International Civil Aviation Organization

RASG-MID Steering Committee

Sixth Meeting (RSC/6)
(Cairo, Egypt, 25 – 27 June 2018)

Agenda Item 4: Coordination between RASG-MID and MIDANPIRG

RSA ON GNSS VULNERABILTIES

(Presented by the Secretariat)

SUMMARY

This paper presents a Draft RASG-MID Safety Advisory on GNSS Vulnerabilities.

Action by the meeting is at paragraph 3.

REFERENCES

- CNS SG/8 Report
- MIDANPIRG/16 Report
- RASG-MID/6 Report

1. INTRODUCTION

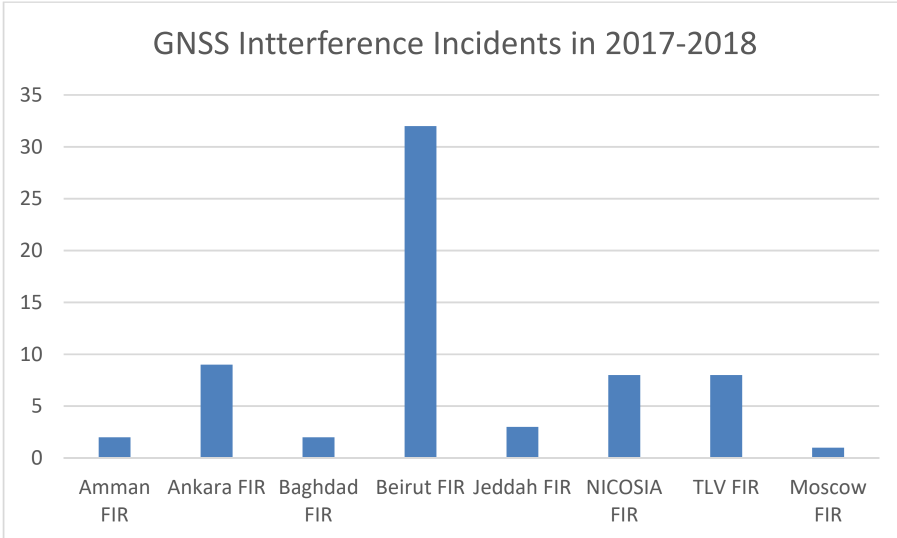
1.1 The Sixteenth meeting of MIDANPIRG (MIDAPIRG/16) was held in Kuwait, 13-16 February 2017.

1.2 The ACAC/ICAO Joint Workshop on GNSS was held in Rabat, Morocco, 7-8 November 2017. The Workshop addressed the GNSS vulnerabilities and recommended implementation of realistic and effective mitigation strategies to ensure the safety and regularity of air services.

2. DISCUSSION

2.1 The Sixteenth meeting of MIDANPIRG (MIDANPIRG/16) recognized the impact of the GNSS signal interference and vulnerabilities and agreed that as a first step it is needed to gather data on actual interference causes and users were also requested to collect data from pilots using the reporting form adopted by the meeting.

2.2 Sixty-five (65) interference incidents have been reported by users in 2017 and 2018 as depicted in the following Graph:



2.3 The RASG-MID/6 meeting agreed that IATA and ICAO MID Office to develop a RASG-MID Safety Advisory (RSA) on GNSS vulnerabilities taking into consideration the outcome of the ACAC/ICAO Workshop.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) review and amend, as deemed necessary, the Draft Safety Advisory at **Appendix A**; and

b) endorse the following Draft Conclusion:

DRAFT CONCLUSION 6/X: RSA ON GNSS VULNERABILITIES

That, States and stakeholders are invited to review the Draft Safety Advisory at Appendix A; and provide comments/inputs to the ICAO MID Office before 15 September 2018, in order to consolidated the Final version for endorsement by the RASG-MID/7 meeting.

RASG-MID SAFETY ADVISORY – 14

(RSA-14)

June 2018

MID-Region

GUIDANCE MATERIAL REALTED TO GNSS VULNRABILTIES

Date of Issue:	June 2018
Revision	Version 1.0
Document Ref. No.:	

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

GNSS VULNERABILITIES

1. INTRODUCTION

GNSS Vulnerability has been identified as a safety issue by the Sixth Meeting of the Middle East Regional Aviation Safety Group (RASG-MID/6) (Bahrain, 26 – 28 September 2017).

The Sixteenth meeting of MIDANPIRG (MIDANPIRG/16) recognized the impact of the GNSS signal interference and vulnerabilities and agreed that, as a first step, it is needed to gather data on actual interference causes and users were also requested to collect data from pilots.

With the increasing dependence on GNSS, it is important that GNSS vulnerabilities are properly addressed. This Safety Advisory is addressing this need through the development of Regional monitoring and reporting procedures, and identification of a clear set of mitigation measures that States should deploy to minimize the GNSS vulnerabilities operational and safety impact.

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 GPS for area navigation and precision approach. Aircraft avionics such as the Flight Management Systems (FMS) require GPS 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 GPS timing data. At the same time, GNSS vulnerabilities are being exposed and threats to denial of GNSS services are increasing.

GNSS signal vulnerabilities caused by threats like radio frequency interference, space weather induced ionospheric interference, multipath, 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.

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. More information about the GNSS Vulnerabilities can be found in MID DOC 0X – The Guidance on GNSS implementation in the MID Region.

3. 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. MONITORING

The success of many of countermeasures mentioned in (3) 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 - both in terms of types of threat and number of threats – it is necessary to monitor the threat environment and the impact on performance.

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

Its recommended that States deploy 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.

5. RISK ASSESSMENT AND MITIGATION STRATEGIES

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 or a safety impact.

The following are examples of reported impact of the GNSS interference on Aircraft Operations in the MID Region (2016 – 2018):

- Loss of GPS1 (fault)/ Loss of GPS2 (fault)
- Observation of “Map shift” on Navigation display
- Switching to an alternative navigation mode (IRS displayed, VOR/DME)
- Degraded PBN Capability (NAV Unable RNP)
- GPS POS Disagree

The following example is to assess the risk of the GNSS outage. For this purpose, three situations are considered:

1- Momentary Outage: A single, very short-term, limited breadth GNSS outage (on the order of seconds or a minute)
2- Serious Outage: a single, moderate length, limited breadth GPS outage (on the order of minutes or hours, over a confined region)
3- Severe Outage: a long-term, wide breadth GPS outage (on the order of days over wide areas or a series of moderate length outage over a wide area).

Situation (Disruption)	Likelihood	Impact				Assumption
		En-route	Terminal	NPA	PA	
Momentary	Known to occur (4)	negligible	negligible	Moderate (could result in missed approach)	Moderate (could result in missed approach)	There is timely detection and alerting
Serious	Could occur (3)	Minor	Minor	Major	Major	Controller vectoring of Aircraft in en-route and terminal areas.
Severe	Not Likely to occur* (2)	Major	Major	Major	Major	Vectoring Aircraft result in excessive controller workload due to long time outage

**A severe outage is considered to be an extremely unlikely event, probably only encountered in such situations as major military conflicts or solar effect.*

Mitigation Strategies

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 procedures and processes to enable operations or define a fall-back 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 and the availability of radar;
- the avionics in aircraft using the airspace (e.g. most aircraft in high-level airspace will have IRS and/or DME/DME updating of navigation systems);
- 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 aircraft route spacing and/or separation in the airspace under consideration.

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

Application	Alternative Conventional Navigational Aid
En-route Airspace	DME/DME VOR/DME
Terminal Airspace	DME/DME
Precision approach	ILS
Non Precision Approach	IRS DME/DME VOR/DME

Depending on the threat assessment, traffic levels and weather conditions, an ANS provider might find it appropriate to retain some or all of the existing ILS operations at an airport or within an area under consideration.

The regulator should conduct safety oversight of the service provider’s GNSS based Services and validate the safety aspects of mitigation strategies.

6. REPORTING

State ANS providers have the responsibility to report the status of air navigation services. If the status of a service changes or is predicted to change, users should be notified via direct communications from ATS and/or via a NOTAM or aeronautical information system (PANS-ATM ICAO DOC 4444).

ANSP must be prepared to act when anomaly reports from aircraft or ground-based units suggestsignal 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 (xxxxxxx@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) broadcasting the anomaly report to other aircraft, as necessary; and
c) 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.

References:

- Annex 10 Aeronautical Telecommunications, Volume I ─ Radio Navigation Aids
- Annex 11 Air Traffic Services
- PANS-ATM, ICAO doc 4444
- 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.

APPENDIX A

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

Note: Only applicable fields need to be filled!

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:	
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 [ ] 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 [ ] During the arrival in Beirut we had GPS invalid alert message. After landing both GPS receivers recover. It is something that happens lately in Nicosia FIR. Has nothing to do with a failure but rather with some military presence nearby. It happened again departing from Beirut it lasted 20 minutes and as we approach, Cairo FIR came back to normal.
Problem duration:	[ ] continuous for 20 minutes [ ] intermittent

- END -