International Civil Aviation Organization

A42-WP/108[1]
TE/33
30/7/25

WORKING PAPER

ASSEMBLY — 42ND SESSION

TECHNICAL COMMISSION

Agenda Item 24 : Aviation Safety and Air Navigation Priority Initiatives

MITIGATING GNSS VULNERABILITIES IN AVIATION: STRENGTHENING RESILIENCE AND OPERATIONAL CONTINUITY

(Presented by International Coordinating Council of Aerospace Industries Associations (ICCAIA), Civil Air Navigation Services Organisation (CANSO), International Federation of Air Line Pilots' Associations (IFALPA) and International Business Aviation Council (IBAC))

EXECUTIVE SUMMARY

This paper examines the current landscape of GNSS vulnerabilities, their implications for aviation, potential mitigations and proposes a series of recommendations to ICAO and the civil aviation community aimed at mitigating the effects of GNSS jamming and spoofing.

Action: The Assembly is invited to:

a) call on Member States to develop interference detection systems and support means to provide timely and operationally relevant information about GNSS interference to operators;
b) instruct ICAO to work with States and/or industry to support the development of standards and guidance means to provide operationally relevant information about interference to operators;
c) instruct ICAO to expedite efforts to define and standardize complementary PNT (C-PNT) systems that extend beyond the capabilities of current conventional navigation aids;
d) instruct ICAO to accelerate the development of standards for signal authentication for GNSS core constellations and augmentations;
e) instruct ICAO to work with States, standards development organizations (RTCA, EUROCAE, IEEE and others) and industry to develop requirements and supporting performance standards for time synchronization across all flight domains to promote operational safety and efficiency. This should include guidance concerning required levels of assured time synchronization to include accuracy, integrity and continuity of time synchronization; and
f) urge States to work with industry/encourage industry/support industry to continue development and deployment of technologies that make GNSS receivers and aircraft that incorporate them more resilient to GNSS jamming and spoofing.

Strategic Goals:	This working paper relates to the Strategic Goals *Every Flight is Safe and Secure*; and *Aviation Delivers Seamless, Accessible and Reliable Mobility for All*.
Financial implications:	None.

[1] Arabic, Chinese, English, French, Russian and Spanish versions provided by ICCAIA.

References:	A32-20: *Development and elaboration of an appropriate long-term legal framework to govern the implementation of GNSS*

1. INTRODUCTION

1.1 Global Navigation Satellite Systems (GNSS) are essential for modern aviation, providing critical position, navigation, and timing (PNT) information that supports various functions to enhance operational safety and efficiency. However, the increasing incidents of GNSS radio frequency interference (RFI) in the form of jamming and spoofing present significant challenges to aviation safety and operational reliability.

1.2 This paper examines the current landscape of GNSS vulnerabilities, their implications for aviation, potential mitigations and proposes a series of recommendations to ICAO and the civil aviation community aimed at mitigating the effects of GNSS RFI (i.e., jamming and spoofing).

2. DISCUSSION

2.1 For several years, instances of GNSS RFI have been increasing. The current situation is that operational disruptions due to GNSS RFI have become a daily occurrence in some regions of the world resulting in degradations to safety margins, operational reliability, and efficiency of civil aircraft operations.

2.2 Interference with GNSS signals can be categorized into two main types: 1) unintentional interference, which includes signals from electronic devices, environmental factors and unintentional jamming from nearby systems (e.g., defective/inadequate installed GNSS repeaters); and 2) intentional interference, which encompasses deliberate actions aimed at disrupting GNSS signals such as jamming and spoofing.

2.3 The GNSS RFI may affect GNSS systems in different ways. It may cause minor impacts, such as the reduction of the number of satellites used in the GNSS PVT (position, velocity and time) solution, but it also may impair the proper functioning of GNSS systems, preventing them from outputting correct data or making them provide erroneous data.

2.4 Because of the degradation of the GNSS systems caused by RFI, at the aircraft level, the functionalities of some systems are lost (e.g. automatic dependent surveillance — broadcast (ADS-B) out; required navigation performance (RNP)) and/or they do not operate properly (e.g. terrain awareness and warning system (TAWS) false alerts). This degradation of aircraft capabilities reduces the aviation safety margins and has become a daily occurrence in some airspaces, largely due to aircraft operations that occur in proximity to conflict zones.

2.5 GNSS RFI –Consequences

2.5.1 Mitigating the risks resulting from GNSS RFI has become a critical risk management activity for aircraft operators with few pragmatic options currently available to guarantee operational reliability, considering increasing levels of intentional jamming and spoofing. This is unlikely to change in the near term due to the number of conflict zones, globally and the proliferation of easily accessible technologies to jam and/or spoof GNSS signals.

2.5.2 Differences in avionic suites and disparate airline specific operational procedures add additional layers of complexity to in-flight procedural mitigation, as does the varying approaches to certifying contingency procedures by State regulators.

2.5.3 The characteristics of airspace where GNSS becomes unusable also plays a role in the reversion process. Losing functional capabilities and services that depend on GNSS can result in operational disruptions and increased crew and air traffic controllers' workload, and thus in degradation of safety margins.

2.5.4 In continental airspace where fallback to use of conventional ground based navigation aids (GBNA) may be possible, GNSS RFI may still present challenges. For example, issues with aircraft systems such as TAWS false alerts may also elevate risks to safety of flight as it can lead to crew losing confidence in the system and disregarding TAWS true alerts.

2.5.5 When exposed to RFI, airborne GNSS receiver recovery time can exceed 30 minutes with consequent increase in the risk of operational disruption. In some instances, the North Atlantic being a case in point, aircraft may be refused entry into oceanic airspace if GNSS derived services such as universal time coordinated synchronization are deficient, e.g., loss of data comm prior to oceanic entry waypoint.

2.5.6 Some spoofing events have resulted in erroneous time and/or date being reported by GNSS receivers. In some cases, a corrupted time reference may persist even after the aircraft is no longer receiving the active spoofing signals. This can cause issues with many downstream systems (e.g., unable to log into data networks due to time synchronization security/authentication system checks).

3. MITIGATION OF GNSS RFI

3.1 GNSS RFI is a very complex problem, and no single mitigation is completely effective in all operational situations. Effective mitigation of GNSS RFI will by necessity involve multiple layers of protection including, technological solutions at the receiver level and at aircraft level, technical solutions implemented at the source, and operational mitigations such as reversion to alternative means of navigation.

3.2 *Protection at the Source.* Changes to enhance GNSS robustness are theoretically possible through modifications of the satellites and satellite signals.

3.2.1 Mitigations at the source take a very long time to implement as typically a significant portion of the entire constellation would have to be replenished before the capability is available. Such techniques are also limited in that there is only so much power and bandwidth available and the GNSS RFI sources will always have an advantage of being much closer to the victim of the RFI. Furthermore, changes will typically also be required in the user equipment to take advantage of changes made in the satellites and signals which can further extend the timeline for such mitigations to be available.

3.2.2 Use of dual frequency multi-constellation (DFMC) GNSS provides some robustness to GNSS RFI. The modernized signals with higher chipping rates (i.e. wider bandwidths) provide more processing gain against unwanted RFI. However, such advantages are limited to around 15 dB improvement over the RFI susceptibility of Global Positioning System (GPS) L1 signals. Furthermore, introduction of future more modernized signals that could provide additional robustness, but this is a process that would literally take decades. Use of DFMC GNSS is already on the roadmap for civil aviation and the improvement in robustness is well understood. The frequency diversity associated with DFMC provides some mitigation for RFI that might occur on only one of the two frequencies. However, for intentional GNSS RFI it is likely that the perpetrator will deny service or generate spoofing signals on both frequencies.

3.2.3 For certain types of spoofing attacks, cryptographic authentication techniques can be used to ensure that the users can determine the signals they are tracking are in fact real desired signals and not spoofing signals. Such techniques require changes to both the satellite systems and the user equipment to

be enabled and may have limited effectiveness against signal rebroadcasting attacks. Also, such techniques result in some burden to the user community due to the necessity to manage cryptographic keys which must be periodically updated through some secure methods. Some efforts are underway to add cryptographic authentication capabilities to satellite-based augmentation system (SBAS) Standards. Galileo already offers a cryptographic authentication service as part of the standard signal in space. However, ICAO standardization of this existing service has just begun. While potentially beneficial in some circumstances, these means of mitigating spoofing attacks will not be available for many years unless efforts are made to accelerate the standardization.

3.3 *Mitigations at the receiver level.* Some interesting technologies for mitigation of GNSS RFI at the receiver level exist. Advanced signal processing algorithms may be employed to improve the detection of jamming and/or spoofing signals. These techniques can be very effective at detecting when GNSS RFI is present. However, such receiver mitigation techniques may be less capable in detecting any and all (e.g., more sophisticated) spoofing attacks.

3.4 *Mitigation of RFI through Multi-Element Antennas.* Adaptive Antennas or controlled reception pattern antennas (CRPA) have been used in military applications for more than 40 years. Such antennas have not seen commercial use for a variety of reasons. Some CRPA technology has export limitations due to the military applications. Furthermore, CRPAs have traditionally been bulky, power hungry and expensive compared to conventional fixed radiation pattern antennas (FRPAs) deployed in civil aviation applications so far. Although the situation with export limitations is changing, significant barriers to the deployment of CRPAs still exists due to high costs, and uncertainties associated with being able to certify that GNSS integrity performance is maintained even in the presence of RFI.

3.5 *Mitigations at the Aircraft PNT Level.* GNSS RFI can be mitigated at the aircraft level by integrating multiple sensors' of PNT information and layering protection at each PNT sub system level (e.g. Antenna, GNSS, Inertia, Navigation …). These integrations can be used for both detection and mitigation of GNSS RFI. By cross-comparing GNSS position with other sensors, many spoofing events can be detected. In case of GNSS denied or not trustable GNSS event, other non-GNSS sensors used in the multi-sensor integration can also be used as a backup source of PNT. However, in many cases, the alternative navigation sensors will not provide a long-term level of service equivalent to GNSS which may require operational mitigations such as flying alternative procedures designed for use by conventional navigation aids.

4. CONCLUSIONS

4.1 Many technological solutions to make GNSS more robust exist. However, none are known to be completely effective in all cases. There is a limit to how robust GNSS can be made, so some reversion to backup navigation capability will likely always be part of the overall solution.

4.2 A significant portion of current GNSS RFI is military in nature and advanced coordination with civil aviation authorities is not always possible. Therefore, safety of flight consideration is driving additional investigation into Alternate and/or Complementary Positioning Navigation and Timing (APNT or CPNT) options in addition to reliance on reversion to use of conventional navigation aids.

4.3 Despite ICAO and ITU resolutions, the aviation sector is still suffering from GNSS RFI, and therefore additional measures and actions are needed to ensure safety. Furthermore, the GNSS RFI threats are expected to continue to evolve over time, thus the need for action is urgent.

— END —