Experiences with GNSS interference and methods how to overcome and detect GNSS interference

Sigurd A. Bjelkarøy
CTO
Norwegian Special Mission
Gardermoen, Norway
E-mail: sab@nsm.aero

ABSTRACT

Global Navigation Satellite Systems (GNSS) are essential for modern aviation, yet they are vulnerable to deliberate and unintentional radio-frequency interference (RFI). Recent years have seen a dramatic rise in jamming and spoofing events worldwide, affecting both commercial aviation and other critical sectors.

This paper provides an overview of current global interference trends, their operational consequences, and real-world cases from civil aviation and flight inspection. As PBN-dependent navigation becomes the standard, building robust GNSS resilience is essential.

Finally, it presents practical methods for detecting and characterizing GNSS RFI during flight inspection, describing advanced receiver technologies and airborne signal-monitoring techniques to detect and avoid GNSS interference, and the use of controlled-reception pattern antennas (CRPA). The paper aims to equip flight inspectors with information to assist in both detecting GNSS interference and allowing flight inspection to be performed in areas with known GNSS interference.

INTRODUCTION

Modern aviation's dependence on GNSS has enabled numerous advancements, yet it has also introduced a weakness. While GNSS provides unprecedented precision for navigation and timing, its signals are remarkably weak by the time they reach the Earth's surface, making them susceptible to interference.

Reports from 2024 indicate a 500% increase in GPS spoofing incidents, with an estimated 1,500 commercial flights encountering such events daily. The maritime sector is similarly affected, with over 10,000 vessels reported impacted in Q2 2025 alone.

Conflict zones are typically heavily affected by GNSS related RFI.

IATA reports a 65% increase in GNSS loss events in 2024 versus 2023. In Northern Norway, particularly near Kirkenes and surrounding airports, GPS jamming was recorded almost every day in early 2024. In 2023, 294 days of jamming were recorded in Norway's northeast alone.

UNDERSTANDING GNSS INTERFERENCE

Interference generally falls into two categories: jamming and spoofing.

GNSS Jamming: The intentional transmission of RF signals to overpower legitimate satellite signals. This creates a "denial of service" by lowering the signal-to-noise ratio until the receiver can no longer compute a position. Jammers can range from small 10 mW "personal privacy devices" to high-powered multi-watt units.

Natural phenomena can also disrupt GNSS, typically called natural interference or space-weather-induced outages rather than jamming. Solar activity—such as radio bursts, flares, and coronal mass ejections—can disturb the ionosphere, leading to loss of signal tracking, positioning errors, or integrity failures similar to intentional interference.

GNSS Spoofing: A more sophisticated attack where counterfeit signals mimic the structure and timing of authentic satellites. The goal is to deceive the receiver into calculating an incorrect position or time.

Spoofing is considered more dangerous than jamming because a receiver may continue to output navigation data that is subtly or significantly false without triggering an immediate warning.

OPERATIONAL CONSEQUENCES

GNSS interference affects aviation on all levels.

Human Factors

- Increased workload, fatigue, and stress
- Loss of situational awareness
- Mistrust of flight deck systems
- Delayed or inappropriate responses to alerts
- Risk normalization ("this happens all the time")

Impact on aircraft systems

Navigation & Surveillance

- Loss or corruption of **RNAV/RNP**
- **Map shifts** and incorrect own-ship position
- **ADS-B Out/In failures or false targets**
- Downgraded **ADS-C FOM**, forcing loss of reduced separation

Safety-Critical Systems

- **TAWS**: False alerts, inhibited TCAS alerts, lingering failures
- **Runway safety systems** (RAAS/ROPS): False or unavailable alerts
- **HUD/SVS**: Misleading or unusable guidance
- **Weather radar**: Misaligned or displaced returns

Timing & Data

- **Aircraft clock corruption** (critical for CPDLC, ADS-C)
- **CPDLC termination** or repeated failures
- **SATCOM degradation**

Long-term Receiver Corruption

Spoofing can corrupt a receiver's internal state, such as its Almanac data (coarse orbit info). Even though the GPS almanac itself can be downloaded in 12.5minutes, a spoofed receiver may remain unreliable even hours after the interference source has been bypassed depending on how well the receiver reads and handles the almanac data.

This would have lingering effects on systems like

- INS/FMS
- TAWS
- ADS-B

THE SHIFT TOWARD PBN AND THE NEED FOR RESILIENCE

The aviation industry is moving toward Performance-Based Navigation (PBN).

EASA Regulation EU 2018/1048 [2] mandates that by June 6, 2030, Category I approach procedures in Europe must be based exclusively on PBN, typically utilizing SBAS. Conventional aids like ILS category I will be decommissioned or relegated to a minimum contingency network.

This shift makes GNSS resilience a prerequisite for flight safety.

DETECTION AND MITIGATION STRATEGIES IN FLIGHT INSPECTION

Flight inspection (FI) aircraft are uniquely positioned to detect and even localize GNSS RFI sources.

Modern FI systems offer advanced monitoring tools like real time GNSS RF spectrum analyzers, GNSS receivers outputting C/No data for every received satellite, built in GNSS interference detection and it can be equipped with anti jamming GNSS antennas and direction finders.

Airborne Monitoring Techniques

Carrier-to-Noise (C/No) Observations: A sudden drop in C/No often indicates jamming, while an unusually high C/No can be a signature of spoofing.

Spectrum Analysis: Real-time spectrum analyzers integrated into FI systems allow operators to visualize the RF environment around the GPS L1 band (1575.42 MHz) to identify interference spikes.

Advanced GNSS Signal Processing: Techniques like Maximum Likelihood Estimators and Doppler shift calculations help differentiate between signals coming from space and those originating from ground-based interference.

The development of GNSS RFI resilience is highly focused by every GNSS manufacturer so it is more important than ever to make sure your system is equipped with the most modern generation of GNSS receiver with the capability to update its signal processing with firmware updates.

Controlled Reception Pattern Antennas (CRPA)

One of the more effective hardware mitigations is the CRPA. Unlike standard antennas, a CRPA uses an array (e.g., 4 or 8 elements) and adaptive beamforming to dynamically form "nulls" in the direction of a jammer while maintaining gain toward legitimate satellites. This would allow some flight inspection to continue even in environments where standard receivers would fail.

Because the CRPA adjusts the phase of the incoming signal at each antenna element, it will negatively impact RTK performance. This will result in reduced GNSS solution accuracy, limiting it to float solutions at best or, not unlikely down to only SBAS / standalone GNSS position solution due to an increased risk of cycle slips caused by the CRPA phase shifts.

Such accuracy degradation would limit the flight inspection capabilities for ILS, especially when operating close to threshold like for approaches.

This is due to the high accuracy requirements defined in ICAO DOC 8071 [1], but for other NAVAIDS with less stringent accuracy requirements like e.g. VOR the reduction in accuracy will not affect flight inspection capabilities.

CONCLUSION

As the aviation landscape becomes increasingly dependent on GNSS through PBN, the threat of GNSS RFI must be met with both advanced technology and updated operational procedures.

By utilizing specialized equipment like CRPAs, real-time spectrum monitoring, and advanced GNSS engines, flight inspectors can not only protect their own missions but also provide critical data to help localize and eliminate interference sources for the wider aviation community.

REFERENCES

[1] ICAO DOC 8071 Vol 1

[2] EASA Regulation EU 2018/1048

[3] FAA GNSS Interference Resource guide