REPUBLIC of SAN MARINO
CIVIL AVIATION AUTHORITY

Via Consiglio dei Sessanta, 99
47891 Dogana
Republic of San Marino
TEL: +378 (0549) 882929 | FAX: +378 (0549) 882928

SAFETY NOTICE No. 02/2024 Issue 01

GNSS SIGNAL DISRUPTION

Related: See Safety Notices No. 02/2023 Issue 01 & No. 01/2024 Issue 01

Introduction

GNSS Signal Disruption generally refers to GPS Jamming or Spoofing attacks. GPS Spoofing has become more frequent in recent years and may be related to ongoing conflicts around the world. The increased frequency has been highlighted by international aviation safety organisations and operators have been encouraged to take precautions. There have been reports of spoofing attacks on San Marino operators and some attacks may remain unreported. This safety notice outlines the issues and encourages operators to consider their resilience to such attacks.

What is Spoofing?

GPS spoofing refers to the deliberate alteration of a GPS signal for the purpose of sending incorrect position information to an aircraft (or another receiver). The equipment will not register a failure or absence of the GPS signal because, although incorrect, a signal is still being received. Therefore, it is more difficult to detect than GPS jamming which normally causes a sudden loss or degradation in GPS signal and would typically trigger alerts. This could also result in IRS failure rapidly after an attack. However, spoofing may go unnoticed for some time, as the signal may appear genuine and would not normally trigger alerts. For this reason, it may be considered more problematic than GPS jamming, although this also continues to be used.

How Can Spoofing be Detected?

Pilots cannot rely on GPS signal alerts and may need to consider how best to detect GPS spoofing, perhaps involving detailed monitoring and cross-checking with other navigation sources, unexpected flight behaviour, or discrepancies between expected and actual positions as indicated by visual references or ATC communications.

Why is Spoofing a Hazard?

Spoofing is a hazard to aircraft since it may cause pilots to believe incorrect position information and may also disrupt timing information. This may contribute to a number of difficulties, for example, loss of Situational Awareness, flight path deviations or navigation errors causing the pilot to use incorrect Minimum Safe Altitude (MSA) and conflict with obstacles or terrain, unintentionally contravene Air Traffic instructions

and conflict with other aircraft (especially in congested airspace or during critical phases of flight), misalign with ILS, burn more fuel than planned or arrive later than scheduled time. GPS spoofing may also affect factors other than position information; it may also affect timing/ velocity, autopilot and flight management systems (potentially causing unintended manoeuvres), and is often accompanied by disruption of communication frequencies, creating further issues for pilots. It may create security issues if the aircraft unintentionally enters restricted airspace or conflict zones. Finally, it may have financial implications if there are flight delays / diversions / liability issues.

What Should Operators Do?

Operators are encouraged to consider the possibility of a GPS spoofing attack (or jamming) and how they should prepare for it. Considerations could include (but are not limited to) actions such as, for example:

1. Familiarise yourself with guidance on the subject from international safety organisations such as EASA (SIB No.: 2022-02R2; SIB No.:2023-03) UKCAA (SN-2023/001) and FAA (SAFO 24002), and ICAO data on frequently targeted locations such as Turkey, Eastern Europe, Middle East and North Africa (MENA States).

2. Attention to relevant NOTAMs, especially for these regions.

3. Review the aircraft manufacturer's guidance for that specific aircraft type and avionics.

4. Sustained awareness of the issue and related technology developments; ensure crews remain aware and vigilant; if practicable, consider anti-spoofing technologies.

5. Cross checks between GPS and different sources of navigation data such as inertial navigation systems (INS), DME (Distance Measuring Equipment), VOR (VHF Omni-directional Range), and radar. Discrepancies between GPS data and other sources may indicate potential spoofing.

6. Inform ATC, they need to know and may be able to assist.

7. Standard Operating Procedures (SOPs) for proceeding when GPS is considered absent or unreliable (and could even be malicious / misleading).

8. Refresh pre-GPS skills such as conventional instrument flight procedures, visual navigation and dead reckoning.

9. Include spoofing in your crew briefings and training scenarios to include such items as refreshing operations without GPS, failure of the IRS, unreliable AHRS, use of VOR/DME for navigation, realigning/updating the FMS following a failure.

10. ALWAYS Report the incident, it is a Mandatory Occurrence Report (MOR) and it is important for the CAA to know how often and where this occurs.

REPUBLIC of SAN MARINO
CIVIL AVIATION AUTHORITY

Conclusions

GPS Spoofing is a hazard to aviation, and events have been reported by San Marino Operators. We are also aware of some spoofing events that were not reported, and we would urge all Operators and pilots to be active and ensure any GPS disruption is reported to the CAA.

We would also encourage all of our Operators to consider how well prepared you are for a potential spoofing attack. Please do conduct your own research and implement such measures as you believe to be appropriate. Finally, if you have previously experienced spoofing or jamming but did not report at the time, please do report it now as an MOR.

Eng. Marco Conti

Director General

8th February 2024

Digitally signed by:
MARCO CONTI
Date: 12/02/2024
16:23:10