REPUBLIC OF ALBANIA

ALBANIAN CIVIL AVIATION AUTHORITY

SAFETY INFORMATION

ACAA-DFS-SI-No.003

Issue: 01, Revision 00

Date: 06.09.2024

Approved by:

Maksim Et'hemaj

Executive Director of Albanian Civil Aviation Authority

0.1 Record of Amendments

The table below describes the dates and reason for the different amendments of the current procedure.
A vertical black line on the left-hand side of the page identify the changes with the previous version.

Issue No.	Revision No.	Date	Amended by	Reason
01	00	06.09.2024		Initial Issue

0.2 Revision table

Page #.	Issue No.	Revision No.	Date	Edited by

GNSS Interference Safety Information

Introduction

Aviation operations worldwide increasingly rely on Global Navigation Satellite System (GNSS) to improve navigation performance and to support air traffic control surveillance functions. However, the full benefits of GNSS can only be achieved if GNSS signals are adequately protected from electromagnetic interference which can cause loss or degradation of GNSS services.

In recent times, there has been a notable increase in GNSS[1] Interference, by means of jamming and spoofing, particularly in regions surrounding conflict zones and other sensitive areas such as the Mediterranean, Black Sea, Middle East, Baltic Sea, and the Arctic. These interferences disrupt the accurate reception of GNSS signals, leading to various operational challenges for aircraft and ground systems.

For the purpose of this Safety Information (SI), the terminology GNSS will be used indistinctively from Global Positioning System (GPS)[2].

Types of GNSS Interference

GNSS Jamming

GNSS jamming is an intentional radio frequency interference with GNSS signals. This prevents receivers from locking onto satellites signals and has the main effect of rendering the GNSS system ineffective or degraded for users in the jammed area. This type of interference is fairly easy to detect by flight crew.

GNSS Spoofing

GNSS spoofing refers to the deliberate transmission of fake GNSS signals aimed at manipulating the perceived location of a GNSS receiver. This manipulation causes the receiver to erroneously believe it is situated in a different location than its actual position, affecting navigation and timing data in a way that can be very hard to detect by flight crew. GNSS spoofing differs from GNSS jamming, which involves the disruption of GNSS signals, thereby preventing the receiver from determining its location altogether.

Effects and characteristics of GNSS interference

Interference can occur during any phase of flight, leading to re-routing or diversions to ensure safety. Common symptoms of GNSS interference include the following:

Jamming indications

It is common for jamming to precede spoofing. Jamming will result in the loss of GNSS Signal only and

[1] GNSS is the standard generic term for worldwide satellite navigation systems that provide autonomous geo-spatial positioning with global coverage. This term includes the GPS, GLONASS, Galileo, Beidou and other regional systems. GNSS is a term used worldwide and the advantage to having access to multiple satellites is accuracy, redundancy and availability at all times. Though satellite systems don't often fail, if one fails GNSS receivers can pick up signals from other systems like, for example, if line of sight is obstructed. This flexibility makes GNSS receivers much more accurate and reliable than GPS technology alone.

[2] GPS is the United States satellite navigation systems which consists of up to 31 medium Earth orbit satellites in six different orbital planes, with the exact number of satellites varying as older satellites are retired and replaced. Operational since 1978 and globally available since 1994, GPS is currently the world's most utilized satellite navigation system. A GPS receiver can only use signals from the 31 satellites in the Global Positioning System, and if too many of these signals are blocked, the receiver becomes useless until it can find a signal again.

the time from jamming to spoofing varies. When in the presence of GNSS jamming, pilots are expected to observe the following:

- GPS failure message;
- ADS-B failure/warning;
- GPWS terrain caution message;
- EGPWS terrain fail;
- SATCOM loss;
- Loss of SVS.

Spoofing indications

Unlike jamming, a GNSS signal is present, but it has fake information. False GNSS position, time, and date information will be processed by the GNSS receiver as being valid. As soon as this is fed to other systems, failure messages/actions may be expected such as:

- Rapid Estimated Position Uncertainty (EPU) or Actual Navigation Performance (ANP) increase;
- Discrepancies in navigation positions (GNSS position differs from FMS position);
- Aircraft clock time shifts;
- Transponder fail;
- Uncommanded autopilot turns;
- Synthetic vision reversion;
- Wind indicator illogical;
- Abnormal differences between ground speed and true airspeed;
- Spurious terrain awareness and warning system (TAWS) alerts; and
- Potential deviations in hybrid positions (inertial reference system (IRS)/GNSS).

FIRs affected by jamming and spoofing (updated on July 5, 2024)[3]

Although GNSS jamming or spoofing can be encountered anywhere in the world, according to the data collected so far, the mainly affected FIRs to date are the following:

The southern and eastern Mediterranean, and the Middle East

FIR Nicosia LCCC,
FIR Beirut OLBB,
FIR Damascus OSTT,
FIR Tel-Aviv LLLL,
FIR Amman OJAC,
The north-eastern part of FIR Cairo HECC,
The eastern part of FIR Athinai LGGG,
FIR Baghdad ORBB,
FIR Kuwait OKAC,
FIR Bahrain OBBB,
The north-western part of FIR Tehran OIIX, and
The northern part of FIR Tripoli HLLL.

The Black Sea

[3] Latest locations of GNSS interference are available in: Live GPS Spoofing Tracker Map (skai-data-services.com)

FIR Istanbul LTBB,
FIR Ankara LTAA,
The eastern part of FIR Bucuresti LRBB,
FIR Sofia LBSR,
FIR Tbilisi UGGG,
FIR Yerevan UDDD, and
FIR Baku UBBA.

Eastern Europe
FIR Bratislava LZBB,
FIR Budapest LHCC, and
FIR Chisinau LUUU.

The Baltic Sea
FIR Helsinki EFIN,
FIR Tallin EETT,
FIR Riga EVRR,
FIR Vilnius EYVL,
The eastern part of FIR Warszawa EPWW, and
The southern part of FIR Sweden ESAA.

The Arctic
The northern part of FIR Helsinki EFIN, and
The northern part of FIR Polaris ENOR.

Recommendations for air operators

1. Train flight crews to recognise and respond to GNSS interferences;
2. Report any observed GNSS anomalies promptly;
3. Include GNSS jamming/spoofing scenarios in crew training;
4. Assess operational risks and limitations due to GNSS loss;
5. Ensure the availability of alternative non-GNSS-based procedures; and
6. Make sure that flight crew follows company procedures, manufacturer guidance and legal requirements;
7. Always report irregularities.

Note: operators are encouraged to review the information provided in ACAA Safety Information Bulletin ACAA-DAN-SI-No.001 Issue: 01, Revision 02, dated 11.07.2024, on *Aviation safety concerns regarding interference to the Global Navigation Satellite System (GNSS)* for further recommendations.

Recommendations for pilots

Flight crew are encouraged to study and to pay close attention to the GNSS interference phenomena, which is nowadays becoming more frequent.
Whenever a flight is planned to flyover FIRs with high risk of GNSS interference, as well as neighboring FIRs, pilots should review and implement precautionary procedures to avoid the possibility of having potential serious consequences in flight safety.
ACAA recommends operators to adopt precautionary safety measures in case of GNSS spoofing[4], which

[4] Recommendations provided in this SI are not meant to be exhaustive, neither they constitute a

poses a higher risk for flight safety regarding GNSS interference[5], in addition to standard procedures during the following three flight phases: pre-flight; in-flight; and post-flight.

Pre-flight

Briefing – GNSS interference area locations; intentions; ground-based navaids availability; likely system losses; jamming and spoofing indications.
GNSS interference maps – check for the latest updated information; don't rely exclusively on NOTAMs
GPWS – verify impact of GNSS interference; review the basic versus the predictive mode; consider possible mitigation actions, such as voluntarily disabling the equipment.
IRS – make sure to do a full alignment; when necessary, do it manually if inside a GNSS interference area.
Flight planning – consider to file a flight plan based on conventional navaid airways; review CB activity in case of Weather Radar failure; avoid to perform RNP approaches.
Contingencies/emergencies plan review – consider the impact of GNSS interference on a diversion while in the interference area, or afterwards; verify that conventional arrival, approach, and missed approach procedures are available or, if not, check for daylight VMC from MSA down; review enroute safe altitudes (MEA/MORA) and destination/alternate approach corresponding MSA.
Review of technical data – understand the differences between jamming and spoofing and the characteristics of each one of them; make sure to realise the possible impact of GNSS interference in aircraft systems; verify MEL applicable items and determine the possible impact of GNSS interference; be prepared.
Synchronize watches – synchronize mechanical watches to known source before dispatch, in preparation for aircraft clock failure.
Prepare operations at airports within the GNSS interference area if applicable – expect ground GNSS interference and greater system impact; turn off the GNSS receiver via the FMC prior to aligning the IRS, and carry out a manual alignment; be vigilant for automatic capturing of the spoofed GNSS position during alignment; do not plan to perform GPS/RNP approaches, SIDs, STARs.

In-flight

Pre-Spoofing
Prepare – setup by 45 mins/ 300mm prior spoofing area;
Re-Brief Plan – actions; systems loss.
Monitor – EPU/ANP; open sensor/POS REF page; anticipate jamming first; monitor clock.
Increase Vigilance – be prepared for unusual system behavior; cross check alerting app; monitor ATC reports.
Set up aircraft systems – Follow OEM/Operator guidance; de-select GPS to FMS; de-select IRS Hybrid; clock to INT; inhibit EGPWS Look-ahead mode; stow HUD.
In-Spoofing
Aviate, navigate, communicate – apply manufacturer instructions on detecting and dealing with suspected GNSS spoofing; go back to basics; monitor aircraft position using non-GNSS navaids.
Note time on personal watch – record on log.
Check system settings – verify they are correct for spoof protection.
Check GNSS input – verify de-selected.
Check IRS Hybrid mode – verify de-selected.
Heading mode – if needed.

replacement for operators' procedures, manufacturers' instructions and other legal requirements. Furthermore, flight crew and operators are invited to enhance these recommendations to a greater extent in the interest of flight safety.

[5] In case of GNSS jamming, pilots should verify aircraft position using non-GNSS means and should also be aware of critical navigation aids.

Nav source – confirm in FMS.
Report to ATC – closely follow air traffic control (ATC) frequencies; request vectors if needed.
EGPWS – inhibit it at cruise aft, if procedure is allowed.
Post-Spoofing (recovery from spoofing)
Assess GNSS integrity – be certain that spoofing has finished.
GPS sensor page – check for correct time, date, GS, alt.
Thorough inflight system check – assess all systems for failures; carry out in-flight reset of MMR/GPS/GPWS if allowed; re-select GNSS sensor input to FMS; advise ATC of remaining failures.
Oceanic – send early message to OACC of RNP/CPDLC/ADS-C failures; anticipate lower crossing altitudes and rerouting.
Approach – avoid RNP approaches; advise ATC; brief intentions; be prepared for EGPWS false alerts; consider the use of basic modes; anticipate possible ECAM/EICAS alerts; check for alternates.

Post-flight

Report irregularities – fill an Air Safety Report for tracking of the GPS Spoofing problem;
Tech Log – note any GNSS interference in the aircraft tech log each flight, to ensure a hard reset of the GNSS/MMR is carried out;
For any unusual system impacts – send data to avionics manufacturers like Honeywell, Collins, etc.

Conclusion

Repeated or widespread disruptions of the GNSS signals can lead to increased workload of both flight crews and air traffic controllers that can cause cognitive overload or confusion and increase the risk for errors. The combination of two or more of the issues listed in this SI may have cumulative adverse effects on flight safety.
Therefore, the goal of this SI is to improve the knowledge of all stakeholders involved in the aviation industry in the field of GNSS interference and to enhance safety operations worldwide. All stakeholders are invited to work together for further improvement of mitigation actions and procedures in case of GNSS jamming and spoofing.
This SI will be revised to list new issues observed and update recommendations, as a result of ACAA's analysis on the most recent relevant reported occurrences of GNSS interference.