International Civil Aviation Organization

MIDANPIRG Communication, Navigation and Surveillance Sub-Group

Thirteenth Meeting (CNS SG/13)
(Jeddah, Saudi Arabia, 20 – 23 October 2024)

Agenda Item 5: CNS Planning and Implementation Framework in the MID Region

GNSS VULNERABILITIES

(Presented by the Secretariat)

SUMMARY

This working paper outlines the safety of flight risks related to the GNSS spoofing activities reported by various AOs and international organizations in several FIRs in MID Region and recommends a number of mitigation measures for ANSPs and CAAs.

Action by the meeting is at paragraph 3.

REFERENCES

- Assembly Resolution A41-8, Appendix C
- ICAO Doc 9849-GNSS Manual-4th edition (unedited)-2023
- RASG-MID Safety Advisory (RSA-14) on GNSS Vulnerabilities
- MIDANPIRG/21 & RASG-MID/11 (Abu Dhabi, UAE, 4 – 8 March 2024) meeting report

1. INTRODUCTION

1.1 The Global Navigation Satellite System (GNSS) is essential for the implementation of Performance Based Navigation (PBN) and Automatic Dependent Surveillance-Broadcast (ADS-B) which are bringing substantial safety, capacity and environmental benefits to ATM. It is also used in safety-related systems and provides the time reference to synchronize systems (e.g. communication networks) and operations in ATM. However, GNSS is vulnerable to radio frequency interference (RFI) such as jamming, and cyber-attacks (e.g. spoofing). Therefore, it is essential to mitigate GNSS vulnerabilities adequately.

1.2 Modern aircraft are reliant on the signals from GNSS to feed their different systems. In recent months, however, potential spoofing activities reported by various civil air operators increased safety of flight risks to civil aviation operations due to potential loss of aircraft situational awareness and increased pilot and air traffic control (ATC) workload issues, which may have an impact on aviation safety.

2. DISCUSSION

GPS Spoofing

2.1 Spoofing is the broadcast of GNSS-like signals that cause avionics to calculate erroneous positions and provide false guidance.

2.2 Since August 2023, a new variety of GPS spoofing were reported, the spoofing signal is adequately strong and of sufficient integrity to feed the aircraft systems. The result is that within minutes, the IRS becomes unusable, and in many cases, all navigation capability on board is lost. Flight Crews had to request for vectors which could be a significant extra load for the ATC and would severely impact the available airspace capacity. Given the types of airspace that these events are occurring in, this presents significant risk.

Note: Additional hazards might be introduced by implementing performance based navigation (particularly RNAV5) without considering the availability of Surveillance coverage.

2.3 The meeting may wish to note that, after analyzing the reports it was found that the concentration of the occurrences was focused within Baghdad, Tehran and Cairo FIRs.

2.4 The effects of the spoofing on GNSS were observed by flight crew, including:

- Fake (spoofed) GPS signal gives the FMS the indication of 60nm off track;
- Complete loss of navigational capability including IRS failure;
- No reliable on board navigation – ATC vectors required. One flight required ATC vectors all the way to their destination; and
- Potential airspace infringements due to GNSS degradation. One operator almost entering a restricted airspace without clearance.

Recommended Actions

2.5 To address the identified issues, it is recommended to implement the following mitigation measures; to be considered within the FIRs where similar issues had been reported or identified. CAAs and ANSPs were encouraged to:

- Establish a process to collect information on GNSS degradations, in coordination with the relevant National Communications Authorities, and promptly notify the related outcomes to air operators and to other airspace users.
- Ensure that contingency procedures are established in coordination with ANSPs and airspace users, and that essential conventional navigation infrastructure are retained and fully operational.
- Implement appropriate and proactive mitigating measures as a matter of high priority, including the issuance of NOTAMs, e.g. describing affected areas and related limitations (as appropriate and determined at State level).
- Confirm ANSPs' readiness to provide reliable surveillance coverage that is resilient to GNSS interference, such as ground NAV aids for conventional non-satellite based navigation (Distance Measuring Equipment (DME), Very High Frequency omnidirectional range (VOR)).
- Ensure that ANSPs' contingency plans include alternative procedures to be followed in case of large-scale GNSS jamming and/or possible spoofing events.

GNSS Testing Activities and Need for Enhanced Civil/Military Coordination

2.6 While further investigations of the reported GPS spoofing cannot confirm military activities as causes of the outages with certainty, it remains probable for cases near zones of conflict. Therefore, it is appropriate to reiterate that States should use caution when conducting civil and military GNSS and other testing activities which could contribute to operational impact on aviation CNS systems. Airspace users should be informed accordingly. Many States have already put in place efficient civil-military processes to coordinate testing activities and other operations, in particular in the context of military exercises. Considering the potential negative impact of GNSS testing on the safety of flights, States are strongly encouraged to further enhance civil-military coordination related to GNSS.

GNSS RFI Mitigation Plan

2.7 ICAO has developed a GNSS RFI mitigation plan as a part of the GNSS Manual (ICAO Doc 9849). The mitigation plan describes a list of preventive and reactive measures aimed at mitigating the interference risk as far as practicable. The framework recommended by the mitigation plan includes a continuous three-step process of 1) monitoring threats; 2) assessing risks; and 3) deploying mitigation measures. The plan also explains the need to inform AUs in the event of GNSS outages and the necessity to train flight crew and air traffic controllers to be able to recognize interference events and to react appropriately.

RASG-MID Safety Advisory – 14

2.8 The meeting may wish to recall that the Seventeenth Meeting of the Middle East Air Navigation Planning and Implementation Regional Group and Seventh Meeting of the Regional Aviation Safety Group-Middle East MIDANPIRG/17 & RASG-MID/7 held in Cairo, Egypt, 15 – 18 April 2019, endorsed through RASG-MID CONCLUSION 7/1 the RASG-MID Safety Advisory (RSA-14) on GNSS Vulnerabilities, at **Appendix A** (also available under ICAO MID website: https://www.icao.int/MID/Documents/2017/RASG-MID6/RSA%2014-GNSS%20Vulnerabilities.pdf).

2.9 The meeting will recall also that the SARPs have been recently updated to add requirements for DFMC SBAS, new core constellations and additional core constellation signal. In addition, the latest updates on the DOC 9849, GNSS Manual, in particular Chapter 5 GNSS Vulnerability with the significant material added to address recent developments and thinking with respect to jamming and spoofing and the Appendix F GNSS RFI Mitigation Plans addressing current, significant issues with jamming and spoofing concerns.

2.10 To ensure that the guidance materials remain accurate, relevant, and aligned with the latest developments, it is necessary that the RASG-MID Safety Advisory (RSA-14) on GNSS Vulnerabilities be updated to reflect recent developments and changes that have occurred in Annex 10 Volume 1 and GNSS Manual DOC 9849.

2.11 The meeting may wish to recall that MIDANPIRG/18 through DECISION 18/40 established GNSS Guidance Ad-Hoc Action Group tasked to review and prepare a revised version of the Guidance on GNSS Implementation in the MID Region. Therefore, it is proposed that the Ad-Hoc Action Group provides updates to the RASG-MID Safety Advisory (RSA-14) to reflect recent developments and changes to maintain its effectiveness and reliability.

GNSS interference NOTAM Terminology

2.12 The meeting may wish to recall that the MIDANPIRG/20 endorsed, through MIDANPIRG Conclusion 20/18, a NOTAM TEMPLATE FOR GNSS INTERFERENCE. Based on the recent new entry of GNSS Spoofing, additionally, the MIDANPIRG/21 requested ICAO and IATA to revise the template in coordination with the AIM SG:

MIDANPIRG CONCLUSION 21/30: REVISED NOTAM TEMPLATE FOR GNSS INTERFERENCE

That,

a) ICAO and IATA in coordination with AIM SG Chairpersons to develop revised NOTAM template for GNSS interference including jamming and spoofing considering the global and regional developments; by Q4 2024 and

b) ICAO MID Office circulate the revised NOTAM Template for GNSS interference through State Letter for implementation by States.

2.13 The revised NOTAM Template should reflect the recent spoofing activities and its impact on safety of flight operations.

ICAO EUR/MID Radio Navigation Symposium

2.14 Under the theme "***Towards Safe, Reliable and Resilient Air Navigation***" and with the aim to provide recent updates on GNSS constellations and augmentation systems, identify and address emerging challenges including GNSS vulnerabilities and discuss its management plan, in particular possible GNSS jamming/spoofing monitoring solutions, the ICAO EUR/MID Radio Navigation Symposium for EUR/NAT and MID Regions was conducted in Antalya, Turkiye, from 6 to 8 February 2024, organized jointly by the ICAO EUR/NAT and MID Regional Offices.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information in the paper;

b) encourage States and ANSPs to share their experience related to GNSS Spoofing;

c) develop MID region ground-based Navigation Aids Minimum Operating Network to support para 2.5 above; and

d) review and update, as deemed necessary the MID RSA-14, at **Appendix A**.

RASG-MID SAFETY ADVISORY – 14

(RSA-14)

April 2019

MID-Region

GUIDANCE MATERIAL REALTED TO GNSS VULNERABILTIES

Date of Issue:	April 2019
Revision	First Edition – April 2019
Document Ref. No.:	RSA-14

Owner:	RASG-MID

Disclaimer

This document has been compiled by the MID Region civil aviation stakeholders to mitigate the safety and operational impact of GNSS service disruption. It is not intended to supersede or replace existing materials produced by the National Regulator or in ICAO SARPs. The distribution or publication of this document does not prejudice the National Regulator's ability to enforce existing National regulations. To the extent of any inconsistency between this document and the National/International regulations, standards, recommendations or advisory publications, the content of the National/International regulations, standards, recommendations and advisory publications shall prevail**.**

TABLE OF CONTENTS

Acronyms…… 4

Introduction …….. 5

Description …….. 5

Risk Assessment…… 6

Mitigation Strategies……..… 7

Reducing the Likelihood of GNSS Interferences……..… 7

Reducing the Impact of GNSS Interferences…… 8

Monitoring…… 9

Reporting…… 10

References…….. 12

APPENDIX A: GNSS Interference Reporting Form to be Used by Pilots……..…… …… 13

APPENDIX B: Risk Assessment Methodology…….…….…….…… 15

APPENDIX C: GNSS Anomaly for the Period (January 2015- June 2018)…… 20

ACRONYMS

ABAS	AIRCRAFT BASED AUGMENTATION SYSTEM
ADS-B	AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST
AHRS	ATTITUDE AND HEADING REFERENCE SYSTEMS
ANS	AIR NAVIGATION SERVICES
ATC	AIR TRAFFIC CONTROLLER
DME	DISTANCE MEASURING EQUIPMENT
EGPWS	ENHANCED GROUND PROXIMITY WARNING SYSTEM
FIR	FLIGHT INFORMATION REGION
FMS	FLIGHT MANAGEMENT SYSTEM
GBAS	GROUND BASED AUGMENTATION SYSTEM
GLONASS	GLOBAL NAVIGATION SATELLITE SYSTEM
GNSS	GLOBAL NAVOGATION SATELLITE SYSTEM
GPS	GLOBAL POSITION SYSTEM
HAL	HORIZONTAL ALERT LIMIT
ILS	INSTRUMENT LANDING SYSTEM
IRS	INERTIAL REFERENCE SYSTEM
ITU	INTERATIONAL TELECOMMUNICATION UNION
MIDANPIRG	MID AIR NAVIGATION PLANNING AND IMPLEMENTATION GROUP
NAV	NAVIGATION
NOTAM	NOTICE TO AIRMEN
PBN	PERFORMANCE BASED NAVIGATION
POS	POSITION
RAIM	RECEIVER AUTONOMOUS INTEGRITY MONITORING
RF	RADIO FREQUENCY
RNAV	AREA NAVIGATION
RNP	REQUIRED NAVIGATION PERFORMANCE
SBAS	SPACE BASED AUGMENTATION SYSTEM
TAWS	TERRAIN AVOIDANCE WARNING SYSTEM
TSO	TECHNICAL STANDARD ORDER
VHF	VERY HIGH FREQYENCY
VNAV	VERTICAL NAVIGATION
VOR	VERY HIGH OMNI DIRECTIONAL RADIO RANGE
WAAS	WIDE AREA AUGMENTATION SYSTEM

GNSS VULNERABILITIES

1. INTRODUCTION

GNSS supports positioning, navigation and timing (PNT) applications. GNSS is the foundation of Performance Based Navigation (PBN), automatic dependent surveillance – broadcast (ADS-B) and automatic dependent surveillance – contract (ADS-C). GNSS also provides a common time reference used to synchronize systems, avionics, communication networks and operations, and supports a wide range of non-aviation applications.

GNSS Vulnerability has been identified as a safety issue and one of the main challenges impeding the implementation of PBN in the MID Region. The sixteenth meeting of the MID Air Navigation planning and Implementation Regional Group (MIDANPIRG/16Kuwait, 13-16 February 2017) recognized the impact of the GNSS signal interference and vulnerabilities and agreed that the subject should be addressed by the Regional Aviation Safety Group-Middle East (RASG-MID) in order to agree on measures to ensure effective reporting of GNSS interferences, which could be mandated by the States' regulatory authorities. The meeting invited the RASG-MID to consider the development of a RASG-MID Safety Advisory (RSA) related to GNSS vulnerabilities, highlighting the Standard Operating Procedures (SOP) for pilots, including the reporting procedures.

The RASG-MID/6 (Bahrain, 26 – 28 September 2017) agreed that IATA and ICAO MID Office should develop a RSA on GNSS vulnerabilities.

With the increasing dependence on GNSS, it is important that GNSS vulnerabilities be properly addressed. This Safety Advisory provides guidance on set of mitigation measures that States would deploy to minimize the GNSS vulnerabilities impact on safety and air operation. The RSA also includes the regional reporting and monitoring procedures of GNSS anomaly with the aim to analyze the threat and its impact on performance, and assess the effectiveness of the mitigation measures in place.

2. DESCRIPTION

Dependence on GNSS is increasing as GNSS is used for an ever-expanding range of safety, security, business and policy critical applications. GNSS functionality is being embedded into many parts of critical infrastructures. Aviation is now dependent on uninterrupted access to GNSS positioning, navigation and timing (PNT) services.

Aviation relies heavily on GNSS for area navigation and precision approach. Aircraft avionics such as the Flight Management Systems (FMS) require GNSS timing for a large number of onboard functions including Terrain Avoidance Warning System (TAWS) or Enhanced Ground Proximity Warning Systems (EGPWS). Onboard avionics are highly integrated on commercial aircraft and are very dependent on GNSS timing data. At the same time, GNSS vulnerabilities are being exposed and threats to denial of GNSS services are increasing.

There are several types of threat that can interfere with a GNSS receiver's ability to receive and process GNSS signals, giving rise to inaccurate readings, or no reading at all, such as radio frequency interference, space weather induced ionospheric interference, solar storm, jamming and spoofing. The disruption of GNSS, either performance degradation in terms of accuracy, availability and integrity or a complete shutdown of the system, has a big consequence in critical infrastructure. For example, local interference in

an airport could degrade position accuracy or lead to a total loss of the GNSS based services, which could put safety of passengers in jeopardy.
There are two types of GNSS Interference Sources; Intentional and Unintentional sources, the latter is not considered a significant threat provided that States exercise proper control and protection over the electromagnetic spectrum for both existing and new frequency allocations. Solar Effect, Radio Frequency Interference and On-board systems are examples of Unintentional GNSS interference sources. However, the Intentional sources such as Jamming and spoofing are considered as serious threats to the continued safety of air transport.

GNSS Jamming occurs when broadcasting a strong signal that overrides or obscures the signal being jammed. The GNSS jamming might occur deliberately by a military activity or by Personal Privacy Devices (PPDs). GNSS jamming has caused several GNSS outages in the MID Region.

In some States, military authorities test the capabilities of their equipment and systems occasionally by transmitting jamming signals that deny GNSS service in a specific area. This activity should be coordinated with State spectrum offices, Civil Aviation Authorities and ANS providers. Military and other authorities operating jamming devices should coordinate with State/ANS providers to enable them to determine the airspace affected, advise aircraft operators and develop any required procedures.

Spoofing is another source of intentional GNSS Interference, which is a deliberate interference that aims to mislead GNSS receivers into general false positioning solution.

Detailed information about the GNSS Implementation and Vulnerabilities can be found in MID DOC 010 – The Guidance on GNSS implementation in the MID Region.

3. RISK ASSESSMENT

The risk assessment covers affected operations during en-routre, terminal, and approach phase of flights. In addition, the aircraft impact at table (1), which presents an overview of different potential impacts from GNSS interference, needs to be considered for risk assessment.

Understanding the different types of threat and how likely they are to occur is key to conducting an accurate risk assessment. Broadly, the threat types break down as follows:

Threat Source	Threat Type	Description	Impact on the User
Solar Storms	Unintentional	Electromagnetic interference from solar flares and other solar activity “drowns out” the satellite signals in space.	Loss of signal, or range errors affecting the accuracy of the location or timing information.
Jamming	Intentional	Locally-generated RF interference is used to “drown out” satellite signals.	Loss of signal (if the jammer is blocking out all satellite signals) or range errors affecting the accuracy of the location or timing information

Spoofing	Intentional	Fake satellite signals are broadcast to the device to fool it into believing it is somewhere else, or at a different point in time.	False location and time readings, with potentially severe impacts on automated and autonomous devices and devices that rely on precise GNSS timing.
RF Interference	Unintentional	Noise from nearby RF transmitters (inside or outside the device) obscures the satellite signals.	Loss of signal (if the transmitter is blocking out all satellite signals) or range errors affecting the accuracy of the location reading (if the receiver is at the edge of the transmitter's range).
Signal Reflection	Unintentional	Reflection due objects such as buildings	GNSS signals can reflect off relatively due to distant objects, such as buildings, which would cause gross errors in position accuracy if the receiver falsely locks onto the reflected signal instead of the direct signal
User Error	Unintentional	Users over-rely on the GNSS data they are presented with, ignoring evidence from other systems or what they can see.	Can lead to poor decision-making in a range of scenarios

Table 1: Threats types

Depending on the nature of the interference and the nature of the application, a user may be affected in several ways; the impact may range from a small nuisance to an economic, operational or a safety impact. The detailed risk assessment methodology is addressed at **Appendix B**.

4. MITIGATION STRATEGIES

To minimize the risks associated with GNSS vulnerabilities, several mitigation strategies can be deployed to reduce the likelihood and impact of the threat.

4.1 REDUCING THE LIKELIHOOD OF GNSS INTERFERENCES

The likelihood of interference depends on many factors such as population density and the motivation of individuals or groups in an area to disrupt aviation and non-aviation services. To reduce the likelihood of GNSS interference, the following measures may be applied:

a) Effective spectrum management; this comprises creating and enforcing regulations/laws that control the use of spectrum and carefully assessing applications for new spectrum allocations.

b) The introduction of GNSS signals on new frequencies will ensure that unintentional interference does not cause the complete loss of GNSS service (outage) although enhanced services depending upon the availability of both frequencies might be degraded by such interference.

c) State should forbid the use of jamming and spoofing devices and regulate their importation, exportation, manufacture, sale, purchase, ownership and use; they should develop and enforce a strong regulatory framework governing the use of intentional radiators, including GNSS repeaters, pseudolites, spoofers and jammers. The enforcement measures include:

- detection and removal of jammers / interference sources; and
- direct or indirect detection (e.g. use of dedicated interference detection equipment).

d) Education activities to raise awareness about legislation and to point out that 'personal' jammers can have unintended consequences.

e) Multi-constellation GNSS would allow the receiver to track more satellites, reducing the likelihood of service disruption.

4.2 REDUCING THE IMPACT OF THE GNSS VULNERABILITIES

The GNSS signal disruption cannot be ruled out completely and States/ANSPs must be prepared to deal with loss of GNSS signals, and that States conduct risk assessment and implement mitigation strategies. The risk and impacts from these threats can be managed by evaluating the growing threat of GNSS interference, jamming and spoofing.

The disruption of GNSS signals will require the application of realistic and effective mitigation strategies to both ensure the safety and regularity of air services and discourage those who would consider disrupting aircraft operations. There are three principal methods, which can be applied in combination:

a) taking advantage of on-board equipment, such as Inertial Reference System (IRS);

IRS provides a short-term area navigation capability after the loss of GNSS updating. Many air transport aircraft are equipped with IRS and these systems are becoming more affordable and accessible to operators with smaller, regional aircraft. Most of these systems are also updated by DME.

b) Development of contingency procedures and processes to enable operations in a fallback mode in case of loss of GNSS (aircrew and/or ATC).

Procedural (aircrew or ATC) methods can provide effective mitigation in combination with those described above, taking due consideration of:

- the airspace classification;
- the available ATC services (radar or procedural);
- the avionics onboard
- aircrew and air traffic controller workload implications;
- the impact that the loss of GNSS will have on other functions, such as ADS-B based surveillance; and
- the potential for providing the necessary increase in separation between aircraft in the affected airspace.

c) taking advantage of conventional navigation aids and radar, conventional aids can provide alternative sources of guidance.

The regulator should conduct safety oversight of the service provider's GNSS based Services and validate the safety aspects of mitigation strategies, considering the impact on ATM operations. Details on Risk assessment process including some examples are at **Appendix B.**

The data analysis of the reported GNSS vulnerabilities for the period January 2015to June 2018 showed that the impact of the GNSS interference on Aircraft Operations in the MID Region were as follows:

1. Loss of GPS1 (fault)/ Loss of GPS2 (fault)
2. Observation of "Map shift" on Navigation display
3. Switching to an alternative navigation mode (IRS displayed, VOR/DME)
4. Degraded PBN Capability (NAV Unable RNP)
5. GPS POS Disagree
6. EGPWS warning
7. ADS-B Traffic triggered

5. MONITORING

The success of many of countermeasures is dependent on having a detailed understanding of the threats. In order to establish this understanding and to maintain an up-to-date knowledge of the threats - in terms of both types and number of threats – it is necessary to States to monitor the threat environment and the impact on performance.

Monitoring and reporting is required to inform stakeholders of the threats that exist. This would help directly with enforcement (detecting and removing sources of interference) as well as monitoring the response to changes in legislation or education activities.

Receiver autonomous integrity Monitoring (RAIM) provides integrity monitoring by detecting the failure of a GNSS satellite. It is a software function incorporated into GNSS receivers.

In the event of GNSS performance degrading to the point where an alert is raised, or other cause to doubt the integrity of GNSS information exists, the pilot in command must discontinue its use and carry out appropriate navigation aid failure procedures. Should RAIM detect an out-of-tolerance situation, an immediate warning will be provided. When data integrity or RAIM is lost, aircraft tracking must be closely monitored against other available navigation systems.

States may consider the deployment of GNSS threat monitoring system, which allows monitoring of local GNSS interference environment; signal recording and monitoring for situational awareness of any drop in signal quality or signal outage and ground validation of GNSS-based flight procedures. The detection equipment may include localization utilities.

With reference to ICAO Doc 9849:

Given the variety of avionics designs, one service status model cannot meet all operators' requirements. A conservative model would produce false alarms for some aircraft. A less conservative model would lead to missed detection of a service outage for some and false alarms for others. Regardless, only the aircrew, not ATC, is in a position to determine whether, for example, it is possible to continue an ABAS-based instrument approach. In contrast, ATC has access to ILS monitor data and can deny an ILS approach clearance based

on a failure indication. The real time monitor concept is neither practical nor required for GNSS ABAS operations. It may be practical for SBAS and GBAS, but implementation would depend on a valid operational requirement.
Aircraft operators with access to prediction software specific to their particular ABAS/RAIM avionics will find it advantageous to employ that software rather than use the general notification service. In the case of SBAS and GBAS, operators will rely on service status notifications.

6. REPORTING

ANSP must be prepared to act when anomaly reports from aircraft or ground-based units suggest signal interference. If an analysis concludes that interference is present, ANS providers must identify the area affected and issue an appropriate NOTAM.

From the perspective of the aircrew, a GNSS anomaly occurs when navigation guidance is lost or when it is not possible to trust GNSS guidance. In this respect, an anomaly is similar to a service outage. An anomaly may be associated with a receiver or antenna malfunction, insufficient satellites in view, poor satellite geometry or masking of signals by the airframe. The perceived anomaly may also be due to signal interference, but such a determination requires detailed analysis based on all available information.

In case of GNSS anomaly detected by aircrew, **Pilot** action(s) should include:

a) reporting the situation to ATC as soon as practicable and requesting special handling as required;
b) filing a GNSS Interference Report using the Template at **Appendix A**, and forwarding information to the IATA MENA (sfomena@iata.org) and ICAO MID Office (icaomid@icao.int) as soon as possible, including a description of the event (e.g. how the avionics failed/reacted during the anomaly).

Controller action(s) should include:

a) recording minimum information, including aircraft call sign, location, altitude and time of occurrence;
b) cross check with other aircraft in the vicinity;
c) broadcasting the anomaly report to other aircraft, as necessary;
d) notify the AIS Office in case NOTAM issuance is required; and enable the fallback mode and implement related procedure and process (contingency measures).

ANSP action(s) should include:

a) ensuring the issuance of appropriate advisories and NOTAM, as necessary;
b) attempting to locate/determine the source of the interference, if possible;
c) notifying the agency responsible for frequency management (the Telecommunication Regulatory Authority);
d) locate and eliminate source in cooperation with local regulatory & enforcement Authorities;
e) tracking and reporting all activities relating to the anomaly until it is resolved; and
f) review the effectiveness of the mitigation measures for improvement.

ICAO MID Office action(s) should include:

a) collect anomaly related information and determine the course of action required to resolve reported anomalies;
b) follow-up with State having interference incident to ensure implementation of required corrective actions;
c) coordinate with concerned adjacent ICAO Regional Office(s) to follow-up with States under their accreditation areas, when needed; and
d) Communicate with ITU Arab Office and Arab Spectrum Management Group to resolve frequent interference incidents, when needed.

7. REFERENCES:

- Annex 10 Aeronautical Telecommunications, Volume I ─ Radio Navigation Aids
- Annex 11 Air Traffic Services
- PANS-ATM, ICAO doc 4444
- ICAO Doc 9613 PBN Manual
- ICAO Electronic Bulletin 2011/56, Interference to Global Navigation Satellite System (GNSS) Signals.
- GNSS Manual, ICAO Doc 9849
- Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation, STRIKE3 EUROPEAN Initiative, Paper 74
- The report of Vulnerabilities Assessment of the Transportation Infrastructure relying on the Global Position System, US Department of Transportation.
- Operational Impacts of Intentional GPS Interference. (A Report of the Tactical Operations Committee in Response to Tasking from the Federal Aviation Administration. March 2018.
- CANSO Cyber security and Risk Assessment guide.
- ICAO GNSS RFI Mitigation Plan and associated EUROCONTROL Efforts, 8 Nov 2016
- European Global Satellite Agency System, GNSS Market Report issue 4, March 2015
- MID Doc 007 (MID Region PBN Implementation Plan
- MID Doc 010 (The Guidance on GNSS implementation in the MID Region)

Appendix A

1. **GNSS interference reporting form to be used by pilots**
   ** Mandatory field*

Originator of this Report:	
Organisation:	
Department:	
Street / No.:	
Zip-Code / Town:	
Name / Surname:	
Phone No.:	
E-Mail:	
Date and time of report	
Description of Interference	
*Affected GNSS Element	[ ] GPS [ ] GLONASS [ ] other constellation [ ] EGNOS [ ] WAAS [ ] other SBAS [ ] GBAS (VHF data-link for GBAS)
Aircraft Type and Registration:	
Flight Number:	
*Airway/route flown:	

Coordinates of the first point of occurrence / Time (UTC):	UTC: Lat: Long:
Coordinates of the last point of occurrence / Time (UTC):	UTC: Lat: Long:
*Flight level or Altitude at which it was detected and phase of flight:	
Affected ground station (if applicable)	Name/Indicator; [e.g. GBAS]
*Degradation of GNSS performance:	[ ] Large position errors (details): [ ] Loss of integrity (RAIM warning/alert): [ ] Complete outage (Both GPSs), [ ] Loss of GPS1 or Loss of GPS 2 [ ] Loss of satellites in view/details: [ ] Lateral indicated performance level changed from:___to ___ [ ]Vertical indicated performance level changed from: __ to __ [ ] Indicated Dilution of Precision changed from __ to__ [ ] information on PRN of affected satellites (if applicable) [ ] Low Signal-to-Noise (Density) ratio [ ] Others
*Problem duration:	[ ] continuous for 20 minutes [ ] intermittent

Note: Only applicable fields need to be filled!

Appendix B

Risk Assessment

Threats and vulnerabilities

A threat assessment should be performed to determine the best approaches to securing a GNSS against a particular threat. Penetration testing exercises should be conducted to assess threat profiles and help develop effective countermeasures.

Table (B1) presents an overview of different potential impacts from GNSS interference. This is a snapshot of impacts based on input from two manufacturers and not intended to be a comprehensive list of all impacts:

Effect	Affected Operation	Impact
Loss of GNSS-based navigation	Enroute/ Terminal/ Approach	Aircraft with Inertial Reference Unit (IRU) or Distance Measuring Equipment (DME)/DME may have degraded RNP/RNAV. Aircraft may deviate from the nominal track May increase workload on aircrew and ATC May result in missed approach or diverting to other runway in case the aerodrome operating minima cannot be met through conventional precision or visual approaches. Conventional ATS routes, SIDs and STARs would be used.
Larger than normal GNSS position errors prior to loss of GNSS	Enroute/ Terminal/ Approach	Interference could cause the GNSS position to be pulled off but not exceed the HAL (2NM , 1NM, 0.3NM for enroute, terminal and approach phases, respectively).
Loss of EGPWS/ TAWS	Enroute/ Terminal/ Approach	Reduced situational awareness and safety for equipped aircraft. Terrain Awareness and Warning System (TAWS) is required equipment for turbine-powered airplanes > 6 passengers. Loss of GPS results in loss of terrain/obstacle alerting. Position errors as GPS degrades can result in false or missed alerts.
Loss of GPS aiding to AHRS	Flight Control	Can result in degradation of AHRS pitch and roll accuracy with potential downstream effects such as was experienced by a Phenom 300 flight.

Loss of GNSS to PFD/MFD	All flight phases	Can result in: -Loss of synthetic vision display and flight path marker on PFD -Loss of airplane icon on lateral and vertical electronic map displays, georeferenced charts, and airport surface maps without DME-DME or IRU -Loss of airspace alerting and nearest waypoint information without DME-DME or IRU Overall loss of situational awareness to flight crew and increased workload.
No GNSS position for ELT	Search and Rescue	Loss of GNSS signal could result in larger search areas for the Emergency Locator Transmitters (ELTs)

Table B1: Potential Impact from GNSS

Consequence/Impact of risk occurring

Category	Effect on Aircrew and Passengers	Overall ATM System effect
Catastrophic 1	Multiple fatalities due to collision with other aircraft, obstacles or terrain	Sustained inability to provide any service.
Major 2	Large reduction in safety margin; serious or fatal injury to small number; serious physical distress to air crew.	Inability to provide any degree of service (including contingency measures) within one or more airspace sectors for a significant time.
Moderate 3	Significant reduction in safety margin.	The ability to provide a service is severely compromised within one or more airspace sectors without warning for a significant time.
Minor 4	Slight reduction in safety margin.	The ability to provide a service is impaired within one or more airspace sectors without warning for a significant time
Negligible 5	Potential for some inconvenience.	No effect on the ability to provide a service in the short term, but the situation needs to be monitored and reviewed for the need to apply some form of contingency measures if the condition prevails.

Table B2: Impact of Risk Occurring

Likelihood of risk occurring

The definitions in the table (B3) were adopted for estimating the likelihood of an identified risk occurring, for this purpose, five situations are considered:

Event is expected to occur	
1	More frequently than hourly
2	Between hourly and daily
3	Between daily and yearly
4	Between yearly and 5 yearly
5	Between 5 and 50 years
6	Less frequently than once every 50 years

Table B3: Likelihood of risk occurring

Assessment of the level of risk and risk tolerance

All identified risks were reviewed and provided for each an overall risk ranking which is a combination of the two characteristics of consequence and likelihood. For example, a risk with a major consequence but a "5" likelihood would be described as having an "A" or "unacceptable" risk rating. The conversion of the combination of consequence and likelihood into a risk rating has been achieved by use of the following matrix.

Likelihood Criteria		**Consequence Criteria**				
Event expected to occur:		**Catastrophic 1**	**Major 2**	**Moderate 3**	**Minor 4**	**Insignificant 5**
1	**More frequently than hourly**	**A**	**A**	**A**	**A**	**C**
2	**Between hourly and daily**	**A**	**A**	**A**	**B**	**D**
3	**Between daily and yearly**	**A**	**A**	**B**	**C**	**D**
4	**Between yearly and 5 yearly**	**A**	**B**	**C**	**C**	**D**
5	**Between 5 and 50 years**	**A**	**B**	**C**	**D**	**D**
6	**Less frequently than once every 50 years**	**B**	**C**	**D**	**D**	**D**

Table B4: Risk Assessment Table

The previous matrix provides a guide to determine which risks are the highest priorities from the perspective of the timeliness of the corrective action required. The following table outlines the position in more definitive terms.

Safety tolerability risk matrix

Risk Index Range	Description	Recommended Action
A	Unacceptable	Stop or cut back operation promptly if necessary. Perform priority/immediate risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range
B	High Risk	Urgent action. Perform priority/immediate risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range
C	Moderate Risk	Countermeasures actions to mitigate these risks should be implemented.
D	Low Risk	Acceptable as is. No further risk mitigation required

Table B5: Risk Tolerability Matrix

Sample risk assessment

The risk assessment table (B6) could be used to identify and capture the threats, select the risk rating based on the risk matrix above considering the existing controls. In addition, recommended actions could be selected to minimize the risk.

L = Likelihood
C = Consequence
R = Risk

Threat	Initial Risk			Existing controls	Accept/Reduce	Recommended controls	Residual Risk		
	L	C	R				L	C	R

Table B6: Sample Risk Assessment tables

The table (B7) below is an example of risk assessment for approach phase of flight, the detailed Risk assessment process is at Appendix B

L = Likelihood
C = Consequence
R = Risk

Threat	Initial Risk			Existing controls	Accept/ Reduce	Recommended controls	Residual Risk		
	L	C	R				L	C	R
Between daily and yearly	**3**	**2**	A	-Error message notification by avionic	Reduce	1)using of on-board equipment (IRS); 2)Interference detector by ANSPs 3) executing miss-approach	3	4	C

Table B7: Example Risk Assessment for Approach phase of flight

Another example risk assessment for en-route phase of flight at table (B8)

L = Likelihood
C = Consequence
R = Risk

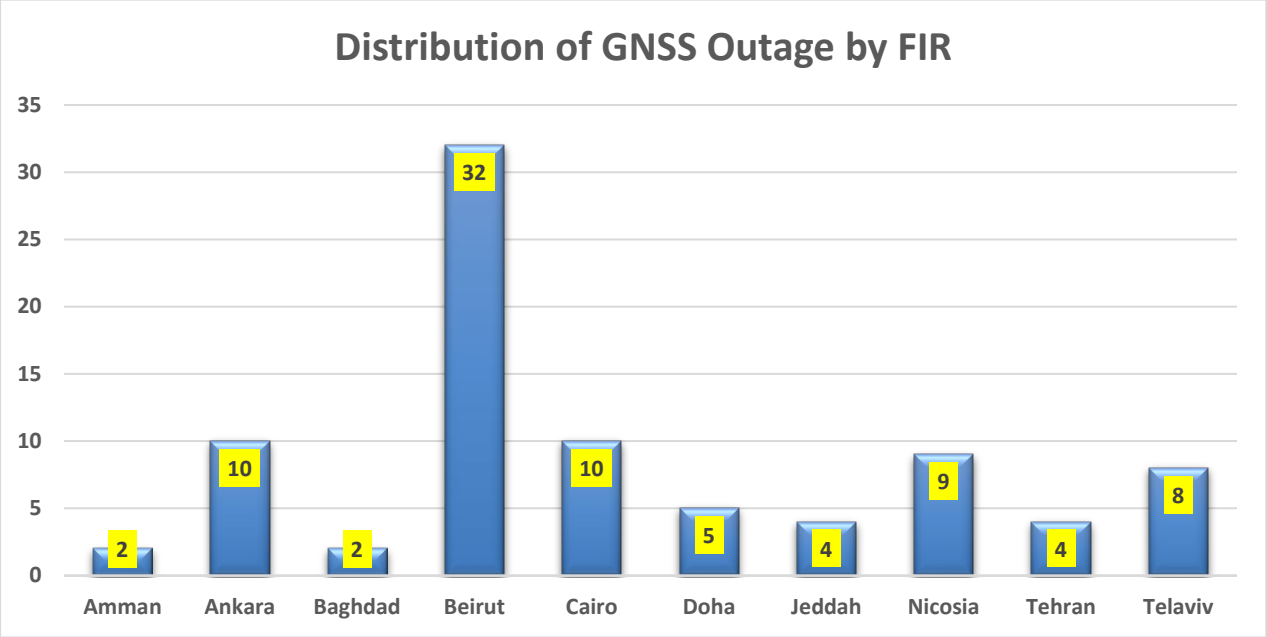
Threat	Initial Risk			Existing controls	Accept/Reduce	Recommended controls	Residual Risk		
	L	C	R				L	C	R
Between 5 and 50 years (short time GNSS Outage)	5	5	D	-Error message notification by avionic -Regulations/ law to protect the GNSS signal	Accept	-			

Table B8: Example risk assessment for enroute phase of flight

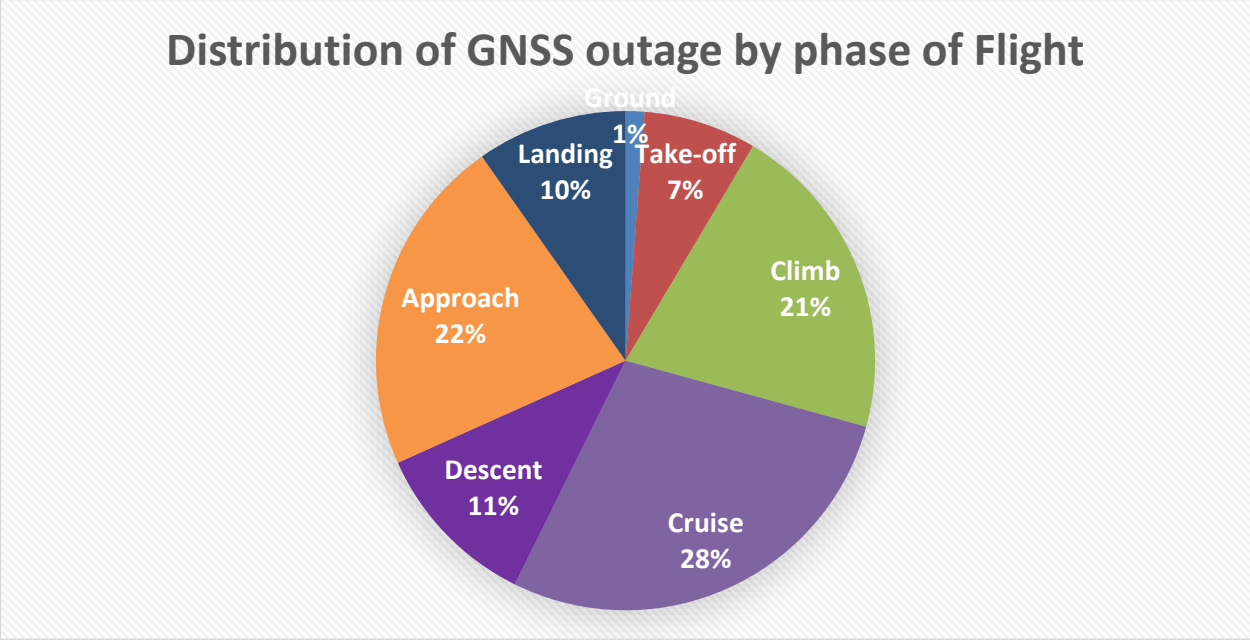
Appendix C

GNSS Anomaly for the Period January 2015- June2018

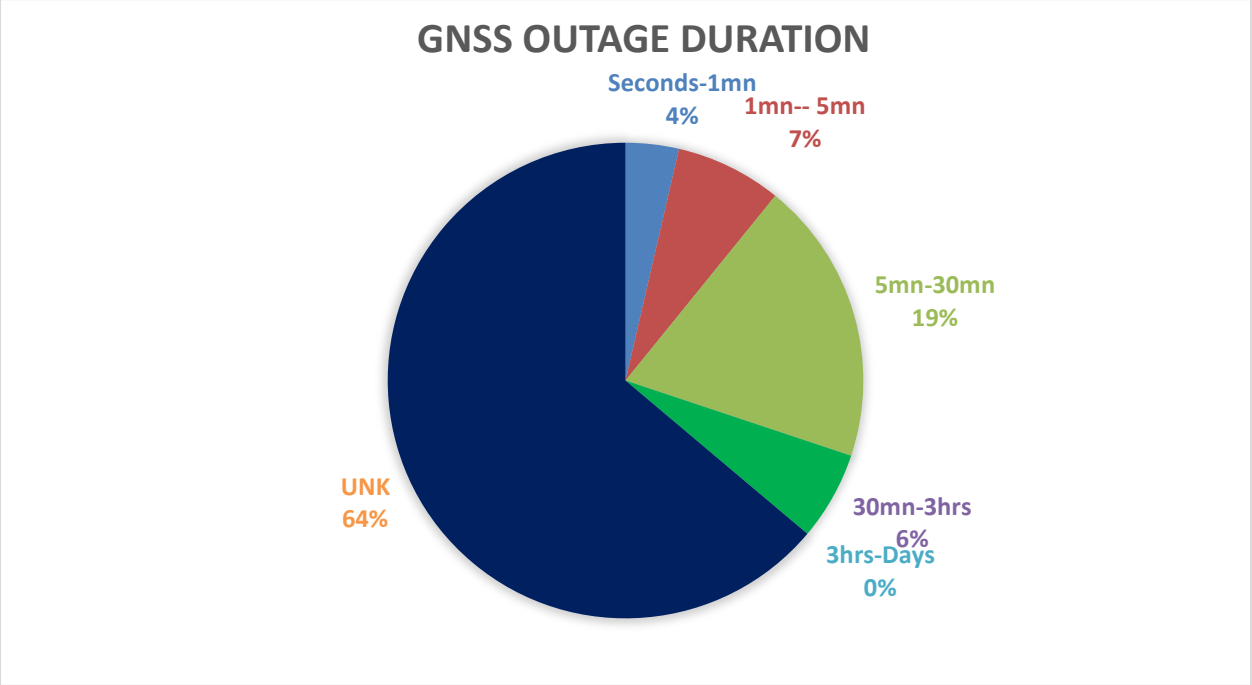
Brief data analysis of the incidents reported during Brief data analysis of the incidents reported by Air Operator is as follows:



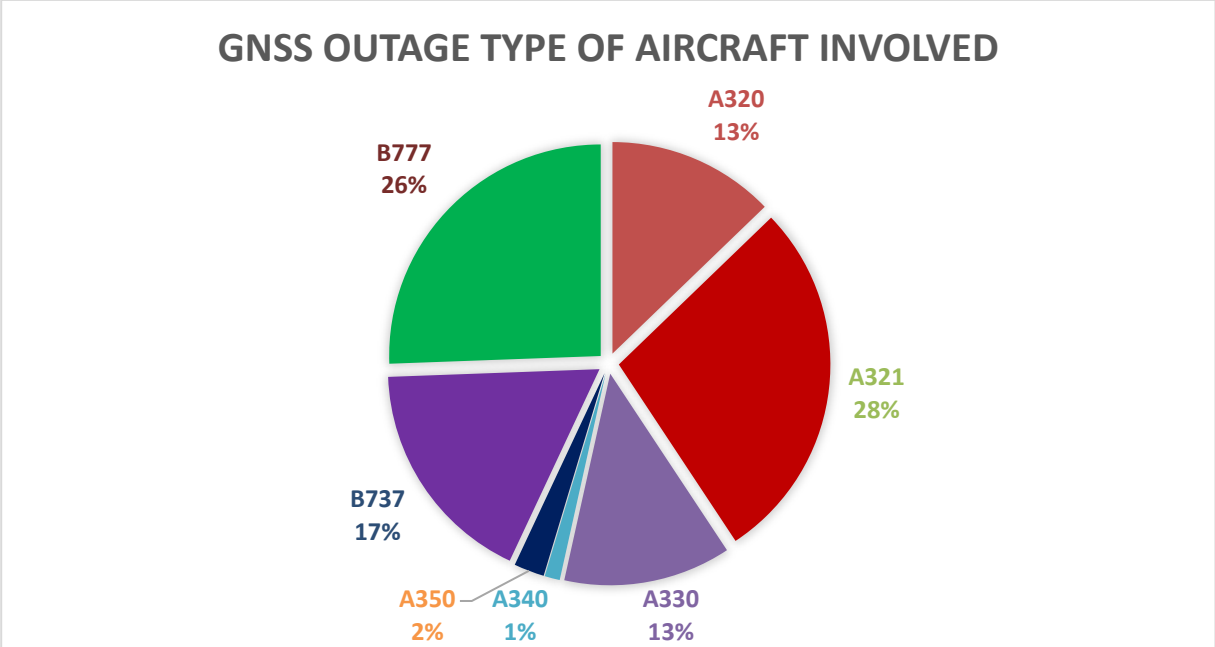
The data revealed that the most significant Flight Information Regions (FIRs) affected Beirut, followed by Cairo, Ankara, and Nicosia.



The data shows that the highest GNSS Outage occurred during the phase of flights cruise, approach, climb, and descent.



The data shows the highest GNSS outage duration was between 5 minutes- 30 minutes. Regarding the Unknown (UNK) it could not be determined as the data was not provided.



The A321, B777, and B737 were most flown aircraft type in areas most affected.

- END -