ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

A UN SPECIALIZED AGENCY

ICAO WRC-27 Preparatory Workshop
GNSS interference

Mathieu HUSSONG

Direction Générale de l'Aviation Civile (French CAA)

ICAO

Workshop on ITU World Radiocommunication Conference 2027 for SAMCAR Region,
(Lima, Peru, 31 August - 1 September 2026)

Presentation Overview

01 **Definitions**

02 **Problems caused by GNSS RFI**

03 **ICAO Position**

04 **ICAO actions**

01 - Definitions of RFI, jamming & spoofing

Radio Frequency interference (RFI) from ITU Radio Regulations, Volume 1: Articles.

The effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation or loss of information which could be extracted in the absence of such unwanted energy.

Jamming

Transmission of non-GNSS RFI signals by an external agent within the GNSS frequency band.

Spoofing

Transmission of GNSS-like RFI signals by an external agent within the GNSS frequency band.

01 - Classification of jamming threats

- **J1 - Collateral Jammers:** Jammers with low power and limited range.
  Example : PPDs used by individuals for privacy purposes

- **J2 - High Power Interference:** Misused military or civil transmitter.
  High power and jamming over a broad area.
  Example : 3rd order harmonics of 525 MHz UHF TV signals.

- **J3 - Targeted Jammers:** those described in J1, when specifically operated against the aircraft.

- **J4 - Targeted Sophisticated Jammers:** Jammers with dedicated features to defeat existing jamming detectors or RFI monitors.
  Example : Jamming guns

J1 : Personal privacy device (PPD)

J4 : Military jamming gun

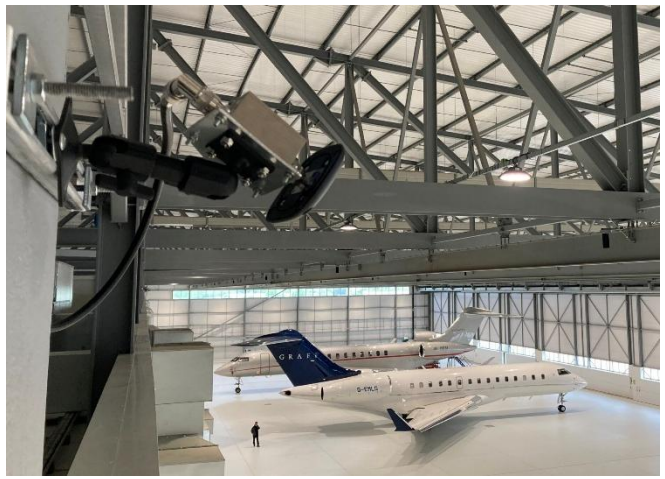
Classification from EU-U.S. Cooperation on Satellite Navigation WG-C Service Resilience Sub-Group : Threats and Countermeasures for Aviation Applications.

01 - Classification of spoofing threats

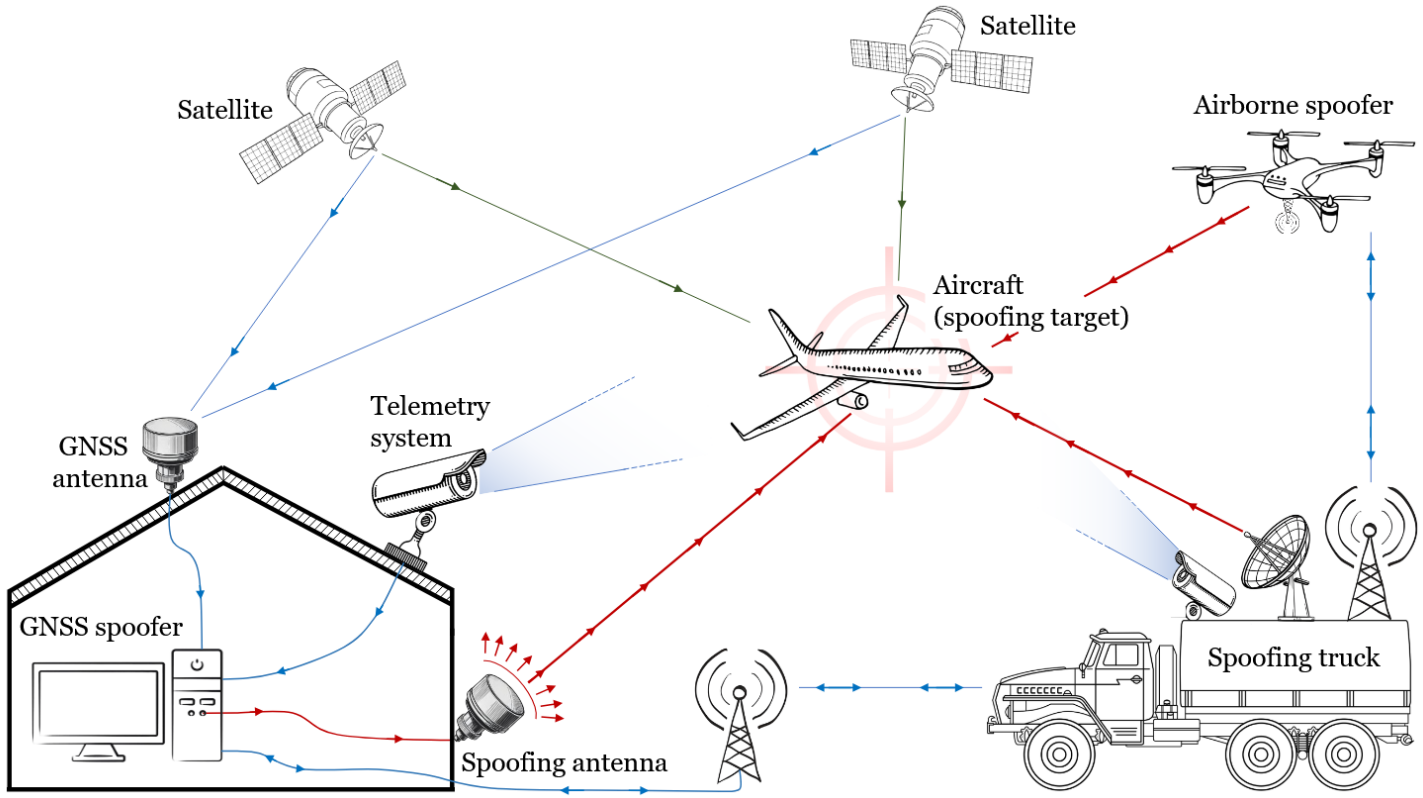
Classification from ED259B.

- **S1 – GNSS Repeaters**
- **S2 - Errant Signals**
- **S3 - Collateral Spoofers - Simulators**
- **S4 - Collateral Spoofers – Re-radiators**
- **S5 - Targeted Spoofers – Simulators**
- **S6 - Targeted Spoofers – Re-radiators**
- **S7 - Targeted Sophisticated Spoofers**

S1 spoofing scenario : GNSS repeater



S7 spoofing scenario

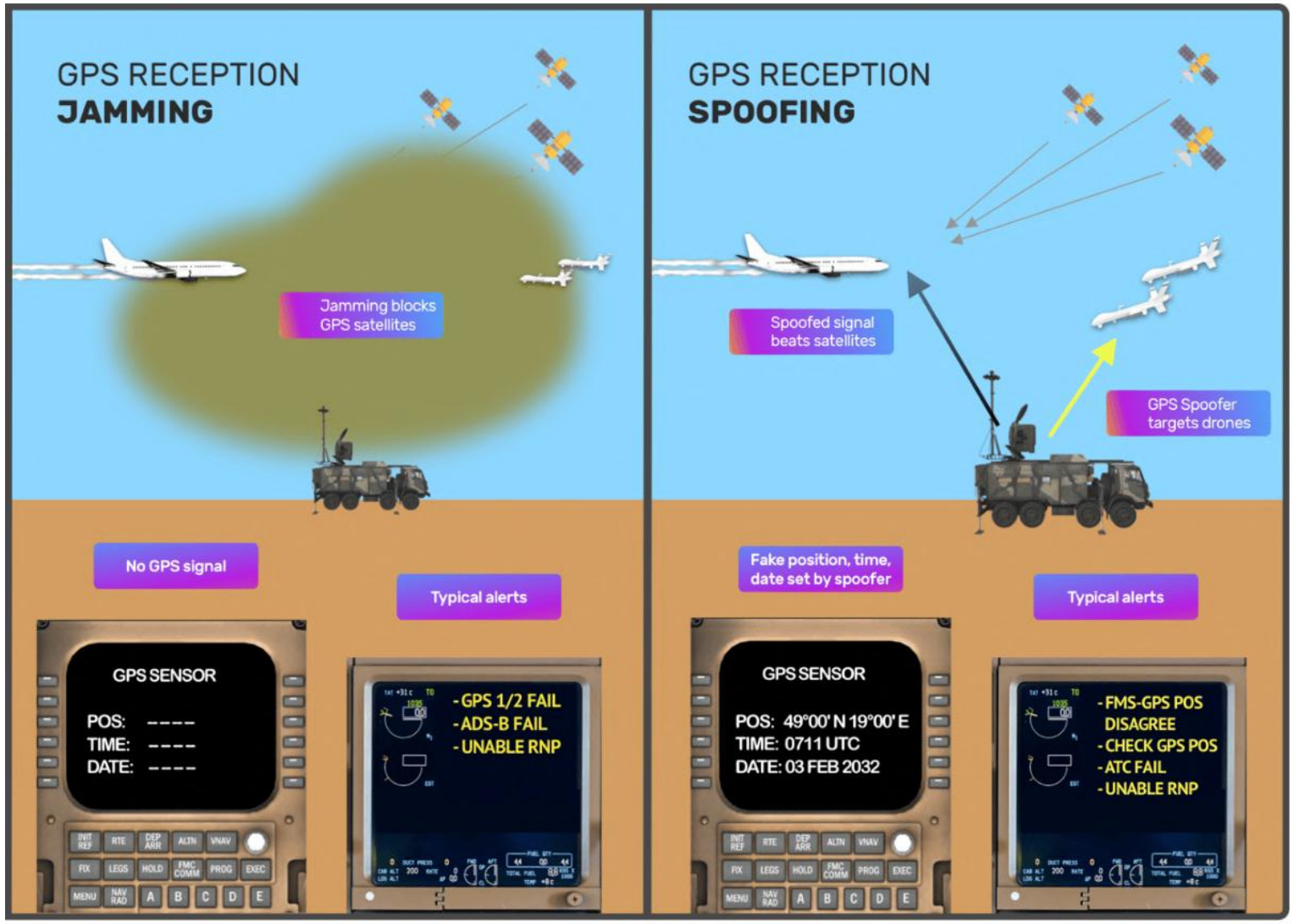


ICAO

02 - Main problems caused by GNSS RFI

Jamming can cause **denial of GNSS service**, causing operational issues (rerouting, delays, …), economical and environmental problems.

Spoofing can modify the estimated position of an aircraft, inducing a **threat on the integrity** of the position, and compromising flight safety.



Source : OPSGROUP, Final report of the GPS spoofing workgroup, September 6, 2024.

02 - Other problems caused by GNSS RFI

GNSS RFI may cause **other problems** to aeronautical systems relying on GNSS.

These problems impact :

- the flight crew
- and/or the air traffic controller
- and/or the aircraft operator.

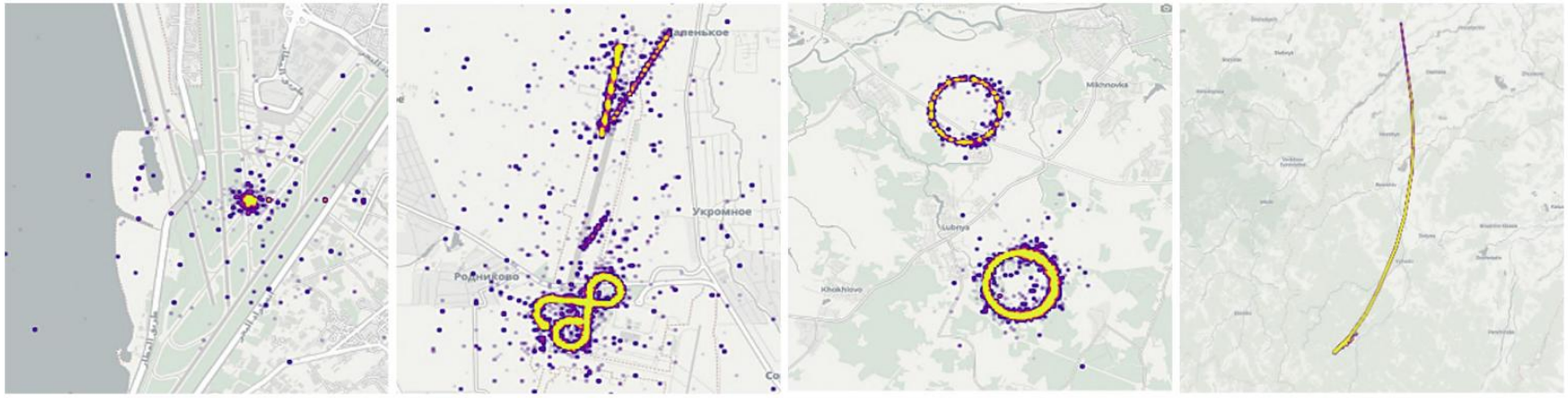
These problems can occur during the exposure time to GNSS RFI, and can persist after the exposure time.

Effect on	Impact
GPS receiver	No or false estimated position
FMS position	Undetected off-track navigation
RNP	Unable RNP, restricted to conventional navigation
Map shift	Wrong runway selection, loss of situational awareness
GPWS	False alerts, Unecessary go-arounds, stress
Weather radar	Ground clutter function not available
Aircraft clock	Incorrect time estimated and displayed
Datalink	CPDLC and ADS-C not available
ADS-B	Unable to fly in ADS-B required airspace
HUD & SVS	Not available, degraded situational awareness
ELT	SAR in wrong location
SATCOM	May be unavailable
Internet / WI-Fi	Some reports of Wi-fi not working correctly

Source : OPSGROUP, Final report of the GPS spoofing workgroup, September 6, 2024.

02 - Trajectory deflections caused by spoofing

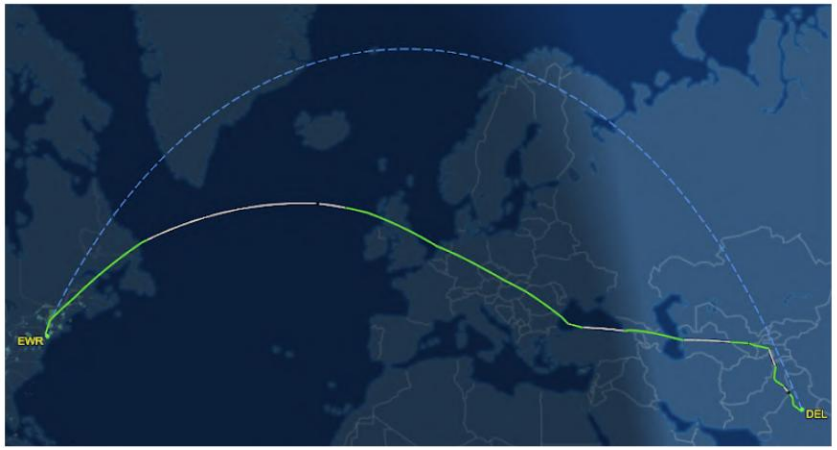
Aircraft affected by spoofing have been observed to estimate various types of erroneous trajectories.



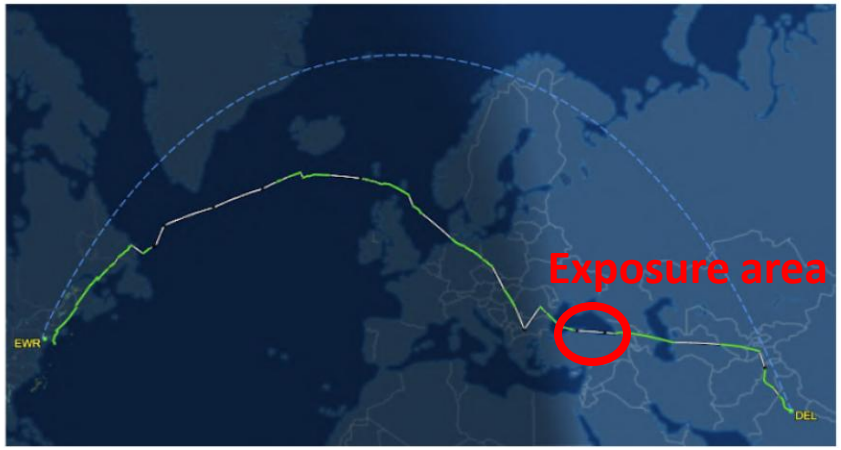
(a) Static location. (b) Holding pattern. (c) Circular pattern. (d) En-route trajectory.

After spoofing exposure, a GPS receiver may appear recovered but still retain corrupted data.

UAL83 (DEL–EWR) flight on 22 May 2024 followed its normal route



On 1 August 2024 flight showed major tracking disruptions caused by GPS spoofing even after spoofing exposure

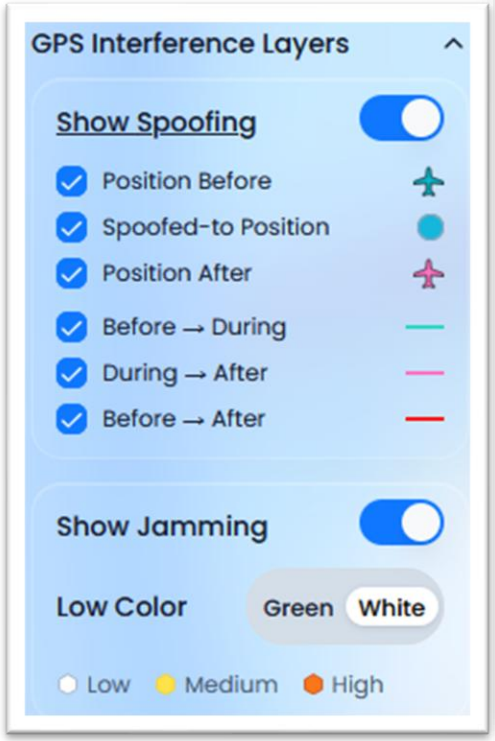


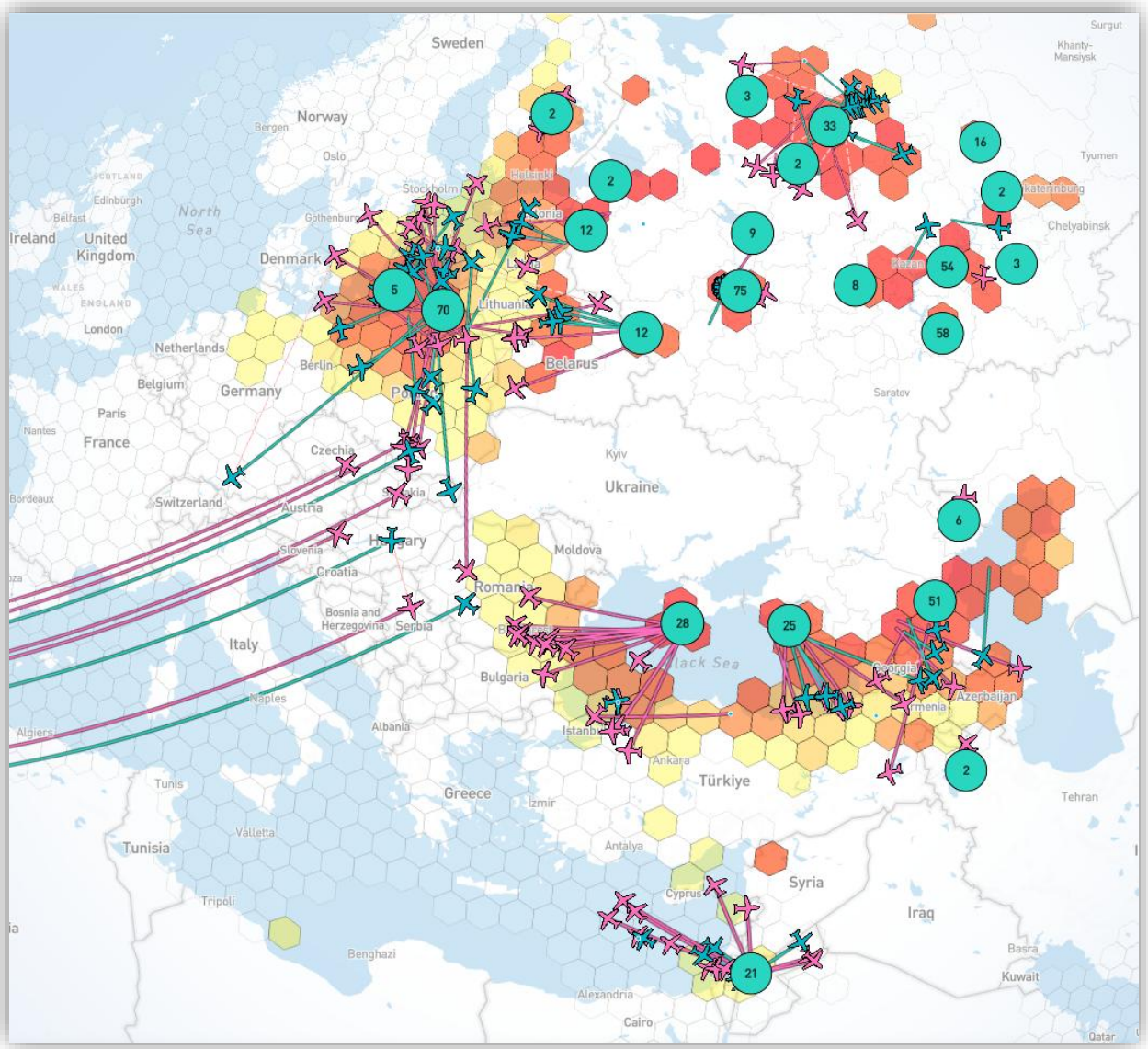
Source : OPSGROUP, Final report of the GPS spoofing workgroup, September 6, 2024.

02 - Where is GNSS RFI happening ?

Jamming and spoofing are observed mostly above / close to **territories under conflict**.

Map of GNSS RFI on 24 February 2026.



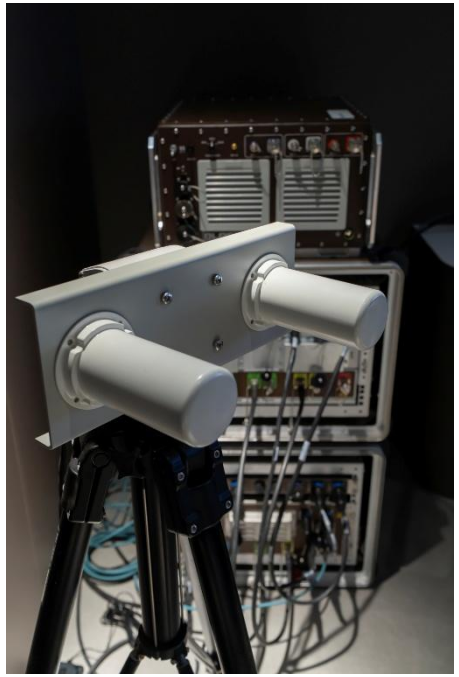


Source : www.gpswise.aero

02 - Growing impact of GNSS RFI – Military use

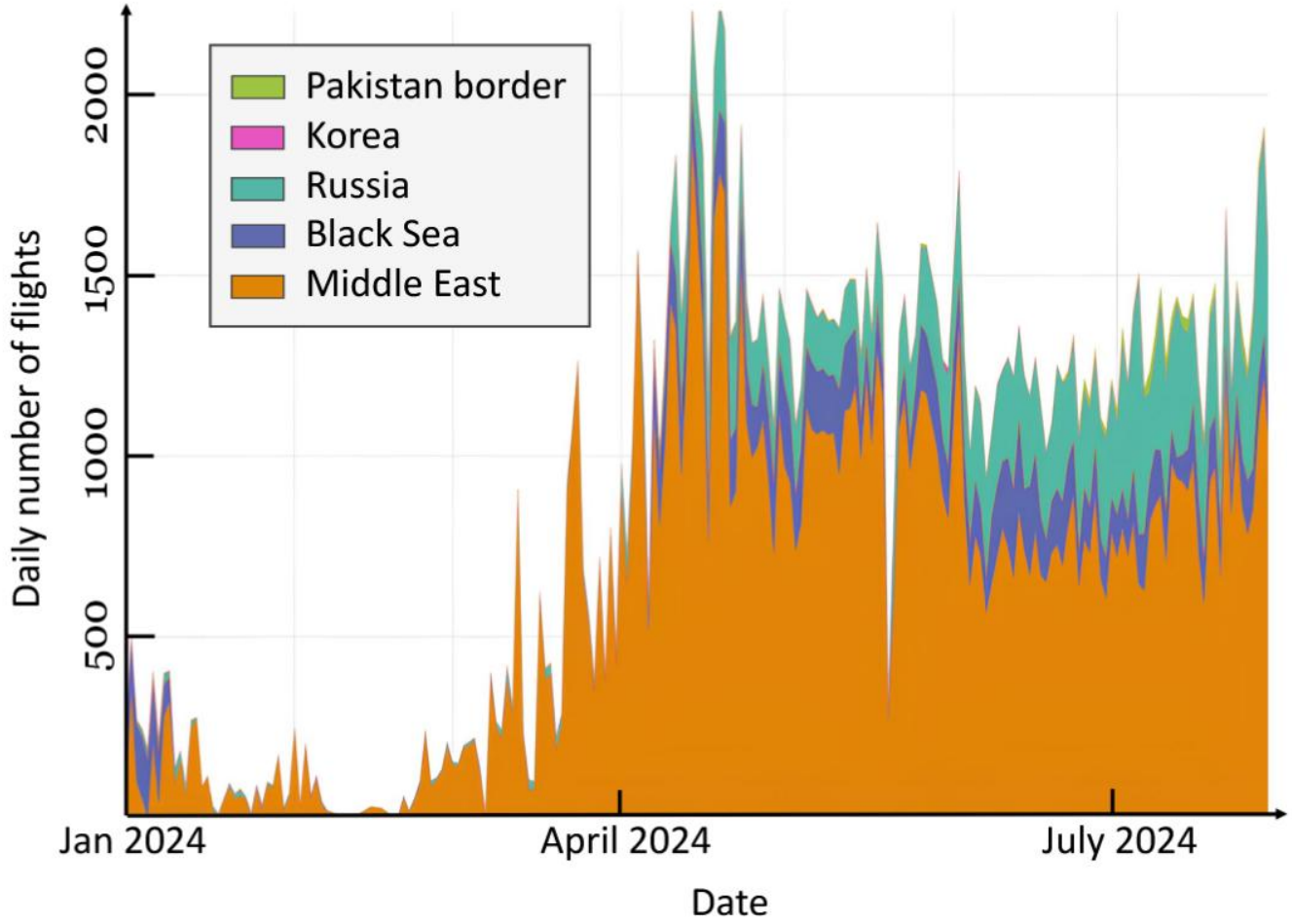
Spoofing events are skyrocketting (+500% in 2024) over the last few years, mostly above territories under conflict.

About 85% of ATM incident reports are on GNSS RFI.



Skyjacker (SAFRAN)

Daily number of spoofing reports in 2024



Sources : OPSGROUP, Final report of the GPS spoofing workgroup, September 6, 2024.
And Eurocontrol voluntary atm incident reporting (evair) safety bulletin 25. Technical report, EUROCONTROL

02 - Growing impact of GNSS RFI – Military use

A **potential** new threat is emerging : space-based jamming.

There is a high degree of confidence that satellite constellations dedicated to GNSS jamming exist.
They could disrupt GNSS signals over large areas.

Sources :

Clements, Z. L., Kriezis, A., & Humphreys, T. E. (2026). Chasing Lightning: Detecting, Characterizing, and Identifying a Powerful Space-Based GNSS Interference

https://youtu.be/tz23G_UXCGA?si=EWj55iBbb_thnLLu

https://docs.google.com/document/d/1EVMyrMr7dvIqNYf9kHNydV9SpZwWv4BrQEyeE35_wvg/edit?tab=t.0

ICAO

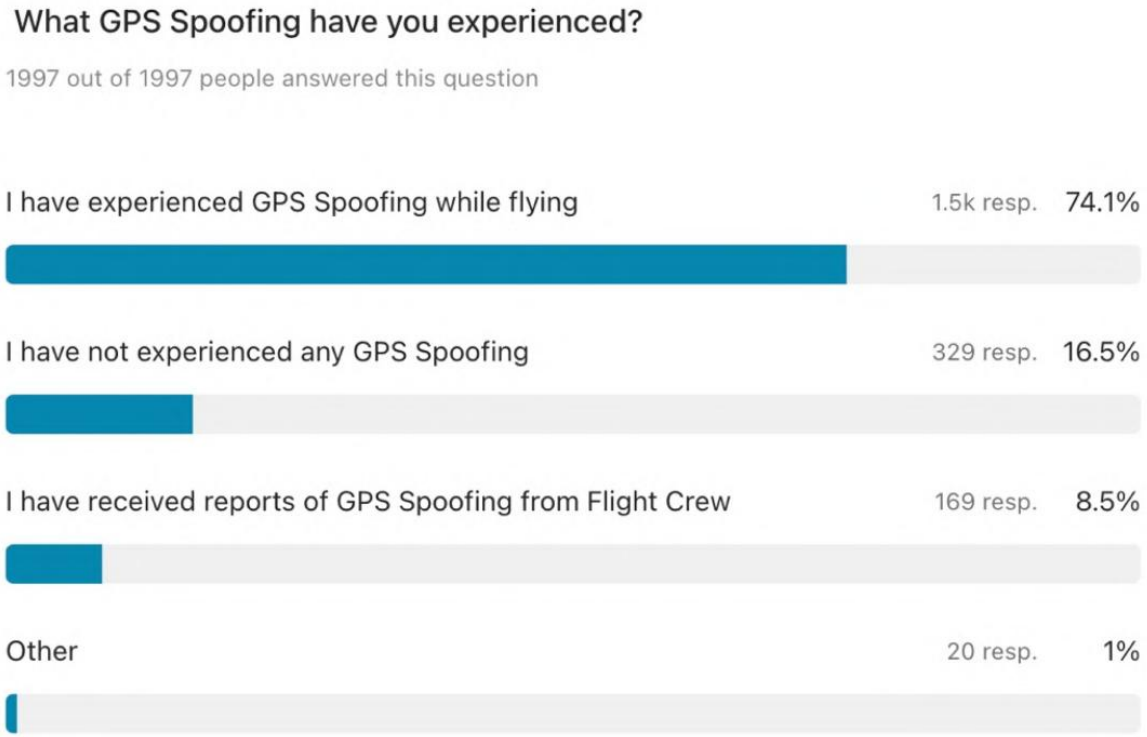
02 - Growing impact of GNSS RFI – Civil use

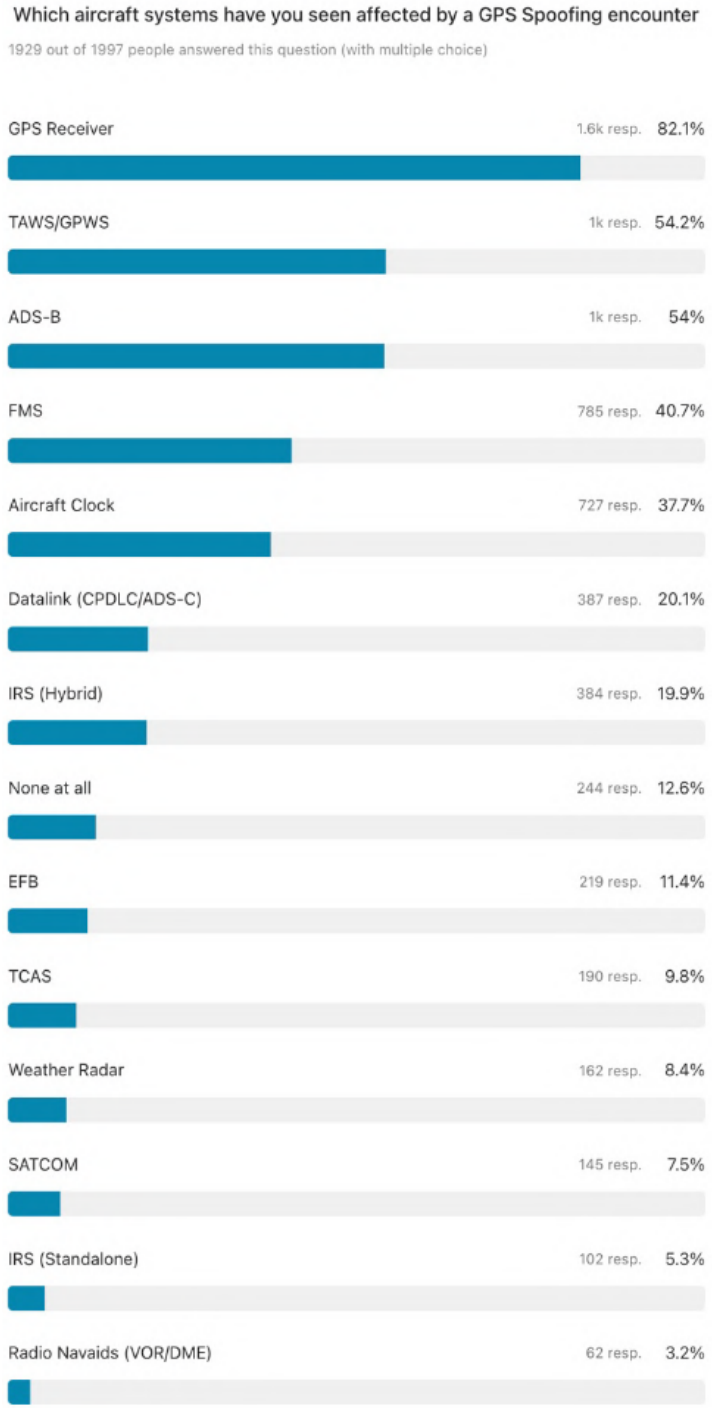
Mont-Blanc Tunnel Project – France 2025 (rejected by French CAA due to threat to civil aviation)

Example : Repeaters installed to extend GNSS coverage indoor.

Errant signals can propagate outside and can be tracked by aircraft receivers, inducing a serious spoofing threat.

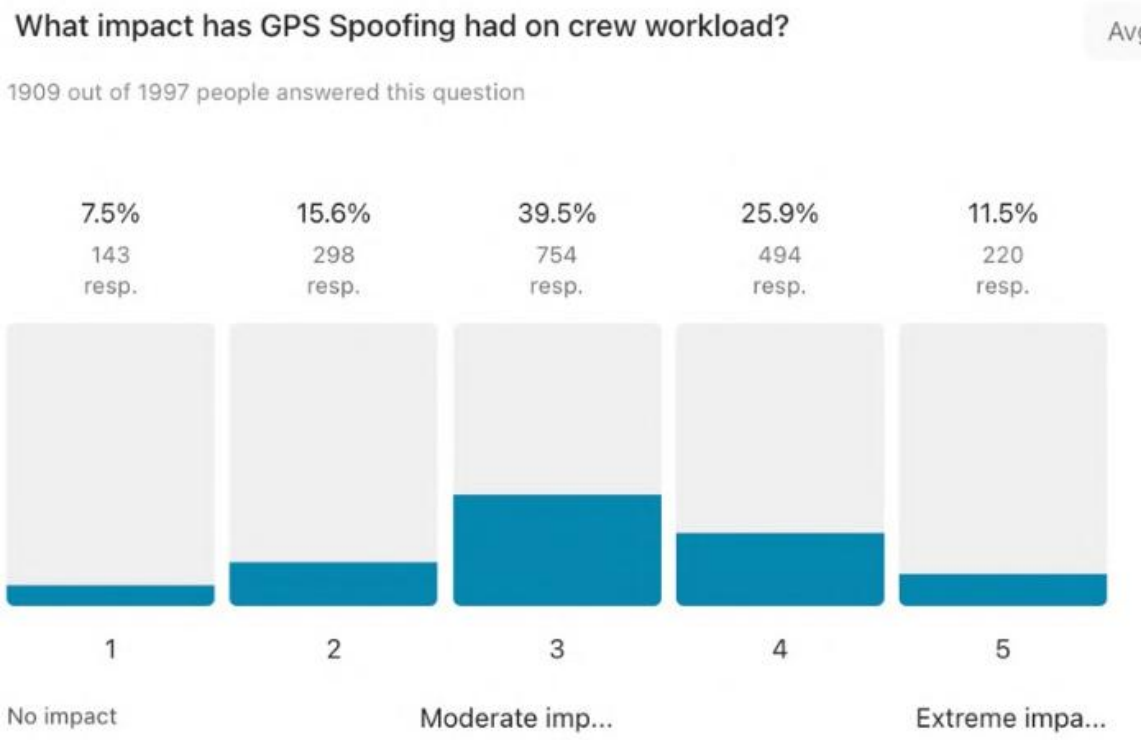
02 - GPS spoofing survey results for flight crew (mostly pilots)

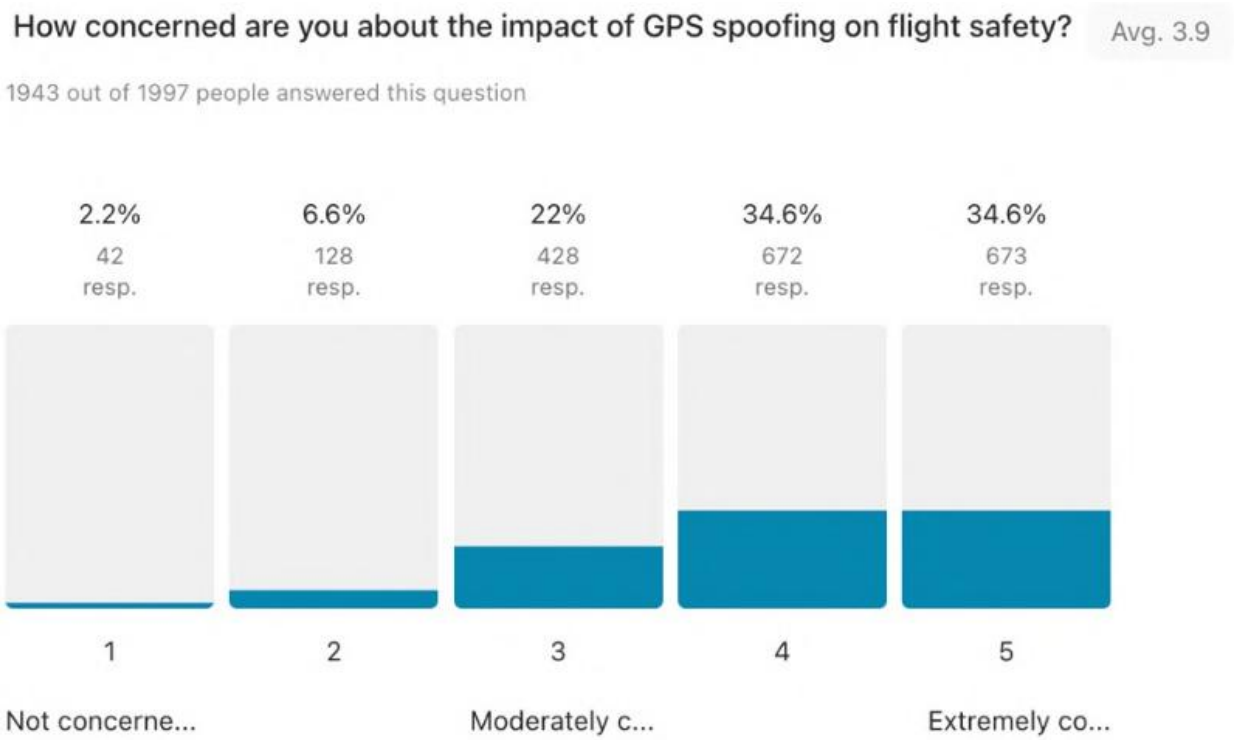




Source : OPSGROUP, Final report of the GPS spoofing workgroup, September 6, 2024.

02 - GPS spoofing survey results for flight crew (mostly pilots) (continued)





Source : OPSGROUP, Final report of the GPS spoofing workgroup, September 6, 2024.

03 - ICAO position

Resolution 42-8 : Consolidated statement of continuing ICAO policies and practices related to a global air traffic management (ATM) system and communications, navigation, and surveillance/air traffic management (CNS/ATM) systems.

The Assembly :

- "Urges States to apply necessary measures to **avoid the commercialization**/proliferation, purchase, possession and the use of illegal transmitters such as jammers[…] ;
- Urges States to ensure close collaboration [...] to ensure that the spectrum used by all CNS systems, and GNSS in particular, is free from harmful interference;
- Urges States to **refrain from any form of jamming, or spoofing affecting civil aviation**;
- Urges States to **coordinate and notify** […] in case of military or other State-authorized security or defence-related operations or training, potentially causing any form of jamming, or spoofing affecting civil aviation;
- Urges States and operators, when assessing the interference risks associated with conflict zones, to consider that the use of satellite-based CNS systems can potentially be impacted beyond those zones."

03 - ICAO position

Joint statement by ITU, ICAO, IMO (2025)

“Noting with grave concern the increasing number of spoofing cases”
“urges States to refrain from any form of jamming and spoofing affection civil aviation”

14th Air Navigation Conference report (2024)

“The conference voiced significant concerns with the recent escalation of GNSS spoofing, and the significant safety risk it poses to civil aviation”
“recommends States to provide guidance on detecting GNSS spoofing”.

ITU WRC-23 Resolution 676

“resolves to urge administrations
1 to apply necessary measures to avoid the proliferation, circulation and operation of unauthorized transmitters that cause, or have the potential to cause, harmful interference to RNSS systems […]
2 to take the following actions to prevent and mitigate harmful interference affecting the RNSS […] :
2.1 to encourage collaboration between spectrum regulators, enforcement authorities and RNSS stakeholders, in particular in the aeronautical and maritime domains;
2.2 to encourage cooperation between aeronautical, maritime and security authorities, as well as spectrum regulators, as appropriate, to address interference risks to RNSS systems […]
3 to report cases, as the affected administration deems appropriate, of harmful interference to the RNSS.”

03 - ICAO position

WRC-27 Agenda Item 4
In accordance with Resolution 95 (Rev.WRC-19), to review the resolutions and recommendations of previous conferences with a view to their possible revision, replacement or abrogation.

ICAO Position (August 2026) :

676 (WRC-23)	Prevention and mitigation of harmful interference to the radionavigation-satellite service in the frequency bands 1 164-1 215 MHz and 1 559-1 610 MHz.	Modify to remove formal recognition that Administrations can deny access to RNSS.

At WRC-23, it was not possible to get States to agree to resolution 676 without making reference to the right of States to interfere with any radio service, as per the ITU Constitution, for security purposes. This right has been existing at ITU since the 1950s.

The resolution is suggesting that if there is not a zone of conflict, this zone should not be interfered.

04 - ICAO guidance material on GNSS RFI

GNSS Manual (ICAO Doc 9849)

Included in the Fifth Edition, 2025:

- Chapter 5: GNSS Vulnerability
  - unintentional, intentional, spoofing classifications and their impacts on receivers, spectrum regulations, ionosphere, solar activities and troposphere effects)
- Chapter 7: Implementation of GNSS-based services
  - 7.11 & 7.12: GNSS status notification & anomaly reporting
  - 7.13: GNSS vulnerability: mitigating the impact on operators
- Appendix F: GNSS Radio Frequency Interference Mitigation Plan

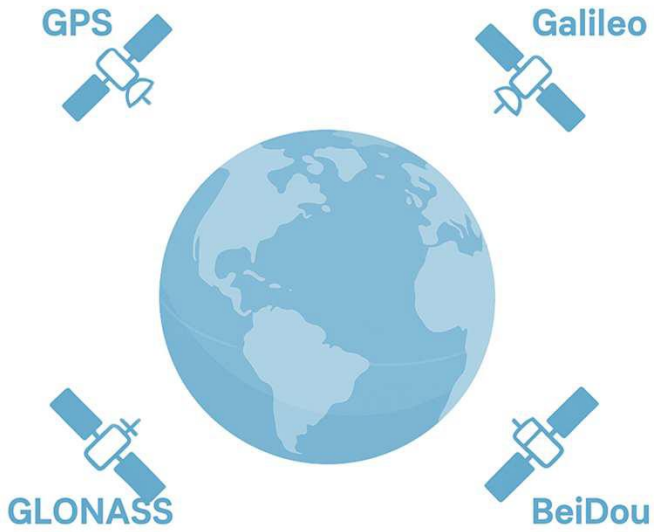
Upcoming

Update to GNSS Manual (Doc 9849): guidance on the detection, reporting, and resolution of GNSS RFI

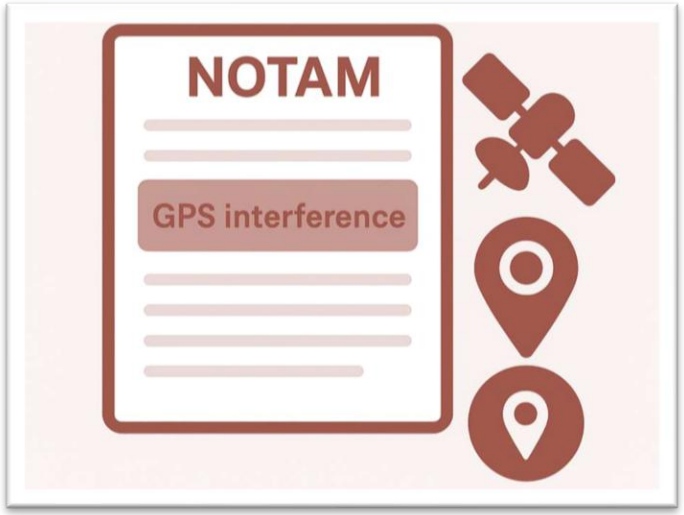
04 - ICAO development on GNSS RFI mitigation

Foster the use of Dual Frequency Multiple Constellations (DFMC) GNSS

- DFMC GNSS uses signals from multiple constellations and two frequency bands (L1/E1 and L5/E5a) to enhance positioning accuracy, **integrity**, and availability.
- Mitigates ionospheric delay errors by combining measurements from two frequencies, improving reliability compared to single-frequency systems.
- Provides global redundancy and robustness by integrating constellations such as GPS, Galileo, GLONASS, and BeiDou.
- Forms the basis for future aviation navigation applications, supporting Performance-Based Navigation (PBN) and Approach with Vertical Guidance (APV) operations.
- Implementation Timeline: Amendment 93 to Annex 10, Volume I introduced provisions to support DFMC GNSS - Initial operational introduction: 2032-2035



04 - ICAO development on GNSS RFI mitigation



Create GNSS RFI NOTAM

- Standardized NOTAM codes for jamming & spoofing
- Enable real-time and systemic collection and dissemination of GNSS interference events

Standardize authentication solutions

- Galileo Open Service Navigation Message Authentication (OSNMA)
  - Provides authentication of Galileo satellite navigation messages to ensure that the received data originates from genuine Galileo satellites and has not been altered
  - Enhances user trust and resilience against spoofing
  - SARPs for Galileo OSNMA: expected 2029

- SBAS Authentication
  - Provides authentication of SBAS messages to ensure that integrity and correction data received by users originate from an authorized SBAS provider and have not been tampered with
  - ICAO SARPs on the optional authentication feature: expected 2027

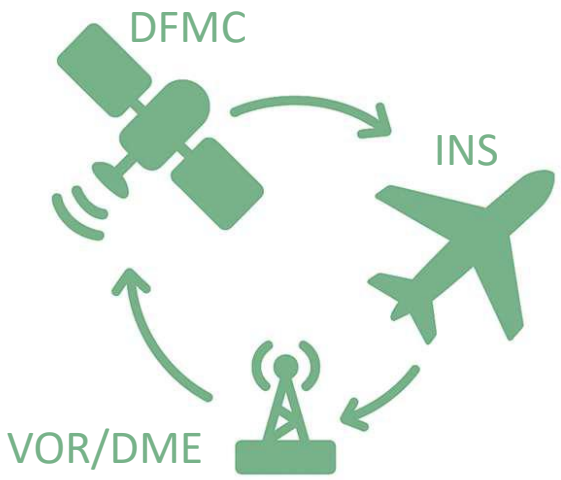
ICAO

04 - ICAO development on GNSS RFI mitigation

Develop complementary PNT (C-PNT)

- Multi-Sensor Integration
- Balanced Capabilities
- Precise Time Sources

- C-PNT provisions expected by 2030



GNSS interference reporting

- Improved reporting procedures between ICAO and ITU

- Guidance for regional reporting through SIRRS

- The Technical Commission of A42 urged States to report GNSS RFI occurrences which cannot be resolved through routine national or international procedures to their accredited ICAO Regional Office, in addition to following the procedures outlined in the ITU Radio Regulations.

Conclusion

- The GNSS interference threat is active and evolving.
- Jamming can cause denial of service, Spoofing poses a threat on the integrity of navigation.
- ICAO calls for action on GNSS RFI issues :
  Need for urgent efforts on spoofing, regarding mitigation techniques, resilience, detection, reporting, and impact understanding.
- Evolution of regulations, standards and recommended practices have started to address short term challenges as well as develop long term solutions.

Thank You

ICAO