SAFETY INFORMATION	АВИАЦИОННАЯ АДМИНИСТРАЦИЯ КАЗАХСТАНА
MITIGATION OF CONSEQUENCES OF FAILURES IN GPS / GNSS	
Date: 17.02.2025	№: GNSS 2024-0001
Flight Operations, ATM/ANS, AAK	Revision: **01**

1. PURPOSE

This safety information has been published in order to recognize and mitigate the consequences of failures in the Global Positioning System (GPS) / Global Navigation Satellite System (GNSS).

2. BACKGROUND

Recent GPS/GNSS jamming and spoofing activities reported by civil air operators operating globally pose a potential safety of flight risk to civil aviation. GPS/GNSS disruptions often occur in and around conflict zones, military operations areas, and areas of counter unmanned aircraft systems (UAS) protection. The term GNSS includes satellite augmentation systems. Jamming and spoofing incidents may pose increased flight safety risks due to possible loss of situational awareness and increased pilot and regional Air Traffic Control (ATC) workload issues.

An analysis of the reports received by the Aviation Administration of Kazakhstan (*hereinafter AAK*) through the system of mandatory and voluntary reporting shows that the number of reports of a temporary loss or degradation of the quality of the GPS signal has a 772% increase compared to 2023:

- 12 months of 2023 – 32 reports
- 12 months of 2024 – 247 reports.

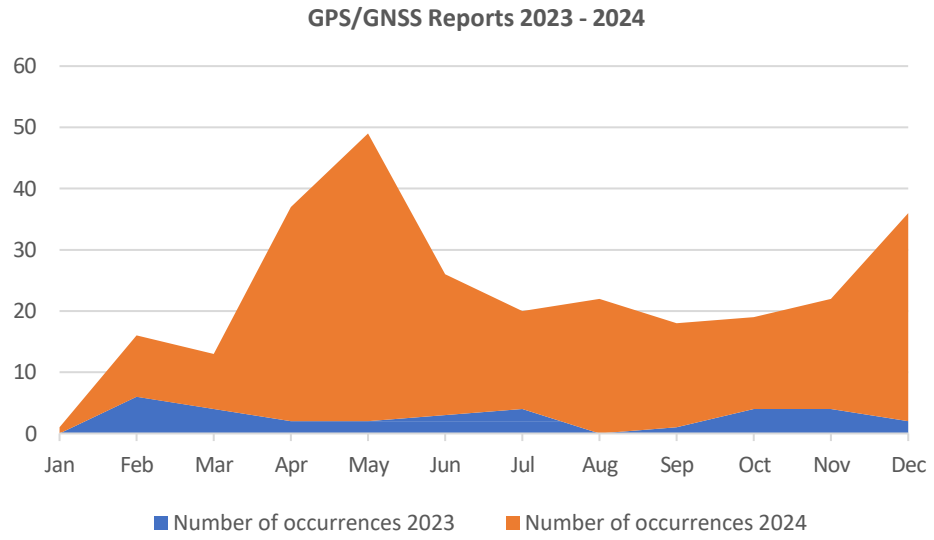

Figure 1. Reports distribution by year

According to the final report of the GPS Spoofing Workgroup, published in September 2024, the number of reported spoofing during three quarters of 2024 had increased by 500%, while the peak in the growth of reports in the Republic of Kazakhstan correlates with the statistics published in the report.

Further analysis of reported GPS/GNSS signal loss or instability showed that in Kazakhstan, 11.11% of events occurred during takeoff or climb, 25.10% during landing, 62.96% enroute and 0.82% during towing operation.

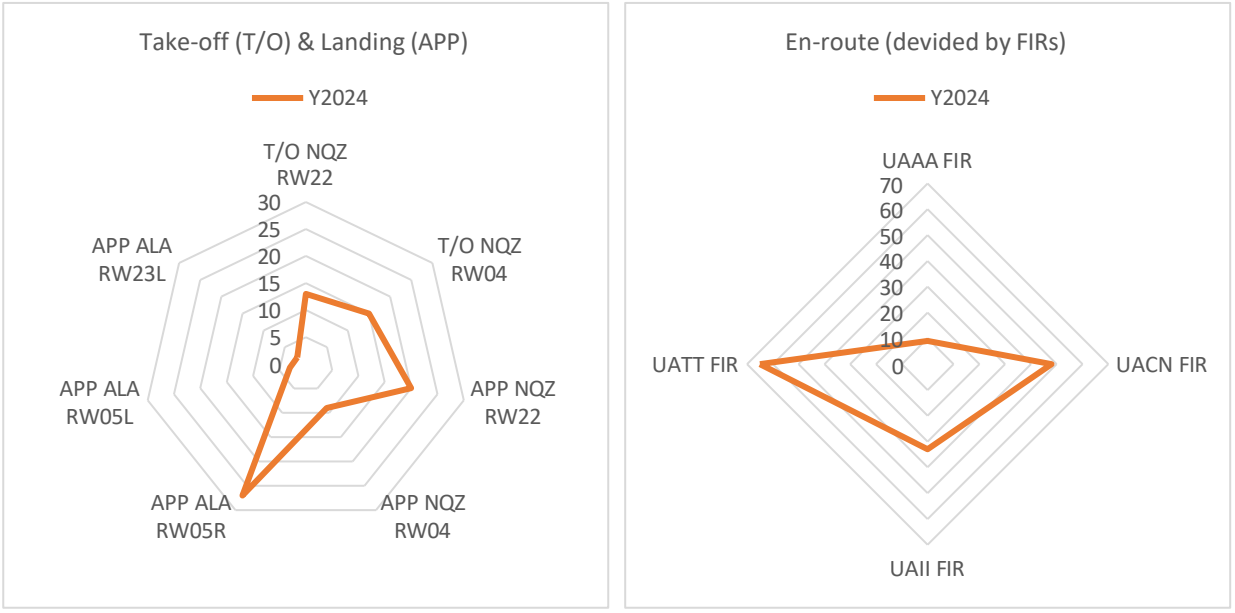

Figure 2. GPS/GNSS reports distribution by aerodromes & FIRs

Operators should be aware of the impact on the specific on-board systems of the operator's aircraft and consider it during risk assessment. Information on the general effects of GPS/GNSS interference, jamming, and spoofing is provided in section 4. GPS SPOOFING IMPACT MATRIX

3. RECOMMENDED ACTIONS

ATM/ANS providers should:

- Establish a process to collect information on GNSS degradations, in coordination with the relevant CAAs, National Telecommunications Authorities, and promptly notify the related outcomes to air operators and to other airspace users;
- Assess the impact of loss or anomalies of GNSS-based timing on CNS systems;
- Issue NOTAMs to provide relevant information to airspace users (as appropriate and determined at State level);
- Provide reliable surveillance coverage that is resilient to GNSS interference, as well as maintain essential conventional navigation infrastructure operational (Instrument Landing Systems, Distance Measuring Equipment (DME), Very High Frequency omnidirectional range (VOR) in support of conventional navigation procedures;
- Ensure that their contingency plans include procedures to be followed in case of large-scale GNSS jamming and/or spoofing events;
- Monitor the traffic closely to prevent any deviation from the flight track/route

Air operators should:

- Ensure that flight crews are aware of and trained on the importance of prompt reporting to air traffic services of any observed interruption, degradation or anomalous performance of GNSS equipment or related avionics (e.g. map shifts, suspected GNSS spoofing, position and duration of the GNSS interference);
- Evaluate different possible scenarios based on the type of operations in order to provide the flight crew with timely information to increase awareness of jamming and spoofing;

- Ensure that GNSS outage or spoofing topic is included in the flight crew ground recurrent training, highlighting the identified operational scenarios to recognize, react in a timely manner to different jamming and spoofing cases;
- Assess operational risks and limitations linked to the loss of on-board GNSS capability, including any on-board systems requiring inputs from a reliable GNSS signal;
- Ensure that operational limitations introduced by the dispatch of aircraft with inoperative radio navigation systems in accordance with the Minimum Equipment List, are considered before operating an aircraft in the affected areas;
- Ensure, in the flight planning and execution phase, the availability of alternative conventional arrival and approach procedures (e.g. an aerodrome in the affected area with only GNSS, including augmentation, approach procedures should not be considered as destination or alternate);
- If subject to FDM requirements and necessary data are available, use FDM programme to identify and assess GNSS spoofing events;
- Concerning spoofing: contact aircraft or equipment manufacturers for instructions on how to deal with spoofing cases of their products and implement the recommendations in the Standard Operating Procedures

GNSS jamming specific recommendations for Air operators:

Ensure that flight crews and relevant flight operations personnel:

- are aware of possible GNSS jamming;
- verify the aircraft position by means of conventional navigation aids when flights are operated in proximity to the affected areas;
- check that the navigation aids critical to the operation for the intended route and approach are available;
- remain prepared to revert to a non-GNSS arrival procedure where appropriate and inform air traffic services in such a case; and
- report to air traffic services any observed irregularities GNSS

GNSS spoofing specific recommendations for Air operators:

Ensure that flight crews and relevant flight operations personnel:

- are aware of possible GNSS spoofing;
- continuously monitor aircraft position using non-GNSS navaids and all available automatic navigation accuracy calculations, including the Estimated Position Uncertainty (EPU) figures;
- Monitor the GNSS time versus non-GNSS time sources;
- Closely monitor the ATC Frequencies in the vicinity of spoofing area;
- Apply the manufacturer's instructions for the aircraft type on dealing with suspected spoofing, non-exhaustive list of examples of possible instructions could be such as:

1. being ready to select HDG mode and manually adjust the flight course.
2. being ready to ask for verification vector from ATC as long as needed.
3. being ready to crosscheck with and switch to alternate PNT such as IRS and/or available ground facilities (Multi-DME and VOR/DME).
4. being ready to exclude the GNSS signals within affected area.
5. being ready to disable automatic INS/IRS updating.

- report to air traffic services any observed irregularities

All parties concerned are reminded of their obligations to report any event impacting safety!

Mandatory Reporting System

Voluntary reporting system

4. GPS SPOOFING IMPACT MATRIX

Spoofing effect	**Aircraft Handling** *Flight Crew*	**ANSP/ATC** *Air Traffic Controller*	**Operational** *Aircraft Operator*
GPS receiver failure	*Impacts other systems* - May appear recovered but still contaminated	- AOG if receiver becomes 'bricked*' (NVM corrupted) - Repair time days or weeks COST	GPS receiver failure
FMS position degraded or failed	- Undetected off-track navigation - Loss of situational awareness - Unplanned entry into Danger Area, other FIR's	- Lateral loss of separation - Vectoring (often many aircraft) - increased workload	- Potential Accident/Incident RISK
Unable RNP	- Restricted to conventional enroute navigation and approaches - Unable RNP SID/STAR Reduced Oxygen Escape route options-	- RNP-4 or better based separation not available e.g., North Atlantic - RNP App/SID/STAR not useable – Increased vectoring for initial approach	- Potential diversion COST
Map Shift	- Wrong runway selection Loss of situational awareness	- Loss of separation during landing Risk of landing on closed runway	- Potential Accident/Incident RISK
IRS	- Hybrid IRS may - cause false FMS position or failure	-	
GPWS	- False EGPWS alerts - Startle effect - Lowered trust in GPWS system overall - Delayed responses - Go-around from unusual altitude/ position - Nuisance alerts cause stress, distraction - Risk of response in low energy aircraft state, stall.	- Level busts - loss of separation due to unexpected EGPWS response maneuver.	- Potential Accident/Incident - Passenger injury RISK

Spoofing effect	**Aircraft Handling** *Flight Crew*	**ANSP/ATC** *Air Traffic Controller*	**Operational** *Aircraft Operator*
Weather Radar	- May impact ability to detect Cb - Ground clutter function not available		- Potential flight into convective activity - Passenger injury RISK
Aircraft Clock	- Incorrect time displayed on clock - Incorrect time fed to other systems		
Datalink (ADS-C, CPDLC)	- CPDLC not available, switch to voice (VHF, HF) - ADS-C not available - Oceanic RCP/RSP cannot be met, PBCS tracks not avail - Reroutes or lower levels can be expected	European capacity constraints due to overuse of VHF - Oceanic PBCS separation not available	- Reroute - Diversion - Lower level, higher fuel burn COST
ADS-B	- Unable to fly in ADS-B required airspace	- ADS-B only airspace not available - ADS-B based separation not available - Risk of incorrect ADS-B based position on screen	- Reroute - Cancellation COST
HUD&SVS	- HUD must be stowed - SVS not available - -Degraded situational awareness		
ELT	- Potential for incorrect aircraft position - broadcast in emergency	- SAR may receive incorrect aircraft position	- SAR in wrong location RISK
RAAS (Runway)	- Unavailable, or may give false warning		- Potential Accident/Incident RISK
ROPS (Runway)	- Unavailable, or may give false warning		- Potential Accident/Incident RISK
SATCOM	- May be unavailable		
EFB	- Some applications use GPS position and will not work correctly (e.g., moving map) Situation awareness degraded		
Internet/Wi-Fi	- - Some reports of Wi-Fi not working correctl		- Pax inconvenience

Spoofing effect	**Aircraft Handling** *Flight Crew*	**ANSP/ATC** *Air Traffic Controller*	**Operational** *Aircraft Operator*
Overall: Complexity of multiple interconnected failures	- Complex go-arounds with multiple failures - Emergency margin of safety reduced		- Potential Accident/Incident RISK - Diversion COST

**"Bricked" device is an electronic device that is no longer functional due to corrupted firmware, a hardware problem, or other damage.*