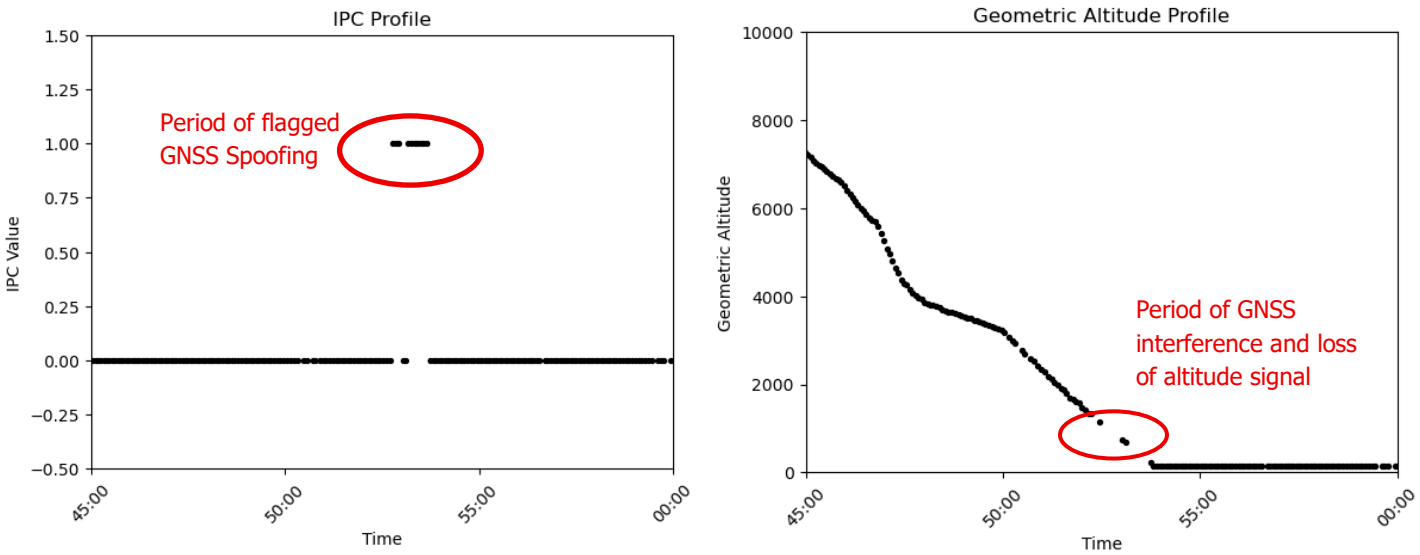


Figure 3. Plots of IPC values (left) and Altitude Profile (right) during the Lima approach.

This case highlights how spoofing-induced false position information can lead to an apparent runway misalignment, even in the absence of large track jumps or jamming-like integrity reductions. The event demonstrates that spoofing can generate credible, but incorrect position solutions, which propagate into the ADS-B track and may contribute to undesired aircraft states if not detected and managed appropriately.

5.2 Interference into Australian Airspace – July 2025

In this event in July 2025, an aircraft operating en-route over Myanmar, a known hotspot for frequent GNSS interference activity, experienced a period of sustained potential GNSS spoofing and jamming of approximately four minutes that caused its ADS-B-reported position to drift significantly from its true location. Although the aircraft was physically operating thousands of miles away, the spoofed GNSS-derived position was displaced far enough to appear within the Melbourne Flight Information Region (FIR), which constitutes Australian airspace (see Figure 4).

The Melbourne FIR covers a vast portion of the Indian Ocean, extending several thousand miles to the west. During the spoofing interval, the false ADS-B position placed the aircraft more than 3000 miles from its actual location, entering Melbourne-controlled airspace despite the aircraft never approaching Australia. While the Melbourne FIR is not directly adjacent to the known hotspot, this illustrates how large-scale synthetic position shifts can cross international boundaries and triggering surveillance visibility in airspaces far removed from the aircraft's true operating region.

During the GNSS interference incident, the ADS-B system continued broadcasting the false position as if it were valid. Although no aircraft in Australian airspace were impacted, the event demonstrates how GNSS spoofing occurring in one region can manifest operationally in another, potentially complicating air traffic monitoring, situational awareness, or automated surveillance tools reliant on ADS-B feeds.

This case highlights the importance for Australian Air Traffic Management (ATM) to be aware of global GNSS interference trends and to monitor for unexpected or implausible aircraft tracks entering the FIR. In the event of anomalous ADS-B targets, controllers may need to observe the aircraft closely and, where appropriate, use secondary position sources for navigation and separation.

This example reinforces that GNSS spoofing impacts are not geographically contained, even when the interference originates thousands of miles away, the synthetic ADS-B trajectory can cross multiple FIR boundaries, posing challenges for surveillance fidelity and airspace management.

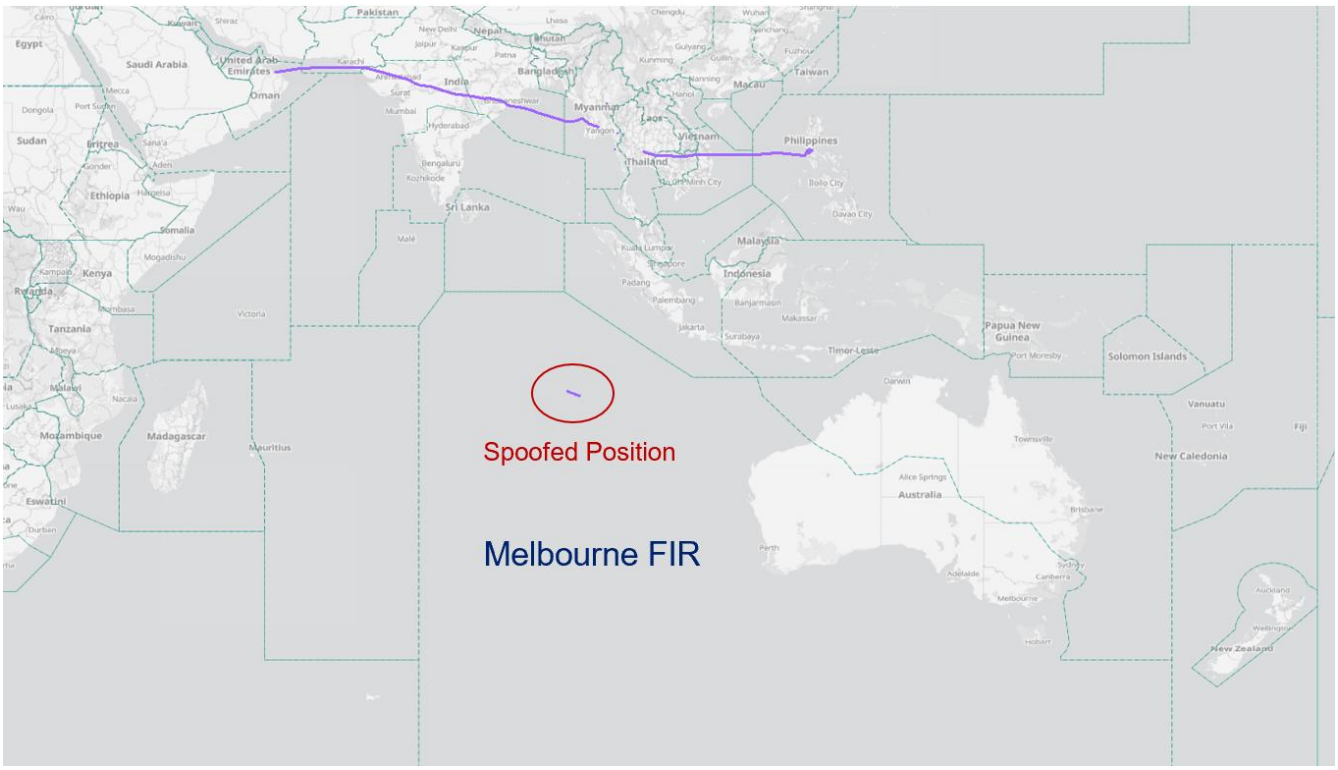


Figure 4. Map showing a spoofed position of an aircraft above Myanmar appearing in Australian Airspace.

Figure 5 below shows the behaviour of PIC and IPC values during the spoofing event. The left panel illustrates the PIC value fluctuations, where the aircraft transitions from stable, high-integrity GNSS operation (PIC = 11) into a period of significant degradation intermittently dropping to values below 6, and even 0. The presence of scattered PIC points across a wide range of values reflects instability in the GNSS-derived position rather than a single, steady jamming signature. Although the PIC values can be spoofed, creating the appearance the position is accurate, the IPC is independent of the PIC value and flags the event as spoofed. This is critical for monitoring and alerting applications, reducing the occurrences of false-negatives.

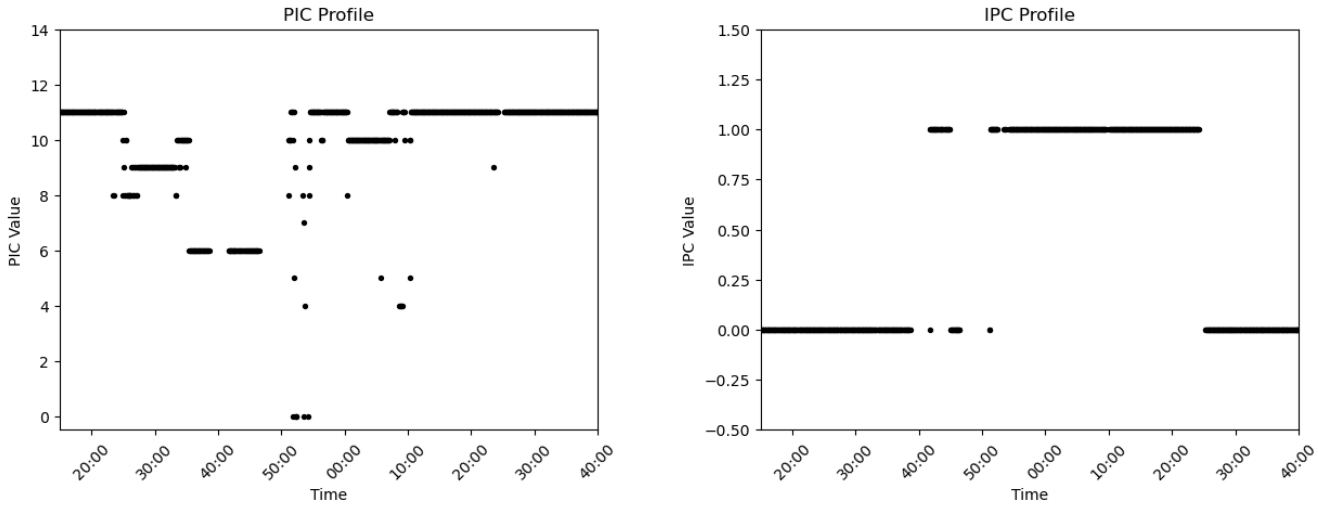


Figure 5. Plots of PIC values (left) and IPC values (right) during a Myanmar spoofing incident.

5.3 Spoofing incident near Townsville, Australia – September 2024

In this event, an aircraft operating near Townsville in northern Australia in September 2024 experienced two distinct episodes of potential GNSS spoofing, each resulting in displacement of its reported ADS-B position. Figure 6 shows the two spoofed

positions of 15 seconds and 30 seconds resulting in jumps of the aircraft trajectory. Figure 7 shows the Aireon IPC flag identified correspond to deviations from the aircraft's actual trajectory. The IPC flag is preceded by a short period of degraded PIC value, a common occurrence in spoofing events (OPSGROUP, 2024).

After the flagged IPC periods, although the aircraft visually resumes transmitting a valid trajectory, the low PIC value indicate degraded quality in the ADS-B throughout the remainder of the flight. This especially impacted the geometric altitude, which is calculated using GNSS altitude. Systems such as the EGPWS rely on GNSS altitude and may result in false alerts.

Figure 6. Map of a spoofing incident near Townsville on 4 September 2024.

Unlike some spoofing events that cause large lateral offsets or cross-FIR incursions, this example demonstrates a shorter-duration, localised spoofing signature. The event nevertheless reinforces that GNSS spoofing is occurring within Australian airspace, and that even brief interference episodes can generate false ADS-B positions that may affect situational awareness and automated monitoring tools.

This case also highlights the usefulness of IPC as a detection mechanism. Although the spoofed GNSS positions appear continuous and consistent, the IPC correctly marks them as invalid due to their inconsistency and impacts to GNSS-dependent fields, including altitude. This distinction is critical for operators and ANSPs seeking to identify and classify local interference events.

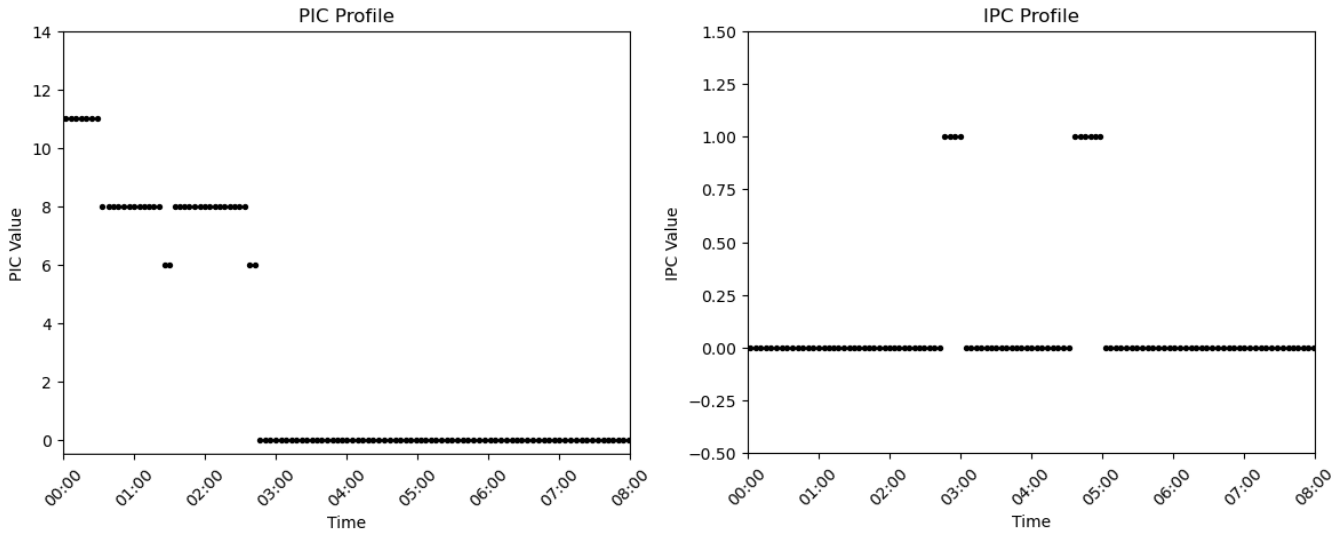


Figure 7. IPC values for the flight near Townsville on 4 September 2024.

6. Conclusion

The case studies presented in this paper demonstrate that GNSS spoofing is no longer a phenomenon confined to conflict zones or politically sensitive regions. While early industry attention focused on interference around the Eastern Mediterranean and the Black Sea, the events analysed here show that civil aviation in all areas of the world are impacted including, South America, Southeast Asia, and Australia. Spoofing can occur during all phases of flights in both the oceanic and terrestrial environments.

Equally important is the diversity of spoofing signatures and operational consequences. Some events involve subtle lateral shifts that place aircraft on the incorrect runway centreline, while others generate large synthetic trajectories that appear thousands of miles away from the true aircraft position. Short, intermittent bursts can produce repeated IPC failures, while sustained spoofing can result in cross-FIR incursions or persistent false altitude solutions. These variations highlight that spoofing does not present as a single, uniform problem. It manifests in multiple ways, affects different avionics subsystems, and creates a wide range of operational risks.

Across all the incidents profiled, Aireon's space-based ADS-B system, specifically its IPV and IPC capabilities, consistently detected anomalies that were otherwise invisible to traditional onboard GNSS integrity metrics. In many cases, integrity indicators such as NIC and PIC remained nominal during spoofing, because the aircraft's receiver indicated the counterfeit signals were authentic. By providing a GNSS-independent reference track, Aireon's tools reliably identified when ADS-B-reported positions deviated from the aircraft's true trajectory, enabling early detection and characterisation of spoofing events anywhere in the world.

Recognition of GNSS signatures through monitoring/detection and having a pre-determined response plan remains an important method for mitigating the impacts of GNSS interference. This reinforces the need for global, space-based surveillance and integrity monitoring as aviation navigates an environment where GNSS interference is becoming increasingly widespread, unpredictable, and technically sophisticated. As reliance on GNSS continues to grow, the ability to detect and understand spoofing events will be essential for ensuring the resilience of aviation's PNT infrastructure.

References

Aireon (2025). *Air traffic surveillance data for the aviation community*. Available at: https://aireon.com (Accessed: 15 April 2026).

Aireon (2024). *GNSS Interference and Spoofing in the Baltics*. Aireon LLC.

CANSO (2026). Global Navigation Satellite System Interference: Jamming and Spoofing. Civil Air Navigation Services Organisation (CANSO). Available at: https://canso.org (Accessed: 15 April 2026).

Dolan, J. & Garcia, M. (2018). *Aireon Independent Validation of Aircraft Position via Space-Based ADS-B*. ESAVS, Berlin.

Dolan, J., Garcia, M. & Sirigu, G. (2023). *Aireon Space-Based Aircraft Position Validation and Multilateration*. DASC, Barcelona.

Garcia, M., Sirigu, G. & Dolan, J. (2025). *Observations of Trends in GNSS Anomalies Affecting Aviation*. Aireon White Paper.

ICAO (2018). *Annex 10 to the Convention on International Civil Aviation, Volume IV – Surveillance and Collision Avoidance Systems*, 5th Edition, International Civil Aviation Organization.

ICAO (2018). *Annex 10 to the Convention on International Civil Aviation: Volume IV – Surveillance and Collision Avoidance Systems*. ICAO.

Iridium (2024). *Iridium NEXT Constellation Overview*. Available at: https://www.iridium.com (Accessed: 15 April 2026).

OPSGROUP (2024). *Report of the 2024 GNSS Spoofing Workgroup*, OPSGROUP, London. Available at: https://ops.group/blog/GNSS-spoofing (Accessed: 15 April 2026).

RTCA (2009). *Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance-Broadcast (ADS-B) and Traffic Information Services-Broadcast (TIS-B)*, DO-260B/ED-102A, RTCA, Washington, DC.

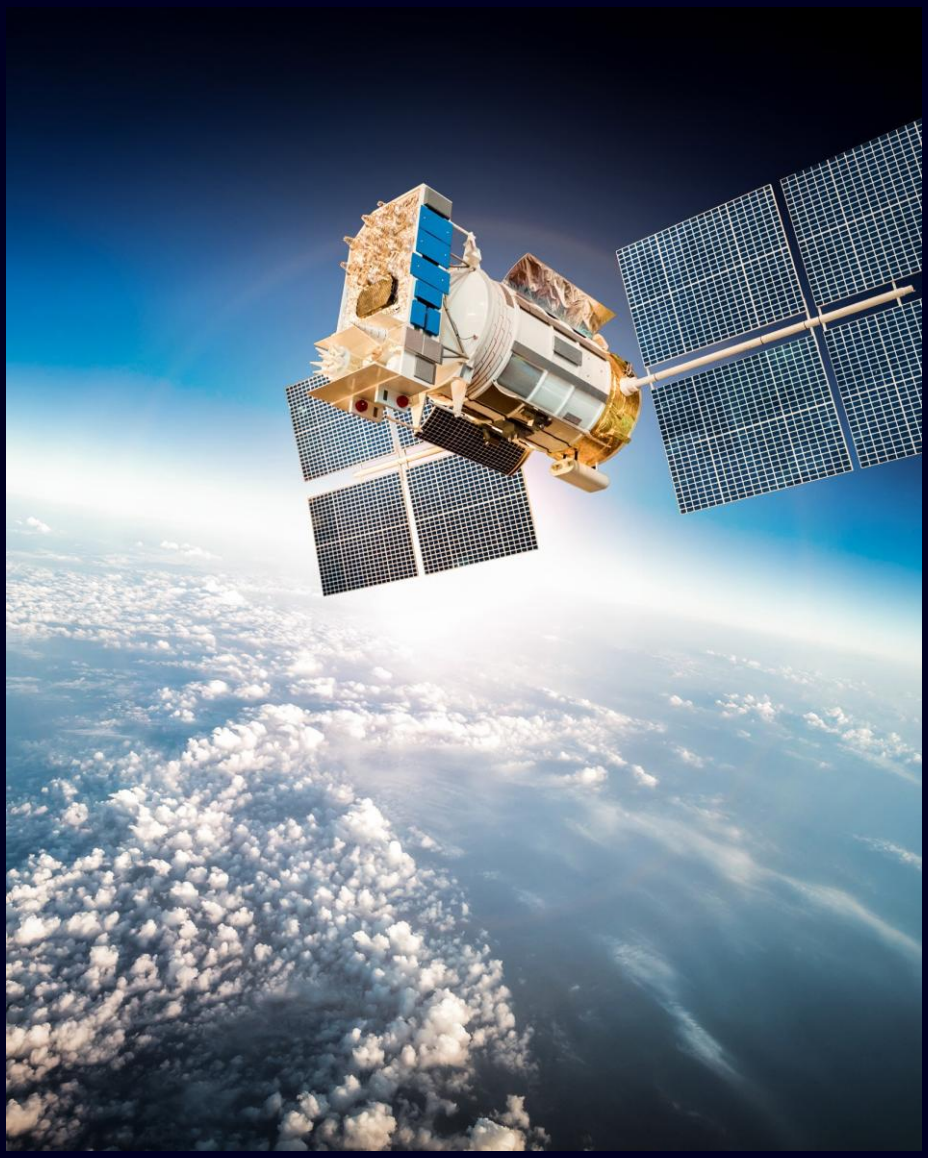
RTCA (2020). *DO-260C: Minimum Operational Performance Standards for 1090 MHz Extended Squitter ADS-B and TIS-B*. RTCA, Washington, DC.

About FrontierSI

FrontierSI is a social enterprise focused on bringing the best people together to anticipate and solve large problems using our space and spatial expertise. Through collaboration with government, research, and industry networks, we bring innovative ideas through to real-world products and services to create commercial and public good impact. We focus our deep spatial expertise in positioning, geodesy, spatial data management and data analytics to develop and implement solutions to meet challenges across multiple sectors from defence to resources.

About Aireon

Aireon deployed the world's first global space-based air traffic surveillance system, providing real-time aircraft monitoring capabilities around the world, including over the poles, over the oceans and in remote areas. Since 2019, the world's Air Navigation Service Providers (ANSPs) have trusted Aireon to provide its high-fidelity global data set to enable the safe and efficient management of aircraft through their airspaces. Powered by Iridium's networked constellation of 66 satellites, Aireon's ADS-B data provides continuous air traffic surveillance to areas of the world that previously had no access to this information. Beyond air traffic surveillance, Aireon is leveraging its reliable and trusted data into a family of products for the wider aviation industry, including airlines, airport operators, airframe manufacturers, system integrators, and military an intelligence agency. With its portfolio of diverse products, Aireon is enabling new levels of insight into air operations around the globe, leading to more data-driven decision making, safer operations, and less impact on the environment.



pnt@frontiersi.com.au

linkedin.com/company/frontiersi

frontiersi.com.au

FRONTIER SI