

Jamming and/or Spoofing

GNSS Interference Resource Guide

2026



VERSION 1.1

FLIGHT TECHNOLOGIES AND PROCEDURES DIVISION



FLIGHT TECHNOLOGIES AND PROCEDURES DIVISION

Interference



Jamming & Spoofing

Federal Aviation Administration
Flight Technologies and Procedures Division, AFS-400
800 Independence Ave SW
Building 10A / 8th Floor
Washington, DC 20591
Phone: (202) 267-4623

Document Changes

Version	Date	Description of Change
Version 1.0	12/04/2025	Initial Version
Version 1.1	03/12/2026	• Added Diagram 1-5 • Additional and edited bullets in Section 4 • Various minor edits throughout the document • Updated paragraph 4.9

Contents

Section 1: Introduction	1-1
1.1 Purpose	1-1
1.2 Background	1-2
Figure 1-1, Daily Spoofing Trends from January to August 2024 (Multiple Regions)	1-3
Figure 1-2, Daily Spoofing Trends from September 2024 to June 2025 (Multiple Regions)	1-3
Figure 1-3, Daily Spoofing Trends from January to June 2025 (Multiple Regions)	1-4
Figure 1-4, Daily Spoofing Trends from January to June 2025 (Middle East)	1-5
1.3 Applicability	1-6
1.4 Overview	1-7
Figure 1-5, GNSS Vulnerabilities	1-7
1.5 How Jamming and Spoofing Work	1-8
1.6 Receiver Autonomous Integrity Monitoring (RAIM)	1-8
1.7 Lingerin g Effects of Spoofing	1-9
Section 2: Human Factors	2-1
2.1 Human Factors	2-1
Section 3: Impact on Aircraft Systems	3-1
3.1 Introduction	3-1
3.2 Jamming and/or Spoofing Effects	3-2
Table 3-1 Summary of GNSS Interference on Aircraft Systems	3-2
3.3 ADS-B	3-4
3.4 Aircraft Clock	3-4
3.5 Automatic Radio NAVAID Tuning	3-4
3.6 CPDLC, ADS-C	3-4
3.7 EFB	3-5
3.8 ELT	3-6
3.9 Navigation	3-6
3.10 HUD and SVS	3-7
3.11 Inertial Navigation System (INS)	3-7
3.12 Runway Safety Alerting Systems	3-8

3.13 TAWS	3-8
3.14 TCAS	3-9
3.15 Weather Radar	3-10

Section 4: Pilot Guidance & Suggested Procedures 4-1

4.1 Introduction	4-1
4.2 Early Recognition	4-1
4.3 Use of EFB as a Mitigation	4-3
4.4 Pilot Guidance Before, During and After GNSS Interference	4-4
Figure 4-1: Before, During and After Interference	4-4
4.5 Preflight	4-5
4.6 Pre Jamming and/or Spoofing	4-8
4.7 Jamming and/or Spoofing	4-10
4.8 Clear of Interference	4-13
4.9 Oceanic Considerations	4-14
4.10 Approach	4-15
4.11 Post Flight	4-15

Section 5: Training 5-1

5.1 Introduction	5-1
5.2 Ground School	5-1
5.3 Flight Training	5-2

Appendix A: Current and Past Data A-1

A.1 Current Data Links	A-1
A.2 Areas of High Jamming and/or Spoofing Incidents	A-1
Table A-1 GNSS Spoofing From July-Aug 2024 of Top Impacted FIRs	A-1
Table A-2 Areas of Major Spoofing: Eastern Mediterranean Sea	A-2
Table A-3 Areas of Major Spoofing: Black Sea	A-5
Table A-4 Areas of Major Spoofing: Russia and Baltic Region	A-6
Table A-5 Areas of Major Spoofing: India/Pakistan border	A-8

Table A-6 Areas of Major Spoofing: Iraq, Iran A-8

Table A-7 Areas of Major Spoofing: North and South Korea A-9

Table A-8 Areas of Major Spoofing: Around Beijing, China A-9

Appendix B: Links to Useful Information B-1

B.1 Websites for Jamming and/or spoofing Information B-1

Appendix C: Glossary and Acronyms C-1

C.1 Glossary C-1

C.2 Acronym List C-4

Table C-1 Acronyms C-4



Section 1: Introduction

1.1 Purpose

The Federal Aviation Administration (FAA) [Flight Technologies and Procedures Division](#) (AFS-400) developed this resource guide to provide United States (U.S.) operators and pilots with the most current information regarding Global Positioning System (GPS)/ Global Navigation Satellite System (GNSS) jamming and/or spoofing. This resource guide refers to any interruption to the GPS/GNSS signal-in-space (SIS) as “GNSS interference”.

The GPS is a U.S. satellite constellation nominally consisting of 21 satellites and 3 operational spares orbiting the Earth in six orbital planes. In contrast, GNSS is a term covering any satellite constellation and satellite augmentation system providing positioning, navigation, and timing (PNT) services. Other than the GPS constellation, there are a number of other satellite constellations, e.g., Galileo from Europe, BeiDou from China, and GLONASS from Russia. There are also various regional GNSS augmentation systems.

Jamming. Emissions that do not mimic GNSS signals (e.g., GPS and Wide Area Augmentation System (WAAS)), but rather interfere with the civil receiver’s ability to acquire and track GNSS signals. Jamming can result in denial of GNSS navigation, positioning, timing and aircraft dependent functions.

Spoofing. Emissions of GNSS-like signals that may be acquired and tracked in combination with or instead of the intended signals by civil receivers. The onset of spoofing effects can be instantaneous or delayed, and effects can persist after the spoofing has ended. Spoofing can result in false and potentially confusing, or hazarding misleading, position, navigation, and/or date/time information in addition to loss of GNSS use.

Note: The above definitions of jamming and/or spoofing match those in the Pilot/Controller Glossary of the Aeronautical Information Manual/Publication (AIM/AIP). Appendix D of this document contains a glossary and acronym list of terms this guide uses.

The impacts of safety hazards from GNSS interference rapidly spread over the past few years and is persistent. As the threat of GNSS jamming and spoofing is constantly changing, the FAA will update this resource guide to provide the best guidance in the rapidly changing environments.

This guide is not formal FAA policy and is not regulatory. For specific aircraft and avionics system information, refer to your Airplane Flight Manual (AFM) and/or AFM Supplement. The information this guide provides is generic and may or may not apply to your aircraft. The guide is for informational purposes only and the FAA’s best recommendations for safety of flight when experiencing GNSS interference. This guide also offers safety suggestions to help mitigate impacts of GNSS interference. The FAA will announce publication of any new, formal FAA policy and/or regulatory change(s) regarding GNSS interference via an FAA Notice and use of the Federal Register. Updates to this guide will provide links for quick access to such new FAA policy and regulations on GNSS interference.



1.2 Background

The National Airspace System (NAS) has experienced numerous GNSS interference events in many regions of the United States. Most of these events were associated with planned U.S. Government national security sanctioned activities, varying in scope and duration. The purpose of this intentional activity was to support planned equipment testing or military exercises in defined areas in the NAS. Other, less frequent unplanned GNSS interference events were associated with faulty commercial equipment blocking the reception of a GNSS signal in a localized area, or inadvertent reradiated GNSS signals from avionics repair shops in and around airports. In the above examples the effect on NAS operations was manageable with little disruption to the flying public.



However, in 2022 there were two GNSS interference events that had significant impacts on commercial aviation.

- ➔ **Denver International Airport (DEN):** Multiple aircraft reported unreliable GNSS within the vicinity of Denver's airport, caused by an unauthorized transmitter broadcasting on the GNSS frequency, affecting civilian flights, air traffic control, and other GNSS-dependent systems. The interference also impacted surface (road and highway) and rail users.
- ➔ **Dallas Area:** Dallas experienced a significant GNSS interference event that disrupted air travel with the re-routing of some aircraft. The source of the interference was never identified, yet GNSS jamming and/or spoofing effects were felt by aircraft landing at airports in the Dallas area as well as transitioning overhead.

In the fall of 2023, GNSS interference incidents increased in complexity and frequency. According to the [International Air Transport Association](#) (IATA) report from September 2024, the rate of loss of GNSS per 1,000 flights increased 65% in the first half of the year over that of 2023. GNSS interference continues to increase, especially near conflict zones where interference extends well beyond the front lines and impacts aircraft operating hundreds of nautical miles away.

Figures [1-1](#) through [1-4](#) provide a look at Daily Spoofing trends in various regions. Spoofing in aviation is an increasing concern, especially in designated regions. Upward trends in GNSS interference may cause an increase in pilot loss of situational awareness which can cause: failure to comply with their air traffic clearance; misinterpreting their positions and reporting false positions to ATC; inadvertent disruption of their flight planned path; loss of separation from other aircraft; inability to transition safely to another acceptable means of navigation without GNSS.



Figure 1-1, Daily Spoofing Trends from January to August 2024 (Multiple Regions)

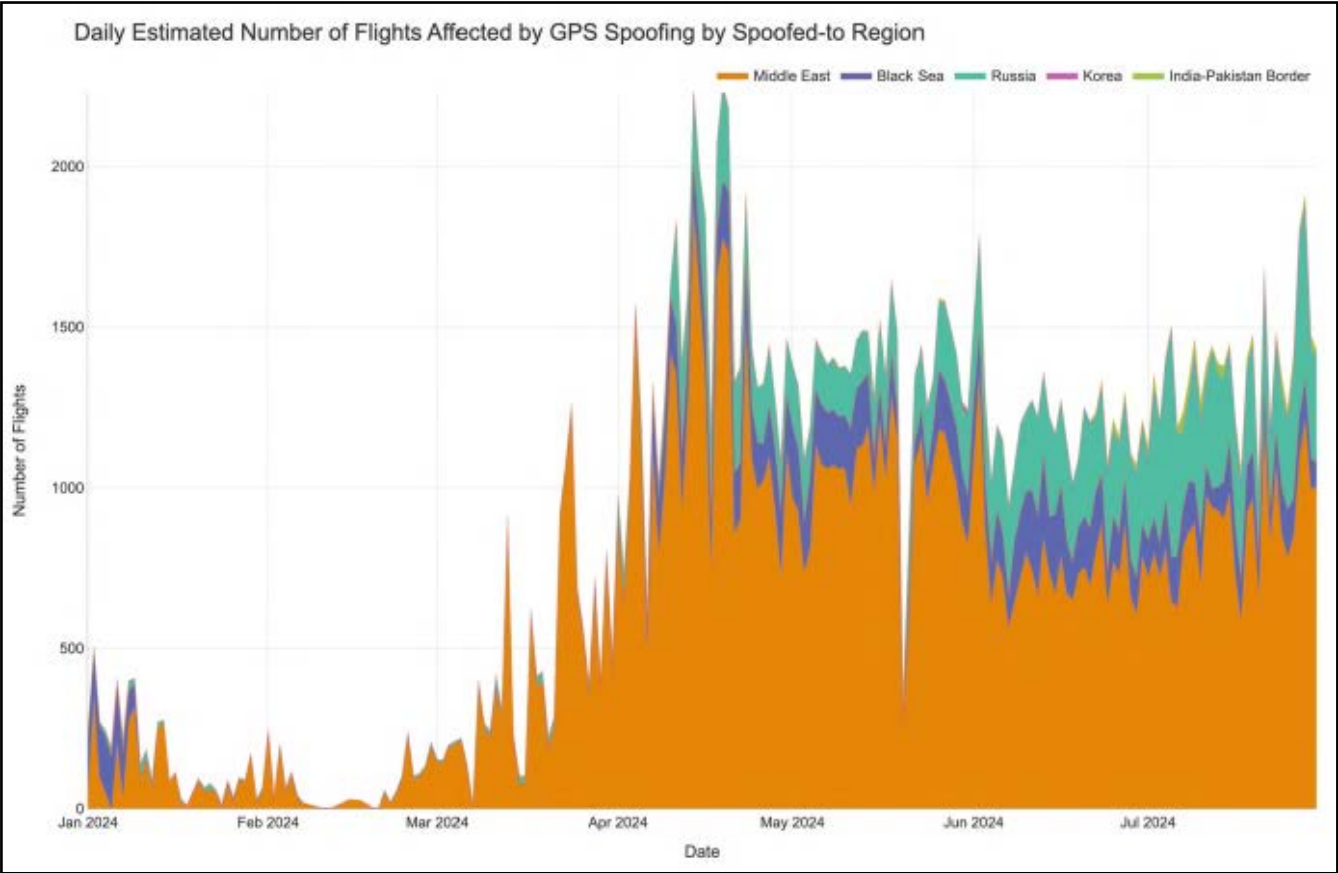
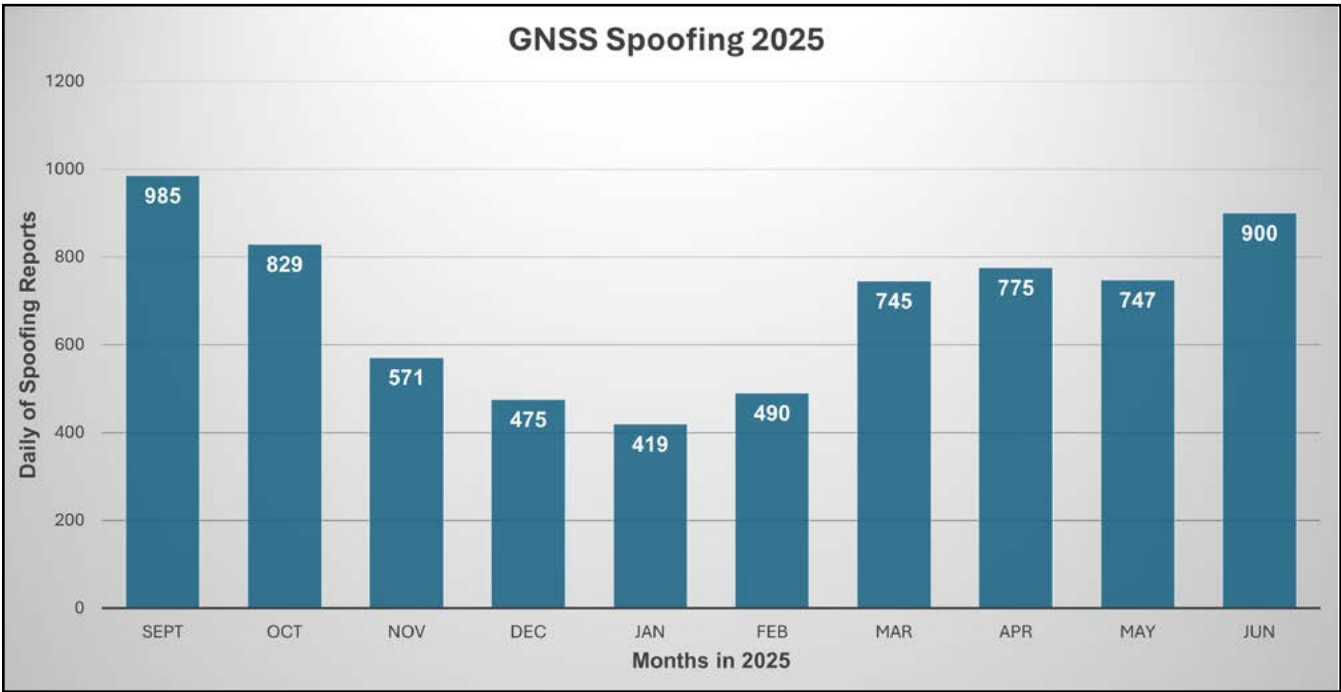


Figure 1-2, Daily Spoofing Trends from September 2024 to June 2025 (Multiple Regions)



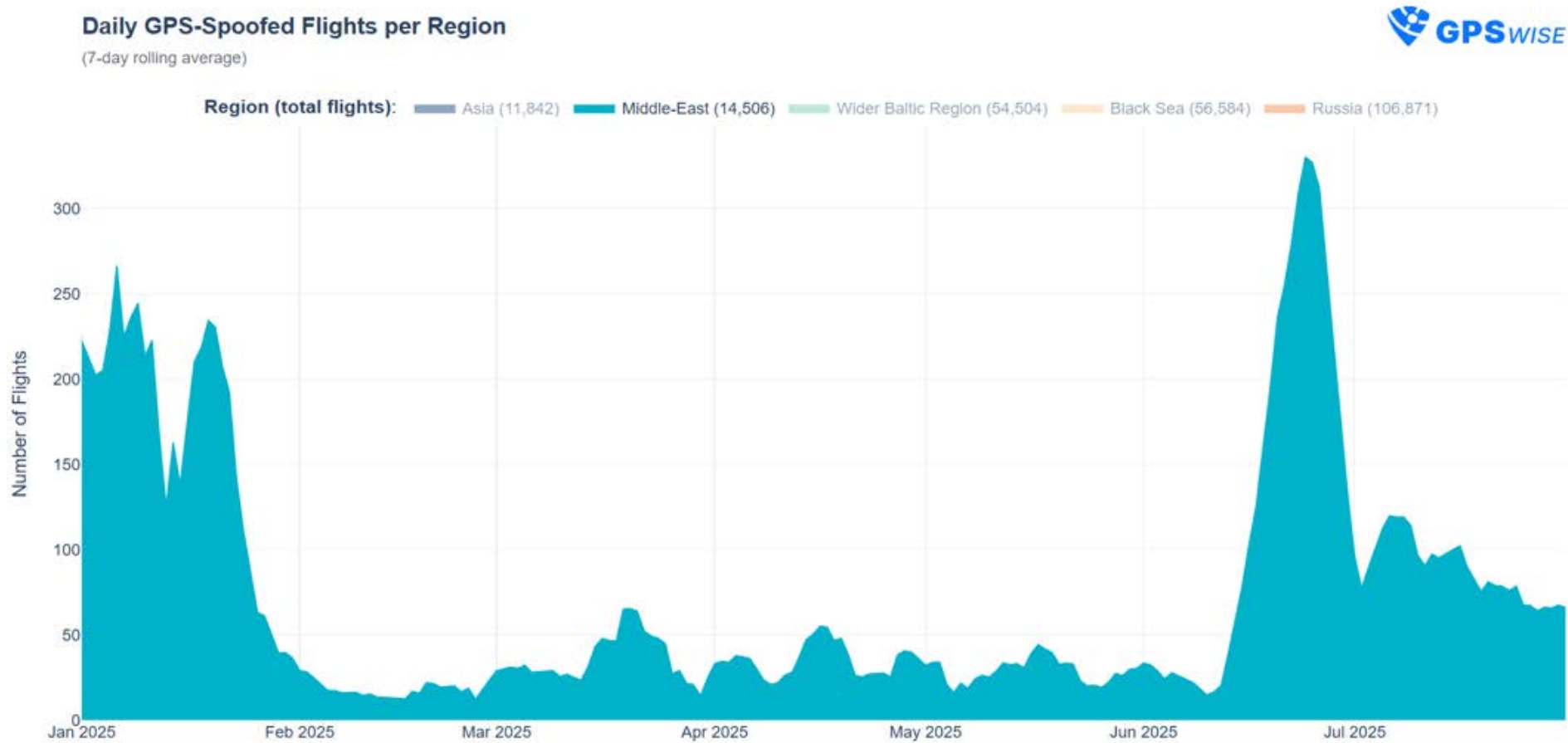
I N T R O D U C T I O N

**Figure 1-3, Daily Spoofing Trends from January to June 2025 (Multiple Regions)**

I N T R O D U C T I O N



Figure 1-4, Daily Spoofing Trends from January to June 2025 (Middle East)





Azerbaijan Airlines Flight 8243

Azerbaijan Airlines Flight 8243, an Embraer 190, crashed near Aktau, Kazakhstan, on December 25, 2024, after experiencing “physical and technical external interference,” according to early investigations. The flight was en route from Baku, Azerbaijan, to Grozny, Russia, when it experienced jamming, followed by spoofing. Without the use of GNSS, the crew unsuccessfully attempted two NDB approaches in deteriorating weather conditions, resulting in the decision to divert. While departing the Grozny area, the aircraft was struck by a missile. After crossing the Caspian Sea, the flight crew attempted an emergency landing in Aktau when it crashed. The crash resulted in 38 fatalities and 29 survivors.



1.3 Applicability

The FAA intends this guide for use by U.S. and foreign operators conducting operations in U.S. sovereign airspace in accordance with the U.S. AIP. Operators should use this guide in coordination with their aircraft’s Original Equipment Manufacturers (OEM) and operating manuals under Title 14 of the Code of Federal Regulations (CFR). Later revisions of this guide may expand the applicability of this information to air traffic controllers, FAA personnel overseeing Part 142 training centers, and other FAA lines of business.

The global aviation community may use this guide as well. This guide reminds all operators to abide by the rules of the air published in sovereign States’ AIPs. Nothing in this guide provides a means to deviate from a State’s AIP. The FAA encourages operators to coordinate questions and concerns about a State’s AIP with their Civil Aviation Authority (CAA).





1.4 Overview

GNSS signals are vulnerable to interference because of their extremely low power. Some sources of interference include ionosphere effects, solar activity, GNSS repeaters, and intentional acts of jamming and/or spoofing (see figure 1-5). GNSS interference can occur in any location at any time. Currently GNSS interference is persistent in and near conflict areas around the world.

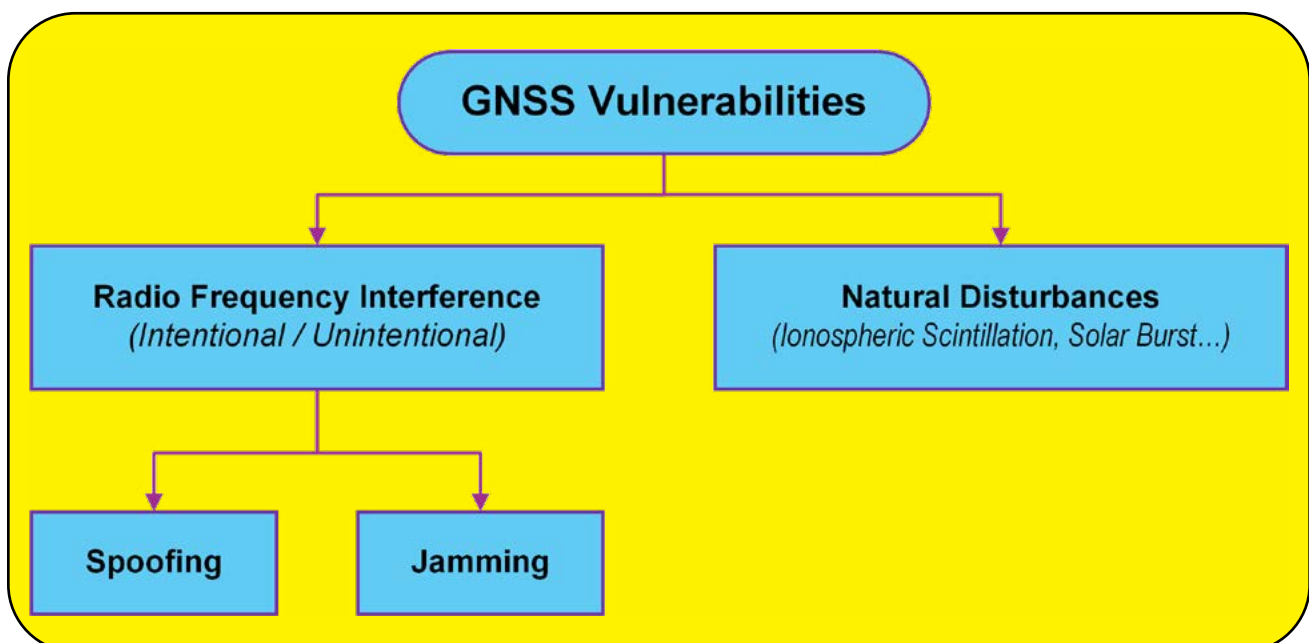
GNSS interference has been used to prevent drone use at highly attended events (e.g. Euro 2024, Olympics), military have used it near border areas/sensitive protected areas, and commercial drivers of trucks/taxis use GNSS interference to jam or spoof their locations. Furthermore, DOD and certain law enforcement agencies have the capability to use counter-drone systems to jam or spoof GNSS signals and force unauthorized drones to land.



In response to the rapid rise in GNSS interference around the world, the FAA released [SAFO 24002](#) providing information and guidance to operators and manufacturers regarding operations in areas impacted by GNSS interference. This guide builds upon the SAFO and provides more comprehensive information and guidance on GNSS interference.

Note: The U.S. government regularly conducts GPS tests, training activities, and exercises that interfere with GPS signals. These events are geographically limited, coordinated, scheduled, and posted via [Notices to Airmen](#) (NOTAMs) and [FAA Public Notices](#). Operators using GNSS should always check NOTAMs for their intended route of flight.

Figure 1-5, GNSS Vulnerabilities





Areas of Conflict

Today, the majority of GNSS interference occurs in areas adjacent to, and in conflict zones (e.g. the Black Sea and the Middle East). These zones of GNSS interference may be where military units use spoofing devices against drones to protect valuable infrastructure. However, the GNSS interference may extend hundreds of miles beyond the immediate conflict area, potentially impacting manned aircraft flying in the vicinity. While spoofing devices are typically found installed on military vehicles, the devices can also be on fixed platforms on land or vessels at sea.



Aircraft monitoring systems vary, regarding alerts and warnings associated with GNSS interference. When interference is present, the aircraft's systems dependent on GNSS may experience degradation or loss messages, a sudden shift or jump in the reported aircraft position, an erroneous time change on the aircraft clock, or several other audio and visual annunciations/alerts. ATC surveillance systems may also see the aircraft make unexpected turns causing gross course changes and clearance deviations due to jamming and/or spoofing. See [Appendix B](#).

1.5 How Jamming and Spoofing Work

Jamming. Jamming is the broadcast of a signal that overpowers the authentic signals coming from GNSS satellites. Jamming disrupts and blocks authentic GNSS signals from the aircraft's GNSS sensor and is often used to provide a means for a spoofing attack.

Spoofing. Spoofing is the transmission of a false signal mimicking the authentic GNSS signal. The false signal may closely resemble an authentic GNSS signal and offer what appears to be a correct code structure, but with altered location or timing data. Often when the false signal is stronger than the authentic GNSS signal, the aircraft's GNSS sensor accepts the false signal as genuine. The aircraft's navigation system then accepts the false signal and calculates an erroneous aircraft position, i.e., a "spoofed" position. By manipulating the aircraft's present position, a "spoofed" aircraft may deviate from their intended flight plan path and ATC clearance.

1.6 Receiver Autonomous Integrity Monitoring (RAIM)

RAIM is a software algorithm in a GNSS sensor contributing to the integrity of the sensor's position solution. Typically, the RAIM algorithms protect against faults from a single satellite by removing the individual satellite's signal from the sensor's position, velocity, time (PVT) solution. RAIM does not protect against GNSS spoofing. The RAIM algorithm's design never had an intent to do so. Thus, the RAIM algorithm cannot distinguish the authentic GNSS signal from false, spoofing signals, especially when the GNSS sensor receives spoofing signals in a consistent format mimicking the GNSS signal.



1.7 Lingering Effects of Spoofing

The broadcast of incorrect data mimicking a GNSS satellite may cause a GNSS receiver to continue to calculate incorrect PNT after the aircraft departs the area of interference, even when in receipt of authentic GNSS satellite signals. GNSS sensors corrupted by interference may be difficult to detect because the receiver may appear to be functioning normally while providing false information for hours after the event. GNSS receivers may need a ground reset or in some instances, a full “factory reset”. Interference can have lingering effects in several aircraft systems, such as:

- ➔ **Inertial Navigation System (INS):** Spoofed GPS data can corrupt the INS, causing it to continue calculating an incorrect position even after leaving the area of spoofing.
- ➔ **Flight Management System (FMS):** The FMS may persist in using the inaccurate data integrated during the spoofing event.
- ➔ **Terrain Avoidance and Warning Systems (TAWS):** False terrain warnings can be triggered based on incorrect GPS for the duration of the flight including the en route and the approach phases.
- ➔ **Automatic Dependent Surveillance-Broadcast (ADS-B):** False, spoofed positions may be reported, misleading air traffic control and other aircraft.
- ➔ **Clock Time:** A corrupted master clock can affect time-sensitive systems and communications, such as Controller Pilot Data Link Communication (CPDLC) datalinks.

Reporting GNSS Interference

The FAA encourages pilots to submit “real-time” reports to ATC during a GNSS interference incident and follow-up with a written report. This will greatly aid the FAA in collection and analysis of data to foster development of mitigation solutions. Please go to FAA’s [Report a GPS Anomaly](#) website and provide the details of any GNSS interference and include the following information:

- | | |
|---|--|
| <ul style="list-style-type: none"> ➔ Aircraft type and registration information, ➔ Date, time, and location of GNSS interference, ➔ Phase of flight, ➔ Instrument approach type (if applicable), ➔ Altitude, | <ul style="list-style-type: none"> ➔ Make/Model of GPS receiver, ➔ Maintenance actions (if applicable and known), ➔ GNSS interference description, and ➔ Consequences/operational impact on your flight. |
|---|--|



Intentionally Blank



Section 2: Human Factors

2.1 Human Factors

In aviation, safety relies on pilots and air traffic controllers to effectively manage risks, adapt to operational changes, and minimize errors. When GNSS interference disrupts the accuracy of instruments providing positioning, navigation, and timing information, it can have significant implications related to human factors. Human factors is a field dedicated to understanding human capabilities and optimizing interactions with technology to reduce human error. Being aware of human factors issues related to GNSS interference can aid in earlier detection, recognition, and response to these problems. This chapter offers an overview of some key human factors considerations associated with GNSS interference, although related information is interwoven throughout this guide.



- ➔ **Increased Workload.** Handling GNSS interference can elevate pilot and air traffic controller workload, particularly when extra tasks are required to diagnose and address issues, manage other aircraft systems impacted by the interference, switch to less efficient backup navigation systems, or reroute the flight. High workload may lead to a higher rate of errors and a corresponding reduction in safety margins.
- ➔ **Increased Fatigue.** The increased workload from managing GNSS interference can eventually cause task-induced fatigue. The main symptoms of this type of fatigue include tiredness (distinct from sleepiness), headaches, body aches, and bleary eyes. Fatigue can negatively impact memory, problem-solving abilities, decision-making, manual dexterity, and response times to critical safety events. A fatigued flightcrew or air traffic controller may also tend to concentrate on a single issue, allowing other problems to arise unnoticed. Additionally, flightcrew may rely more heavily on automated systems, which can be problematic if those systems are also affected by GNSS interference.
- ➔ **Increased Stress.** Handling GNSS interference can heighten immediate operational stress for pilots and air traffic controllers. Addressing GNSS interference can create intense pressure, particularly in situations where dependence on GNSS information is significant. Key symptoms of stress include feelings of excitement, an increased heart rate, and even alterations in the secretion of stress-related hormones. Occupational



stress has been demonstrated to delay response times to problems, impair the detection of critical information presented on flight deck displays, and diminish perceptual-motor coordination.

- ➔ **Reduced Situation Awareness.** GNSS interference can lead to confusion about the aircraft's position and status, impacting pilot and air traffic controller situation awareness of navigation and system conditions. For example, GNSS interference can cause a sudden jump in the aircraft's position and decreased confidence in navigation capability. Inaccurate GNSS data can complicate the process of making safe and informed decisions.
- ➔ **Mistrust in Flight Deck Systems.** GNSS interference can lead to mistrust in flight deck systems when the technology's validity, reliability, or robustness is compromised. Once trust in these systems is lost, it can be difficult to regain. This mistrust may ultimately impact how flightcrews utilize information and respond to alerts. Mistrust may result in an improper response to GNSS interference to include something as simple as failing to report the interference to ATC. One example of when mistrust in flight deck systems can arise is during a final approach, where the aircraft's actual position differs from what is shown on the navigation display. In such a scenario, a pilot may see the runway ahead but notice a discrepancy on the navigation display. The pilot must then rely on visual cues from the external environment to verify the aircraft's position and disregard the navigation display. Requesting radar vectors, if available, may also be necessary. This situation challenges the typical pilot mindset of "trusting your instruments."
- ➔ **Delayed or Inaccurate Responses to Alerts.** Delayed responses can occur when pilots and air traffic controllers experience cognitive overload due to the increased effort needed to manage GNSS interference, and the desensitization that results from frequent false alarms. For example, GNSS interference may cause a high number of Engine Indicating and Crew Alerting System (EICAS) warnings which can lead to complacency or even missing important warnings not related to GNSS interference.
- ➔ **Normalization of Risk.** Risk normalization refers to the gradual acceptance of dangerous or risky behaviors as normal over time. As GNSS interference becomes more common, organizations and pilots may develop a higher tolerance for risk. Individuals may start by accepting minor deviations from standard procedures, which can eventually lead to the acceptance of more significant deviations. This mindset can be reinforced by the hazardous attitude of thinking, "It worked before, so maybe we can push the limits a bit further." Consequently, this increases the overall risk to flight safety.
- ➔ **Degraded Crew Resource Management.** Without adequate training and clear procedures for handling GNSS interference, pilots of multi-crew aircraft might disagree on the appropriate actions to take. Such conflicts can undermine crew resource management (CRM) throughout the flight.
- ➔ **Communication Challenges.** GNSS interference can disrupt data link communications that rely on GNSS data. When this occurs, pilots may have to switch to voice communication with air traffic control, including providing position reports at mandatory reporting points. This shift increases pilot and air traffic controller workload and heightens the risk of misunderstandings and miscommunication, particularly in high-traffic areas where all aircraft are using voice communication.



Section

3

Section 3: Impact on Aircraft Systems

3.1 Introduction

For specific aircraft system information, refer to your Airplane Flight Manual (AFM) and/or AFM Supplement. The system information provided in this guide is generic and may or may not apply to your aircraft. It is for informational purposes only and to provide safety suggestions to help mitigate jamming and/or spoofing.

This section is devoted to the impact that jamming and/or spoofing have on aircraft systems. GNSS interference may include the following system anomalies:

- ➔ **Aircraft Position/Navigation:** Aircraft may not be able to align their systems on the ground or may be deviating from the intended flight path, with navigation displays showing on course during flight. (See [3.5](#) and [3.9](#))
- ➔ **Communication:** Loss of data link systems and SATCOM. Pilots may need to revert to VHF voice communications. (See [3.6](#))
- ➔ **Surveillance:** Loss of Automatic Dependent Surveillance (ADS-B Out/In and ADS-C). (See [3.3](#) and [3.6](#))
- ➔ **Safety:** Inaccurate aircraft clock, loss of Runway Awareness Systems and TAWS forward-looking function, etc. (See [3.4](#), [3.8](#), [3.12](#), [3.13](#) and [3.14](#))
- ➔ **Pilot displays:** Synthetic/Combined Vision Systems (SVS/CVS) unusable, Electronic Moving Map on Navigation Display inoperable, Electronic Flight Bag and Head Up Display (HUD) unreliable, etc. (See [3.7](#), [3.10](#), and [3.15](#))

Abnormal System Responses





3.2 Jamming and/or Spoofing Effects

Table 3-1 provides a summary of known aircraft systems impacted by GNSS interference. Some of the systems are hyperlinked (underlined) to more detailed information further down in this section. This detailed information provides specific effects of jamming and of spoofing for those individual systems.

Note: This table does not attempt to address all of the effects of GNSS interference on all aircraft and their systems. Aircraft owner/operators should seek information on the GNSS interference effects on their specific aircraft systems from the aircraft manufacturer and the avionics manufacturers.

Table 3-1 Summary of GNSS Interference on Aircraft Systems

System	Possible System Impacts
<u>ADS-B Out</u>	→ Loss of/or erroneous ADS-B transmissions
<u>ADS-B In</u>	→ Missing Traffic → False Traffic Locations → Erroneous Traffic Alerts
<u>Aircraft GNSS-based Clock</u>	→ Incorrect time displayed on clock → Incorrect time fed to other systems
<u>Automatic Radio Navigation Aid (NAVAID) Tuning</u>	→ Degraded or not available
<u>Data Link for Automatic Dependent Surveillance-Contract (ADS-C) and CPDLC</u>	→ CPDLC not available → ADS-C not available → Time stamp mismatches
<u>Electronic Flight Bag (EFB)</u>	→ GNSS dependent applications may not work
<u>Emergency Locator Transmitter (ELT)</u>	→ Incorrect aircraft position broadcast in emergency
<u>Navigation System</u>	→ GNSS-based navigation failure → GNSS-based navigation course guidance erroneous and may not be immediately apparent to the pilots → Hybrid inertial navigation system erroneous due to updating by a spoofed GNSS
<u>Head-Up Display (HUD) & Synthetic Vision System (SVS)</u>	→ HUD inop → SVS not available
<u>Internet/Wi-Fi</u>	→ Wi-Fi may not work correctly



System	Possible System Impacts
Navigation Display/Moving Map	→ Wrong runway selection
Runway Safety System	→ Unavailable, or may give false warning
Satellite Communications (SATCOM)	→ Loss of SATCOM function when reliant on GNSS
Terrain Awareness and Warning System (TAWS)	→ Erroneous TAWS alerts that may inhibit actual TCAS alerts
Traffic Alert and Collision Avoidance System (TCAS)	→ May be inhibited due to continual TAWS alerts
RNAV/RNP System	→ Restricted to ground-based NAVAIDs → Loss of all PBN aircraft eligibility for all RNAV and RNP operations requiring GNSS positioning
Weather Radar	→ Loss of all weather radar functions dependent on GNSS





3.3 ADS-B

During Jamming, the ADS-B function of the transponder can no longer receive accurate position data from satellites and may display a failure light on the transponder. Since ADS-B relies on GNSS for position data, jamming can prevent aircraft from broadcasting their correct location. If spoofed, the ADS-B functionality is impacted because it may send out inaccurate location data. To summarize:

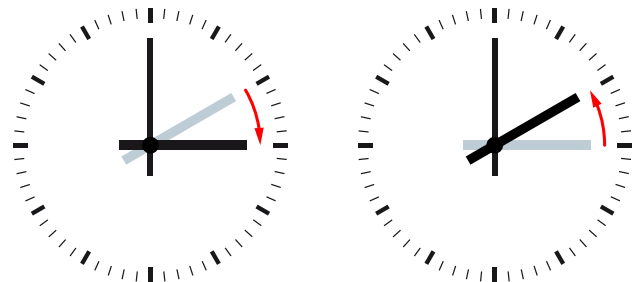
ADS-B Out. ADS-B depends on GNSS position to broadcast the aircraft position and may not have any other inputs from alternative navigation systems. Spoofing may result in the broadcast of a false ADS-B position.

ADS-B In. During spoofing, ADS-B traffic may display false aircraft locations on navigation display, as the result of incorrect ADS-B OUT data from other aircraft and/or traffic may be missing. Some systems with an alerting capability (e.g. ADS-B Traffic Advisory System (ATAS)) may give erroneous or missing alerts.

Note: Some aircraft have hybrid ADS-B systems not impacted by GNSS interference.

3.4 Aircraft Clock

Aircraft clocks operate using precise time signals, normally from GNSS, to constantly update time/date and serve as navigation and flight management tools. During jamming, GNSS updating of the clock may not occur and clocks may be switched to internal (INT) mode. If spoofed, GNSS-based clocks may display incorrect time and/or date, impacting other aircraft systems reliant on time. Pilots may be required to use an alternate time source independent of GNSS, such as a back-up aircraft clock or an analog wristwatch.



3.5 Automatic Radio NAVAID Tuning

Since the navigation system uses a listing of nearby NAVAIDs for auto-tuning based on the aircraft location, this function can be degraded or not available. The overall navigation solution can be further complicated if the navigation system can no longer automatically tune to nearby Very High Frequency Omnidirectional Range (VOR) or Distance Measuring Equipment (DME) NAVAIDs due to spoofing.

3.6 CPDLC, ADS-C

CPDLC: The aircraft clock provides a timestamp to CPDLC downlinks. Two distinct impacts to CPDLC have been observed after the aircraft clock time is altered by spoofing:

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

Some corrupted timestamps can cause the Uplink Delay Monitor to

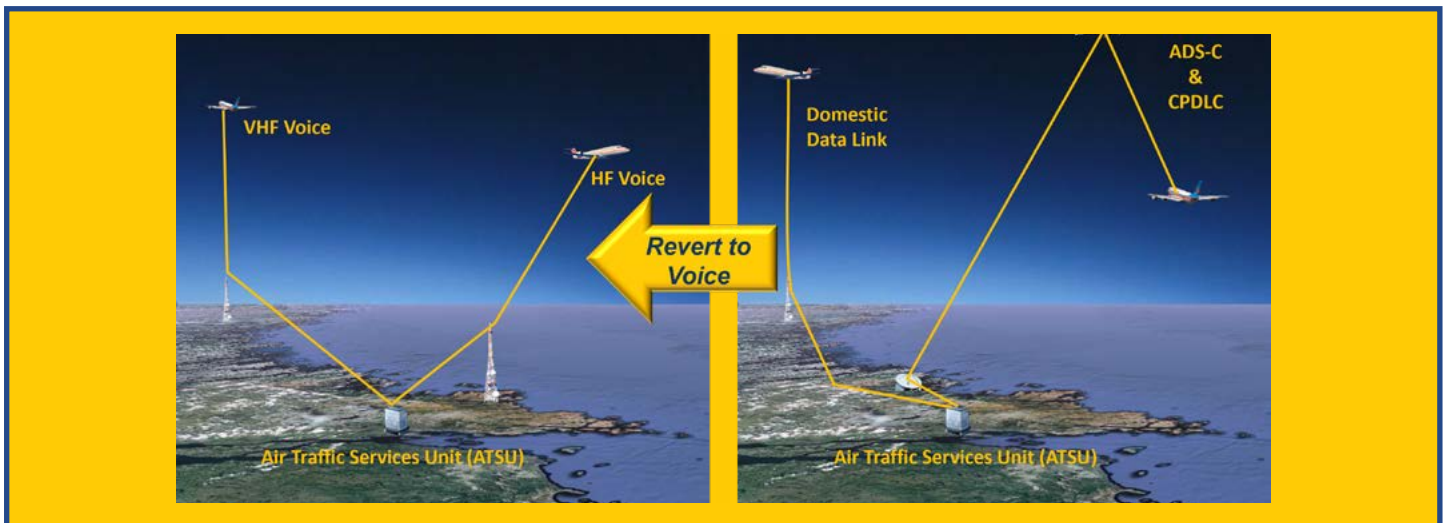




display the message header, “UPLINK DELAY EXCEEDED.” Pilots can still respond to this message and continue to send and receive CPDLC messages as normal.

Note: Pilots should report any loss of CPDLC and revert to voice communication using UHF/VHF or HF voice in oceanic airspace.

ADS-C (Automatic Dependent Surveillance-Contract): An essential component of the ADS-C report is the Figure of Merit (FOM). FOM is a statistically derived value on the reliability and accuracy of aircraft navigation data, which is interpreted by the air traffic control system in use. After having been spoofed, a common lingering “symptom” is low FOM, or low position confidence. This equates to the downgrading of the Required Navigation Performance (RNP) status of the flight and a disqualification from eligibility for reduced separation standards. This disqualification for reduced separation minima means that not only is the previously-spoofed aircraft directly impacted, but aircraft in the vicinity may also be prevented from using optimal altitudes due to the increased longitudinal and lateral separation required. In some FIRs, this can necessitate the controller to descend downgraded aircraft out of the most congested or optimal altitudes. As with CPDLC, the aircraft clock provides a timestamp for ADS-C reports. Incorrect time stamps on ADS-C reports can also result in these being discarded by the air traffic system, which will also disqualify aircraft from utilizing reduced separation minima. If ADS-C is not available in remote airspace, pilots should revert to voice communications and request a new ATC clearance.



3.7 EFB

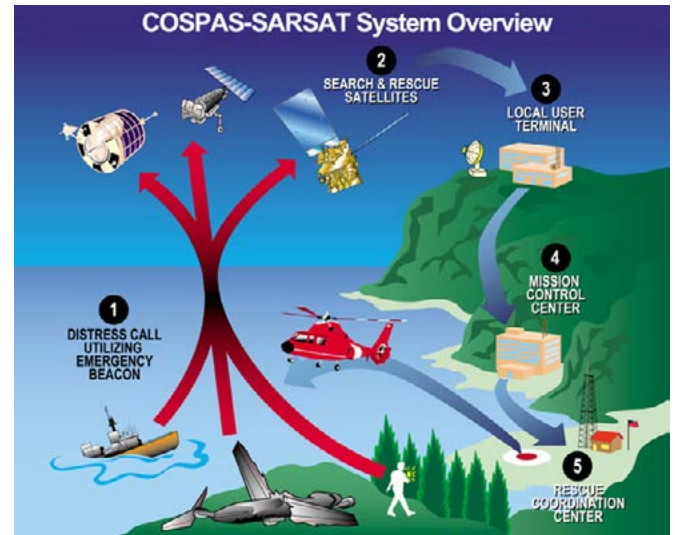
Ownship refers to the aircraft’s position as determined by GNSS and displayed as an aircraft icon on the maps view. During spoofing, EFB applications that depict GNSS-derived aircraft position may not depict accurate ownship data. This can degrade situational awareness and increase pilot workload. Pilots should remove EFB ownship if the position becomes unavailable or is insufficient for the EFB application. For flights planned in or around areas of expected interference, aircraft operators and pilots should develop procedures to remove EFB ownship depiction at a planned point along the flight to preempt the possible disruption. Though not an approved source of navigation, EFBs may provide a means for situational awareness and may recover quicker than the aircraft navigation system.



3.8 ELT

ELTs transmit distress signals on 406 MHz using GNSS position to the COSPAS-SARSAT System, a satellite-aided search and rescue (SAR) system. The GNSS position comes from a receiver within the ELT instead of the aircraft GNSS receiver. The International COSPAS-SARSAT Program monitors these distress transmissions and can determine the aircraft position by:

1. GNSS location transmitted within the emergency distress signal (i.e. GNSS receiver inside of the emergency beacon).
2. Time and frequency of arrival between aircraft beacon transmissions and COSPAS-SARSAT satellites to determine the aircraft location. This is independent of the transmitted GNSS location.



Normally, the two ways to determine aircraft position match. However, there have been instances where the GNSS location transmitted by the ELT was a spoofed location. Since there is an alternative to determining the aircraft position other than the spoofed transmission, the actual position can still be determined through time and frequency of arrival between aircraft beacon transmissions and COSPAS-SARSAT satellites.

3.9 Navigation

GNSS interference can significantly impact the primary means of navigation and may require pilots to use other navigation aids. Each make/model/series of aircraft may respond differently.

During jamming, loss of the GNSS sensor will likely cause multiple system alerts (both aurally and visually) and multiple central alerting system (CAS) messages, resulting in a loss of PBN aircraft eligibility for all RNAV and RNP operations requiring GNSS positioning. The pilot may need to revert to multi-sensor PBN without GNSS or to ground-based NAVAIDs, e.g., VOR/DME or NDB. Loss of GNSS for navigation can also result in erroneous wind and ground speed indications and may affect other information displayed in navigation systems (e.g. fuel calculations, etc.) A new ATC clearance may also be required.

Spoofing may be so insidious, that pilots may be unaware it is occurring.

During spoofing, multi-sensor PBN systems may incorrectly select the spoofed GNSS sensor as having the highest integrity. In this case, the system may incorrectly select it as the most reliable source, neglecting that its updated positions are false. A spoofed position may cause a “map shift” on the navigation display showing a false position of the aircraft and may cause the pilots to lose situational awareness. Pilots may not be immediately aware of being spoofed as the aircraft subtly drifts or turns off course. Once spoofing is recognized, if the aircraft is unable to revert to a reliable navigation sensor, then pilots should request ATC assistance. Radar vectors and/or route deviations may be necessary. If the aircraft is on a GNSS-based instrument approach, the pilot will need to either transition to a visual or an instrument approach based on ground-based NAVAIDs. The pilot may need to execute a missed approach and request a ground-based NAVAID approach.



3.10 HUD and SVS



During GNSS interference, the flight path (trend) vector (FPV) may be impacted. The FPV shows where the aircraft is actually going, and this can be laterally displaced or misaligned by the loss of the GNSS signal or a false position. This causes the HUD system to be unreliable, with no indication given to the pilot.

SVS is an electronic means to display a synthetic image of the external scene topography to the flight crew. SVS requires an accurate terrain and obstacle database, a precision navigation position, and a display. This display may be a PFD, HUD, or secondary display. SVS is the foundation building block for Synthetic Vision Guidance System (SVGS) and the synthetic

image portion of a Combined Vision System (CVS). The SVS may be significantly impacted because a jammed GNSS signal may cause the system to display a misleading position of terrain and an inaccurate position of the aircraft relative to the displayed terrain. This is because SVS is not receiving accurate location data. Spoofing may completely cause a change in location and a shift in the SVS display. This can cause the pilots to lose situational awareness while being close to the ground.

3.11 Inertial Navigation System (INS)

The impact on an inertial navigation system depends on whether the system is self-contained or a hybrid system. INS is the general language used for an approved inertial navigation system.

Self-Contained. Self-contained inertial navigation systems use internal sensors (accelerometers and/or gyroscopes) to track motion and calculate position and orientation without relying on external signals. Since



these systems are not directly dependent on GNSS signals for their primary function, they are not affected by GNSS interference.

Hybrid. Hybrid units integrate inertial sensor data with GNSS signals to achieve greater accuracy and long-term stability. These systems may be vulnerable to jamming and spoofing as follows:

➔ **Jamming:** Over time, GNSS jamming may significantly degrade the performance of hybrid inertial navigation systems, as the system loses the external position updates that help correct drift.

➔ **Spoofing:** GNSS spoofing can mislead hybrid inertial navigation systems, potentially causing the aircraft to deviate from its intended route. When hybrid systems are loosely coupled with GNSS, interference can corrupt an inertial navigation system's present position and outputs



to other aircraft systems. When tightly coupled with GNSS, the filtering between GNSS and an inertial navigation system may defeat some, but not all, GNSS interference. There is risk of potential corruption of an inertial navigation system's present position outputs to other aircraft systems.

3.12 Runway Safety Alerting Systems



Some aircraft have a runway alerting system, Runway Awareness and Advisory System (RAAS), that provides situational awareness while taxiing. This software enhancement aids in reducing runway confusion and runway incursion incidents through visual/aural annunciations at critical points, such as “Approaching Runway 31 Left” and confirmation when an aircraft is lined up on the runway prior to takeoff. The TAWS database in conjunction with GNSS and other onboard sensors monitor movement of an aircraft around the airport and may be impacted by GNSS

interference. During jamming, the aircraft may receive an EICAS message of RUNWAY SYS and if spoofed, a message of RUNWAY POS.

Another type of runway safety alerting system, Runway Overrun Prevention System (ROPS) provides pilots with information about whether the aircraft can safely stop in the available remaining runway. This system generates alerts for the pilot to apply available deceleration means (i.e. reverse thrust, brakes). This system may be vulnerable to spoofing and jamming due to inaccurate/missing GNSS position inputs.

3.13 TAWS

During spoofing, a significant safety concern is the degraded functionality of the look ahead feature of TAWS. This feature uses GNSS to calculate the aircraft's computed altitude relative to known runways, terrain, and obstacles to create advance caution and warning envelopes. As a result, these systems may be impacted, leading to false alerts. Even if spoofing is known to the pilots to cause unwarranted alerts, the result is additional stress and distraction.

The TAWS has shown that it is not always capable of recovering following a spoofing event, even if other systems appear to be functioning normally using an accurate GNSS signal. This results in erroneous TAWS alerts occurring later in flight, to include the “approach” phase of flight. “Basic” TAWS is not impacted by spoofing because it uses radio altimeters to measure the aircraft's height over the ground.

Example From an Actual Pilot Report:

Coming back from Queen Alia, where heavy GNSS interference occurred, another TAWS event was relevant: during the approach, just after the waypoint TIXUM, an unexpected terrain warning came out. The crew was aware that this was most probably another false warning caused from the previous interference; so at the decision of the captain, having positive contact under radar control, with correct indications from the ILS, and with confirmation from the air traffic controller of the aircraft position, the crew (aware of the GNSS interference checklist) elected not to start a terrain escape maneuver towards real high terrain with completely wrong indications (MSA almost 13000 ft) and continued to intercept the ILS 28 in Bergamo-Italy (BGY/LIME). When well established on the ILS 28, at around 500ft, a RAAS callout CAUTION TAXI-WAY happened, which was disregarded as well, as we observed the still compromised warning system, due to the previous spoofing.

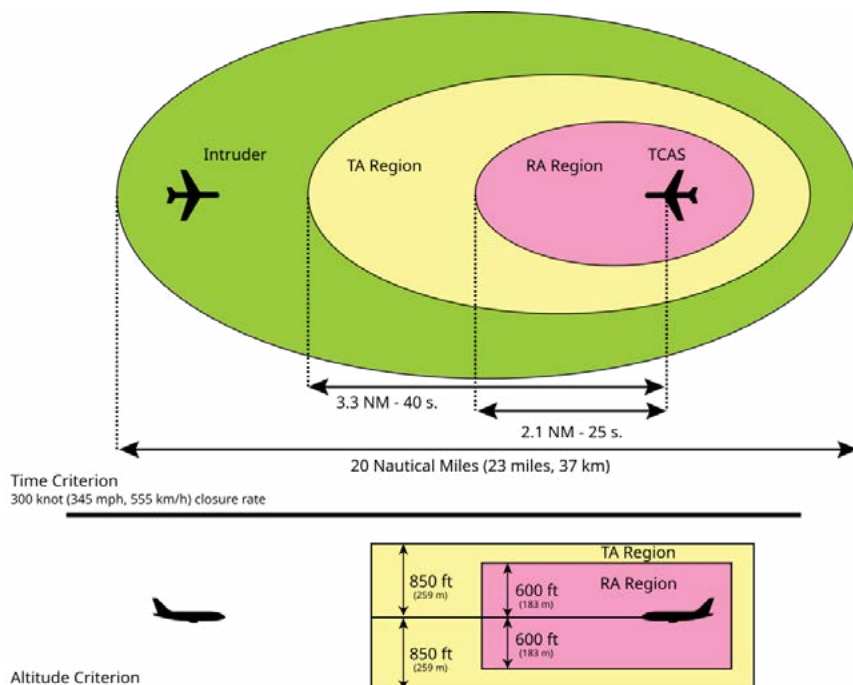


3.14 TCAS

TCAS relies on direct interrogation of aircraft transponders and is not reliant on GNSS or ATC Surveillance. Neither GNSS nor ADS-B are used for the generation of a Resolution Advisory (RA).

- ➔ Effects of GPS spoofing on ADS-B In may result in false ADS-B targets displayed as spoofed target positions. These false ADS-B targets will not set off TCAS RAs (e.g., “CLIMB, CLIMB”) as there are no actual aircraft at those positions.
- ➔ During/following spoofing, due to alerting priority, false TAWS alerts (caused by previous spoofing) may inhibit legitimate TCAS TAs and RAs.
- ➔ There may also be some systems where the ADS-B is deeply integrated, in which and ADS-B failure may cause a transponder failure, resulting in a TCAS failure.

Additionally, Non-TCAS traffic advisory systems such as ATAS (ADS-B Traffic Advisory System) and EFB software rely on GNSS and ADS-B. While these sources may generate a traffic advisory (e.g., “Traffic”), they do not generate RAs. Depiction of non-TCAS traffic information source varies.



Example of ACAS Protection Volume between 5,000 and 10,000 feet (1,524 and 3,048 meters)

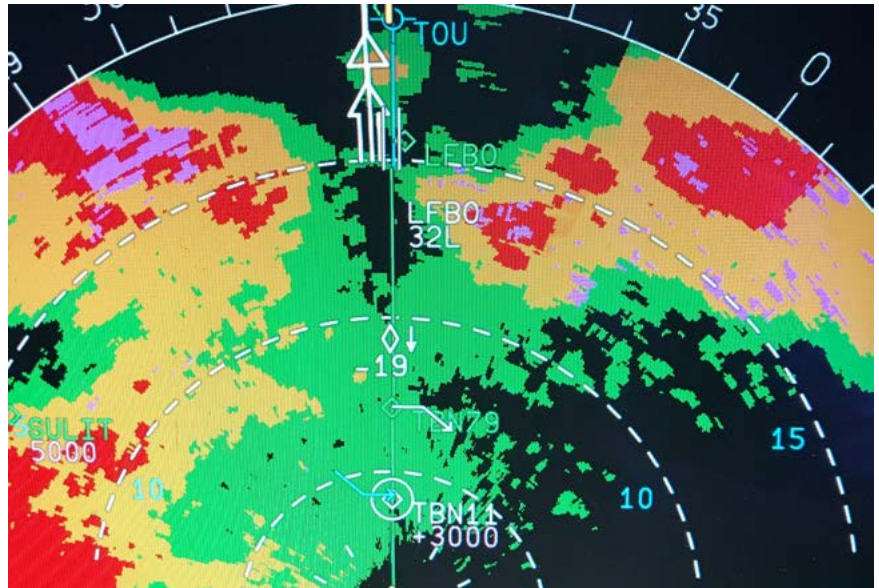
Pilots are advised to comply with an RA, unless doing so would jeopardize the safe operation of the flight.





3.15 Weather Radar

The aircraft weather radar depends on a precise GNSS geolocation to tag radar returns with accurate position and altitude, and to align this information with the flight path, terrain, and weather overlays. When GNSS interference occurs, the aircraft may miscalculate its position, causing weather cells to appear displaced relative to the aircraft and creating the risk that a pilot could unintentionally fly the aircraft into those cells. GNSS interference may also cause timing errors that degrade Doppler velocity measurements, reducing the resolution of weather boundaries. Because weather-radar data is fused with information used by ADS-B, TAWS, and other situation-awareness systems, any degradation in GNSS accuracy can affect multiple systems that rely on consistent and precise positional information.





Section 4: Pilot Guidance & Suggested Procedures

For specific aircraft system information, refer to your Airplane Flight Manual (AFM) and/or AFM Supplement. The system information provided in this guide is generic and may or may not apply to your aircraft. It is for informational purposes only and to provide safety suggestions to help mitigate jamming, spoofing or both.

4.1 Introduction

The guidance in this section provides recommendations for aircraft operators and pilots to help mitigate jamming and/or spoofing, especially when operating in known areas of GNSS disruptions. Operators and pilots should be aware that GNSS interference can occur at any geographical location, time and altitude. **This guide is advisory only and does not take priority over FAA policy or OEM guidance.**

Pilots need to be vigilant of anomalies that may include:

- Changes in actual navigation performance.
- Aircraft clock changes (e.g., incorrect time).
- Incorrect navigation position.
- Any large shifts in the displayed GNSS position on Primary flight display (PFD)/navigation display.

Pilots should not hesitate to alert ATC to any observed interruption, degradation or anomalous performance of GNSS equipment or related avionics and should take note of the duration of the interference. Pilots should report the interference by going to the FAA's [Report a GPS Anomaly](#) website.

This section includes suggested procedures that are shaded in gray. Operators should consider the procedures offered in this guide as an outline that can be adapted to specific aircraft (i.e. make, model and series).

4.2 Early Recognition

Early recognition of jamming and/or spoofing is important for pilots to be able to correct faulty navigation inputs as soon as possible by using alternate navigation sources that are not dependent on GPS (i.e. radar vectors, use of ground-based NAVAIDs, or a non-hybrid inertial navigation system, etc.) Procedures and CRM are necessary components to mitigate any anomaly until the aircraft is safely recovered to where maintenance can be performed, if required.

Jamming is relatively easy to detect because the messages on the aircraft's Electronic Centralized Aircraft Monitor (ECAM) or EICAS will indicate a failure of the navigation system to receive GPS signals. Other indications may include:

- ➔ Inability to use GNSS for navigation, including waypoint navigation.
- ➔ Failure indications from systems dependent on GNSS (e.g., ADS-B, TAWS).



Spoofing is more insidious and indications may include:

- ➔ Disagreement in navigation position, such as GNSS/FMS position alerts.
- ➔ Abnormal differences between Ground Speed and True Airspeed.
- ➔ Time and date shift.
- ➔ Spurious TAWS alerts
- ➔ A deviation of GNSS-based navigation position.

Differences in avionic suites and software packages add layers of complexity to inflight procedural mitigations. Aircraft operators should work with their OEMs to determine the impacts to their specific aircraft systems. Manufacturers, operators, and ATC should be aware of the general indications and effects of GNSS interference, such as:

- ➔ Inability to use GNSS for navigation.
- ➔ Flight deck alerts regarding position error, e.g., increase in Actual Navigation Performance (ANP).
- ➔ Inability to use GNSS as a position update source for an inertial navigation system.
- ➔ Loss of or degraded RNAV, to include RNP.
- ➔ Loss of/discrepancies in or erroneous aircraft position on navigation display aircraft position on navigation display (e.g., own-ship position on moving map displays and EFB software).
- ➔ Navigation system switching to an alternate navigation source (e.g., IRS updates using ground-based aids).
- ➔ NAVAID automatic tuning function degradation (e.g., spoofing may cause erroneous NAVAIDs to be selected with the automatic tuning function of some navigation systems).
- ➔ Loss of or erroneous ADS-B in/out data.
- ➔ Erroneous or misleading TAWS.
- ➔ Erroneous TAWS alerts inhibiting legitimate TCAS advisories.
- ➔ Inaccurate display of traffic on the traffic display, including possible erroneous traffic advisories.
- ➔ Loss of or misleading information on SVS.
- ➔ Position and groundspeed-dependent FMS effects (e.g., erroneous estimated time of arrival, estimated fuel at waypoint indication).
- ➔ Loss of or erroneous aircraft clocks updated with GNSS.
- ➔ Inability to log on to or continue CPDLC.
- ➔ Loss of weather radar integrations such as the automatic tilt function.
- ➔ Loss of or erroneous wind and ground speed indications.
- ➔ Erroneous attitude and heading reference system (AHRS).
- ➔ Loss of or erroneous indication on a HUD.



- ➔ Loss of or erroneous data for ATC surveillance systems reliant on ADS-B data.
- ➔ Loss of or erroneous data for flight tracking systems reliant on GNSS, resulting in potential airspace infringements and/or route/altitude deviations.

4.3 Use of EFB as a Mitigation

An EFB or computer tablet may aid in detecting jamming and/or spoofing. The EFB or tablet with a separate GPS input and moving map software may be less vulnerable to jamming and/or spoofing because it may be shielded from GNSS inference due to its location inside the airframe. Though not an authorized navigation source, pilots may be alerted to a sudden difference between the aircraft navigation display and their EFB map display.

Note: Any hardware installed on an aircraft must be in accordance with FAA regulations.

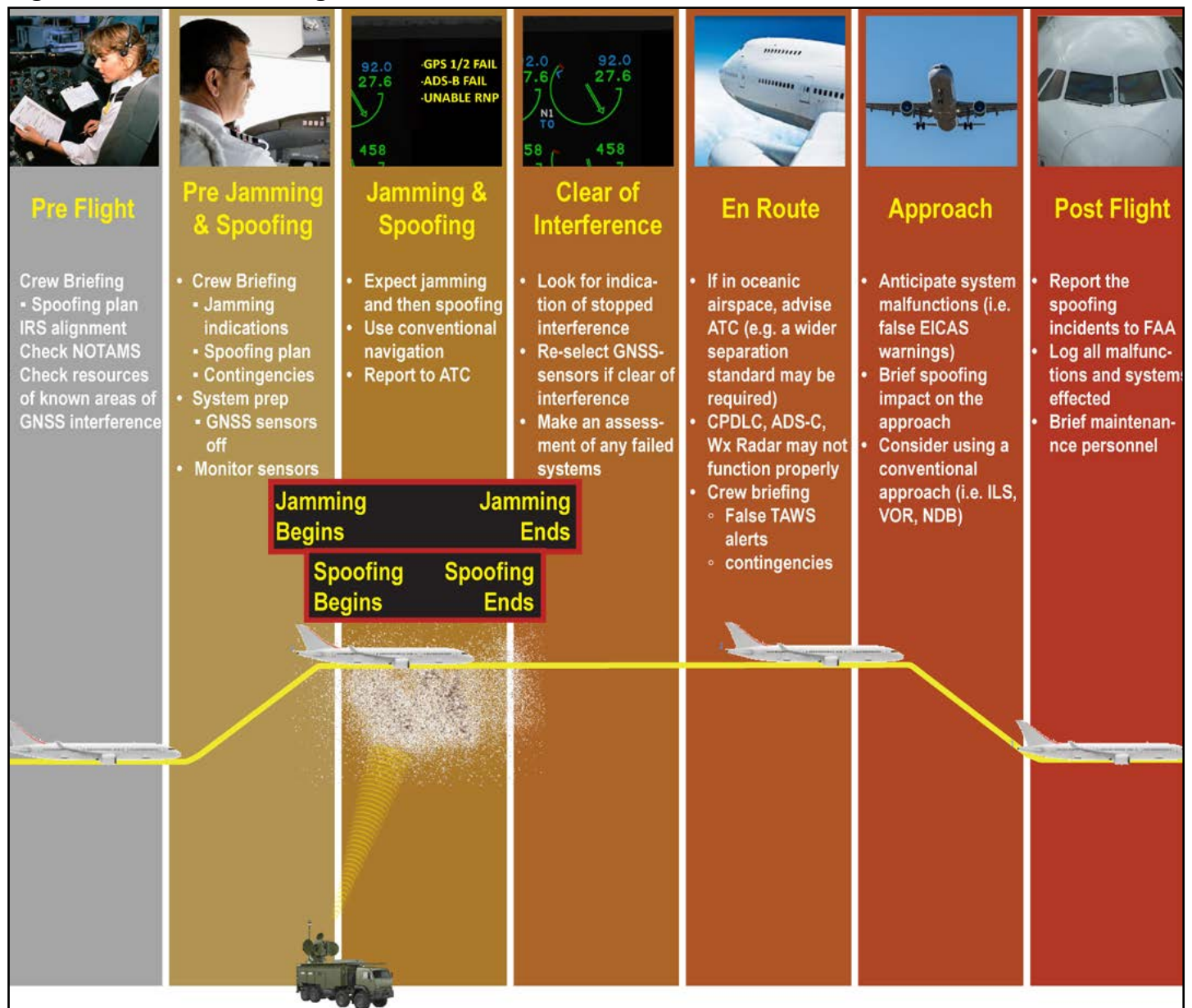




4.4 Pilot Guidance Before, During and After GNSS Interference

Figure 4-1 illustrates the stages of entering and leaving an area of GNSS interference and offers some pilot guidance during each stage of the process (i.e. from preflight to post flight). Because GNSS interference is a recent and emerging threat to civil aviation, not everything is known. This guide will be updated as needed to provide the most current guidance. Therefore, any guidance offered in this resource guide is subject to change as more information becomes available. See the contact page on the last page of this guide to send your comments.

Figure 4-1: Before, During and After Interference





4.5 Preflight

Flight Planning

[Appendix A](#) provides links to current spoofing maps and areas of known interference. In addition to checking the weather and NOTAMs, determine if the route of flight is near or through any known “hot spots” of interference. If the route of flight goes through a known area of interference, consider an alternate route, if possible.

- ➔ In areas with known interference, file published airways between ground-based NAVAIDs, if possible. Consider a plan of using only ground-based NAVAIDs or Minimum Operational Network (MON) airports when in the vicinity of interference areas. Consider weather avoidance when routing near jamming and/or spoofing, as it can disrupt weather radar.
- ➔ Plan for possible contingencies for “no GPS” capability. This planning should include the use of ground-based NAVAIDs for en route and determining the availability of MON airports with Standard Instrument Departures (SID), Standard Instrument Arrivals (STAR) and conventional based approaches (i.e. ILS, VOR, NDB etc.).
- ➔ In preparation for false TAWS alerts, review safe altitudes along the route of flight to include Minimum En Route IFR Altitude (MEA), Minimum Off-Route Altitude (MORA), and minimum terminal area altitudes (e.g. Minimum Safe Altitude (MSA)).
- ➔ Contingency planning includes having adequate fuel to more than one alternate should it be necessary to divert to a location clear of interference or clear of weather.



Additional Preparations

In addition to the normal preflight activities, pilots should consider a few additional details to prepare for jamming and/or spoofing:

- ➔ Pilots should synchronize/set their personal watches or other timekeeping device to the current time, and make sure the timekeeping device cannot be spoofed (i.e., disable automatic time updates to GPS, as applicable).
- ➔ As part of the normal Minimum Equipment List (MEL) and maintenance log review, take some extra time to review the required actions for equipment outages that are vulnerable to jamming and/or spoofing.
- ➔ Most aircraft inertial systems (e.g. IRS) are part of an overall navigation solution and were not necessarily designed to be separated from the overall navigation solution. However, if entering an area of known jamming and/or spoofing, consider aligning the IRS during preflight and disable GNSS updating. This may impact the navigation capability and must only be performed in accordance with the AFM, AFMS or specific OEM instructions.



Pre-Flight Briefing

If the flight is expected to enter known jamming and/or spoofing areas, it is important to thoroughly brief the following:

- ➔ Expected point of entry and exit from the interference area.
- ➔ Plan of action before, during and after departing the interference area.
- ➔ Transitioning from GNSS to all available ground-based NAVAIDs until leaving the spoofing area, or later.
- ➔ Expect GNSS dependent system anomalies during and after jamming and/or spoofing:
 - Because of the safety concerns associated with false TAWS alerts, it is important to brief the possibility of alerts happening on the departure, en route, or approach phase of flight. Discuss a plan of action if receiving TAWS alerts after a spoofing anomaly. Consider the elevation of terrain anywhere near the route of flight, when considering evasive maneuvers as a response to the TAWS alert.(See paragraph [3.13](#)).
- ➔ Contingency planning for possible emergencies within the area of interference (e.g. engine failure, depressurization) to include any planned escape routes to safety.
- ➔ RNP requirements along the route of flight and possible spoofing impacts.





Sample Preflight Procedures

PREFLIGHT

Pilots should:

- Check NOTAMs for local and en route GNSS Interference
- Identify entry and exit points of interference areas
- Determine alternate routes to avoid interference areas and coordinate with flight dispatchers/ flight followers, if applicable
- Identify alternative navigation should GNSS be jammed or spoofed (e.g. ILS, VOR/DME, NDB, etc.) for en route and approach
- Synchronize watches or independent time devices to the current time
- Consider routing and weather, especially thunderstorm activity, if weather radar fails
- Brief the possible effects of GNSS interference to include:

Jamming Indications

- GNSS Failure Message
- ADS-B Failure/Warning
- Data Link failure (CPDLC and ADS-C)
- SATCOM loss
- Loss of SVS

Spoofing Indications

- Impact on TAWS and planned responses at various phases of flight
- GNSS position message
- Rapid increase in EPU/ANP
- Time change on aircraft clock
- ADS-B erroneous position data
- Unexpected turns from the previous course
- Shift in aircraft position on navigation display (GNSS position differs from FMS position)
- Illogical ground speed and wind depictions



4.6 Pre Jamming and/or Spoofing

Briefing Review

Before reaching areas of known jamming and/or spoofing, allow time to adequately brief and prepare for possible GNSS interference. The FAA recommends avoiding direct RNAV routing in the vicinity and through areas of known jamming and/or spoofing because GPS/GNSS may be lost. It is better to stay on established airways where ground-based NAVAIDs may be used as an alternative to GNSS. Brief the following to other pilot(s), if applicable:

- ➔ Review possible indications of jamming and/or spoofing to include:
 - False TAWS alerts/warnings and possible override of TCAS/ACAS alerts.
 - Outage or false ADS-B targets.
 - Loss of CPDLC.
- ➔ Review jamming/spoofing procedures and checklists if GNSS are no longer available or reliable.
- ➔ Review any escape routes for an emergency descent should it be necessary due to de-pressurization or an emergency resulting in one engine inoperative (OEI) and diversion airport options.

Prepare the Flight Deck (*May be prior to takeoff or en route*)

Prepare the flight deck in accordance with OEM and operator procedures. The following are some suggestions to consider, if possible:

- ➔ De-select GNSS input to navigation system. This will only prevent spoofed signals from entering the navigation position and will not prevent other systems from being impacted (i.e. TAWS, ADS-B, etc.).
- ➔ Inhibit GNSS updating of an inertial navigation system.

Note: With some avionics, a clock set to “internal” drives an ADS-C FOM degradation, which may make the aircraft ineligible for Performance-Based Communication and Surveillance (PBCS) separation standards. In some ground systems, this can trigger discontinuation of data communications services (ADS-C and CPDLC).

- ➔ Change clock to “Internal” (INT)/manual.
- ➔ Inhibit TAWS Look Ahead Mode.
- ➔ Stow HUD.





Sample Pre-Jamming and/or Spoofing Procedures *(These are suggested procedures and the list should be customized to fit your specific aircraft.)*

FLIGHT DECK PREPARATION *(May be prior to takeoff or en route)*

Include the following while preparing the flight deck:

- Review maintenance logs and any MEL requirements. Review MEL requirements for possible loss of equipment during GNSS interference.
- If takeoff is from an airport/area of known GNSS interference:
 - Perform a manual alignment of IRS and deselect the “hybrid mode” or GNSS updating, if possible
 - Plan and brief a ground-based NAVAID instrument departure or request radar vectors to ensure obstacle clearance
 - Inhibit the enhanced mode of TAWS, if possible. This step can instead be done immediately after takeoff, as appropriate. This will disable the look-ahead function described in [paragraph 3.13](#) of this guide. In most instances, this will not affect the “basic” function of TAWS

Should spoofing occur on the ground with a position shift,

DO NOT TAKEOFF UNTIL RESOLVED

It may be necessary to inhibit GNSS updates to FMC. This may be reselected after takeoff when aircraft is no longer impacted by GPS interference

Note: Consider reactivating all functions of TAWS after the aircraft has departed the area of GNSS interference. If TAWS is continuously alerting en route, consider inhibiting the enhanced mode of TAWS as per OEM recommended procedures.

PRE-Jamming and/or Spoofing

- Brief the following prior to entering an area of known GNSS interference:
 - Intentions during jamming and/or spoofing
 - Contingency/Emergency procedures and intentions
 - Prepare to use ground based NAVAIDS and radar vectors
- Monitor EPU/ANP for any increase in value
- Clock INT
- GNSS Deselect from navigation system
- Inertial navigation system Deselect “hybrid mode”/inhibit GNSS updating
- TAWS Inhibit Enhanced Mode
- Navigate (Green Needles) use ground-based NAVAIDS
- Auto tuning Manual
- One COMM radio Tuned to 121.5 with volume adjusted to monitor



Expanded Scan with Vigilance

Stay vigilant while monitoring the following:

- ➔ Any dramatic changes in EPU and ANP values;
- ➔ Position relative to ground-based NAVAIDs;
- ➔ Aircraft clock for incorrect time (should be compared with independent timekeeping device);
- ➔ GNSS Date (Sensor Page) for any changes to the date;
- ➔ Position information as indicated by handheld GNSS devices, cell phone Apps, or EFB that differs from the FMS position; and
- ➔ Pilot reports in the vicinity notifying ATC of jamming and/or spoofing.



4.7 Jamming and/or Spoofing

Jamming

Jamming may occur before spoofing with several failure messages of systems that use GNSS. Jamming system failures may include:

- ➔ GNSS.
- ➔ ADS-B.
- ➔ TAWS (if look-ahead type).
- ➔ SVS.
- ➔ SATCOM.

Onset of Spoofing

Spoofing signals take the place of authentic GNSS satellite signals. The GNSS receiver will not distinguish between an “authentic” and “false” signal which causes a false position, time, and date to be displayed. Pilots may not be aware spoofing is occurring due to reception of false signals overriding authentic GNSS signals. However, there are some indications on the flight deck that are indicative of spoofing that will provide pilots with information to execute procedures for alternate navigation while maintaining situational awareness. Some of these indications are:

- ➔ GNSS position shifts several miles in seconds.
- ➔ IRU and GNSS positions differ significantly.
- ➔ EPU or ANP values rapidly increasing.



- ➔ Change in heading as commanded by the autopilot (drifting from the course or sudden commanded turn)
- ➔ Clock time and/or difference between the Captain/FO clocks.
- ➔ EICAS/ECAM cautions and warnings:
 - CHECK GNSS.
 - FMS-GPS DISAGREE.
 - ATC FAIL.
- ➔ ADS-B with a Failure or Caution message.
- ➔ Data Link (CPDLC and ADS-C failure indications).
- ➔ SVS reverting to standard attitude display (blue over brown).
- ➔ Navigation Display of the following:
 - Wind direction radically changes.
 - Unreasonable ground speed indications.
 - GNSS symbol separates and moves away from IRS symbol.
- ➔ TAWS false terrain warning.



Pilot Procedures During Spoofing

When spoofing is confirmed by one or more indications above, it is important to have procedures in place to distinguish reliable systems from compromised ones, which should no longer be trusted. Pilots should note the time on an independent time source like a watch while prioritizing the basic axioms of aviation of: aviate, navigate, and communicate. This will aid in keeping situational awareness while executing operator/OEM procedures.





Sample Jamming and/or spoofing Procedures

Jamming and/or Spoofing (Entry)

- Monitor EPU/ANP for any increase in value
- Cross check aircraft clock with watch/independent time source
- Monitor any shift of position on the navigation display
- Note any unreasonable ground speed or wind speed changes

If Unplanned Entry

- Auto Flight System..... Heading Mode

(Use flight magnetic courses until established with a non-GNSS navigation source or radar vectors)

- Clock INT

(Note time on watch/alternate time source)

- Clock Set Manually
- GPS Deselect from navigation system
- Inertial navigation system Deselect “hybrid mode”/inhibit GNSS updating
- TAWS Inhibit Enhanced Mode
- Request radar vectors ,or proceed via conventional NAVAIDs
- Notify ATC of Jamming/Spoofing and report:
 - Time (from watch or independent time source),
 - Notify ATC of any loss of ADS-B Out
 - Location from known (radial and distance from ground-based NAVAIDs),
 - Speed,
 - Magnetic heading,
 - Altitude, and
 - Duration of the anomaly



4.8 Clear of Interference

When departing an area of GNSS interference, it is important to look for indications that all jamming and/or spoofing have ceased. However, pilots should expect that jamming and/or spoofing could re-occur in a different location. Allow enough distance from the GNSS interference before resuming GNSS based RNAV.

Note: Use OEM guidance for the adequate distance/time from GNSS interference before attempting to restore aircraft systems to normal operation.

The following are positive indications that you have departed from areas of GNSS interference:

- ➔ Correct UTC time as compared with an independent time source (i.e. watch).
- ➔ Correct GNSS date.
- ➔ Navigation display has returned to acceptable or normal displays of wind and ground speed.
- ➔ The correct aircraft position has returned and has been cross checked by using ground-based NAVAIDs.

When clear of jamming and/or spoofing, conduct an assessment of some of the aircraft systems to include:

- ➔ CPDLC with no termination or delay messages.
- ➔ ADC-C assessment in coordination with ATC.
- ➔ Weather radar is correctly depicting that which can be seen (i.e. cumulus clouds, etc.).
- ➔ Multi-mode receiver (MMR) in-flight reset in accordance with OEM/operator procedures.
- ➔ TAWS computer in-flight reset in accordance with OEM/operator procedures.

After assessment of those systems that can be checked in-flight, in accordance with OEM guidelines, re-activate the following systems used for normal flight outside of jamming and/or spoofing areas:

- ➔ Reselect GNSS sensor input to navigation system.
- ➔ Reselect the inertial navigation system hybrid mode.
- ➔ Advise ATC of any relevant system that is still impacted and cannot be reactivated during flight.



Sample Post Jamming and/or spoofing Procedures

CLEAR OF INTERFERENCE

- Monitor for any indication of continuing or recurring of jamming and/or spoofing
- Auto Flight System Normal Navigation Mode
- CLOCK GPS Updating
- (The clock should remain in INT until certain that the GNSS receiver has recovered by cross-checking position against flight plan magnetic headings and ground-based NAVAIDs.)
- IRS Select “hybrid mode”/enable GPS updating
- TAWS Reset to Enhanced Mode

If no further indication of GNSS interference, then proceed using normal procedures. File a written report to the FAA at [Report a GPS Anomaly](#).

If there continue to be GPS/GNSS system anomalies due to spoofing, proceed to the destination using ground-based NAVAIDs and plan on a ground-based NAVAID approach that does not require GNSS for any portion of the approach or missed approach. Advise ATC of the remaining failures and intentions. Brief the ground-based NAVAID approach and terminal operation and actions to be taken should there be any unexpected TAWS alerts during the approach and landing phase.

4.9 Oceanic Considerations

GNSS interference usually occurs over land, but residual effects on aircraft systems can persist, and in some cases, continue into the oceanic environment. These effects increase the workload for both flight crews and Air Navigation Service Providers (ANSP). Notification of GNSS interference to air traffic control, regardless of where or when in flight it was experienced, is a requirement in all FAA-controlled oceanic airspace. (See [ZNY NOTAM A0251/25](#), and [Pacific](#) and [Alaska](#) Chart Supplements).

Early notification to air traffic control of degraded capabilities enables improved coordination and strategic planning of flights and also assists the FAA in monitoring the impacts of GNSS interference on aircraft operating in the NAS.

Some oceanic airspace or tracks are exclusionary based upon equipment and qualification. When navigation system degradations are reported by pilots or interpreted by the ATC system, operators can expect re-routes or significant altitude changes outside of exclusionary airspace. (See [NAT Doc 006](#), [NAT OPS Bulletin 2025-001](#), NAT HLA ([NAT Doc 007](#)), and [ZAN NOTAM A0238/24](#)).



4.10 Approach

After jamming and/or spoofing, pilots should consider that the GNSS dependent systems may not be working normally even if they appear to be functioning properly. Therefore, it is better to use approach procedures based on ground-based NAVAIDs and avoid any approach that requires GNSS. Inform ATC of malfunctioning aircraft systems and request a ground-based NAVAID approach (i.e. ILS, VOR, NDB, if available). If in Visual Meteorological Conditions (VMC), consider requesting radar vectors for a visual approach and landing. If a non-GNSS approach is not available during Instrument Meteorological Conditions (IMC), consider requesting an alternate where a ground-based approach or visual conditions are available.

Follow all OEM guidance, and include a flight crew briefing on responses to possible false TAWS warnings. The briefing should include any means of distinguishing false TAWS warnings from authentic terrain warnings. Include a review of the minimum altitudes for terrain clearance in the terminal area of the approach such as Minimum Safe Altitude (MSA), Minimum Vectoring Altitude (MVA) and Minimum Descent Altitude/Height (MDA/H). Be prepared to execute a missed approach from a higher altitude than normal due to TAWS alerts, and do not climb through unauthorized altitudes. Additionally, consider the possibility of distracting ECAM/EICAS alerts that may occur during the final approach and brief those that can safely be disregarded. However, comply with any a resolution advisory (RA), unless doing so would jeopardize the safe operation of the flight. These alerts are valid.



4.11 Post Flight

If GNSS jamming and/or spoofing is suspected during flight, pilots should perform the following:

- ➔ Document GPS/GNSS interference in the maintenance log to ensure maintenance clears all system faults. It may be necessary for maintenance personnel to perform a “hard reset” of the GNSS/MMR systems and if necessary, a factory reset or replacement of damaged systems. These actions are recommended as a standard maintenance task for aircraft flying through known interference areas, and/or upon crew reports of the GPS effects described.
 1. If GPS interference from a previous flight leg caused GPS to remain INOP, or incorrect date/time is observed, power cycle of the MMR circuit breakers on the ground may resolve this issue.
 2. After cycling the circuit breakers, perform an operational test on the Global Positioning System to ensure it is functioning normally. To verify GPS signal is available, go to the appropriate page to confirm accurate GPS position is displayed. To verify date/time are correct, go to the STATUS page and verify that the date shown is correct.

Note 1: Resetting of circuit breakers must be in accordance with OEM guidance.

Note 2: Repeated reset of the circuit breaker may lead to premature failure.



3. Even in cases where the GPS recovers and the date/time were not affected after flying through GPS interference, a maintenance check of the GPS position/time/date on the ground to verify the GPS is in good working order before the next flight is recommended.
- ➔ Go to the FAA site, [Report a GPS Anomaly](#) and provide the details of any GNSS interference including any observed interruption, degradation or anomalous performance of GNSS equipment or related avionics (e.g., map shifts, suspected GNSS spoofing, lost or misleading position, time anomalies, etc.) Include the duration of the interference, if known (See the bullet points of information that should be included in the report on page 1-4).





Section 5: Training

For specific aircraft system information, refer to your Airplane Flight Manual (AFM) and/or AFM Supplement. The system information provided in this guide is generic and may or may not apply to your aircraft. It is for informational purposes only and to provide safety suggestions to help mitigate jamming, spoofing or both.

5.1 Introduction

This section provides some ground and simulator training guidance.

5.2 Ground School

The following are suggested ground school topics for participants to know and understand:

- Understanding alternative navigation capabilities/navigating without GNSS.
- Definitions of jamming and/or spoofing.
- Flight deck indications of jamming.
- Flight deck indications of spoofing.
- Long-term effects of spoofing.
- How jamming and/or spoofing works.
- Locations of regions most prone to jamming and/or spoofing.
- [SAFO 24002](#).
- Human factors involved with the impacts of jamming and/or spoofing.
- Dangers of false terrain alerts.
- Aircraft systems impacted by jamming and/or spoofing.
- Steps to mitigate jamming and/or spoofing during preflight, pre-jamming and/or spoofing.
- Best courses of action during jamming and/or spoofing.
- How to restore aircraft systems after jamming and/or spoofing.
- Understand the necessity of reporting during a jamming and/or spoofing.



5.3 Flight Training

Pilots should train with written procedures/checklists to be prepared for possible jamming and/or spoofing. Simulator training should incorporate the following:

- ➔ Unexpected TAWS alerts and go-arounds at higher altitudes other than the typical go-around on short final.
- ➔ TAWS alerts in the approach phase and spurious warnings at various other phases of flight.
- ➔ Scenarios that simulate a corrupted FMS position causing the aircraft to turn off the previously established route.
- ➔ Simulated position shift on the navigation display including during an approach.
- ➔ Scenarios that simulate the aircraft clock changing from the correct UTC.
- ➔ Practice of briefings for entering possible areas of jamming and/or spoofing.
- ➔ Simulation of multiple failures of aircraft systems that have a GNSS component that is spoofed.
- ➔ Simulation of spoofing on the ground during taxi and properly addressing the anomalies.
- ➔ Proficiency of alternative navigation to using ground-based NAVAIDs and a ground-based NAVAID approach (i.e. Localizer, ILS, VOR, NDB, etc.).





Appendix A: Current and Past Data

A.1 Current Data Links

This appendix highlights those areas of high jamming and/or spoofing instances since September 2023. Pilots need to be particularly vigilant in areas around eastern Europe, the Black Sea and the Eastern portion of the Mediterranean Sea. To review those FIRs the highest number of incidents of jamming and/or spoofing, see Table A-1 and the specific threats in those FIRs on the remaining pages of this appendix.

A.2 Areas of High Jamming and/or Spoofing Incidents

The tables below reflect historical data to show those regions with the most impact. GNSS interference is a highly fluid situation and may rapidly change to affect other regions that are not listed below.

Table A-1 GNSS Spoofing From July-Aug 2024 of Top Impacted FIRs

FIR	Country	Spoofing Incidents
Nicosia	Cyprus	5655
Tel-Aviv	Israel	3228
Cairo	Egypt	2375
Ankara	Turkey	1195
Samara	Russia	1186
Moscow	Russia	988
Lahore	Pakistan	492
Minsk	Belarus	372
Beirut	Lebanon	371
Delhi	India	316
Sofia	Bulgaria	235
Bucharest	Romania	231
Athens	Greece	193
Amman	Jordan	169
Riga	Latvia	169
Jeddah	Saudi Arabia	115
St. Petersburg	Russia	77
Istanbul	Turkey	67
Tallinn	Estonia	57
Vilnius	Lithuania	51

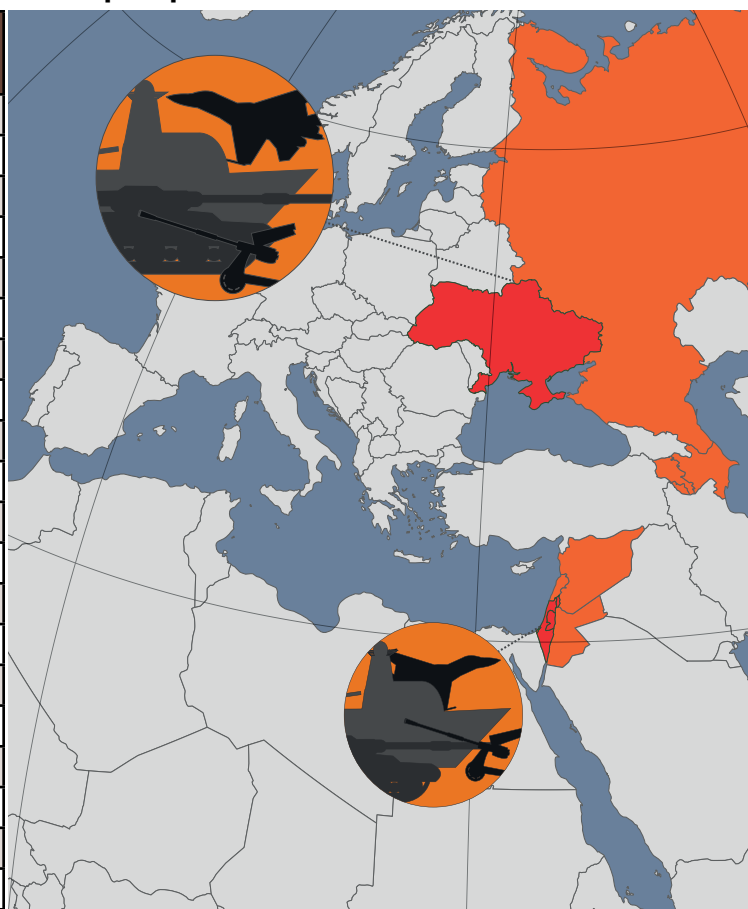




Table A-2 Areas of Major Spoofing: Eastern Mediterranean Sea

FIR, Country	Map	Areas of Spoofing
Nicosia FIR - Cyprus		➔ Highest spoofed FIR to date ➔ Entire FIR impacted, including approaches
Beirut FIR – Lebanon		➔ Entire FIR impacted ➔ Beirut Airport, including on the ground





FIR, Country	Map	Areas of Spoofing
Tel Aviv FIR – Israel		→ Entire FIR impacted
Cairo FIR – Egypt		→ Sinai Peninsula, NE portion → Cairo Airport → Airways L550, L560 & A16, → Within 200nm of CVO (Cairo) VOR





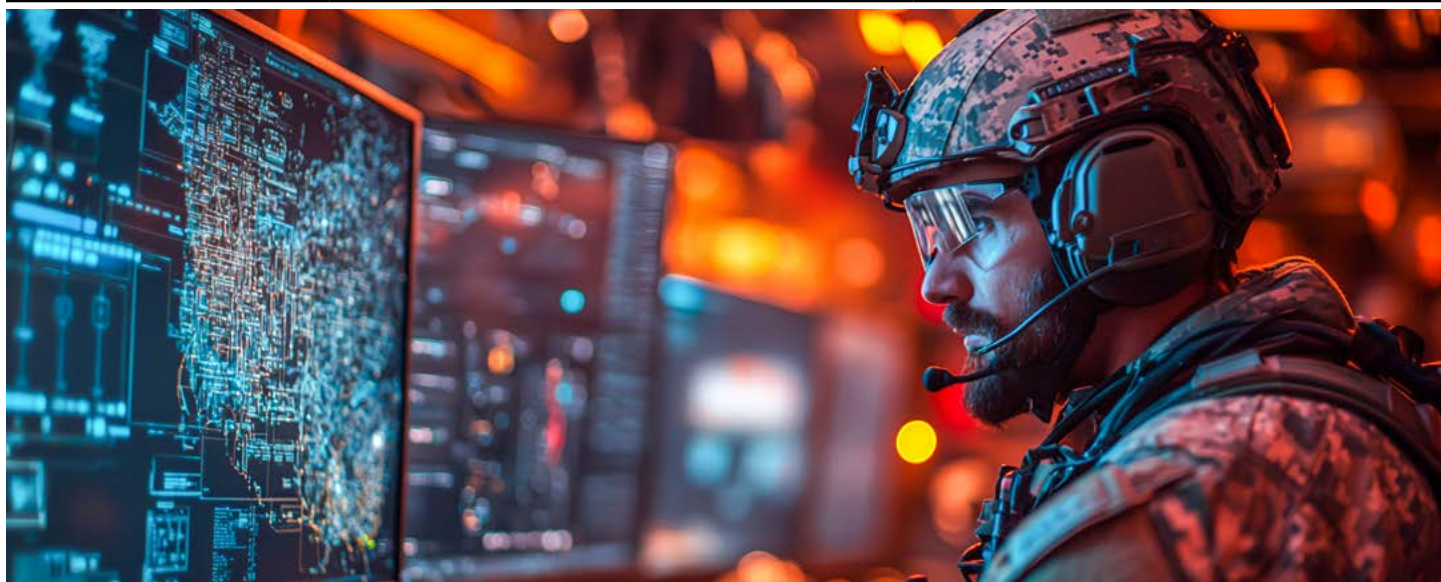
FIR, Country	Map	Areas of Spoofing
Jeddah FIR – Saudi Arabia		➔ Routing to and from Egypt near Cairo FIR ➔ Airways L550, L560, UB411
Amman FIR – Jordan		➔ Entire FIR impacted ➔ OJAM/Amman Marka, OJAI/Queen Alia, OJAJ/Aqaba





Table A-3 Areas of Major Spoofing: Black Sea

FIR, Country	Map	Areas of Spoofing
Ankara/Istanbul FIRs - Turkey		➔ Northern Turkish coastline ➔ Western Black Sea area, near Istanbul ➔ Airways UM859, UN743, UL746 ➔ Simferopol Airport (Crimea) ➔ Krasnodar
Sofia FIR - Bulgaria		➔ Over water areas in the east of the Sofia FIR ➔ Over land close to the Black Sea coastline in the area of Burgas and Varna ➔ Simferopol





FIR, Country	Map	Areas of Spoofing
Bucharest FIR – Romania		➔ Southeast quadrant ➔ Area between Brasov, Bucharest and Constanta ➔ Simferopol

Table A-4 Areas of Major Spoofing: Russia and Baltic Region

FIR, Country	Map	Areas of Spoofing
Samara & Moscow FIRs - Russia		➔ Nizhny Novgorod and Samara ➔ Moscow and Yaroslavl





FIR, Country	Map	Areas of Spoofing
Tallinn, Riga and Vilnius FIRs – Estonia, Latvia, Lithuania		→ Eastern parts of Riga FIR (Latvia) and Vilnius FIR (Lithuania) → Airway M864 → Smolensk
Helsinki FIR – Finland		→ Helsinki/Tallinn FIR boundary → EFLA/Lahti and EFHK/Helsinki → Smolensk





Table A-5 Areas of Major Spoofing: India/Pakistan border

FIR, Country	Map	Areas of Spoofing
Lahore & Delhi FIRs – Pakistan & India		➔ Areas northwest of New Delhi ➔ Area of Lahore ➔ Along border

Table A-6 Areas of Major Spoofing: Iraq, Iran

FIR, Country	Map	Areas of Spoofing
Iraq, Iran (Baghdad and Tehran FIRs)		➔ Sporadic/occasional spoofing ➔ Between ORBI/Baghdad Airport and the northern ORBB/Baghdad FIR boundary ➔ Iranian border (OIIX/Tehran FIR)





Table A-7 Areas of Major Spoofing: North and South Korea

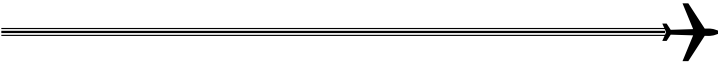
FIR, Country	Map	Areas of Spoofing
North/South Korea (Pyongyang and Incheon FIRs)		➔ Few Incidents ➔ North/south Korean border ➔ Oceanic portion of the FIR

Table A-8 Areas of Major Spoofing: Around Beijing, China

FIR, Country	Map	Areas of Spoofing
China		➔ Beijing Airport



C U R R E N T A N D P A S T D A T A



Intentionally Blank



Appendix B: Links to Useful Information

Documents

- [SAFO \(24002\)](#) *(Sometime it is necessary to click the refresh button in DRS)*
- [AIM](#) *(Click Button to Expand References)* 
- [AIP](#) *(Click Button to Expand References)* 
- [EASA - Information on Conflict Zones](#)
- [EASA SIB](#)
- [NAT Ops Bulletin 2025-001](#)
- [ICAO Strategic Guidance 14ANC Working Paper 063](#)
- [Best Practices for Airport GPS Disruption Resiliency](#)



Tools/Trackers

- [GPSJAM.org](https://gpsjam.org)
- [Live GPS Spoofing and Jamming Tracker Map](#) (*SKAI Data Services/GPSwise*)
- [Flightradar24: GPS jamming map](#)
- [FAA: Prohibitions, Restrictions, and Notices](#)
- [EASA - Conflict Zone Information Bulletins \(CZIBs\)](#)
- [EUROCONTROL GNSS Threat Assessment Tool](#)
- [FAA: Public Notices](#) (*Government GPS Interference Testing, Training and Evaluation*)

Videos

- [Airbus - Navigation, Equipment, Jamming and/or spoofing](#)
- [Boeing - 737 GPS Interference](#)
- [GPS Jamming \(& spoofing\) explained](#) (*Flightradar 24 Video*)

Websites/Articles

- [Airbus Safety First 2024. GNSS Interference](#)
- [Flightradar24 article: GPS Jamming](#)
- [GPSWISE, Navigating the future: Mitigating GPS Spoofing & Jamming Risk in Aviation](#)
- [IATA SIRM Insights](#) (*Lists Indications and Useful Links*)
- [SKYBRARY: GNSS Jamming and/or spoofing](#)
- [SKYBRARY: Interference to GNSS Signals](#)
- [OPSGROUP: GPS Spoofing Final Report](#)
- [FAA: Report a GPS Anomaly](#)



Flight Planning Links

- [NOTAMS](#)
- [NOTAM Search](#)
- [Aeronautical Information Publication \(AIP\)](#)
- [Aeronautical Information Manual \(AIM\)](#)
- [Predictive RAIM](#)
- [Temporary Flight restrictions](#)
- [Aviation Weather Center](#)
- [FAA Flight Planning Information](#)
- [Flight Service 1800wxbrief](#)
- [FAA Flight Plan Quick Guide](#)
- [Critical DME List](#)
- [SkyVector](#)
- [FAA Form 7233-4](#) (*Pre-Flight Checklist and International Flight Plan Form*)

L I N K S T O U S E F U L I N F O R M A T I O N



Intentionally Blank



Appendix C: Glossary and Acronyms

C.1 Glossary

A

Area Navigation (RNAV). A method of navigation (formerly known as “Random Navigation”) which permits aircraft operation on any desired flightpath within the coverage of ground- or space-based navigation aids or within the limits of the capability of self-contained aids, or a combination of these.

C

COSPAS-SARSAT. COSPAS-SARSAT is an international satellite-based Search-and-Rescue system established by Russia, Canada, USA, Denmark and France to locate emergency radio beacons transmitting on 406 MHz.

D

Distance Measuring Equipment. Equipment (airborne and ground) used to measure, in nautical miles, the slant range distance of an aircraft from the DME navigational aid.

Distance Measuring Equipment (DME)/DME (D/D) RNAV. Refers to RNAV using DME ranging from at least two DME facilities to determine position.

DME/DME/Inertial (D/D/I) RNAV. Refers to navigation using DME ranging from at least two DME facilities to determine position along with use of an aircraft inertial navigation system (INS) e.g. using INS to provide sufficient position information during limited DME gaps.

F

Fault Detection and Exclusion (FDE). is a GPS/GNSS receiver function that enhances navigation integrity by identifying and removing faulty satellites from the position solution. FDE is an advanced form of RAIM (Receiver Autonomous Integrity Monitoring) that allows continued navigation without interruption, requiring at least six satellites to function effectively (or five with baro-aiding).

Flight Management System (FMS). An integrated system that may be just an RNAV system or, when meeting appropriate airworthiness requirements, can be an RNP system. FMS typically consist of inputs from airborne sensors and serves as a computer for navigation guidance and aircraft performance. The FMS supports outputs



to displays and annunciations that PBN operations require and is often directly coupled to the aircraft's flight guidance system.

G

Global Navigation Satellite System (GNSS). GNSS is a generic term to denote a global satellite positioning and time determination system, which includes one or more satellite constellations, aircraft receivers, and system integrity monitoring.

Global Positioning System (GPS). GPS is a U.S. satellite-based radio navigation system that provides a positioning service anywhere in the world. The service provided by GPS for civil use is defined in the GPS Standard Positioning System Signal Specification. GPS is the U.S. core GNSS satellite constellation providing space-based positioning, velocity, and time. GPS is composed of space, control, and user elements.

I

Inertial Navigation System (INS). INSs are self-contained systems comprised of gyros and accelerometers that provide aircraft attitude (pitch, roll, and heading), position, and velocity information in response to signals resulting from inertial effects on system components. Once aligned with a known position, INSs continuously calculate position and velocity. INS position accuracy decays with time. This degradation is known as "drift."

J

Jamming. Emissions that do not mimic Global Navigation Satellite System (GNSS) signals (e.g., GPS and WAAS), but rather interfere with the receiver's ability to acquire and track GNSS signals. Jamming can result in denial of GNSS navigation, positioning, timing and aircraft dependent functions.

O

Oceanic Airspace. Airspace over the high seas. Generally, "oceanic" is included in the airspace designation (e.g., Oceanic Control Area (OCA)), and direct controller-pilot VHF voice communications are not available. ATC is provided using at least some elements of procedural control in accordance with ICAO.

R

Receiver Autonomous Integrity Monitoring (RAIM). A software algorithm in a GPS sensor that verifies the integrity of the sensor's position output using GPS measurements, or GPS measurements and barometric aiding.

RNP System. A navigation system installed in an aircraft supporting onboard performance monitoring and alerting along with the other requirements of the public standards for RNP found in RTCA DO-236(), DO-283(), or DO-229(). An installed RNP system may support a myriad of RNAV and RNP NavSpecs, provided the installed aircraft equipment meets all the requirements for each individual NavSpec.

**S**

Spoofing. Spoofing as emissions of GNSS-like signals that may be acquired and tracked in combination with or instead of the intended signals by receivers. The onset of spoofing effects can be instantaneous or delayed, and effects can persist after the spoofing has ended. Spoofing can result in false and potentially confusing, or hazardously misleading, position, navigation, and/or date/time information in addition to loss of GNSS use.

T

Terrain Awareness and Warning System. This electronic safety system provides aural and visual alerts to pilots to prevent Controlled Flight Into Terrain (CFIT) accidents by warning of potentially hazardous proximity to the ground, mountains, or other obstacles. TAWS integrates data from GPS, terrain databases, radio altimeters, and aircraft performance to give earlier, more comprehensive warnings than older systems like the Ground Proximity Warning System (GPWS).



C.2 Acronym List

Table C-1 Acronyms

Acronym	Meaning
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependent Surveillance–Broadcast
ADS-C	Automatic Dependent Surveillance-Contract
AHRS	Attitude and Heading Reference System
ATC	Air Traffic Control
AFM	Airplane Flight Manual
AFMS	Airplane Flight Manual Supplement
AFS	Flight Standards Service
ANP	Actual Navigation Performance
ANSP	Air Navigation Service Provider
ATN	Aeronautical Telecommunication Network
CFIT	Controlled Flight Into Terrain
CFR	Code of Federal Regulations
CPDLC	Controller-Pilot Data Link Communications
COSPAS-SARSAT	Not a single acronym but a combined international system where COSPAS is a Russian acronym for “Space System for the Search of Vessels in Distress,” and SARSAT is an English acronym for “Search and Rescue Satellite Aided Tracking”
CVS	Combined Vision System
DOD	Department of Defense
DME	Distance Measuring Equipment
ECAM	Electronic Centralized Aircraft Monitor
EFB	Electronic Flight Bag
EICAS	Engine Indicating and Crew Alerting System
ELT	Emergency Locator Transmitter
EPU	Estimated Position Uncertainty
EU	European Union
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FCOM	Flight Crew Operating Manual
FIR	Flight Information Region
FMS	Flight Management System
FPV	Flight Path Vector
FOM	Flight Operations Manual
FOM	Figure of Merit



Acronym	Meaning
GLOSNAASS	Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPWS	Ground Proximity Warning System
HIL	Horizontal Integrity Limit
HUD	Head Up Display
IATA	International Air Transport Association
ILS	Instrument Landing System
IMU	Inertial Measurement Unit
INS	Inertial Navigation Systems
INT	Internal (Manual)
IRS	Inertial Reference System
MDA	Minimum Descent Altitude
MDH	Minimum Descent Height
MEA	Minimum En Route Altitude
MON	Minimum Operational Network
MORA	Minimum Off-Route Altitude
MMR	Multi Mode Receiver
MSA	Minimum Safe Altitude
MVA	Minimum Vectoring Altitude
NAVAID	Navigational Aid
NAS	National Airspace System
NDB	Non-Directional Beacon
NOTAM	Notice to Airmen
OEI	One Engine Inoperative
OEM	Original Equipment Manufacturer
PBCS	Performance Based Communication and Surveillance
PFD	Primary Flight Display
PNT	Position, Navigation, Timing
PVT	Position, Velocity, Time
RAAS	Runway Awareness and Advisory System
RAIM	Receiver Autonomous Integrity Monitoring
RFI	Radio Frequency Interference
RNAV	Area Navigation
ROP	Runway Overrun Protection
ROPS	Runway Overrun Prevention System
ROW	Runway Overrun Warning

G L O S S A R Y A N D A C R O N Y M S



Acronym	Meaning
SAFO	Safety Alert for Operators
SATCOM	Satellite Communications
SVGS	Synthetic Vision Guidance System
SVS	Synthetic Vision System
TAWS	Terrain Awareness and Warning System
TCAS	Traffic Alert and Collision Avoidance System
TOC	Table of Contents
VMC	Visual Meteorological Conditions
VOR	Very High Frequency Omnidirectional Range
WAAS	Wide Area Augmentation System
Wi-Fi	Wireless Fidelity

Please Provide Feedback

*In our continuing effort to improve the
quality of service we provide to you,
the Federal Aviation Administration would appreciate any
feedback you may have on this guide and how we can improve it:*



Please Indicate “GNSS Interference Resource Guide” in the Subject Line

Mail to: 9-AWA-AVS-AFS-400-flight-technologies-procedures-division@faa.gov