National Aviation Academy

International Journal of Transportation Research and Technology

e-ISSN: 3079-6075

DOI: 10.71108/transporttech.vm03is01.03

Research Article

Blockage and Outage of Aircraft Navigation System: An Implication and Solution for Sustainability of Aviation

Tapdig Imanov*

European Leadership University, Famagusta, TRNC

Timescale of article

Received: 10 October 2025
Accepted: 29 October 2025
Published: 25 June 2026

Corresponding author

Tapdig Imanov
timanov@yahoo.com

Keywords

Global Navigation Satellite System, Aircraft Systems, Jamming, Interface, Trajectory, Radio Frequency Interference

Cite this article as:

Imanov, T. (2026). Blockage and Outage of Aircraft Navigation System: An Implication and Solution for Sustainability of Aviation. *International Journal of Transportation Research and Technology*, 3(1), 26-44.
DOI: 10.71108/transporttech.vm03is01.03

Abstract

Recently, there have been an increasing number of blockages and outages of Global Navigation Satellite Systems signals for civil aircraft by applying jamming, spoofing, and interference modes that threaten flight safety. The purpose of this study is to investigate the impact of intentionally interference of satellite signals, and its negative implication on systems and flight path involved aircraft The methodology considers various applications for countermeasures that affect aircraft navigation systems while GNSS signals are missing. The practical implications demonstrate that, even if all satellite navigation signals and radio navigation systems are turned off, alternative aircraft equipment is able to prevent disasters. Low Range Radio Altimeter interfacing with a Ground Proximity Warning System is the best and most reliable implemented technology to warn and avoid the threat. Modern developments allow the use of countermeasures with Quantum, AI-Powered, and Geomagnetic navigation system technologies to provide stable flight sequences, ensuring the safety of aircraft and passengers.

1. Introduction

Modern life is enabling multiple innovative technologies in various sectors and countless industries, including air transportation. For air transportation systems, the critically important components are the use of Global Navigation Satellite Systems (GNSS), such as GPS, Galileo, GLONASS, and Beidou, for air traffic management and route optimization. Growth of the GNSS system provides accurate navigation, enhanced communication, and due timing. However, recent trends have observed that GNSS technologies are vulnerable to external intrusion and face regular threats from interference using jamming and spoofing. Using jamming on GNSS signals creates radio frequency interference that is similar to the GNSS signals themselves, which can overpower them and lead to a loss of positioning, navigation data, and timing. The effectiveness of a spoofing attack differs from jamming with its sophisticated implications. Applying fake signals in GNSS operations is directly linked to selected object navigation receivers, deceiving them with transmitted radio frequencies while manipulating calculations of incorrect positions and fluctuating a time scale. Interference with the aircraft navigation system leads to an outage of the Flight Management System (FMS), the terrain database of the Traffic Collision Avoidance System (TCAS), the Ground Proximity Warning System (GPWS) and interconnected avionics devices. Meanwhile, the loss of GNSS signals affecting the whole navigation system of the aircraft causes operational malfunctions, disrupts signal interfaces, and creates ramifications for safety risks and accidents. GNSS is an integral part of the modern global airport systems. Jamming and spoofing GNSS signals near airports can compromise and disrupt overall operations, mostly causing imprecise approaches and missed landings, leading to flight delays. As stated in the European Aviation Safety Agency (EASA, 2024) report, since the beginning of 2022, there has been observed significant growth in jamming and spoofing the GNSS. The published EASA Safety Information Bulletin (EASA SIB 2024-02R3) indicates RFI-affected geographical areas and airports throughout the world (Table 1).

Table 1. RFI Areas and Regions (adopted from IATA, 2024)

The Black Sea Area	**LTBB, LTAA, UGGG, LRBB, LBSR, UDDD, UBBA**	**Istanbul, Ankara, Tbilisi, Bucuresti, Sofia, Yerevan, Baku**
The Middle East: Southeastern Mediterranean Area	LCCC, OLBB, OSTT, LLLL, OJAC, HECC, LGGG, ORBB, OKAC, OBBB, OIIX, HLLL.	Nicosia, Beirut, Damascus, Tel-Aviv, Amman, N-E Cairo, Athina, Baghdad, Kuwait, Bahrain, Tehran, Tripoli
The Baltic Sea Area	UMKK, EFIN, EETT, EVRR, EYVL, EPWW, ESAA	Kaliningrad, W-Helsinki, Tallin, Riga, Vilnius, E-Warszawa, S-Sweden
Eastern Europe Area	LZBB, LHCC, LUUU.	Bratislava, Budapest, Chisinau
North Atlantic Region	BIRD, NUUK	Icelandic, Greenlandic
SAM region	SAEF, SARR, SBBS, SBRE	Ezeiza, Resistencia, Brasilia, Recife
MID-Asia region	VIDF, VABF, VYYF, ZPKM	Delhi, Mumbai, Yangon, Kunming
Africa region	FACA, DNKK	Cape Town, Kano

The recently analyzed data, relying on the Network of Analysts and open sources, has concluded that the RFI interference to GNSS jamming and/or spoofing tends to further increase by its severity and intensity. The effect of the RFI on GNSS is not limited to the flight information regions (FIR) emphasized in EASA's SIB. This document is a valuable motivational resource to assist IATA airline members in determining the operational risks associated with the weakening of onboard GNSS-related functionality. According to the International Air Transport Association (IATA, 2024) analysis over the past year, shows that the GNSS outage trend in the first six months of 2024 (GPS signal disruptions per thousand of flight hours) has increased significantly compared to 2023, as demonstrated in Fig. 1.

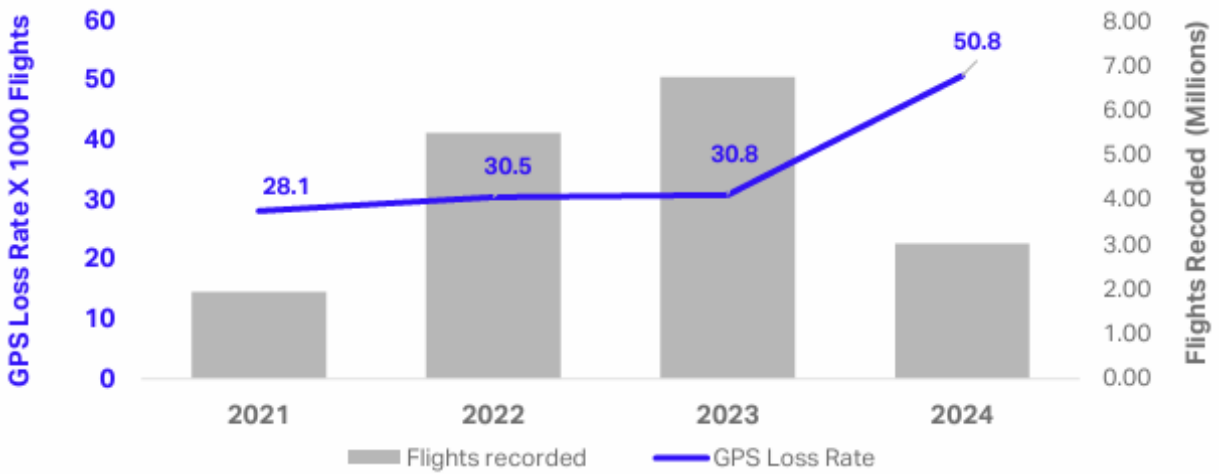

Fig. 1. GNSS signals loss records (IATA, 2024)

Alongside EASA publications, the IATA (2024), in the frame of the Flight Data Exchange (FDX) program, evolved the activity, revealing RFI hotspots in other regions. The results identified increasing GNSS outages between 2021 and 2024, posing a safety risk across wider geographical areas, Fig. 2. It is notable to highlight that the report reflects real aircraft-recorded data and is not based on statistical analysis or predictions. Thus, FDX continues to provide an updated geographic identification of the RFI hotspots, where threats to flight safety exist.

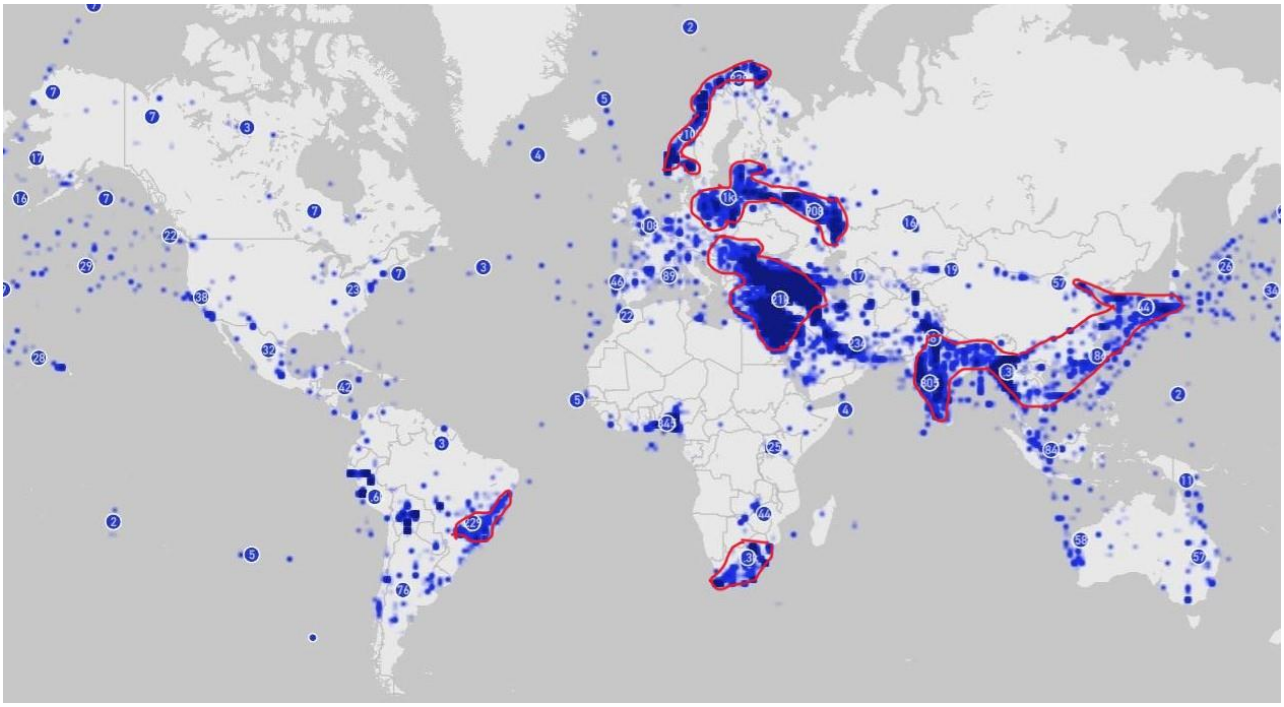

Fig. 2. GNSS RFI Recorded Events between January and June, 2024 (IATA, 2024)

It helps determine the safety controls for member airlines in order to effectively mitigate GNSS interference risks. Because airlines periodically experience the effects of RFI on GNSS in various flight phases, these effects lead to rerouting or diversions of their flight paths. Additionally, the nearby areas covered by RFI jamming GNSS are a potential reason for degradation of aircraft communication, navigation, and surveillance (CNS) systems. To mitigate the limitations of GNSS signal transmission, the International Civil Aviation Organization (ICAO, 2003) has proposed an Automatic Dependent Surveillance-Broadcast (ADS-B) surveillance system that uses onboard aircraft navigation systems to obtain accurate aircraft position. Implementation of the system is intended to assess and support ATC services, particularly focusing on separation and airspace safety (Ali et al., 2015).

However, the challenge of GNSS jamming and spoofing, either intentional or unintentional interferences, delimited normal operation of the aircraft and under the present conditions (NordSky, 2024), GNSS outages impact degraded abilities with ramifications of (i) Loss of waypoint navigation, (ii) Area Navigation (RNAV) approach capability, (iii) inability to perform required navigation performance (RNP) operations,(iv) triggering of terrain warnings, possibly with pull-up commands, (v) scattered aircraft position on the navigation display (ND), (vi) loss of ADS-B functionalities,(vii) failure of time reference, and (viii) Airspace infringements and route deviations (ICAO, 2022).

The purpose of this study is to investigate the impact and implications of the loss of satellite signals on systems and flights of involved aircraft. Limitation of the study a lack of publications describing real situations and events with significant fatal implications involving RFI. Most studies rely on simulations or controlled lab environments which arises the practical, technical, and operational application is prevented being fully effective investigations.

Due to even modern aircraft avionics systems lack real-time detection capabilities of jamming and spoofing, they are unable to precisely alert crew members (Radoš et al., 2024). However, most avionics equipment is able to recognize the loss of GNSS signals (jamming) and struggles to detect spoofing; consequently, crew alerts are basic in the form of “GPS signal lost” or “NAV accuracy degraded,” but not a clear detection warning. GNSS jamming and spoofing affects not just navigation but also dependent systems like ADS-B, CPDLC, TAWS, and EGPWS, yet, literature often treats these systems in isolation.

Therefore, the current study will make a significant contribution to airlines' activities as a tool to pre-emptively reroute or prepare crews for high-risk zones upon RFI attack. Additionally, the validated outcomes fill the gap in scientific literature, introducing the reliability integration of independent landing and warning systems for application in the future researches.

2. Literature Review

One of the important sources of reference signals for synchronization and provision of navigation and positioning services is GNSS. For aircraft navigation systems and accurate positioning, the GNSS application is the best source of reference signals for the synchronized aircraft radio frequency (RF). However, due to the increased provision of services and the use of satellite navigation systems, there are an increasing number of threats and risks, accompanied by harmful interference targeted these systems (Psiaki et al., 2016; Hexagon, 2025). Jamming and spoofing attacks expose navigation systems to security risks (Wu et al., 2020), which negatively affect flight safety. Humphreys et al. (2008) developed a counter-measurement system for spoofing attacks performed on a commercial standard receiver and successfully tested it; later, the strategy to detect spoofing attacks on cryptographically protected GNSS signals was presented in the studies of Humphreys (2013) and Meng et al. (2022).

Altaweel et al. (2023) argue that an important consideration for effective detection of intrusion in GNSS signals and to maintain countermeasures and integrity affected by spoofing and jamming attacks consists of precisely differentiating between authentic and non-authentic signals. Most of the latest literature reviews and scientific research emphasized the detection and localization of GNSS RFI interferences based on ADS-B data. However, to continuously support an acceptable level of safety in aviation, it is necessary to detect the GNSS jamming promptly and secure the incident decisively.

For that reason, existing literature described various detection methods for jamming and spoofing aircraft and GNSS aeronautical navigation systems, which concluded only on strategies and roadmaps (Felux et al., 2024). GNSS intrusions, using radio frequency interference (RFI) and their impact on passenger flight aircraft were conducted in several analyses. Data from ADS-B and avionics, collected by the airline's team for monitoring flight performance for the specific flights that showed warnings to alert the crew about RFI effects on GNSS, have been examined by many researchers (Scaramuzza et al., 2015; Darabseh et al., 2019; Jonáš & Vitan, 2019; Lukeš et al., 2020; Liu et al., 2020; Liu et al., 2021; Murrian et al., 2021; Osechas et al., 2021; Fol & Felux, 2022; Liu et al., 2022; Figuet et al., 2022; Joseph et al., 2023; Blois et al., 2023; Felux et al., 2024).

On the other hand, to solve the current issue related to RF interference to GNSS signals, there is a demand to find out effective countermeasure technology and optimal preventive methodologies. The studies by Qiao et al. (2023) and He et al. (2024) have suggested focusing on the development of technologies for satellite navigation interference monitoring. Conversely, the study by Radoš et al. (2024) provided a detailed and organized overview of ways to detect interference from both GNSS jamming and spoofing combinations. Therefore, the study's

conclusion underscores the significance of emphasizing machine and deep learning methods. Machine learning methods are used to detect and classify the signal to prevent interference where such attacks are more common. In addition, it is able to initiate processing methods of signals, as well as the application of positioning techniques.

Ghanbarzade & Soleimani (2025) have drawn attention to the limitation of traditional methods for RFI analysis, and the idea is supported by studies by Zidan et al. (2020) and Issam et al. (2020), relying on predefined threshold values, which are predicted not to be effective in all scenarios and are susceptible to false identifications of alarm. In contrast, Bose (2021) and Nayfeh et al. (2023) consider that the use of machine learning (ML), deep learning (DL), and artificial intelligence (AI) methods in the investigation of GNSS interference enhances detection by analyzing patterns in large datasets of known signals. These contemporary techniques are able to improve accuracy detection over time by adapting to complex scenarios (Zidan et al., 2020). Albeit, recent achievements reveal a notable shortcoming in detecting jamming and spoofing attacks in GNSS while using ML and deep learning techniques. As far as most studies are concerned, they focus exclusively on either spoofing or jamming, neglecting the simultaneous occurrence of both threats, which limits detection robustness (Zidan et al., 2020; Bose, 2021; Nayfeh et al., 2023; Ghanbarzade & Soleimani, 2025). Meanwhile, ML and DL have the potential for adaptation in major research concentrating on specific systems like GPS or GLONASS, whose implementations remain applicable for validation of RFI detection methods (Aissou et al., 2021; Jullian et al., 2022).

Sustainability of satellite signals and airspace information, particularly while transmitting via quantum sensors in quantum optics, has contributed important progress in developing quantum communication networks (Pirandola et al., 2020). Atomic clocks, another significant application of quantum sensors, are essential for GPS and telecommunications that require exact time measurements in synchronizing worldwide communication systems (Ludlow et al., 2015). The GPS technology, which has a tremendous opportunity for both civilian and military navigation, relies on the accuracy of these quantum sensors to provide location data (Wineland & Dehmelt, 2021). The demonstration of the precision and sensitivity of quantum optics, atomic clocks, and magnetometry may prove advantageous in enhancing precision navigation and timing (PNT), as it can provide navigation locations that are independent from GPS operation. Traditionally, these systems have relied strongly on GPS technology, but GPS comes with inherent vulnerabilities such as signal jamming, spoofing, and signal degradation. These limitations create a critical need for more resilient, autonomous, and accurate navigation systems. Quantum sensors, particularly quantum-based inertial sensors, are emerging as the solution to these challenges, offering unprecedented precision without reliance on external signals like GPS (Abraheem et al., 2025).

3. Method

The current paper uses a qualitative research method, therefore the methodology uses various significant theoretical scientific interpretation from different authors with similar occured events which is important to involve multiple literature sources. The collected data contributes to accomplish to solve the research question concerned with observed object. The analysis method consists of available data for conducting in the sample of the flight J2 8243 to evaluate the RFI influence on civil aviation aircraft. RFI generation has a comprehensive dataset that includes examples of GNSS signals under various conditions, such as normal operations, jamming, spoofing, and combined threats. The collection of the data was achieved utilizing real-world GNSS signal data generated from various sources and a simulation tool. Additionally, the Digital Flight Data Recorder (DFDR) and ADS-B data sets were retrieved and processed for use in the subsequent illustration of the geographical area of interest subject to RFI and to identify differences between the fake and the actual flight path of the specific aircraft. Finally, the study describes the observed trends and actual parameters obtained from a scheduled flight conducted on an Embraer aircraft through an area during known RFI occurrences.

4. Resul and Discussion

4.1. Impact of RFI on aircraft operation experiencing jamming and spoofing

Updated statistical data concerning GNSS disruption and related incidents highlight the growing challenge of GNSS interference in civil aviation. Eurocontrol (2021) estimates that 38.5% of European air traffic destinations operate across regions regularly affected by RFI and 5% of air traffic requires special assistance due to GNSS interference. A significant part of the information reported by the flight crew emphasizes that without backup navigation systems, the aircraft are experiencing the most severe disruptions (Fol & Felux, 2022). Furthermore, the ADS-B data analysis validated the substantially higher number of GNSS jamming incidents in 2024 (Felux et al., 2024). The result of an investigation by OPSGroup (2024) has revealed a catastrophic trend, reporting a 500%

increase in GPS spoofing incidents. Civil Aviation Spoofing Surge has an average of 1,500 flights per day that are intensively affected around conflict zones. These disruptions over the airspace of Israel, Lebanon, and Russia forced aircraft rerouting and posed risks to flight safety.

Referring to EASA (2023) SIB as per Table 1, there are some notable instances of aircraft experiencing jamming and spoofing GNSS signals. The rise in jamming and spoofing is particularly active in regions experiencing geopolitical tensions. However, the incident that occurred in Mexico City (Buesnel & Holbrow, 2017), where pilots reported GPS signal loss and receiver outages while on final approach to the international airport, is suspected to be caused by illegal jamming devices. A GPS jammer installed near Harbin Airport, China, in 2019, disrupted aircraft navigation, forcing authorities to intervene. In March of the same year, there were reports of "circle-style" GPS spoofing in Tehran, the capital of Iran (Buesnel, 2020), which was not a military area. Due to the conflict since 2022, GPS jamming was widespread in Ukraine, affecting civilian aircraft, while disruptions complicated navigation and communication for pilots. Interference affected GPS in several NATO exercises, impacting the aviation sector in Estonia, Latvia, and Lithuania (Garcia et al., 2024; Pultarova, 2025). The Middle East, Eastern Europe, and the Mediterranean and Black Sea regions also reported GPS interference incidents, with aircraft flying over experiencing unreliable ADS-B signals. Some flights had to be tracked using Multilateration (MLAT) instead of GPS, causing aircraft to deviate up to 80 nautical miles from their intended flight paths. Pilots had to rely on radar vectors from air traffic control (ATC) to navigate safely (OPSGroup, 2024). The Fig. 3 is representing occurrence examples over Mediterranean and Black Sea regions RFI affected aircraft an incorrect diversion trajectory.

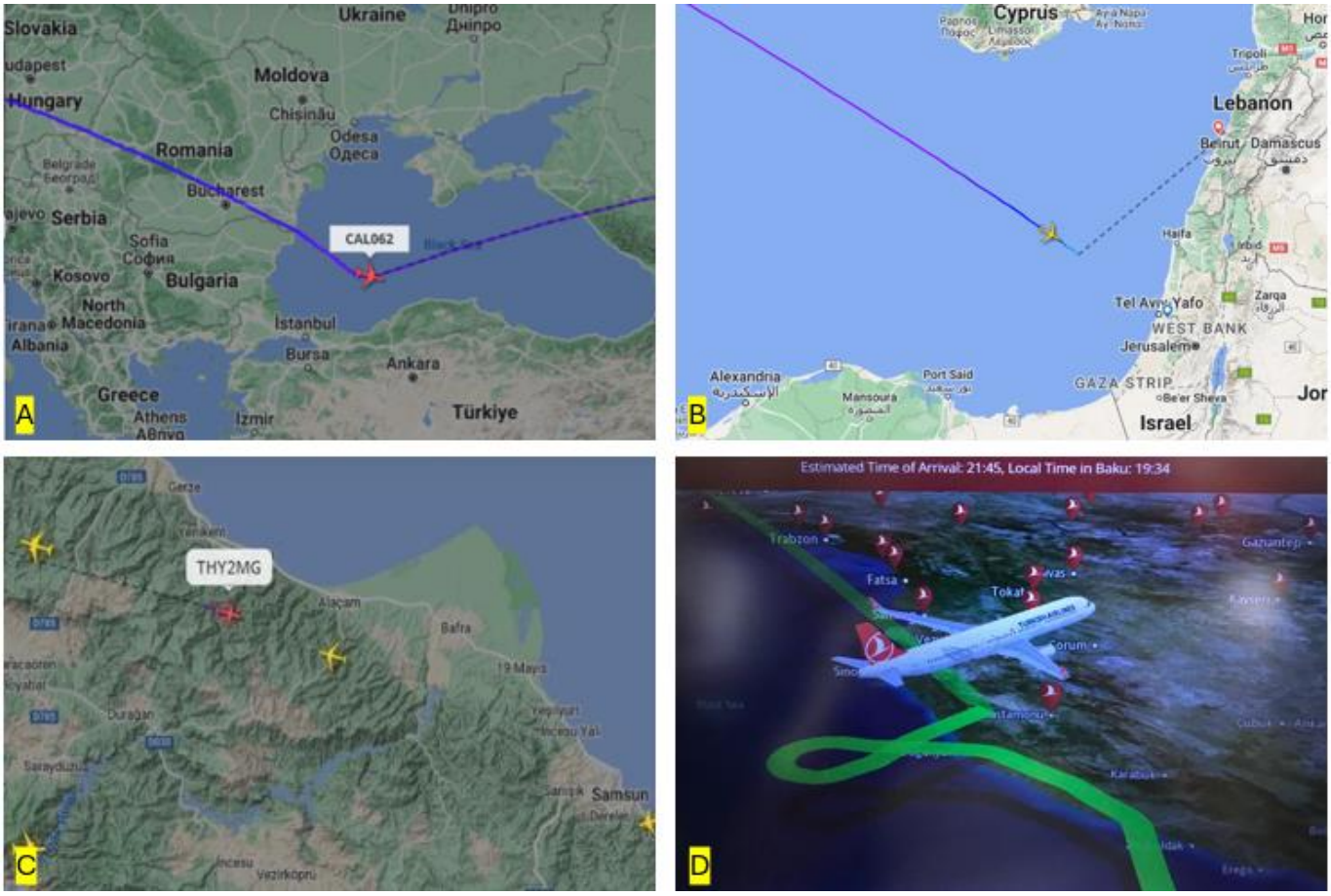

Fig. 3. (A, B, C, D). Aircraft affected by RFI attacks over the Mediterranean and Black Sea regions (Sources: A and B Lomas, 2025; C and D: Author's own work)

Can GPS jamming happen accidentally, especially if the aircraft navigation equipment receives an authentic GNSS signal? - Occurs only if corresponding multi-mode receivers (MMRs) fail or the interface between electronic systems becomes inoperative for technical reasons. Once increasingly, research, manufacturer information letters, and authority awareness reports are seeing it cause deliberately, in an illegal way, rendering the devices used in air vehicles. GPS jamming is illegal, excluding conflict regions, where possible to apply. Using the modern

Multilateration (MLAT) technique, Flightradar24 can track flights experiencing GPS jamming and spoofing in the region of intrusion. Fig. 3(A) shows the Boeing 777 China Airlines flight C162 over the Black Sea near the northern coast of Turkey being tracked via MLAT, dictated to weak and unreliable GPS and ADS-B signals in the crossed area. Fig. 3(B) is a similar incident in which United Airlines Boeing 787-10 flight UA84 (New York-Tel Aviv) in March 2024, which was a victim of GPS spoofing, leading to an incorrect maneuver plotted for the aircraft's flight path (Lomas, 2025). In June 2024, again over the Black Sea, the Turkish Airlines flight TK 334, Istanbul-Baku, (Fig. 3(C)) Airbus A321 spoofing of GPS signals, resulted in the aircraft appearing in places that it should not appear (Fig. 3(D): taken from the passenger display unit by the author during the given flight).

Analysis of the particular aircraft types or families to identify their vulnerability affected by jamming and spoofing, in short, on a global scale against RFI attacks will lead to similar results. The implication of such an intrusion action on GNSS usually impacts appropriate receivers providing navigation systems, either Boeing or Airbus, as well as other regional and business jet aircraft. The consequence is the disruption of functionality in most flight management systems, including GPS, FMGC, TCAS, GPWS, MMR, FMS, and others. Airbus (2019) has released an in-service information, (bulletin) for Airbus aircraft in the event of GNSS loss and interference. This information letter includes announcement messages on the navigation and alerting displays, which serve as cockpit and system effects to significantly increase flight crew awareness. However, Boeing and other types of aircraft design a similar warning effect, albeit with different display names and character of messages. Description of the common cabin and system display effects and functions are containing the functional and system effects corresponding to cockpit effects on the PFD, ND, ECAM (EICAS) by alerts/status/ INOP systems indications with voice messages.

The incident employing jamming GPS signals potentially disrupted and affected navigation, communications, and surveillance systems on Azerbaijan Airlines Flight J2-8243 on 25 December 2024 (Summers, 2025; Domogala, 2025). Sequentially, this flight was affected by GPS spoofing near western Russian airspace, misleading aircraft into reporting incorrect positions, thereby leading to dangerous miscalculations of actual flight coordinates. Pilots lost GPS-based guidance and needed to rely on alternative navigation methods using radionavigation aids. The Grozny ATC tower's assistance with vectoring during the procedure did not promise a solution for the proper approach and landing. The situation resulted in increased cockpit workload and stress for pilots, particularly in low-visibility conditions in the airspace where RFI was used. At the final stage of descents, ADS-B transmitted the wrong navigation coordinate; however, the aircraft has flown near Grozny airport which happens in the situation of electronic warfare interference. The next scenario is revealing the exact and clear impact of spoofing on the real aircraft, which experienced, during the guidance to the airport destination, an unexpected case of occurrence that nearly caused a collision with the mountain top. Following ATC instructions, the aircraft takes the wrong course due to incorrect calculations of the navigational positions, redirecting the aircraft in the opposite direction. Meanwhile, the flight crew is unable to define their accurate location in the airspace contaminated with fake signals.

During the transmission of the GNSS signals, it is important that the waves' spatial variety and capture phase by the aircraft receivers reflect the different directions of arrival (DoA) of the derived signals (Rothmaier et al., 2021). Under standard conditions, these metric angles need to be different for each active satellite; usually, three are necessary for aircraft needs. Consequently, an aircraft antenna receives signals from three satellites distributed across the entire sky for position calculation. However, signals generated from a spoofer will arrive from a single direction. In some cases, if the RFI equipment has an enhanced attack capability, it will transmit from a few directions using multiple transmitting antennas mounted. Then all signals will be transmitted maliciously from a single antenna, and aircraft displays will show a false alert and a fake position. The spoofing detection, based on measured DoAs, is shown in Fig. 4 for the concept of three satellites. Angles/directions of signals i and j are different when coming from the authentic satellites (black arrows) but nearly identical when coming from a single spoofing source (red arrow).

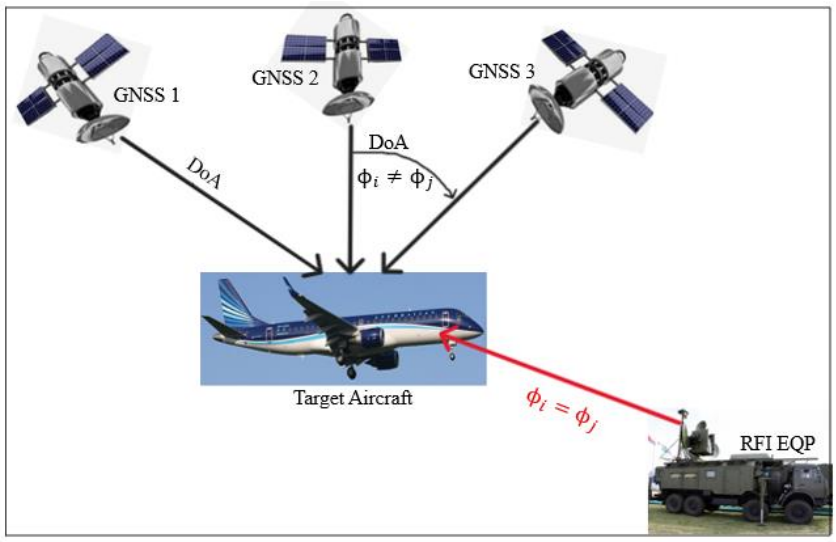

Fig. 4. Authentic diverse signal directions from GNSS and spoofing signal directions from RFI equipment (Source: Author's own work)

The difference in signal angles or directions between authentic satellites and a spoofing source can be expressed using spatial processing techniques. One useful equation for detecting spoofing based on direction of arrival (DoA) can be derived from the Neyman-Pearson Likelihood Ratio Test (LRT) that is independent of prior probabilities (Van Trees, 2001). The general hypothesis test is presented in Equation 1.

$$\log \Lambda\,(y) = h_0^T R^{-1} y - \frac{1}{2}(h_0^T R^{-1} h_0) \tag{1}$$

Whereas;

log Λ(y) - conditioned on (y)

Λ (y) - is the likelihood ratio test statistic

y – represents the observed measurements of signals of DoA

h_0 – represents the expected difference between the DoAs of signals from authentic satellites under null hypothesis (H0).

R - is the covariance matrix of the original DoA measurements.

The study by Rothmaier et al. (2019a) first used a new version of a hypothesis iteration algorithm from Neyman-Pearson and found its efficiency and effectiveness to identify groups of fake satellites, even when there was weak multipath interference. Later research conducted by Rothmaier et al. (2021) enhanced the development of the previous study, considering necessary tests for reasonable performance under real-world conditions. Presented flight test data and data collected during a government-sponsored live spoofing event to support the validation of the theoretical derivations. Recognizing the uncertainty associated with using noisy measurements to determine the presence of a spoofing attack, the new framework study approaches the decision problem as a statistical hypothesis test. The null hypothesis is introduced as ($H0$), representing the nominal situation without spoofing and the alternate hypothesis, considered as ($H1$), represents a spoofed situation attack on the object of interest. Using the formulated hypothesis in accordance with equations created by authors, which derives the formula, the distribution of the statistic likelihood ratio test [log Λ(y)] was conditioned on the observed measurements of DoA signals under nominal and spoof conditions. The threshold (γ) is found by solving the quantile function or inverse cumulative density function (cdf) of the random variable log Λ(y) conditioned on $y \sim H0$ for $PFAmax$, Equation 2.

$$\gamma = \frac{1}{2}\,\bar{\phi}^T R^{-1} \bar{\phi} \; + \; \Phi^{-1}\left(P_{FA_{max}}\right) \sqrt{\bar{\phi}^T R^{-1}\,\bar{\phi}} \tag{2}$$

γ - Detection threshold

Φ^{-1} - Quantile function

$\bar{\phi}$ - arc ($\bar{\phi} = \Delta\theta$) between the two and more satellites normalized by the measurement standard deviation (σ) for different maximum false alert probabilities.

$P_{FA_{max}} -$ *is* the false alert probability or statistical significance level

The optimization problem is solved using the result of the detection threshold (γ), where Φ^{-1} is the quantile function or inverse cumulative density function (cdf) of the Standard Normal distribution.

Application of the theoretical base of the study by Rothmaier et al. (2021) is the best methodology example to check the validity on the aircraft affected by RFI on flight J2 8243, as demonstrated in Fig. 5.

Fig. 5. RFI activation result on the aircraft flight J2 8243 trajectory paths (need to place on horizontal layout) (Source: Author's own work)

Under nominal conditions, the normalized azimuthal DoA measurements from GNSS are multipath, both in flight and after the descent stage upon entering Russian airspace. The flight profile includes descents with a heading of 291 degrees and turns with various banks. The data collection retrieved from the DVDR and ADS-B report for the given flight provides a detailed description of the event. The black line shows a standard normal flight trajectory according to the flight plan to the desired destination assigned to Grozny airport. After the first step impacted by jamming, the aircraft lost both GPS functions; therefore, the onboard navigation units measured the erroneous location. Activation of the spoofing (marked with a red line from RFI EQP) generated identical DoA signals that misled the aircraft. In turn, having two circles over the Grozny region, the aircraft was redirected to the fake destination; meanwhile, the ADS-B transmitter indicated fake positions. The over bounds of the measurement error ensure a fake navigational location and behavior of the aircraft 60 km away from the actual position, which supports the likelihood of the false alert probability and the multipath restriction strategy (Rothmaier et al., 2021).

All satellite signals spoofed from the same transmitter, makes the situation complicated and more dramatic, means that all signals come from the same direction under spoofed conditions. Due to violations of the receiver, it cannot lock emitted signals by the spoofer and still assumes that it is tracking some authentic satellite signals. When the attacker uses multiple antennas to transmit fake signals from multiple sources, it reduces the detection capability of GNSS signals (Rothmaier et al., 2019b) by the aircraft navigation receivers. The intrusion to GNSS waves by using RFI may occur, either unintentionally in result of failure caused by instrumentation or communication systems (Berglund et al., 2011; National Academies of Sciences, Engineering, and Medicine, 2023) or intentionally, mainly observed in conflict zones, which may limit use of GNSS signals or prevent for their intended purpose. Actually, the intentional RFI is caused by harmful transmitters, where sending out noise at the carrier frequency (jamming) or false signals (spoofing), converted to pseudo-random noise codes to trick a receiver into calculating a false position (Chew et al., 2023).

4.2. The available prevention tools and potential solution to prevent application of RFI to GNSS and aircraft

Many scientific investigations, modern technology, various experiments conducted by scientific research institutes, and special laboratories have not yet given positive results for the protection of aircraft from the introduction of jamming and spoofing. Nevertheless, as numerous reports of aviation authorities and bodies studying this problem show, attacks on civilian aircraft using RFI increase year after year. Society and the relevant industries have not yet received any kind of protection warranties for solving this problem. Additionally, the proposed detection tools and methods are only intended to monitor and identify the source of false signals generated against GNSS operations.

The latest developed receivers and software to track the flights advantageously use the Multilateration (MLAT) method, which positions accuracy near ADS-B capability, with an error margin of 10-20 meters. However, the main limitation with MLAT tracking is aircraft altitude, that the signal from the lowest altitude below between 5,000 and 10,000 feet decreases and the aircraft is no longer displayed on the map (Petchenik, 2025). Besides airspace alerts, some researchers have proposed long-term ways to mitigate GNSS interference, such as Spatial Processing and GNSS-Band Radio Interference on Operational Avionics (Rothmaier et al., 2021; Osechas et al., 2022), Automatic Gain Control (AGC) monitoring (Meng et al., 2022), Carrier-to-Noise Density Ratio (C/No) monitoring (Hegarty et al., 2018), the Cross Ambiguity Function (CAF) monitoring (Zarrinnegar et al., 2023), and using Navigation Message Authentication (NMA) (Götzelmann et al., 2023). Finally, Safran Electronics & Defense's sector is currently working on a new device, developing the Interference Detection Mitigation (IDM) algorithms, enabling it to detect GNSS interference and immediately switch to a resilient, autonomous source, ensuring mission continuity (Safrangroup, 2025).

The risks associated with spoofing and jamming attacks are often emitted by military bases and have an omnidirectional range. Affecting civil aircraft even at high altitudes could threaten passenger safety. Safran's solution for flight safety is developing an ultra-compact, highly reliable, and powerful hybrid inertial navigation system (INS) that can be integrated into civil aircraft to ensure precise, safe navigation (Safrangroup, 2025). The most powerful mitigation against RFI, particularly for suppression jamming and spoofing is a dynamic sensor data fusion system. The dynamic sensor data fusion system is designed for suppression, jamming, and spoofing and is the most expensive option; however, it interfaces sensors for GNSS and IRS, which contributes to system sustainability. Most commercial aircraft categories are equipped with IRS, ensuring reliable signal transmission and providing accurate position data even during periods of GNSS jamming or spoofing (Dovis, 2015; Fernández-Hernández et al., 2019).

4.3. IRS/INS solution for GNSS RFI

Based on the data analysis, it's safe to assume that IRS/INS plays a crucial role in maintaining the functionality of aircraft navigation systems, whether due to jamming, spoofing, or other disruptions when GNSS signals are interfered with. Relying on the high reliability of modern IRS systems, new-generation aircraft are often designed to combine IRS with GNSS to enhance the accuracy of navigation even when satellite signals are unavailable for any reason. The IRS is, by the modern operational configuration, at a significant advantage, even if GNSS data do not support the combined functions.

- Independent Navigation: Operates independently, calculates an aircraft's position using input signals from accelerometers and gyroscopes to track the aircraft's movement from a known starting position.
- Fallback System: The Flight Management System (FMS) continues using IRS data to provide velocity and attitude data for automated flight operations and determine the aircraft's position.
- Backup Support Radio Navigation System: Within the Radio Navigation Aids range, the aircraft is able to use IRS signals to improve IRS-based navigation for VOR-DME (VHF Omnidirectional Range and Distance Measuring Equipment) operation as an alternative navigation positioning source.
- Dead Reckoning Navigation: IRS continuously estimates the aircraft's velocity and position relative to its initial location, allowing the aircraft to continue navigating using dead reckoning.
- Drift Angle Correction: Since IRS navigation is based on dead reckoning, using external sources, like radio navigation aids, corrects the positioning data due to accumulated small errors causing a drift.

The Fig. 6 represents block diagram of IRS/INS modules estimating the navigation data using components of input signals and output navigation parameters of aircraft systems.

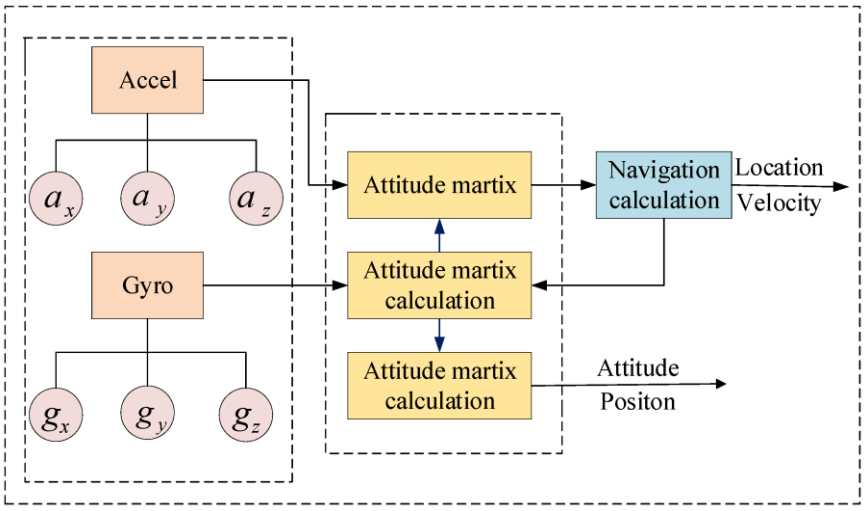

Fig. 6. Block diagram of IRS/INS modules estimating for the navigation data (Xiao et al., 2022)

An inertial system is a "self-contained" equipped in aircraft providing as additional source for navigation system. Moreover, it needs appropriate data inputs to compensate the errors, increasing position accuracy. The Inertial Measurement Unit (IMU) is the main module containing the accelerometers and gyroscopes, responsible for collecting motion data. Accelerometers detect changes to determine velocity and position while measuring linear acceleration along three axes (X, Y, and Z), integrating these data over time. Gyroscopes measure angular movement, helping determine the aircraft's heading and attitude (pitch, roll, and yaw). Unlike mechanical gyroscopes, modern IRS measurement units use Ring Laser Gyros (RLGs) or Fibre Optic Gyros (FOGs) to precisely orient attitudes. The duration and accuracy of an IRS are gradually improved depending on the quality of the integrated IMU (ICAO, 2018). Previous stabilized platforms of the IRS have a position error of 2 nm/hr; a high-performance IRS could guarantee a drift in the magnitude of 1 NM/hour (Stanisak et al., 2024), and the modern RLG in inertial systems tends to have error rates of 0.6 nm/hr, which an RNP10 requirement could be met for multiple hours.

Inputs about the present position (PPOS) are undoubtedly necessary before a flight is initialized with a known starting position to ensure accurate tracking throughout the flight, which is carried out by the Alignment System. Consequently, the Air Data Computer (ADC) is working alongside pitot-static sensors to refine altitude and speed calculations and to feed this data to the IMU. The value of barometric altitude helps stabilize the vertical velocity, meanwhile the value of True Air Speed (TAS) allows for the calculation of wind speed and direction, in order to provide initial outputs to measure the inertial altitude and drift angle. The Inertial Reference Unit (IRU) is a processor that computes the IMU input data, integrates it over time, and provides navigation outputs to appropriate aircraft systems. IRS continuously tracks heading reference and aircraft attitude (pitch, roll, and yaw), helping pilots to maintain situational awareness as well as supporting instrument-based flight. Receiving the pitch, roll, and yaw angles into the flight control unit, the IRS supplies precise orientation and movement data to the autopilot system, ensuring stable flight control and manoeuvring. Typical output data from the inertial system fed to other aircraft avionics and other systems includes:

- Magnetic Heading and Drift Angle.
- True Air Speed (TAS) and True Heading
- Ground Speed (G/S), Vertical Speed and Rate
- Latitude, Longitude, Pitch, Roll, and Yaw
- Altitude
- Wind Speed and Direction.

Finally, the Cockpit Displays (ND, PFD, and announcement devices) supply pilots with real-time heading, pitch, roll, and navigation data. A combined interface control panel and display unit is used for initializing and entering necessary latitude and longitude position data while the aircraft is on the ground. A typical IRS interface control panel is introduced in Fig. 7 (Flightvectors, 2025).

Fig. 7. A typical IRS control panel and display unit used on Boeing 757/767 (Flightvectors, 2025)

The IRS is a single navigation system that provides positioning, altitude, velocity, and timing, ensuring a reliable interface with LRRA and GPWS to avoid ground proximity collisions when aircraft navigation systems are disrupted by GNSS due to jamming or spoofing. Penetration of fake signals generated by RFI equipment on the modular avionic unit (AMU) used on Embraer 190 and Integrated Modular Avionics (IMA) installed on Boeing and Airbus aircraft for a backup (2nd set) unit is secured and is implemented through a similar concept. Either MAU or IMA architectures-nearly equivalent systems-integrate multiple functions into a single system for efficiency and flexibility. This is particularly evident in the Boeing 787 Dreamliner, where avionics functions are distributed across modular computing platforms. Airbus is implementing IMA systems in aircraft like the A380 and A350, allowing avionics applications to run on shared computing resources rather than separate dedicated units. The MAU/IMA systems, which receive signals from various aircraft sensors (except GPS), such as IRS, Low Range Radio Altimeter (LRRA or radar altimeter), and Ground Proximity Warning Systems (GPWS), interact with each other to prevent terrain collisions, as validated empirically during Flight J2 8243, relying on Low Range Radio Altimeter's transmitted data, Fig. 8.

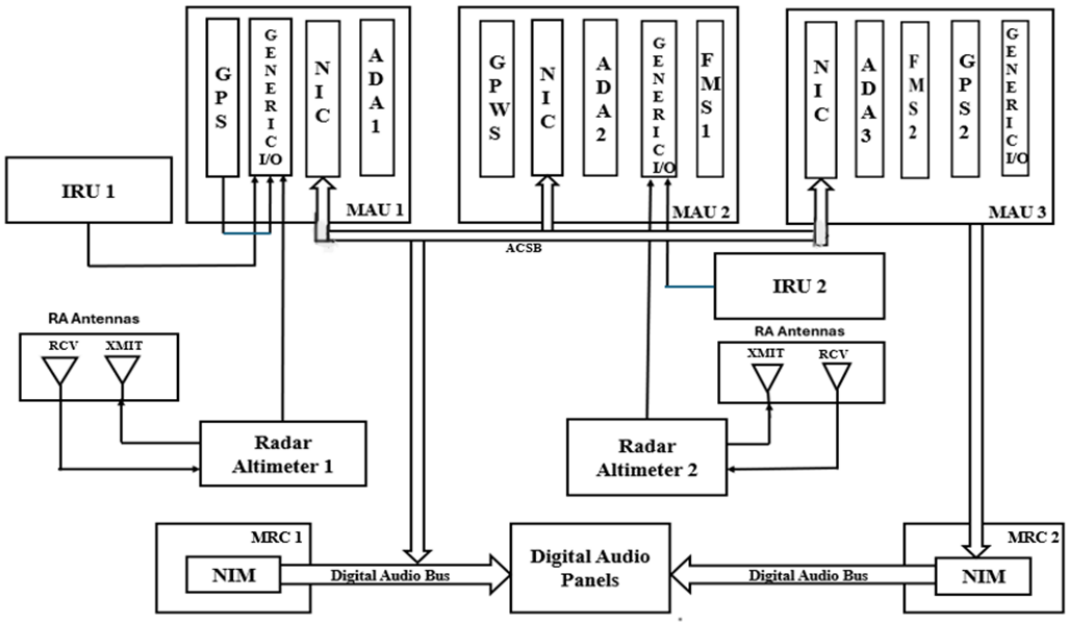

Fig. 8. Block diagram: Interface between Navigation hardware of the Aircraft Embraer E190 (System Schematic Manual (SSM), 2025)

MAU/IMA uses IRS data for precise aircraft positioning while helping in navigation and flight management as well as terrain awareness. Radio altimeter connection provides real-time altitude readings above the ground, which are used for landing approach, terrain avoidance, and GPWS alerts. In turn, the GPWS interaction processes voice message to alert pilots of potential terrain hazards. The reason why the MAU/IMA unit might not receive GPS signals is dedicated functionality, considered to secure IRS operability in the cases of RF interference against civilian aircraft to secure flight safety and passenger lives. Partitioned avionics architecture is an excellent design decision taken by aircraft manufacturers, taking into account increasing intentional intervention by jamming and spoofing and the geography of armed conflict zones. Following this incident, the European Union Aviation Safety Agency (EASA) issued a warning to airlines to refrain from flying in western Russian airspace due to heightened safety concerns. The EASA safety board notes that Russian authorities haven't provided adequate proficiency in airspace risks related to RFI implementation (Villamizar, 2025).

4.4. The incoming modern technology implementation to obstacle the RFI

AI-based and Quantum technologies are being developed to detect and mitigate RFI, including jamming and spoofing threats, particularly in GNSS. However, it does not guarantee the reliable operation of aircraft during such attacks. These AI-driven GNSS interference detection solutions enhance traditional detection methods by learning from new data and adapting to evolving threats. AI algorithms improve the reliability of GNSS-dependent applications by identifying and classifying jamming and spoofing attempts (Bong et al., 2023). The BREGO Project, funded by the European Space Agency, uses AI and machine learning to detect and mitigate GNSS threats in real time. The U.S. Space Force developed the PNT-SENTINEL Program, applying an AI-powered system that geolocates interference sources and predicts patterns of GPS jamming and spoofing (Gutierrez, 2024; Slingshot Aerospace, 2025). In addition, the study by Aftatah and Zebbara (2024) focuses particularly on the utilization of artificial intelligence (AI) approaches; thereby, the authors aim to highlight the importance of artificial intelligence in improving the security of navigation systems via intelligent systems for timely detection and neutralizing these threats. Alongside the AI-powered Navigation System to counter GPS jamming and spoofing threats, the Quantum application concept is the most considered technology to isolate the attacks in the near future. SandboxAQ develops the AQNav security geo-magnetic navigation system, leveraging AI algorithms, quantum sensors, and the Earth's crustal magnetic field in the case if GPS is unavailable or compromised. The product of the latest technology in modern systems is going to provide an all-weather and terrain-agnostic, unjammable, and spoofless navigation solution in a real-time regime (Macey, 2024).

It is expected that quantum technologies will significantly improve the positioning, navigation, and timing (PNT), especially inertial navigation. Time standards and frequency transfer (TFT) are fundamental, which provide precise timing for global navigation satellite systems (GNSS) (Jozsa et al., 2000; Giovannetti et al., 2001). Quantum technology is an emerging area that utilizes the manipulation and control of individual quanta for multiple applications and is expected to have strategic and long-term impacts. However, a precise forecast of quantum technology deployment is not possible, since the transition from the laboratory to real-world applications has not been implemented or is in progress (Krelina, 2021). The quantum technologies are anticipated to have extensive use in space. Using these technologies will lead to combined networks of quantum sensing and communications with other emerging technologies, such as artificial intelligence and laser communication. The deployment of practical employment around the Earth will ensure a response to the growing anti-satellite threats (Krelina, 2023). Quantum sensors play a crucial role in transforming critical sectors by leveraging the unique principles of quantum mechanics, thereby enabling unprecedented precision, security, and efficiency. Real-world uses of quantum sensors in Quantum Key Distribution (QKD) for accurate navigation and spotting hidden threats, along with combining them with current systems and Artificial Intelligence (AI) for quick decision-making, are still being developed (Abraheem et al., 2025). The elements of quantum sensors, which have found applications in navigation systems, mainly consist of atomic clocks and gyroscopes. Atomic clocks based on quantum principles provide precise timekeeping, which is essential for global positioning systems (GPS) and satellite communications. Quantum gyroscopes offer highly accurate rotational measurements, crucial for navigation in autonomous vehicles, drones, and aerospace applications (Khang & Rath, 2025).

5. Conclusion

The increasing prevalence of GNSS (Global Navigation Satellite System) jamming and spoofing poses a significant threat to modern aviation, particularly in regions affected by geopolitical conflict or military activity. These disruptions compromise the integrity of satellite-based navigation systems, which are critical for aircraft

positioning, route tracking, and approach procedures. Operational Impacts of GNSS Interference - jamming involves the deliberate transmission of radio frequency signals that overpower legitimate satellite signals, rendering navigation systems unreliable or unusable. Spoofing, on the other hand, deceives receivers by broadcasting false GNSS signals, potentially leading aircraft off course or misrepresenting their true location which is experienced aircraft Embraer-190 over Russian airspace. The consequences of such interference contributed to loss of positional awareness during critical flight phases such as approach and landing of the flight J2 8243. Due to increased workload for pilots even reverted to alternative navigation methods does not affect to avoid the fatal incident. The potential miscommunication with air traffic control especially when automated systems are compromised and ILS has been deactivated at airport destination, influenced reduced effectiveness of onboard safety systems. The crash of Azerbaijan Airlines flight J2 8243 in December 2024 near Grozny is a tragic example of how GNSS interference can exacerbate already dangerous conditions. Consequently, this incident underscores the vulnerability of civil aviation to GNSS disruptions, especially in conflict zones where such tactics are increasingly employed.

Although it remains clear that GNSS jamming is not directly caused the accident, its presence contributed to a degraded situational environment. Navigation signal blockage has hindered the crew's ability to accurately assess their position and trajectory. Stressful conditions were intensified by unreliable instrumentation, increasing the margin for error during emergency manoeuvres. Jamming and spoofing GNSS signals compromised and disrupted overall operations, mostly causing imprecise approaches and missed landings, leading to conducting twice go around procedure while avoiding collisions with mountain. However, the targeted aircraft used IRS data as well, for precise aircraft positioning while helping in navigation and flight management meanwhile providing terrain awareness. Radio altimeter provided real-time altitude readings above the ground, during two landing approach sensing terrain avoidance, having connection with GPWS which alerted to crew members to cancel the landing with both attempts. In turn, the direct GPWS interaction with LRRA is potential navigation tools to avoid terrain hazards. The finding reveals that reliable interaction between EGPWS and LRRA, while receiving a signal from IRS, has avoided terrain collision after two unsuccessful approaches, thus filling the gap of the lack of reliable terrain awareness during repeated approaches. This is a dedicated functionality which is secured by IRS operability in the cases of RF interference against civilian aircraft and if not receive GPS signal, to secure flight safety and passenger lives. As aviation continues to rely heavily on satellite-based navigation, the risks posed by jamming and spoofing must be addressed through robust detection and mitigation technologies including multi-sensor fusion and inertial backup systems. In this context pilot training and procedural updates to handle GNSS outages effectively can be reached by international collaboration and common regulations to monitor GNSS interference, especially in sensitive airspace. Numerous incidents serve as a sobering reminder that GNSS integrity is not just a technical issue-it is a matter of life and safety in the skies. Finally, GNSS jamming and spoofing are no longer hypothetical threats-they are real, present, and increasingly dangerous. The J2 8243 accident serves as a stark reminder that even indirect interference can have fatal consequences when combined with hostile environments. Aviation must evolve to meet this challenge, ensuring that the skies remain safe, even when signals go dark.

References

Abraheem, S. M., Ali, M. E., & Abuali, R. M. (2025). Emerging Trends in Quantum Sensors: Applications in Defense and Communication. *Middle East Journal of Pure and Applied Sciences* (MEJPAS), 1(1), 19-37.

Aftatah, M., & Zebbara, K. (2024). A Comprehensive Survey on Secure Navigation for Intelligent Systems: Artificial Intelligence Approaches to GPS Jamming and Spoofing Detection. In: Mejdoub, Y., Elamri, A. (Eds.), *Lecture Notes in Networks and Systems*: Vol.1123. Proceedings of the *International Conference on Connected Objects and Artificial Intelligence* (pp. 105-110). Springer. https://doi.org/10.1007/978-3-031-70411-6_17

Airbus. (2019). *In-service Information, GNSS loss and GNSS Interferences on Airbus A/C*. Ref: 34.36.00049.

Aissou, G., Slimane, H. O., Benouadah, S., & Kaabouch, N. (2021). Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference* (UEMCON) (pp. 0649-0653). IEEE. https://doi.org/10.1109/UEMCON53757.2021.9666744

Ali, B. S., Ochieng, W. Y., Schuster, W., Majumdar, A., & Chiew, T. K. (2015). A safety assessment framework for the Automatic Dependent Surveillance Broadcast (ADS-B) system. *Safety science*, 78, 91-100. https://doi.org/10.1016/j.ssci.2015.04.011

Altaweel, A., Mukkath, H., & Kamel, I. (2023). GPS Spoofing Attacks in FANETs: A Systematic Literature Review. *IEEE Access*, 11, 55233-55280. https://doi.org/10.1109/ACCESS.2023.3281731

Berglund, H.T., Blume, F., Estey, L., & White, S. (2011). GPS/GNSS Interference from Iridium Data Transmitters. In *Proceedings of the American Geophysical Union Fall Meeting* 2011, San Francisco, CA, https://www.researchgate.net/publication/259677698_GPSGNSS_Interference_from_Iridiu_Data_Transmitters

Blois, M., Studenny, J., O'Keefe, K., & Liu, B. (2023). Baseline spoofing detection for aircraft with standard navigation hardware. *Proceedings of the 36th International Technical Meeting of the Satellite Division of the Institute of Navigation* (pp. 824–835). https://doi.org/10.33012/2023.19413

Bong, J. H., Kim, D., & Jeong, S. (2023). AI-based Algorithm for GNSS Spoofing Detection. In 2023 *14th International Conference on Information and Communication Technology Convergence* (ICTC), (pp. 1630-1632). IEEE. https://doi.org/10.1109/ICTC58733.2023.10392390

Bose, S. C. (2021). GPS spoofing detection by neural network machine learning. *IEEE Aerospace and Electronic Systems Magazine*, 37(6), 18-31. https://doi.org/10.1109/MAES.2021.3100844

Buesnel, G. (2020). *Thousands of GNSS jamming and spoofing incidents reported in* 2020. https://rntfnd.org/2020/12/24/thousands-of-gnss-jamming-and-spoofing-incidents-reported-in-2020-guy-buesnel/

Buesnel, G., & Holbrow, M. (2017). *GNSS Threats, Attacks and Simulations, PNT Advisory Board Baltimore*, 28-29. https://archive.gps.gov/governance/advisory/meetings/2017-06/buesnel.pdf

Chew, C., Roberts, T. M., & Lowe, S. (2023). RFI mapped by spaceborne GNSS-R data. NAVIGATION: *Journal of the Institute of Navigation*, 70(4), Article 618. https://doi.org/10.33012/navi.618

Darabseh, A., Bitsikas, E., & Tedongmo, B. (2019). Detecting GPS jamming incidents in OpenSky data. In *Proceedings of the 7th OpenSky Workshop*, 67, 97–108. https://doi.org/10.29007/1mmw

Domogala, P. (2025). *The dangers of GNSS interference*. https://ifatca.org/article/the-dangers-of-gnss-interference/

Dovis, F. (2015). *GNSS interference threats and countermeasures*. Artech House.

EASA. (2023). *EASA SIB No.: 2023-05-Europe, Subject: Safety Information Bulletin, Operations – ATM/ANS – Aerodromes Possible Risks Emerging During Summer* 2023. https://ad.easa.europa.eu

EASA. (2024). *EASA SIB No.: 2022-02R3 Global Navigation Satellite System Outage and Alterations Leading to Communication / Navigation / Surveillance Degradation*. https://www.easa.europa.eu/en/domains/air-operations/global-navigation-satellite-system-outages-and-alterations

Eurocontrol. (2021). *EUROCONTROL Think Paper #9 - Radio Frequency Interference to satellite navigation: An active threat for aviation?* https://www.eurocontrol.int/publication/eurocontrol-think-paper-9-radio-frequency-interference-satellite-navigation-active

Felux, M., Fol, P., Figuet, B., Waltert, M., & Olive, X. (2024). Impacts of global navigation satellite system jamming on aviation. NAVIGATION: *Journal of the Institute of Navigation*, 71(3), Article 657. https://doi.org/10.33012/navi.657

Fernández-Hernández, I., Walter, T., Alexander, K., Clark, B., Châtre, E., Hegarty, C., Appel, M., & Meurer, M. (2019). Increasing international civil aviation resilience: A proposal for nomenclature, categorization and treatment of new interference threats. In *Proceedings of the 2019 international technical meeting of the institute of navigation* (pp. 389-407). https://doi.org/10.33012/2019.16699

Figuet, B., Waltert, M., Monstein, R., & Felux, M. (2022). Impact of GNSS outage on mid-air collision risk. In *Proceedings of the 2022 International Workshop on ATM/CNS (IWAC)* (pp. 41–48). https://doi.org/10.57358/iwac.1.0_41

Flightvectors. (2025). *Cockpit B757/767*. https://www.flightvectors.com/Aircraft-Cockpit-Posters-Procedure-Trainers/Boeing-Cockpit-Posters-Procedure-Trainers/B757-B767/

Fol, P., & Felux, M. (2022). Identification and operational impact analysis of GNSS RFI based on flight crew reports and ADSB data. In *Proceedings of the 7th International Workshop on ATM/CNS (IWAC)* (pp. 33–40). https://doi.org/10.57358/iwac.1.0_33

Garcia, M., Dolan, J., & Sirigu, G. (2024). *GPS interference and spoofing in the Baltics*. Aireon. https://aireon.com/wp-content/uploads/2024/05/Aireon-White-Paper_GPS-Interference_May2024.pdf

Ghanbarzade, A., & Soleimani, H. (2025). *GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning*. https://doi.org/10.48550/arXiv.2501.02352

Giovannetti, V., Lloyd, S., & Maccone, L. (2001). Quantum-enhanced positioning and clock synchronization. *Nature*, 412, 417-419. https://doi.org/10.1038/35086525

Götzelmann, M., Köller, E., Viciano-Semper, I., Oskam, D., Gkougkas, E., & Simon, J. (2023). Galileo open service navigation message authentication: Preparation phase and drivers for future service provision. NAVIGATION: *Journal of the Institute of Navigation*, 70(3), Article 572. https://doi.org/10.33012/navi.572

Gutierrez, P. (2024). *GMV-led Project Develops AI-based Jamming and Spoofing Mitigation*. https://insidegnss.com/gmv-led-project-develops-ai-based-jamming-and-spoofing-mitigation/

He, Y., Li, B., Chen, J., Wang, Z., Xiao, W., & Lu, Z. (2024). Overview of the development of satellite navigation blanket interference monitoring. *Frontiers in Physics*, 12, Article 1487384. https://doi.org/10.3389/fphy.2024.1487384

Hegarty, C., Odeh, A., Shallberg, K., Wesson, K., Walter, T., & Alexander, K. (2018). Spoofing detection for airborne GNSS equipment. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation* (pp. 1350-1368). https://doi.org/10.33012/2018.16008

Hexagon. (2025). *What Are Global Navigation Satellite Systems?* https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss

Humphreys, T. E. (2013). Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 49(2), 1073–1090. https://doi.org/10.1109/TAES.2013.6494400

Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., & Kintner, P.M. (2008). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation* (ION GNSS Conference) (pp. 2314-2325).

IATA. (2024). *Global Navigation Satellite System GNSS Radio Frequency Interference, Safety Risk Assessment*. https://ic.iata.org/sites/default/files/iata_sih_document_attachment/IATA_Safety_Risk_Assessment_GNSS_Interference.pdf

ICAO. (2003). *Operational use of ADS-B in Non-Radar Airspace Generic Design Safety Case*. ICAO Separation and Airspace Safety Panel (SASP).

ICAO. (2018). *Manual on Testing of Radio Navigation Aids*. Volume I - Testing of Ground-based Radio Navigation Systems, DOC 8071, Fifth Edition.

ICAO. (2022). *Assembly-41st Session Technical Commission Aviation Safety and Air Navigation Standardization*. GNSS Interference, Working Paper A41-WP/196

Issam, S. M., Adnane, A., & Madiabdessalam, A. I. T. (2020). Anti-Jamming techniques for aviation GNSS-based navigation systems: Survey. In *Proceedings of the 2020 IEEE 2nd international conference on electronics, control, optimization and computer science* (ICECOCS) (pp. 1-4). IEEE, https://doi.org/10.1109/ICECOCS50124.2020.9314449

Jonáš, P., & Vitan, V. (2019). Detection and localization of GNSS radio interference using ADS-B data. In *Proceedings of the 2019 International Conference on Military Technologies (ICMT)* (pp. 1–5). IEEE. https://doi.org/10.1109/MILTECHS.2019.8870034

Joseph, A., Bartolone, P., Griggs, J., Schnaufer, B., Phan, H., & Malhotra, V. (2023). GNSS radio frequency interference mitigation in Collins commercial airborne receivers. *Engineering Proceedings*, 54(1), Article 18. https://doi.org/10.3390/ENC2023-15420

Jozsa, R., Abrams, D. S., Dowling, J. P., & Williams, C. P. (2000). Quantum clock synchronization based on shared prior entanglement. *Physical Review Letters*, 85(9). https://doi.org/10.1103/physrevlett.85.2010

Jullian, O., Otero, B., Stojilović, M., Costa, J. J., Verdú, J., & Pajuelo, M. A. (2022). Deep learning detection of GPS spoofing. In *International Conference on Machine Learning, Optimization, and Data Science* (pp. 527-540). Springer. https://doi.org/10.1007/978-3-030-95467-3_38

Khang, A., & Rath, K. C. (2025). *The quantum evolution: Application of AI and robotics in the future of quantum technology* (1st ed.). CRC Press.

Krelina, M. (2021). Quantum technology for military applications. *EPJ Quantum Technology*, 8(1), Article 24. https://doi.org/10.1140/epjqt/s40507-021-00113-y

Krelina, M. (2023). The prospect of quantum technologies in space for defence and security. *Space Policy*, 65, Article 101563. https://doi.org/10.1016/j.spacepol.2023.101563

Liu, Z., Lo, S., & Walter, T. (2020). GNSS interference characterization and localization using OpenSky ADS-B data. *Proceedings of the 8th OpenSky Symposium*, 59(1), Article 10. https://doi.org/10.3390/proceedings2020059010

Liu, Z., Lo, S., & Walter, T. (2021). GNSS interference detection using machine learning algorithms on ADS-B data. *Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation* (pp. 4305–4315). https://doi.org/10.33012/2021.18111

Liu, Z., Lo, S., & Walter, T. (2022). GNSS interference source localization using ADS-B data. *Proceedings of the 2022 International Technical Meeting of the Institute of Navigation* (pp. 158–167). https://doi.org/10.33012/2022.18241

Lomas, C. (2025). *GPS jamming: the benign, the bad, and the scary*. https://www.flightradar24.com/blog/inside-flightradar24/types-of-gps-jamming/

Ludlow, A. D., Boyd, M. M., Ye, J., Peik, E., & Schmidt, P. O. (2015). Optical atomic clocks. *Reviews of Modern Physics*, 87(2), 637-701. https://doi.org/10.1103/RevModPhys.87.637

Lukeš, P., Topková, T., Vlček, T., & Pleninger, S. (2020). Recognition of GNSS jamming patterns in ADS-B data. In *Proceedings of the 22th International Conference on New Trends in Civil Aviation (NTCA 2020)* (pp. 9–15). https://doi.org/10.23919/NTCA50409.2020.9291039

Macey, J. (2024). *AI & Quantum Powered Navigation System to Counter GPS Jamming Threats*. https://www.defenseadvancement.com/news/ai-quantum-powered-navigation-system-to-counter-gps-jamming-threats/

Meng, L., Yang, L., Yang, W., & Zhang, L. A. (2022). A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sensing*, 14(19), Article 4826. https://doi.org/10.3390/rs14194826

Murrian, M. J., Narula, L., Iannucci, P. A., Budzien, S., O'Hanlon, B. W., Psiaki, M. L., & Humphreys, T. E. (2021). First results from three years of GNSS interference monitoring from low Earth orbit. NAVIGATION: *Journal of the Institute of Navigation*, 68(4), 673–685. https://doi.org/10.1002/navi.449

National Academies of Sciences, Engineering, and Medicine. (2023). *Analysis of Potential Interference Issues Related to FCC Order 20-48*. National Academies Press. https://doi.org/10.17226/26611

Nayfeh, M., Li, Y., Al Shamaileh, K., Devabhaktuni, V., & Kaabouch, N. (2023). Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. *Computers & Security*, 126, Article 103085. https://doi.org/10.1016/j.cose.2022.103085

NordSky. (2024). *Understanding GNSS Jamming and Spoofing: Challenges and Solutions*. https://www.nordsky.com/understanding-gnss-jamming-and-spoofing/

OPSGroup. (2024). *GPS Spoofing: Final Report published by Work Group*. https://ops.group/blog/gps-spoofing-final-report/

Osechas, O., Felux, M., Fohlmeister, F., & Dautermann, T. (2021). Impact of RFI on GNSS and avionics–A view from the cockpit. *Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation* (pp. 1142–1159). https://doi.org/10.33012/2021.18055

Osechas, O., Fohlmeister, F., Dautermann, T., & Felux, M. (2022). Impact of GNSS-Band Radio Interference on Operational Avionics. NAVIGATION: *Journal of the Institute of Navigation*, 69(2), Article 516. https://doi.org/10.33012/navi.516

Petchenik, I. (2025). *How We Track Flights with MLAT*. https://www.flightradar24.com/blog/inside-flightradar24/how-we-track-flights-with-mlat/

Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4), 1012-1236. https://doi.org/10.1364/AOP.361502

Psiaki, M. L., Humphreys, T. E., & Stauffer, B. (2016). Attackers can spoof navigation signals without our knowledge. Here is how to fight back GPS lies. *IEEE Spectrum*, 53(8), 26–53. https://doi.org/10.1109/MSPEC.2016.7524168

Pultarova, T. (2025). *How Ukraine's Drones are Beating Russian Jamming*. https://spectrum.ieee.org/killer-drones

Qiao, J., Lu, Z., Lin, B., Song, J., Xiao, Z., Wang, Z., & Li, B. (2023). A survey of GNSS interference monitoring technologies. *Frontiers in Physics*, 11, Article 1133316. https://doi.org/10.3389/fphy.2023.1133316

Radoš, K., Brkić, M., & Begušić, D. (2024). Recent advances on jamming and spoofing detection in GNSS. *Sensors*, 24(13), Article 4210. https://doi.org/10.3390/s24134210

Rothmaier, F., Chen, Y. H., Lo, S., & David Powell, J. (2019a). Single GNSS antenna heading estimation. *Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation* (pp. 2159–2171). https://doi.org/10.33012/2019.16915

Rothmaier, F., Chen, Y. H., Lo, S., & Walter, T. (2021). GNSS spoofing detection through spatial processing. NAVIGATION: *Journal of the Institute of Navigation*, 68(2), 243-258. https://doi.org/10.1002/navi.420

Rothmaier, F., Chen, Y., & Lo, S. (2019b). Improvements to steady state spoof detection with experimental validation using a dual polarization antenna. *Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation* (pp. 967–983). https://doi.org/10.33012/2019.16989

Safrangroup. (2025). *Meeting the challenges of "jamming" and "spoofing" in civil aviation*. https://www.safran-group.com/news/meeting-challenges-jamming-and-spoofing-civil-aviation-2025-01-15

Scaramuzza, M., Wipf, H., Troller, M., Leibundgut, H., Rämi, S., & Wittwer, R. (2015). GNSS RFI detection: Finding the needle in the haystack. *Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation* (pp. 1617–1624). https://www.ion.org/publications/abstract.cfm?articleID=13064

Slingshot Aerospace. (2025). *Slingshot to Develop Geolocation and AI-based GPS Jamming and Spoofing Detection Technology for US Space Force*. https://www.everythingrf.com/news/Details/19542-slingshot-to-develop-geolocation-and-ai-based-gps-jamming-and-spoofing-detection-technology-for-us-space-force

Stanisak, M., Wilkens, C., & Musmann, F. (2024). *High-precision Reference Positioning in Case of GNSS Jamming*. https://icasc.co/wp-content/uploads/2024/08/High_Precision-Reference-Positioning-in-Case-of-GNSS-Jamming.pdf

Summers. C. (2025). *GPS Spoofing, Jamming Attacks in the Air Are Increasing, Experts Say*. https://www.theepochtimes.com/us/gps-spoofing-jamming-attacks-in-the-air-are-increasing-say-experts-5925866

System Schematic Manual. (2025). *System Schematic Manual* (SSM), Chapter 34: Embraer E190, Available at: Author Library.

Van Trees, H. L. (2001). *Detection, Estimation, and Modulation Theory* (Part I). John Wiley & Sons. https://doi.org/10.1002/0471221082

Villamizar, H. (2025). *Impacts of GPS Spoofing on Commercial Aviation*. https://www.airwaysmag.com/new-post/gps-spoofing-commercial-aviation

Wineland, D. J., & Dehmelt, H. G. (2021). Precision quantum clocks: From superposition to hyperfine interactions. *Reviews of Modern Physics*, 90(4), 173-199.

Wu, Z., Zhang, Y., Yang, Y., Liang, C., & Liu, R. (2020). Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access*, 8, 165444–165496. https://doi.org/10.1109/ACCESS.2020.3022294

Xiao, J., Li, Y., Zhang, C., & Zhang, Z. (2022). INS/GPS Integrated Navigation for Unmanned Ships Based on EEMD Noise Reduction and SSA-ELM. *Journal of Marine Science and Engineering*, 10(11), Article 1733. https://doi.org/10.3390/jmse10111733

Zarrinnegar, K., Tohidi, S., Mosavi, M. R., Sadr, A., & de Andrés, D. M. (2023). Improving Cross Ambiguity Function Using Image Processing Approach to Detect GPS Spoofing Attacks. *Iranian journal of electrical & electronic engineering*, 19(1), Article 2584. http://ijeee.iust.ac.ir/article-1-2584-en.html

Zidan, J., Adegoke, E. I., Kampert, E., Birrell, S. A., Ford, C. R., & Higgins, M. D. (2020). GNSS vulnerabilities and existing solutions: A review of the literature. *IEEE Access*, 9, 153960-153976. https://doi.org/10.1109/ACCESS.2020.2973759