# Effects of Manipulated GNSS Signals on Aircraft and Mitigation Measures

## NOTE

*This paper supersedes 23ADOBL01, of the same name.*

## BACKGROUND

Civil aircraft have increasingly reported incidents related to manipulated satellite-based signals, posing serious safety risks. These Global Navigation Satellite System (GNSS) signals, critical to aircraft systems, can be compromised through two primary interference types:

**Jamming**: Blocking of GNSS signals, causing a loss of data from one or more satellites.

**Spoofing**: Transmission of fake satellite signals with a structure similar to the desired GNSS signals, possibly leading to the output of misleading data.

Modern avionics integrate GNSS signals with various aircraft systems. GNSS manipulation can degrade critical Position, Navigation, and Timing (PNT) systems, Terrain Awareness and Warning System (TAWS), Runway Overrun Awareness and Alerting System (ROAAS), Autobrake, Automatic Dependent Surveillance (ADS), Controller-Pilot Data Link Communications (CPDLC), and timing mechanisms, all of which rely on accurate data for safe and efficient operations.

GNSS interference, intentional or accidental, poses various threats to safety. GNSS interference can cause flight deck effects, reduce situational awareness and increase workload. It can occur without notice as areas affected by interference are not always published by NOTAMs, often leaving crews unprepared.

Furthermore, even after exiting manipulated areas, some systems may fail to recover fully, generating false warnings and increasing workload or impairing navigation capabilities for the intended approach. On the longer term manipulated GNSS data can undermine system reliability, causing pilots to lose trust in safety critical systems.

This briefing leaflet focuses on the effects of GNSS interference on aircraft systems, potential consequences and recommended actions and mitigating measures.

## AFFECTED AIRCRAFT SYSTEMS

Various aircraft systems can be affected by manipulated GNSS signals. Some of these effects can even occur long after the jamming or spoofing event has occurred, possibly even on a subsequent flight.

### FMS & IRS

In many aircraft avionics architectures, the FMS position utilizes both the Inertial Reference Systems (IRS) and GNSS for high-accuracy navigation. Losing the GNSS signal, the FMS would continue to use the IRS and its last known position. When in range of radio navigation aids (e.g., VOR, DME), it would utilize these to enhance the IRS location.

However, some avionics architectures are designed to give precedence to GNSS data over other positional sources such as the IRS or radio navigation aids. In such systems, even if the IRS and radio-based position data remain valid and accurate, the navigation system may still adopt and rely on erroneous GNSS data in the event of jamming or spoofing. This prioritization can result in a falsely computed position being accepted as correct, potentially misleading the flight crew and compromising positional and situational awareness.

### Terrain Awareness and Warning System (TAWS)

The predictive modes of EGPWS/TAWS are fed directly with raw GNSS position data to provide terrain proximity alerts, ensuring that the aircraft maintains a safe altitude relative to the ground and obstacles. GNSS manipulation can lead to:

**False terrain alerts:** Incorrect positioning data may cause TAWS to issue unwarranted terrain alerts or fail to provide necessary warnings, leading to undesired evasive maneuvers or increasing the risk of Controlled Flight Into Terrain (CFIT).

**Degraded situational awareness:** With inaccurate terrain data, pilots may become confused or distracted, especially in poor visibility conditions, further elevating safety risks.

**Impaired decision-making:** Pilots rely on timely and accurate alerts from TAWS to make critical decisions. Manipulated GNSS data can undermine the system's reliability, causing pilots to either disregard warnings or make inappropriate decisions.

### Runway Overrun Awareness and Alerting System (ROAAS)

The primary function of ROAAS is to calculate whether the remaining runway length is sufficient for safe deceleration during landing or rejected takeoff. GNSS manipulation can interfere with this calculation by:

**Incorrect runway length assessment:** GNSS errors could lead ROAAS to incorrectly assess the aircraft's distance from the runway threshold or end, miscalculating the remaining runway length. This increases the risk of runway excursions by providing pilots with inaccurate information.

**Impaired decision-making:** Pilots rely on timely and accurate alerts from ROAAS to make critical decisions, especially in low-visibility conditions or when dealing with adverse weather. Manipulated GNSS data can undermine the system's reliability, causing pilots to either disregard warnings or make inappropriate decisions.

### Impact on Autobrake and Deceleration Systems

ROAAS works in conjunction with other aircraft systems, such as autobrakes, to optimize braking performance and prevent runway overruns. GNSS manipulation can disrupt this process by:

**Inaccurate speed and position data:** ROAAS uses GNSS data to determine the aircraft's speed and location in real time, which is essential for triggering braking actions. Spoofing or jamming GNSS signals may cause the system to miscalculate stopping distances, resulting in either over- or under-braking.

**Compromised autobrake efficiency:** Incorrect GNSS information can lead to misjudgments about when and how the autobrake system should engage, potentially resulting in longer stopping distances and increasing the risk of runway excursions.

### Automatic Dependent Surveillance (ADS)

Both ADS-B (broadcast) and ADS-C (contract) rely on GNSS-derived positional data to transmit aircraft location, speed, and altitude to air traffic controllers and other aircraft. GNSS manipulation could:

**Transmit false position information:** Spoofing or jamming can cause the aircraft to broadcast incorrect locations, leading to confusion in air traffic management and heightened mid-air collision risks.

**Loss of surveillance:** Jamming could cause a complete loss of ADS transmission, rendering the aircraft "invisible" to both ground control and other aircraft.

**Inefficient traffic management:** Degraded ADS performance could disrupt optimal traffic flow, increase separation minima, and cause delays or inefficient routing.

### Controller-Pilot Data Link Communications (CPDLC)

CPDLC allows for digital communication between pilots and air traffic controllers, relying on GNSS for position reports and timing. GNSS manipulation can lead to:

**Incorrect positional reports:** Erroneous GNSS data can result in incorrect position reporting, causing air traffic controllers to issue inaccurate instructions, compromising safety.

**Communication delays or failures:** Timing issues introduced by GNSS manipulation may result in message latency or synchronization issues, degrading communication effectiveness and leading to operational delays or miscommunication.

### Timing Systems

GNSS is a critical source of timing information for numerous aircraft systems, including navigation and communication. GNSS manipulation can affect:

**System synchronization:** Inaccurate date and time data can cause desynchronization between different onboard systems or between the aircraft and external infrastructure (e.g., ground stations), leading to cascading operational inefficiencies.

**Faulty coordination with ground infrastructure:** Many ground-based systems, including radar, rely on synchronized timing with airborne systems. GNSS manipulation can cause mismatches in data, resulting in suboptimal control and monitoring of aircraft.

## POTENTIAL CONSEQUENCES

Manipulated GNSS signals can pose safety risks due to:

1. Loss of GNSS as the primary navigation source affecting the aircraft's navigation accuracy and integrity. This can affect Performance-Based Navigation (PBN) requirements, and thus, prevent the aircraft from flying certain routes, terminal areas or RNP approaches.

2. Misleading position data spoofed into the navigation system, potentially causing the aircraft to deviate from its intended route.

3. Loss of aircraft communication systems such as CPDLC, ADS-B, ADS-C.

4. Approach and landing hazards due to manipulated signals during critical phases of flight leading to unstable approaches or missed approaches.

5. The occurrence of false EGPWS/TAWS warnings causing distraction and/or leading to the execution of avoidance maneuvers. Avoidance maneuvers can pose extra risk regarding aircraft performance at high altitude or traffic proximity in busy airspace.

6. The failure to provide genuine EGPWS/TAWS warnings.

7. False warnings having a long-lasting effect on the crew's trust in the aircraft's warning systems: a pilot receiving a false warning due to system position inaccuracy may be tempted to disregard a similar, but real, warning later.

8. Workload increase.

## RECOMMENDED ACTIONS & MITIGATING MEASURES

IFALPA encourages OEMs and operators to make a risk assessment, determining if safe operations can be guaranteed through regions where GNSS signals are likely to be manipulated.

IFALPA encourages OEMs and operators to establish appropriate crew operating procedures and training. These procedures should guarantee safe operation even in the case of GNSS spoofing attacks. Proper training of the flight crew guarantees adequate handling of these occurrences.

ANSPs are encouraged to retain sufficient networks of independent communication, navigation and surveillance for assured service provision without GNSS. At a minimum, ANSPs must be able to support the safe recovery of affected traffic.

As long as no robust solutions are available to safely mitigate the effects of GNSS jamming and/or spoofing, conventional radio navigation aids such as VOR, DME and ILS should remain available to the maximum extent possible.

Crews should consider the following during flight preparation or when suspecting GNSS interference:

- Review any technical/operation/safety bulletins issued by the aircraft manufacturer and your company manuals. When routes are planned through geographical regions where

such manipulation is expected to occur, operators should ensure that flight crews are informed about the threat of encountering manipulated GNSS signals.

- During briefings, consider the potential risks associated with signal loss or degradation, and the impact this may have on systems requiring GNSS data.

- The occurrence of a false EGPWS/TAWS warning, or absence of a genuine warning, should be considered.

- Take non-availability of RNP/RNAV approaches into consideration for fuel planning. Approach procedures to the destination and alternate should not depend solely on GNSS.

- The effects of spoofing can occur long after the spoofing event has occurred, possibly even on a subsequent flight of the aircraft.

- Pilots need to make sure that they constantly monitor the aircraft equipment performance closely for any discrepancies or anomalies.

- Consider the use of non-GNSS-based navigation systems as much as feasible. Be aware of airspaces and procedures that may require operative GNSS equipment.

- If you receive an RNP ALERT during approach in IMC, remember that conducting a (non GNSS-based) missed approach is a safe course of action.

- If you elect to continue the approach due to VMC, visually verify obstacles or dangerous terrain. Assess there are no other threats and be mindful that other systems may be degraded.

- In the event you experience, or suspect, GNSS signal degradation or loss, report it to ATC as soon as practicable. Also, report it to your operator via an Air Safety Report, or any other means you may have.

- In the event you experience, or suspect, GNSS signal degradation or loss, report it in the aircraft technical log to enable a ground reset.

## CONCLUSION

Manipulated GNSS signals are a growing threat to aviation safety, impacting navigation and critical systems. Collaborative efforts among pilots, air traffic controllers, operators, and regulators are essential to raise awareness, enhance training, and improve operational resilience. Proactive measures are crucial to maintaining the integrity of navigation systems and ensuring air travel safety.

IFALPA will continue to monitor developments in this area and provide updates as necessary. Safety is our top priority, and we encourage the aviation community to remain vigilant and proactive in addressing this emerging threat.