GNSS Anti-Jam Systems for Civil Aviation

Dr. Mirko Stanisak

System Engineer
Aerodata AG
Braunschweig, Germany
Phone: +49 531 2359-304
E-mail: mirko.stanisak@aerodata.de

Frank Musmann

Project Manager
Aerodata AG
Braunschweig, Germany
Phone: +49 531 2359-341
E-mail: frank.musmann@aerodata.de

ABSTRACT

Controlled radiation pattern antennas (CRPA) are an effective way to counter radio frequency interference (RFI) affecting global navigation satellite systems (GNSS). By weighting the distinct antenna inputs, commercially available GNSS anti-jam systems can adapt their overall directivity dynamically to minimize their sensitivity towards interferers, allowing for GNSS positioning even with strong interferers present.

In civil aviation, such anti-jam systems were initially used in specialized mission systems, for example for reference positioning in automatic flight inspection systems (AFIS). Here, they enable flight inspections even in challenged conditions. Despite the severe consequences of GNSS interference on primary navigation equipment (i.e. critical functions used operationally by the pilots), anti-jam systems currently lack international harmonization and technical standards, preventing their regular use in the cockpit.

This paper details the working principles of CRPA anti-jam systems, their use in civil aviation, and the resulting performance under challenged conditions. It also describes how the European Aviation Safety Agency (EASA) approved their operation for primary systems in case of GNSS jamming. Tests in heavily affected areas show a remarkable improvement in availability and stability of various GNSS-dependent functions.

INTRODUCTION

Most GNSS satellites orbit the Earth in a Medium Earth Orbit (MEO) at a height of approximately 20,000 km. Subsequently, their broadcast signals are attenuated vastly due to free space loss (FSL) and are received by users at very low power levels only. For typical GNSS receivers, the GNSS signals are below the ambient noise level and must be recovered by correlating the known GNSS codes.

Due to the low power levels, GNSS positioning is highly susceptible to radio frequency interference (RFI) in the frequency bands used. The interfering signals are received stronger than the real GNSS signals over large areas, even for small interfering output power levels. GNSS RFI can be caused both intentionally (i.e. conscious attack) or accidentally (e.g. due to defective equipment).

Intentional GNSS RFI has been a problem affecting the operational accuracy and integrity of satellite navigation globally, with various hotspots (especially at unstable political situations) where GNSS positioning must be considered to be unusable. Attacks on the GNSS include jamming and spoofing.

GNSS jamming is a denial-of-service attack, where the interfering signal overpowers the GNSS signals, so that a GNSS receiver is no longer able to calculate and output a position/velocity/time (PVT) solution. Thus, GNSS jamming can be detected easily and primarily threatens the availability and continuity of GNSS-based operations.

In contrast, GNSS spoofing is a more sophisticated attack, targeted at fooling the receiver into outputting wrong PVT solutions. Depending on the source and characteristics, GNSS spoofing potentially cannot be detected by the users without an external cross check with an independent PVT source. Thus, GNSS spoofing primarily threatens the accuracy and integrity of GNSS-based operations.

The correctness of GNSS positioning and timing is crucial for various domains and applications. Numerous industries depend significantly on clean GNSS spectrums. All member states of the International Telecommunication Union (ITU) are thus required to implement national spectrum management and monitoring systems, which shall protect approved spectrum users against interference. Nevertheless, official information about the local usability of GNSS signals is hard to find.

One way to judge the global impact of GNSS RFI is using ADS-B data. Automated dependent surveillance broadcast (ADS-B) is an internationally harmonized surveillance system, where equipped aircraft broadcast their own GPS position via their Mode-S transponders. By analyzing this data, online service provider like GPSJAM [1], GPSWise [2] or the Stanford GPS Laboratory [3] generate daily updated overviews of the global GNSS RFI situation. An example is shown in Figure 1.

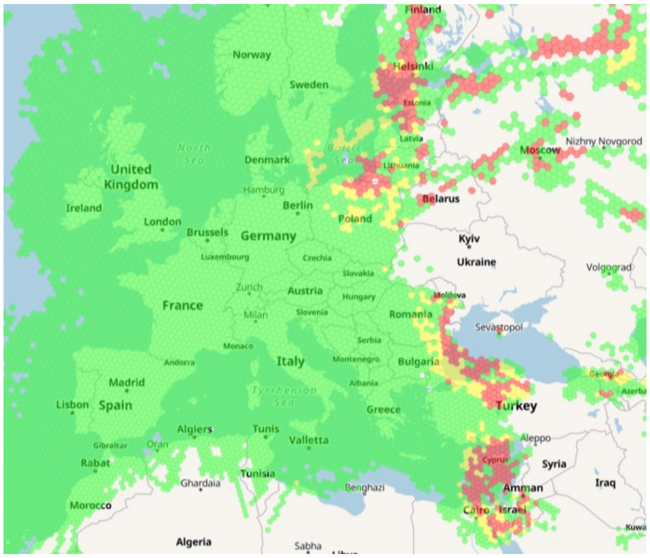

Figure 1: Typical GNSS RFI Situation, derived from ADS-B Data (source: gpsjam.org [1])

ADS-B data for such analyses is of course only available for areas with significant civil air traffic. Subsequently, for combat areas with flight restrictions, these algorithms cannot detect RFI. Nevertheless, the globally observed ubiquity of GNSS RFI indicates that various countries are either not able or not willing to address sources of GNSS RFI effectively. Even if often not targeted specifically, civil aviation is significantly suffering from GNSS RFI.

In civil aircraft, GNSS is used primarily via navigation GPS receivers, which are tightly regulated for meeting the required accuracy, integrity, availability and continuity. All components involved, including the GNSS antenna and the GNSS receiver, must comply with internationally harmonized ICAO standards. This ensures that the worst performing permitted components can be combined while still meeting all performance requirements. This is done via technical standard orders (TSO) for the GNSS antennas and receivers, which require this equipment to be developed and tested according to certain minimum operational performance specifications (MOPS). This ensures that the overall performance meets all requirements under all considered conditions, but limits the GNSS technologies available for navigation in aviation.

The receivers usually only support GPS with its legacy L1 C/A signal, which has been broadcast since the very beginning of the GPS program. All other signals readily available from the four global core constellations (GPS, Glonass, Galileo and Beidou) are subsequently not used for aircraft navigation at all. Also, the standards only foresee very limited tests for in-band interference, resulting in low incentives for the manufacturers of aircraft GPS receivers to employ additional mitigation techniques. In addition, only narrowband L1 active and passive antennas are currently approved, but no other types of GNSS antennas.

In addition to these constraints, the certification standards lack mandatory requirements or tests for mitigation of unlawful GNSS RFI. This is the reason why GPS receivers for aircraft navigation are highly susceptible to GNSS RFI and can be significantly affected both by jamming and spoofing[4][5]. The real-world impact of both types of attack has been documented extensively in different parts of the world, partially severely degrading the overall levels of safety. The consequences of RFI in modern highly integrated avionics suites are very complex and are not directly predictable.

On the one hand, GNSS jamming results in a loss of positioning, which can be detected easily and affects the availability and continuity of operations primarily. The pilots are prepared for such types of events and can use alternative means for navigation, as long as suitable alternative ground-based navigation aids (like ILS's, VOR's, and DME's) are available and usable. It is thus imperative to ensure that enough ground-based navigation aids remain available to allow seamless operations without GPS.

GNSS spoofing on the other hand can threaten the integrity during GPS-based operations. Depending on the complexity of a spoofing attack (which can be tailored to specific aircraft in military spoofing scenarios), a GNSS spoofer can theoretically create hazardous misleading information and steer an aircraft off course. The consequences could be catastrophic in this case. Most reported spoofing attacks, however, are not so complex and result in completely implausible PVT outputs, which can increase the pilot's workload but can usually be handled well.

Nowadays, additional complexity arises from the deep integration of the GPS receiver in modern cockpit avionics. Here, the current GPS-based PVT solution is often used in various other aircraft systems, including (but not limited to)

- ADS-B out / in
- Terrain Awareness and Warning System (TAWS)
- Autopilot (AP) / Flight Director (FD)
- Flight Management System (FMS)
- Fuel Management
- Navigation Display (ND)
- Hybrid Inertial Reference Systems (IRS)
- Synthetic Vision System (SVS)
- Wind Shear Detection Services (WSDS)
- Runway Awareness and Advisory System (RAAS)
- Cockpit clocks
- Datalink communication

As the integration of GPS information into other systems is under the authority of the integrator, numerous different factors can affect the real consequences of GNSS jamming and spoofing, including the type of aircraft and installed options. This poses a major challenge for pilots, especially as not all aircraft flight manuals (AFM) detail the consequences of GNSS jamming and spoofing for the respective aircraft. While each of these failures can be handled well by the pilots without any serious consequences, the sum of failures in various subsystems can notably degrade the overall safety margins.

It is important to note here that hybrid inertial reference systems (i.e. IRS with mandatory GNSS updates for a tightly coupled GPS/IRS solution) are particularly affected by GNSS spoofing, too. Compared with full-scale loosely coupled inertial reference systems, these systems use inertial measurement units with limited performance, which can bridge short periods of GNSS unavailability but do not provide a continuous free-inertial positioning solution. In case of GNSS spoofing, the overall position solution can degrade very quickly, which cannot be detected or corrected by the system itself under certain conditions. Most pilots are not aware of this direct link between such hybrid inertial reference systems and GNSS.

Based on this background, this paper will introduce GNSS anti-jam systems first, which can mitigate GNSS RFI to a certain extent. Subsequently, their use for flight inspection purposes and for primary navigation will be detailed, along with corresponding test results.

GNSS ANTI-JAM SYSTEMS

With jamming being a major threat to GNSS operation, its mitigation is a major task, especially considering the ubiquitous use of GNSS in numerous applications. Various approaches have been discussed and implemented over the years.

Most high-grade GNSS receivers nowadays integrate proprietary mitigation techniques to harden themselves against the most common types of interference. Algorithms like adaptive notch filters, pulse blanking or vector tracking are commonly used, but are effective against specific interfering signals only. In addition, while undoubtedly very adequate in many applications, such filters are not used in aircraft navigation equipment as these functionalities are not covered by the corresponding standardization documents.

In contrast to such receiver-level mitigations, GNSS RFI can be addressed better on the antenna level, i.e. before even entering the GNSS receiver itself. The basic idea of such GNSS anti-jam systems is to actively attenuate signals coming from interferers while amplifying signals coming from the GNSS satellites. This is done using controlled reception pattern antennas (CRPA) consisting of numerous individually receiving antenna elements. Such active anti-jam systems have existed for years but have only recently shifted from military to commercially available components. The phase-controlled signals from all antenna elements are processed by a control unit, which uses highly adaptive algorithms to determine individual varying delays for each input. This way, the overall directivity of the antenna array is modified in a way that interfering signals are attenuated (nulling) while signals from GNSS satellites are amplified (beamforming).

The actual performance of commercially available anti-jam systems is mainly dictated by the number and quality of the antenna elements and the available (digital) processing power. The more antenna elements are used, the more individual interferers can be suppressed. With n elements, up to (n-1) elements can be suppressed individually. The suppression rate (usually given for continuous wave interfering signals) indicates the ratio of directivity between an interferer and GNSS satellites. The higher the suppression ratio, the more robust the GNSS receiver can operate in challenged conditions.

Subsequently, GNSS anti-jam systems with more antenna elements and higher suppression rates are more capable of operating in challenged conditions, especially with multiple simultaneous interferers with different characteristics. However, in practice, system behavior varies due to due to differing algorithms and strategies.

CRPA anti-jam systems have been in use for decades, but predominantly in military applications. Due to this, especially more advanced anti-jam systems are often subject to export restrictions, although these restrictions are currently being lifted.

The integration of active anti-jam systems into an aircraft is not a straight-forward endeavor. Due to the lack of applicable certification standards, the systems cannot easily be installed. Instead, they must be installed and certified as part of an aircraft modification under the responsibility of an approved design organization (DO). Such a modification must be planned and tested meticulously and require the qualification of the individual components for harsh environmental conditions. In addition, it must be ensured that no newly installed component affects any of the aircraft's functions adversely over the complete operational envelope.

The CRPA antenna itself usually is rather small in size but often has a larger footprint than regular airborne GNSS antennas. Subsequently, one part of the modification is to analyze the mechanical influence of the CRPA and to ensure overall safety over its operational service life. Figure 2 depicts the CRPA anti-jam antenna installed next to other antennas on a flight inspection aircraft.

Figure 2: Installed CRPA Antenna (black) on the Top of a Flight Inspection Aircraft

The anti-jam control unit usually must be installed within the fuselage in close vicinity of the antenna and requires electrical power. The output RF line of the control unit is functionally identical to the RF line of a regular GNSS antenna and can be connected to GNSS receivers directly.

Of course, both components must be tested extensively to ensure that the installation does not affect any other vital systems negatively. Once installed on the airframe, the clean RF output of the GNSS anti-jam system can be used by virtually any GNSS receiver on board instead of a conventional GNSS antenna. This paper will address its use for flight inspection systems and for primary navigation in the next sections.

GNSS ANTI-JAM SYSTEMS FOR FLIGHT INSPECTION SYSTEMS

Automatic Flight Inspection Systems have been using dedicated high-quality GNSS receivers for decades. Unlike the primary aircraft navigation GPS receivers, such modern GNSS receivers do not only enable the reception and use of numerous signals from the various GNSS constellations but also incorporate sophisticated and proprietary RFI mitigation techniques. They can usually be flexibly configured for best performance in a variety of applications.

For meeting the accuracy requirements of flight inspections, standalone GNSS positioning is often not sufficient. Subsequently, FIS GNSS receivers are often complemented with additional external information for a highly accurate positioning. Only by using techniques like (phase-) differential GNSS, real time kinematics (RTK) or precise point positioning (PPP) are the resulting GNSS positions sufficiently accurate. However, this results in a rather high susceptibility to various challenges, including sensitivity to RFI.

As discussed in the last section, a GNSS anti-jam CRPA system can be integrated alongside other antennas and systems as part of a flight inspection modification project for use with the AFIS' reference GNSS receiver. It must be ensured that newly installed components neither affect the aircraft's primary functions nor the overall measurement quality adversely. This must be verified by numerous tests.

To provide clean GNSS signals, CRPA systems combine signals from numerous antenna elements. Depending on the current situation, this can also affect the phase center (the virtual measurement point for which the measurements are valid) of the overall antenna. Phase center variations and offsets are known to influence the performance of phase-based reference positioning techniques adversely, resulting in a decreased overall availability and a higher risk of misleading position information.

Subsequently, modern automatic flight inspection systems integrate anti-jam systems inro their reference positioning in a switchable manner. This way, depending on the intended positioning, the FIS operator can flexibly switch between an anti-jam CRPA system (including the control unit) and a regular aircraft fixed radiation pattern antenna (FRPA). This can be achieved both on antenna and on receiver level, as shown in Figure 3.

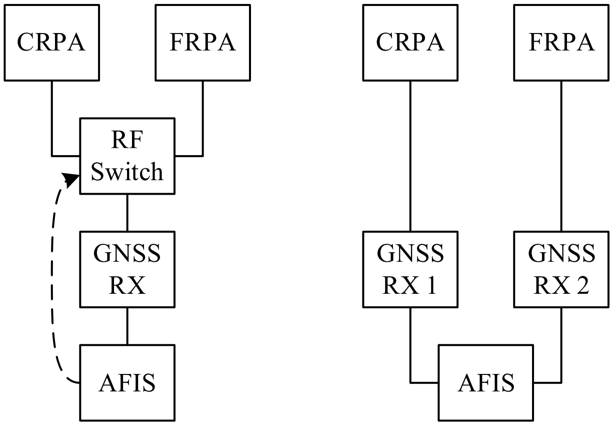

Figure 3: Integration Possibilities for CRPA and FRPA with AFIS. Left: Switching on Antenna Level. Right: Switching on Receiver Level

For switching on antenna level, a single FIS GNSS receiver is connected via an RF switch to both an anti-jam system and to a conventional antenna. The RF switch is operated via the AFIS system, which allows for easy integration, but results in a temporary loss of positioning (due to intermittent signal loss) whenever the switchover occurs.

For switching on receiver level, two FIS GNSS receivers are integrated into the flight inspection system. One GNSS receiver is connected to a conventional GNSS antenna (as done in legacy systems), whereas the second GNSS receiver is connected to the CRPA anti-jam system. This way, both receivers operate concurrently so that switching between both can be done completely in the AFIS. This has the advantage that the output data of both GNSS receivers is available in parallel and can be compared, combined and selected flexibly. The disadvantages here are the additional costs of a second GNSS receiver and possible challenges in case of diverging outputs between the receivers, especially for timing and synchronization purposes.

Either way, the operator of the AFIS can select the desired antenna using the software comfortably depending on the current operational need. However, if high positioning accuracy is required (e.g. for ILS inspections) and GNSS RFI is present, the unavailability of phase-differential GNSS solutions with the anti-jam system requires the use of other systems (e.g. an inertial reference system with updates through an optical threshold detection).

GNSS ANTI-JAM SYSTEMS FOR PRIMARY NAVIGATION

In contrast to their use for the automatic flight inspection systems, CRPA anti-jam systems cannot be simply used with navigation GPS receivers. As discussed before, such systems are not approved for an easy installation via a technical standard order (TSO) due to the lack of certified guidance documents and international harmonization.

At the same time, pilots operating in GNSS denied environments (which are growing continuously) are affected heavily. Different types of aircraft behave differently in case of any RFI affecting their GPS receivers. Due to the loss or degradation of performance of numerous subsystems, their workload increases, the operational alternatives decrease, and the overall level of safety reduces. Especially in modern highly integrated cockpits or when using hybrid GPS/IRS systems, various effects can increase the mental and/or physical workload of the pilots and reduce the safety margins subsequently.

While work is ongoing to allow the use of CRPA anti-jam systems for primary aircraft navigation [6], this process is tedious. For this, CRPA installations and their requirements must be harmonized internationally (on the ICAO side) first. This usually happens via draft standardization documents, which need to be generated first. Only once finished, new TSOs can be issued by the respective authorities, which can then be used by the manufacturers to design and test their equipment. It is estimated that this regulatory task will take years to complete.

However, from a technical perspective, modern GNSS anti-jam systems that can be operated with any GNSS receiver (including typical certified aircraft GPS receivers) are ready and available. The main challenge in the short term is to legally integrate such systems to be used for primary aircraft navigation, despite the lack of applicable standards.

Aerodata AG recently completed a modification project allowing the pilots to switch their navigation GPS receiver between the legacy FRPA antenna and a newly installed anti-jam CRPA antenna in case of GNSS RFI. This marks the first approved use of CRPA anti-jam technology in a civil aircraft wordwide. The supplemental type certificate (STC) was issued by the European Aviation Safety Agency.

The basis for this modification was a comprehensive safety assessment judging the risk of using non-certified equipment (the anti-jam system) and the risk due to the unavailability of numerous other functions due to GNSS jamming. Comparing these risks clearly showed that (with proper mitigation actions, clear design decisions and additional operational limitations in the aircraft's flight manual) a higher overall safety can be achieved by using the anti-jam system.

Extensive tests both in nominal and in GNSS-denied conditions (as detailed in the next section) confirmed the seamless operation of the anti-jam system with the aircraft's avionics.

Despite being implemented for flight inspection aircraft first, this solution is also applicable to various other types of aircraft. Modification programs for different types of aircraft are currently under development. Due to the challenges of operating complex modern aircraft in areas with GNSS RFI, numerous operators are closely looking for cost effective solutions.

TESTS & PERFORMANCE

Extensive test flights were performed following the integration of the GNSS anti-jam system while the aircraft was still under modification, and therefore under the control of the design organization. The intent of these flights was to demonstrate the availability and accuracy of GNSS positioning with and without GNSS RFI. The outputs of both primary aircraft GPS receivers (GPS1 on the pilot's side and GPS2 on the co-pilot's side) and the flight inspection GNSS receiver were recorded for a subsequent thorough analysis.

For a direct performance comparison of the CRPA and the FRPA on primary GPS receivers, only GPS1 was connected to the GNSS anti-jam CRPA system, while GPS2 remained on the approved FRPA antenna. A typical flight deck GPS status indication under presence of GNSS RFI is shown in Figure 4. While GPS2 (right side) could not obtain a valid position fix using the conventional FRPA antenna, GPS1 (left side) still provided a valid and accurate GPS fix using the CRPA system here.

SATELLITE STATUS
EPU 0.31NM
HDOP 1.5
HFOM 39FT
VFOM 82FT
Position [redacted]
Time 09:16:06UTC
GPS ALT 28480FT GSL
GS 489.5KT
Track 105°

GPS STATUS
PILOT GPS1
COPILOT GPS1
GPS SOLN 3D DIFF NAV
SBAS ACTIVE

SATELLITE STATUS
EPU ___NM
HDOP __
HFOM ___NM
VFOM ___NM
Position
Time 09:16:06UTC
GPS ALT ___FT GSL
GS ___KT
Track ___°

GPS STATUS
PILOT GPS1
COPILOT GPS1
GPS SOLN ACQUIRING
SBAS INACTIVE

Figure 4: Example for Cockpit GPS Indication in a GNSS-denied Environment. GPS1 (Left): CRPA Anti-Jam-System. GPS2 (Right): FRPA GPS Antenna

Extensive flights were performed over a large area where GPS is known to usually not be available in aircraft navigation. In comparison between GPS1 with CRPA and GPS2 with FRPA, the overall availability of GPS navigation increased to approximately 99% during these flights.

The test pilots during these flights were impressed by the overall performance and handling of the aircraft under these severely constrained conditions. According to their judgement and compared with similar missions without GNSS anti-jam systems, their workload was hardly increased at all. The GPS1 receiver operated flawlessly and provided valid PVT solutions continuously. No abnormal behavior of any function of the avionics was observed during the flights.

The GNSS receiver used by the automatic flight inspection system for reference positioning also obtained valid and continuous GNSS data throughout these flights. Depending on the operational needs, this receiver can be dynamically switched between a wide-band FRPA antenna and the anti-jam CRPA system.

CONCLUSIONS

Civil aviation is heavily affected by GNSS radio frequency interference. Due to the increasing occurrences of such incidents across different regions of the Earth, flight crews are facing growing challenges. The standards for GPS navigation equipment do not cover this new global reality well. As a consequence, particularly due to unclear integration, counter-intuitive interdependencies and the (partial) lack of suitable ground infrastructure, the overall safety is noticeable under threat.

Modern and powerful anti-jam technologies like CRPA systems can mitigate GNSS RFI effectively but are not generally approved for primary navigation of aircraft. The work to include such techniques is ongoing but will not be ready soon.

Nevertheless, Aerodata AG managed to obtain supplemental type certificates for various aircraft types to use such anti-jam systems for navigation in GNSS-denied environments. Test flights conducted in heavily affected environments show a vast increase of airborne GPS availability with this solution. This solution effectively closes the gap between current operational challenges due to GNSS RFI and the current lack of standardization of CRPA anti-jam systems.

REFERENCES

[1] GPSJAM, https://gpsjam.org/

[2] GPSwise, https://gpswise.aero/map

[3] Stanford GPS Laboratory, "GNSS Interference Detection using ADS-B", https://rfi.stanford.edu/

[4] European Aviation Safety Agency (EASA), *"Safety Information Bulletin 2022-02R3: Global Navigation Satellite System Outage and Alterations Leading to Communication / Navigation / Surveillance Degradation"*, July 2024

[5] Federal Aviation Administration (FAA) Flight Technologies and Procedures Division, "GNSS Interference Resource Guide", March 2026

[6] European Aviation Safety Agency (EASA), *"European Aviation Action Plan for Ensuring Safe Operations during GNSS Interferences"*, Feb. 2026