International Civil Aviation Organization

MIDANPIRG Communication, Navigation and Surveillance Sub-Group

Fourteenth Meeting (CNS SG/14)
(Abu Dhabi, UAE, 19 – 23 October 2025)

Agenda Item 3: CNS Planning and Implementation Framework in the MID Region

UNITED ARAB EMIRATES BEST PRACTICES FOR ENHANCING SURVEILLANCE DATA INTEGRITY AGAINST GNSS INTERFERENCE

(Presented by the United Arab Emirates)

SUMMARY

This paper presents the approach adopted by the United Arab Emirates for the detection, investigation, and mitigation of GNSS interference and spoofing events, with the objective of enhancing data integrity within surveillance systems. It outlines a structured operational workflow for identifying GNSS interference incidents and provides detailed guidance for conducting technical investigations using surveillance playback and data analysis tools.

Furthermore, the paper shares the UAE's structured framework for surveillance data integrity management and encourages regional collaboration and information exchange on GNSS interference monitoring to strengthen collective resilience across the MID Region.

Action by the meeting is at paragraph 3.

REFERENCES

- IATA: Harmful Interference to Global Navigation Satellite System (GNSS) and its impacts on flight and air traffic management operations
- Annex 10, Vol I & IV — Standards for Radio Navigation Aids & Surveillance Radar Systems.
- ICAO Doc 9849 – GNSS Manual
- EUROCAE ED-259 – Interference Detection and Mitigation for GNSS-based systems

1. INTRODUCTION

1.1 The increasing reliance on satellite-based systems such as GNSS and ADS-B has enhanced the efficiency of modern air navigation and surveillance operations. However, it has also introduced new vulnerabilities due to intentional and unintentional interference and spoofing activities. Such disruptions threaten the integrity of surveillance data, with potential implications on flight safety and air traffic management (ATM) efficiency.

1.2 The UAE has established a structured and systematic framework within its Surveillance Data Processing System (SDPS) to detect, investigate, and mitigate GNSS interference and spoofing incidents. This framework is integrated with multi-sensor validation (ADS-B, radar, and multilateration) and supported by a dedicated CNS operational workflow and coordination mechanism with the national Telecommunications Regulatory Authority.

2. DISCUSSION

2.1 The increasing reliance on satellite-based systems such as GNSS and ADS-B has introduced new vulnerabilities to air navigation operations due to the risks of interference and spoofing. These disruptions, whether intentional or unintentional, can compromise the accuracy of aircraft position reporting and affect air traffic management efficiency. Interference may result from electromagnetic emissions or environmental factors, while deliberate actions such as jamming or spoofing involve the transmission of counterfeit signals designed to mislead receivers or surveillance systems. Over the past two years, the United Arab Emirates has observed an increase in reported interference cases and suspected spoofing events, underscoring the importance of adopting robust monitoring and mitigation measures.

2.2 This reduction in surveillance system performance directly impacts the operational of affected aircrafts, subsequently impacts established aviation safety. Such occurrences have become increasingly frequent in specific airspaces, particularly those situated near or within conflict zones.

2.3 To address these challenges, the UAE has established a structured operational workflow within its Surveillance Data Processing System (SDPS) for detecting and investigating GNSS-related anomalies. Once a potential fault is identified—either through pilot reports, air traffic controller observations, or automated alerts—the CNS initiates an investigation to confirm the event and determine its source. The investigation process involves reviewing graphical interface recordings across multiple controller working positions, comparing the behaviour of multi-source surveillance feeds (radar, combined ADS-B, and individual sensors), extracting surveillance data for the affected period, and analysing it using playback and data analysis tools such as RAPS. This process allows investigators to identify indicators of interference or spoofing, such as inconsistent ground speeds, duplicate targets, or incorrect squawk codes.

2.4 When the root cause is confirmed to originate from a specific ADS-B sensor or corrupted data stream, the affected feed is isolated or disabled to prevent inaccurate data from being displayed on the controller working positions. The event is then formally reported through an Interference Complaint Form to the concerned Telecommunications Regulatory Authority for further coordination and frequency management action.

2.5 The UAE further emphasizes the importance of regional cooperation in this area. Sharing anonymized interference data and technical findings among MID States through ICAO regional mechanisms would enhance collective situational awareness and support the development of harmonized response protocols. Additionally, regional radar and surveillance data sharing can significantly improve operational resilience during GNSS disruptions, ensuring continuous situational awareness and maintaining the integrity of surveillance services across the region.

2.6 The increasing reliance on satellite-based systems has increased the concerns is the growing threat of GNSS interference and ADS-B spoofing, which can severely compromise the integrity and accuracy of aircraft positioning data. Such faults may originate from intentional spoofing attempts or unintentional electromagnetic interference, both of which have the potential to mislead air traffic control systems and endanger flight safety.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the best practices and operational workflow adopted by the UAE to detect and mitigate GNSS interference and ADS-B spoofing incidents;

b) encourage MID States to establish similar surveillance integrity investigation frameworks and designate national focal points for GNSS interference reporting;

c) support regional radar and surveillance data-sharing initiatives to enhance operational resilience against GNSS and ADS-B vulnerabilities; and

d) request ICAO MID Office to maintain a regional repository of interference reports and best practices for continuous improvement.

----

4. APPENDIX 1

4.1 GNSS interference or spoofing faults can be detected through pilot reports of signal interference, Air Traffic Controller observation of unusual or inconsistent target behaviour on the surveillance display, or by CNS technical team through CNS monitoring systems. Once identified, the ATC Operations Supervisor promptly notifies the CNS Shift Duty Team to initiate an investigation. Early notification allows the team to preserve relevant system recordings and logs before data overwriting occurs, ensuring that all diagnostic evidence remains available for analysis.

4.2 Upon receiving a fault reported by the ATC Supervisor relating to target misinformation, the technical investigator gathers all relevant information and fault details to assist troubleshooting, following the steps outlined below:

4.2.1 Check the Graphical User Interface (GUI) recordings across multiple positions to verify that the fault is persistent in all Controller Working Positions (CWP) and not limited to the one where it was first observed. This confirms whether the anomaly originates from a single display, the local network, or the Surveillance Data Processing System (SDPS).

4.2.2 While replaying the GUI recordings, verify and compare the system behaviour on the SDPS feed against all available single-source feeds, including combined ADS-B, individual ADS-B sensors, and radar sources. This step establishes whether the inconsistency appears in a single sensor input or in fused surveillance data, which is critical for identifying the source of corruption.

4.2.3 Extract a copy of the surveillance data recording during the incident using the SDPS recording system. Ensure the extracted period covers at least five minutes before and after the reported time to capture the full sequence of the fault. The data is labelled with incident number, time, and affected flight details for traceability.

4.2.4 Import the surveillance data into a radar recorder or analyser system such as RAPS for detailed examination. During playback, the Investigator can isolate individual sensor contributions, review track histories, and identify any missing or duplicated reports. This step also enables measurement of latency and timestamp integrity between sensors, which can indicate GNSS time deviation.

4.2.5 During analysis, verify and compare the behaviour of ADS-B sensor track data with radar plot data. Differences in ground speed, heading, or reported position between the two sources often reveal spoofed or corrupted GNSS inputs. Investigators also check for abnormal message rates, sudden track jumps, or identical track IDs appearing from multiple sensors, which are typical indicators of spoofing.

4.3 While analysing the collected data, the Investigator looks for indicators that may help identify the root cause of the fault. Common ADS-B spoofing or interference indicators are listed below, with additional diagnostic actions:

4.3.1 Incorrect ground speed: If the displayed ground speed appears incorrect, the Investigator verifies the transmitted speed from the aircraft transponder against the I062/185-calculated track velocity derived from radar. A consistent bias or mismatch across several aircraft may suggest GNSS degradation affecting ADS-B velocity vectors rather than individual aircraft malfunction.

4.3.2 Multiple aircraft displaying incorrect ground speed: The Investigator examines common factors such as geographical proximity, flight path, or sensor coverage. If all affected aircraft were received by the same ADS-B sensor, that sensor is marked as the potential source of corrupted data, possibly due to GNSS interference at the receiver site.

4.3.3 Target appearing in two locations: When duplicate targets are observed, the Investigator determines the correct position by cross-checking radar plots and flight plan data, then identifies which sensor provided the false data. This phenomenon typically results from spoofing, where recorded legitimate ADS-B data is retransmitted with a time delay. Because ADS-B transmissions are unencrypted and not verified by interrogation, the SDPS may process both genuine and spoofed reports as valid. The investigation therefore includes checking message timestamps, signal strength, and sensor bearing to distinguish the genuine source.

4.3.4 Target displaying an incorrect squawk code: The Investigator compares the squawk code displayed on the CWP with the code filed in the flight plan. If the discrepancy persists after the pilot resets the transponder or performs a squawk IDENT, spoofing is suspected. Data is then compared across multiple sensors—radar, combined ADS-B, and individual ADS-B—to determine which feed carries the incorrect code. The affected sensor is flagged for immediate verification and, if necessary, temporary isolation.

4.4 Once all surveillance data have been analysed and the indicators reviewed, the Investigator determines the root cause and takes the necessary actions to resolve or mitigate the fault.

4.4.1 If the root cause is traced to one of the ADS-B sensors, it is recommended to disable that sensor's feed in the SDPS configuration to prevent faulty or spoofed data from being displayed on the CWPs. The sensor is then subjected to on-site verification, including GNSS receiver status check, antenna inspection, and interference power-level measurement. If timing instability is observed, the sensor's reference clock is switched to the secondary time source until GNSS stability is restored.

4.5 As soon as the fault is confirmed to be caused by ADS-B interference or spoofing, an Interference Complaint Form is completed and sent to the Telecommunications Regulatory Authority. The form includes frequency range, affected area, time period, and operational impact. The event is logged in the CNS incident management system, and summary findings are shared with ANS Operations and Safety for awareness and future preventive actions.

- END -