Effects of Manipulated GNSS Signals on Aircraft and Mitigation Measures

BACKGROUND

Recent reports show that various civil aircraft have been subject to altered GNSS signals in Azerbaijan, Iran, Iraq, and Turkey. Manipulated GNSS signals can compromise aircraft navigation systems, potentially leading to complete navigation loss, with severe safety implications.

Satellite-based navigation systems are susceptible to different attacks due to their low transmission power. There is a difference between two basic GNSS attack scenarios: **GNSS Jamming** is the deliberate blocking of GNSS signals due to other transmitting devices, e.g. Software-defined radio transmitters, that can be used to transmit signals within the GNSS frequency range.

GNSS spoofing is a more refined attack. The spoofer specifically targets certain aircraft and tries to influence the satellite-calculated position by altering and transmitting false satellite signals. For this kind of attack, the spoofer needs to know the position of the aircraft and can send the false signal to influence the aircrafts' flight path.

Within most aircraft avionics the FMS position is regularly updated by the IRS and GNSS to ensure the highest accuracy. Losing the GNSS signal, an IRS would compute its position from the last known position.

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

However, some avionics architectures feed the GNSS position directly into position computation. This may result in discarding the IRS position for navigational purposes, and/or directly utilizing the spoofed GNSS location for location determination. Thus, these systems are highly susceptible to GNSS spoofing attacks.

GNSS signal interference (intentional or unintentional) can occur at any time, with or without prior notice. In Europe, out of the top 15 FIRs where the highest frequency of GNSS interference events is experienced, only 7 currently have a published NOTAM regarding the problem. Flight Crews should be aware of the potential risks and plan for alternative procedures as necessary.

POTENTIAL CONSEQUENCES

Manipulated GNSS signals can disrupt aircraft navigation systems by:

1. Loss of GNSS as the navigation source: Loss of GNSS can affect the aircraft's navigation accuracy and integrity. This can affect the Performance-Based Navigation (PBN) requirements, and thus, prevent the aircraft from flying certain routes, terminal areas or RNP approaches. Moreover, modern aircraft communication systems may be lost, e.g., CPDLC, ADS-B, ADS-C.
2. Misleading Positioning: Malicious actors may spoof misleading position data into the navigation system, potentially causing the aircraft to deviate from its intended route.
3. Approach and Landing Hazards: Manipulated signals during critical phases of flight, such as approach and landing, can lead to unstable approaches or missed approaches, increasing the risk of accidents.
4. Spurious Warnings: Some aircraft systems utilize the GNSS position directly. For example, the predictive modes of EGPWS/TAWS may trigger false warnings as they are fed directly with the raw GNSS position. As false warnings occur, genuine ones may not, subjecting aircraft to more safety hazards. This could have 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. Moreover, false warnings increase pilot workload and could cause distraction during critical phases of flight.

RECOMMENDED ACTIONS

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

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

As a result of GNSS signal loss or degradation, it is important to consider the following:

- 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 such as EGPWS.
- 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.

CONCLUSION

The potential for manipulated GNSS signals to compromise aircraft navigation systems is a serious safety concern. All stakeholders in aviation, including pilots, air traffic controllers, and regulatory authorities, should work together to raise awareness, enhance training, and take proactive measures to safeguard the integrity of navigation signals and ensure the safety of air travel.

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.

IFALPA believes that future systems in civil aviation need to ensure a more robust system architecture using state-of-the-art Cyber-security measures.