Proceeding Paper

Mitigating GPS Spoofing Threats with Honeywell GPS Aided Inertial Systems †

Matej Kucera[1,*], Radek Reznicek[1], Radek Baranek[1], Pavel Ptacek[1], Daniel Bertrand[2] and Karl Keyzer[2]

[1] Honeywell International, Turanka 100, 627 00, Brno, Czech Republic;
[2] Honeywell International, 2600 Ridgway Pkwy, Minneapolis, MN 55413, USA;
* Correspondence: matej.kucera@honeywell.com
† Presented at European Navigation Conference, ESA ESTEC, Noordwijk, The Netherlands, 22-24 May 2024.

Abstract: GNSS-Inertial integration brings great potential to detect and mitigate the effect of erroneous (spoofed) GNSS data. When a trajectory of an airplane diverges from (or is inconsistent with) inertial data, the integrated system may detect this erroneous GNSS trajectory and may be able to maintain navigation integrity by rejecting this data. GNSS Aided Inertial System can provide both self-contained detection of a GNSS spoofing event as well as mitigation, where mitigation is hard to achieve globally with other commercial aviation systems relying on good ground system coverage. This paper provides an overview of the newly developed Inertial Spoofing Monitor for aviation grade navigation systems, which was designed to detect multiple simultaneous erroneous (spoofed) satellite measurements. The Inertial Spoofing Monitor was then thoroughly tested, and simulations were performed to evaluate and demonstrate the detection, mitigation, and recovery capability of the spoofing monitor. The performance validation followed the process prescribed by Appendix Q of the RTCA DO-384 MOPS (Minimum Operation Performance Standard). The results show great detection, mitigation, and recovery performance of the developed Inertial Spoofing Monitor, but also indicate constraints regarding the assumed sensor error model.

Keywords: GNSS; Spoofing; Inertial; Aviation

Citation: Kucera, M.; Reznicek, R.; Baranek, R.; Ptacek, P.; Bertrand, D.; Keyzer, K. Mitigating GPS Spoofing Threats with Honeywell GPS Aided Inertial Systems.

Academic Editor: Terry Moore

1. Introduction

Today, Jamming and Spoofing events are more and more prevalent across the globe and can significantly impact the avionics and navigation systems in many ways. This can result in disrupting aircraft operation during all phases of flight including departure, en-route, approach, and landing. Therefore, it is necessary to raise the awareness of these challenges and provide reliable protection to the avionics systems against these threats.

Modern IRS/AHRS output tightly integrated Inertial/GPS hybrid navigation parameters. These highly valuable hybrid parameters may be used by Flight Management Systems on Air Transport and Business Aviation aircraft because they provide better accuracy than pure inertial parameters and better integrity, availability, and continuity than pure GPS. Specifically, hybrid parameters are protected from GPS satellite faults or GPS multi-path with Horizontal Protection Limits and Vertical Protection Limits. Furthermore, in case of loss of GPS, the Inertial-Aided systems continues to output valid and protected hybrid parameters with excellent accuracy.

In order to further improve the resilience of hybrid parameters to GPS Spoofing, new algorithms for jamming and spoofing protection were developed and implemented as part of the Clean Sky 2 Deck program – the Inertial Spoofing Monitor. The performance of these algorithms was assessed based on their detection, mitigation, and recovery capabilities.

2. The Honeywell AH-2000 Attitude And Heading Reference System (AHRS)

Inertial systems are the heart of any aircraft. They feed almost every flight-critical avionics system, including flight controls, displays, flight management, heads-up displays, and radars.

Honeywell's AH-2000 is a next-generation, GPS-Aided Micro Electromechanical (MEMS) Attitude and Heading Reference System (AHRS) designed to provide unparallel accuracy and reliability, along with reduces size and weight compared to similar systems.

The AH-2000 provides inertial reference unit-like performance when GPS signals are available. It provides GPS/INS (Inertial Navigation System) hybridized outputs with integrity monitoring, producing the accuracy and stability needed to support advanced avionics like synthetic vision systems, enhanced/combined vision systems and heads-up displays. The AH-2000's performance and high levels of safety assurance are critical to fly-by-wire aircraft and autonomous system operation.

3. Inertial Spoofing Monitor

The GNSS (Global Navigation Satellite System) inertial integration offers the great potential to detect and mitigate the effects of erroneous GNSS data. When the GNSS trajectory diverges from, or is inconsistent with inertial data, the integrated system may detect this erroneous (or alternate – spoofed) GNSS trajectory and may be able to maintain navigational integrity by rejecting this data.

A GNSS Aided Inertial System based solution is very useful for detection of all jamming and spoofing threats (J1 – S7, classification according to [1]) where the GNSS and Inertial Measurement information is inconsistent. It can also provide mitigation by coasting on the inertial position while the GNSS signals are unavailable or declared/suspected to be under a threat.

In general, GNSS and INS can be coupled using a variety of integration schemes. These can range from the simple loosely coupled integration, to the complex ultra-tightly coupled mode in which the INS directly aids the GNSS tracking loops. Within the Honeywell's AH-2000 GNSS aided AHRS (GPAHRS) algorithm, a nominal tightly coupled integration is implemented. It is considered the most widely used implementation for integrated GNSS-INS systems in aviation. As such, the Inertial Spoofing Monitor described here operates continuously and can be implemented directly on top of any tightly coupled GNSS-INS system. However, the concept introduced here is transferable to other types of integration as well.

If spoofing or jamming can be (reliably) detected, a GNSS aided inertial system (hybrid) would stop using the GNSS measurements and start coasting, thus providing mitigation. The error bounds (FOM – Figure of Merit, HPL – Horizontal Protection Level etc.) would grow at a rate reflecting the inertial sensor performance. If the end of jamming or spoofing is detected the GNSS aided inertial system would start using the GNSS measurements and recover (if within linear range of navigation error model). The important advantage is that there is no loss of function (guaranteed continuity in presence of jamming and spoofing).

3.1. Mechanization of Spoofing Monitor in GNSS Aided Inertial System

Erroneous GNSS spoofing signals may be self-consistent, meaning the GNSS receiver-based techniques (such as RAIM or ARAIM – Receiver Autonomous Integrity Monitoring) are not able detect or exclude false GNSS information by themselves. So, for the purpose of GNSS inertial integration, it can be assumed that the GNSS data, as received from the GNSS receiver and used by the integration, are flagged as valid and provides a self-consistent set of measurements reflecting a trajectory that deviates from truth (in case of spoofing). This means that methods that exploit the additional observability of inertial integration will need to be relied upon, for example, through pre-residual (innovation) or post-residual screening. The impact of the difference in the

dynamics of the true trajectory and the alternate spoofing trajectory will be seen as a transient in the measurement residuals or innovations with a magnitude and a duration that are a function of the inertial sensor stability. The measurements will follow the trajectory change according their individual line of sight paths and this will cause residual to differ in size between the satellites.

Estimation algorithms (Kalman filters) weigh the value of the measurements based on the uncertainty in the nominal measurement error versus the uncertainty in the measurement prediction from the integrated solution. If there is a detection that at least one measurement residual is unreasonable for each subset of measurements (wherein each subset excludes one satellite), then we have detected multiple erroneous GNSS measurement and thus can infer that GNSS spoofing may be present. Both pseudorange measurements and carrier-based measurements can be used, the current implementation of the Inertial Monitor considers only the pseudorange measurements.

The sensitivity of the algorithm can be limited by factors such as inertial system accuracies and drift, errors in the lever arms between the inertial system and GNSS antenna, and even airframe bending between the antenna and the inertial system mounting location.

4. Spoofing Threat Definition for GNSS-Inertial Aided Navigation Systems

Spoofing threat categorization for this paper and performance validation is considered according to the DO-384 MOPS focused on GNSS Aided Inertial Systems ([7]), which identify three alternate (i.e., spoofing) trajectories scenarios from impact on position perspective and they are defined as:

1. Position step;
2. Velocity step;
3. Acceleration step.

These test scenarios are used to characterize the system's performance and the validity of the integrity bound under these spoofing conditions.

According to the DO-384 MOPS, the alternate-spoofing trajectory impacts pseudoranges and delta ranges and no other receiver output parameters are assumed to be affected, other than any position or velocity solution from the GNSS receiver, which should be consistent with the pseudoranges and delta range data.

Alternate trajectory signals that match and then diverge from the true aircraft position in a coordinated way may also be well coordinated with true GNSS time, so it can be expected the time associated with the alternative trajectory to be well matched to true GNSS time. That is, if an individual aircraft position can be matched by the alternate trajectory, GNSS time (phase of code at the aircraft location) may be matched equally well.

5. Simulation Framework and Setup

FuseNAV is a Honeywell proprietary simulation toolset part of a larger framework that has been created for algorithm development, Monte Carlo simulations and then transition to prototyping and the target product platform. The FuseNAV simulation toolset is created in MATLAB and Simulink. FuseNAV also consists of strapdown INS based navigation algorithms in the form of Simulink model where different aiding sources can be enabled/disabled, and sensor models are configurable. It has adjustable rates of individual tasks (IMU data integration, measurement update, etc).

For Monte Carlo simulations there is a set of functions for scenario definitions (custom trajectories, world locations, dates, times, etc). It has the ability for parallel simulation computations as well as parallel post-processing of the simulation results and automated report generation.

It has the capability to deploy designed algorithms to real time platforms (National Instruments cRIO, Honeywell AH-2000 and potentially any OS) thanks to C code generation and platform compilation.

5.1. Simulation setup

The FuseNav simulation framework was updated to be able to host the algorithm of the Inertial Spoofing Monitor and to be able to execute the performance validation simulations according to DO-384 Appendix Q [7]. As described in Appendix Q, the testing trajectory is required to have some initial procedure (taxi, take-off, turns, …), normal operation segment as a straight and level flight for at least 1 hour, then GPS outage for 1 – 10 sec, exposure segment for 5 – 60 min, GPS outage for 1 – 10 sec, recovery phase up to 60 minutes and post-recovery phase. The sequence of all testing trajectory segments is shown on Figure 1. The prescribed GPS outage period by standard is not considered fully realistic and representative of currently observed Jamming and Spoofing attacks. During the internal simulation validations, the prolonged outage periods were tested as well to examine the performance of Inertial Spoofing Monitor. These simulations go beyond the scope defined by MOPS, but it was determined that the Inertial Spoofing Monitor is in general capable to detect spoofing even after long GPS signal outages with high dependency on consider inertial sensor models.

Figure 1. Sequence of testing trajectory segments.

Thanks to the updates to the FuseNAV simulation framework and each simulation configuration, the phase 1 – Initial phase – can be fully configured in terms of duration, speed, height, turns, etc. The other phases 2 – 7 are strictly straight and level flight according to the definition in DO-384 Appendix Q.

The overall view on example simulation trajectory is available on Figure 2.

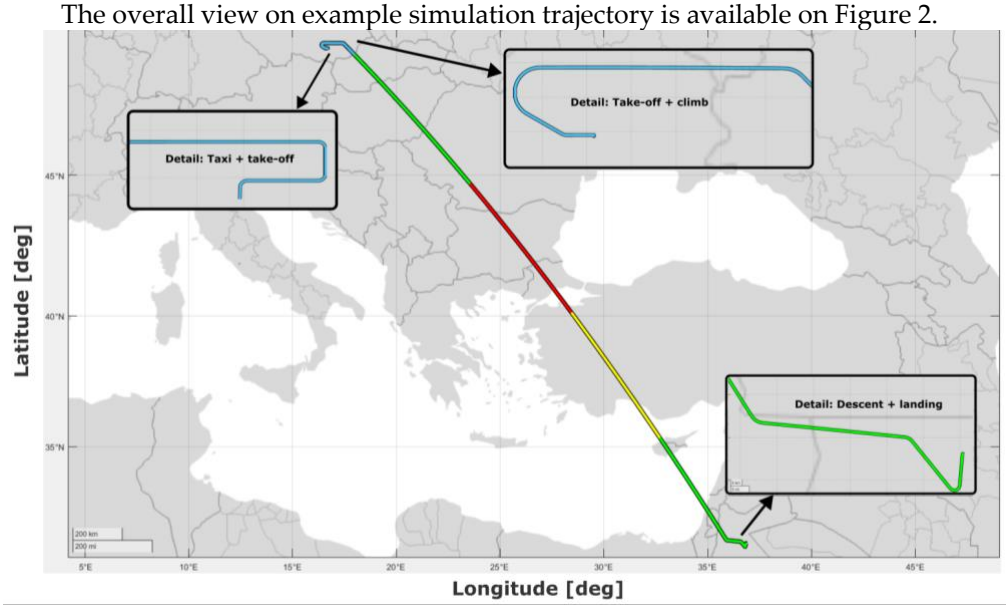

Figure 2. Example of DO-384 Appendix Q trajectory.

The height profile of simulated trajectory is shown in Figure 3.

The above-described trajectory was simulated in the Monte Carlo simulations at 380 locations regularly distributed over the northern hemisphere with random selected initial GPS time of day.

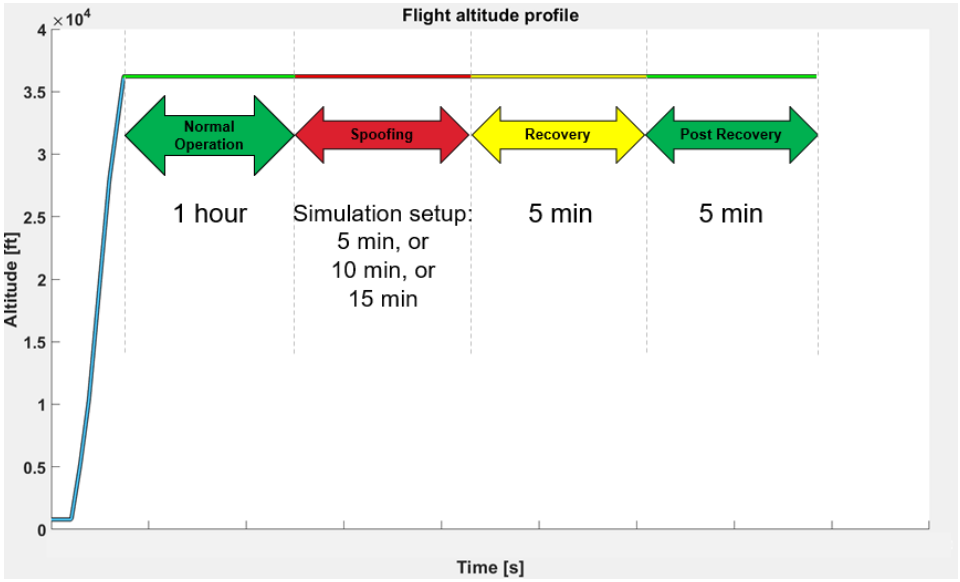

Figure 3. Flight altitude (in tens of thousands of feet) profile with indicated validation segments according to App Q.

5.2. DO-384 Appendix Q testing

The prescribed performance validation logic according to DO-384 Appendix Q [7] was used to evaluate each trial to determine if the trial should be used in the detection and mitigation statistics or whether it should be discarded. If the trial is used, it indicates if the trial should be scored as detected, mitigated and/or recovered.

For prolonged exposure times of alternate trajectory, over time, the coasted solution will no longer be available, but the GNSS aided AHRS system will still be able to provide the GNSS monitoring function for spoofing.

6. Simulation Validations and Results

The summary of results from Monte Carlo simulation Performance Validation testing of Inertial Spoofing Monitor are presented in following sub-sections.

6.1. Position step

First, the outcomes for Position step type of alternate trajectory are provided. It can be considered the easiest spoofing type to detect of the three considered cases defined by DO-384 Appendix Q. Through internal testing, the 0.3 nautical miles position offset was selected as the baseline starting value, which can be reliably detected. In general, the larger the position offset is, the easier it is to positively detect and announce this offset by the detection algorithm. It is worth mentioning the position step is described in Appendix Q as continuous position offset from the nominal true trajectory, and so the position offset moves along the track. Multiple scenarios of the length of exposure times were selected for internal performance validation testing. The shortest exposure segment was defined to 5 minutes, the longest considered exposure segment was 1 hour.

For all simulation scenarios presented within this section a 99% confidence level was considered (according to DO-384). The length of recovery segment was 5 minutes, and the length of post-recovery segment was 5 minutes as well. The AH-2000 sensor model was

considered, and the detection, mitigation and recovery are claimed for all position, velocity and attitude parameters provided by GNSS aided AHRS.

During the development and performance validation testing dozens of MC simulation trials were executed with randomization of several parameters in order to extensively and robustly test the developed spoofing detection and mitigation algorithm. Only a few simulation results are presented in this paper. The results are provided in the form of Claims Table, which is defined again in DO-384 Appendix Q. The performance validation Claims Table example using the Inertial Monitor with the position offset spoofing case is provided in Table 1. Notice that for one testing scenario, one of the simulation trials was discarded from evaluation. There are defined conditions within the Appendix Q under which circumstances a simulation trial shall be discarded. The overall number of simulation trials was selected large enough to accommodate for such events caused by random selection of Worst-Case sensors parameters within the Monte Carlo simulations and sufficiently statistically test the algorithm.

Table 1. Example of Claims Table for Position step performance validation scenarios.

Position Offset	Exposure Time	Detection	Mitigation	Recovery
0.3 nm (555 m)	5 min	3800 trials detected	3799 trials mitigated	3799 trials recovered
3800 valid trials		0 trials not detected	1 trial not mitigated	1 trial not recovered
0.3 nm (555 m)	10 min	3799 trials detected	3799 trials mitigated	3799 trials recovered
3799 valid trials, 1 trial discarded		0 trials not detected	0 trials not mitigated	0 trials not recovered

To further illustrate the detection, mitigation, and recovery capabilities of the developed Inertial Spoofing Monitor, the example of the simulated trajectory during the spoofing exposure is provided in Figure 4. Figure 4 shows the true trajectory (green line), the trajectory estimated by the GNSS aided AHRS algorithm (blue line – under non-spoofing conditions, red line – when spoofing detected) and the offset spoofing trajectory, which would be produced by the spoofer (yellow line).

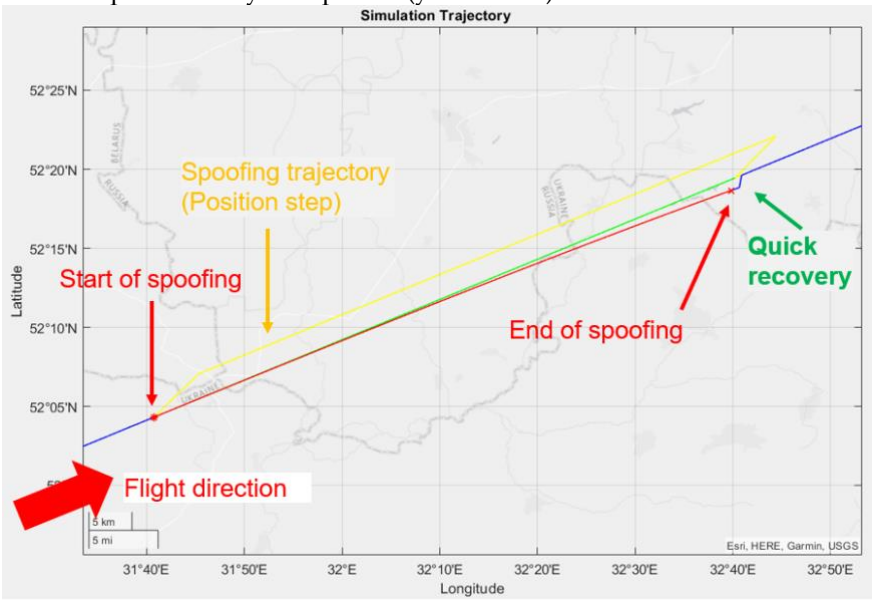

Figure 4. Estimated position by GNSS aided AHRS algorithm during spoofing exposure segment.

Figure 4 nicely demonstrates that the position spoofing offset was successfully detected by the algorithm prior to any effect on the estimated position. The algorithm coasted on inertial measurements during the whole spoofing exposure segment (there is a visible small drift in position due to the coasting). At the end of spoofing, the algorithm was able to determine the end of spoofing and start using the GPS measurements within

the positioning algorithm quickly and independently. The position estimate then quickly recovered very close to true track.

6.2. Velocity step

The velocity step is considered more challenging than the position step type of alternate trajectory. The same approach of performance validation was used as described above with Position offset scenarios. During the development, multiple scenarios with different exposure times were simulated.

Sensitivity analysis of the detection, mitigation, and recovery performance was performed for the 5 minutes exposure time. Based on the results, it was noticed that at around 50 m/s of induced velocity step, the Inertial Spoofing Monitor provides sufficient detection and mitigation performance to claim 99% confidence level. The 50 m/s magnitude of velocity offset was therefore considered for other simulation scenarios with longer exposure times.

The performance validation Claims Table using the Inertial Monitor with the Velocity offset spoofing case is provided in Table 2. It must be noted that for all simulation scenarios for velocity step evaluation, a 99% confidence level (according to DO-384) was used. The length of recovery segment was 5 minutes, and the length of post-recovery segment was 5 minutes as well. The AH-2000 sensor error model was assumed, and the detection, mitigation and recovery are claimed for all position, velocity and attitude parameters provided by GNSS aided AHRS.

Table 2. Example of Claims Table for Velocity step performance validation scenario.

Velocity Offset	Exposure Time	Detection	Mitigation	Recovery
50 m/s (15 000 m)	5 min	3785 trials detected	3784 trials mitigated	3798 trials recovered
3799 valid trials		14 trials not detected	15 trial not mitigated	1 trial not recovered
1 trial discarded				

For a velocity offset, the total size of position offset reached at the end of the exposure segment is shown (in parentheses) in order to indicate the magnitude of the offset.

6.3. Acceleration step

The acceleration step is considered to be the most challenging case of the three spoofing offsets defined by DO-384 Appendix Q for alternate spoofing trajectory. As tested internally, the high success rates of spoofing detection, mitigation and recovery can be achieved for large acceleration offsets thanks to the inertial sensor performance (AH-2000 sensor error model assumed), which might not fully represent the real-world spoofing scenario as the acceleration step is considered as the most sophisticated spoofing attack, and the technical difficulty for attacker will be extremely high.

Moreover, there are additional improvements and enhancements of the Inertial Spoofing Monitor to consider (for example by introduction of additional monitoring) to increase the overall robustness and detection performance to the spoofing attacks. Therefore, the simulations for acceleration step were considered only for testing the capability and limitations of the implemented Inertial Spoofing Monitor rather than the complete performance validation testing.

The simulation parameters considered for this acceleration spoofing example case are shown in Table 3.

Table 3. Parameters of evaluated acceleration step simulation scenario.

Step type	Offset	Exposure time	Recovery time
Acceleration	P_{am} = 40 000 m	5 min	5 min

It is important that any claimed detection, mitigation, and recovery probability for the acceleration step is representative of the performance for the worst case α value. α is the fraction of the exposure time during which the acceleration is offset from truth. For very small α we have large accelerations, approximating a velocity step. But the velocity step test was already covered by the velocity step testing.

The worst case α parameter was determined as a first step, because the claimed detection, mitigation, or recovery for an acceleration step is representative of the performance for the worst case α value.

Required acceleration times: α = 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0 of the exposure time. This worst-case parameter screening would require high number of trial tests on each α, but by the standard it is acceptable to perform lower number of screening test on each of the α values and then run the full test on the found worst case of these α values.

For better understanding, in Table 4 has the values for acceleration step variants for each α, together with position and velocity offset computed.

Table 4. Acceleration step values based on different α value for evaluated case.

Alpha	Acceleration step	Position offset at t = 4s	Velocity offset at t = 4s
0.1	4.68 m/s² for 30 s	37.43 m	18.71 m/s
0.2	2.47 m/s² for 60 s	19.75 m	9.88 m/s
0.3	1.74 m/s² for 90 s	13.94 m	6.97 m/s
0.4	1.39 m/s² for 120 s	11.11 m	5.56 m/s
0.5	1.19 m/s² for 150 s	9.48 m	4.74 m/s
0.6	1.06 m/s² for 180 s	8.47 m	4.23 m/s
0.7	0.98 m/s² for 210 s	7.81 m	3.91 m/s
0.8	0.93 m/s² for 240 s	7.41 m	3.70 m/s
0.9	0.90 m/s² for 270 s	7.18 m	3.59 m/s
1.0	0.89 m/s² for 300 s	7.11 m	3.56 m/s

To perform the worst-case parameter α screening, one full (3800 number of trials) simulation scenario was run with randomly drawn value of α parameter for each trial. Each simulation trial was classified per α parameter value and for each value there was a computed number of unsuccessful simulation trials. Based on this classification the scenario with the worst-case parameter α value was determined (with highest number of unsuccessful trials).

Based on the full-set simulation trial, it was found the number of undetected and unmitigated trials does not pass the validation criteria for 99% success rate since the achieved success rate is 93%. But it can be considered a good starting point for further improvements of the Inertial Spoofing Monitor. To illustrate the achievable performance, the simulation for the best-case α was executed as well with 99.6% success rate. The results show the number of unsuccessful cases is significantly lower here so this case would pass the validation criteria.

7. Summary

The performance validation simulations were performed in order to evaluate and demonstrate the detection, mitigation and recovery capability of developed and implemented Inertial Spoofing Monitor. The performance validation followed the process described by the MOPS DO-384 in Appendix Q ([7]). The FuseNav simulation framework was updated accordingly to be able to evaluate all the requested parameters. All three versions of spoofing offsets (alternate trajectory) were tested with multiple different variations of the offset magnitudes and exposure time durations. The sensor model used for simulations corresponded to the Honeywell AH-2000 platform. The procedure of

validation was selected to follow the process described in the MOPS to get representative, reliable, and comparable results.

Based on the current Performance Validation simulations provided in previous section it can be stated that:

- **Position offset outcomes:**
  - Easiest and the most probable spoofing threat;
  - High detection, mitigation and recovery performance validated for position offset magnitudes larger than 0.3 nm;
  - Limited mitigation observed for longer spoofing exposure time (considering AH-2000 platform).
- **Velocity offset outcomes:**
  - More complex spoofing threat; Detection, mitigation, and recovery performance validated for velocity offsets - high success rate can be claimed for larger velocity offsets;
  - Smaller velocity offsets are detectable depending on an offset magnitude, spoofing direction and timing;
  - Performance improvement is possible by Inertial Monitor updates.
- **Acceleration offset outcomes:**
  - The most complex and the most challenging spoofing threat for inertial based methods;
  - High success rate can be achieved for very large acceleration offsets (probably not fully representative of real spoofing events);
  - Improvements of Inertial Monitor or additional supplementary monitor is needed for better detection and mitigation performance.

Based on the testing, it was noticed that the Inertial Spoofing Monitor is capable of successful detection, mitigation and recovery function under all simulated spoofing cases (Position, Velocity and Acceleration steps). The required performance detection, mitigation, and recovery levels for selected 99% confidence level were achieved and can be claimed for position and velocity offsets. For the most difficult acceleration step, the claims cannot be made based on the assumed sensor error model performance. Further improvements of the design of the Inertial Monitor are planned in the future in order to achieve better performance for the most demanding spoofing cases.

Honeywell's inertial systems are trusted by millions of aircraft operators and passengers every day. Honeywell is at the industry forefront of anti-jamming and anti-spoofing capabilities. New patented technology is being added to Honeywell inertial products for certification in coming years that will dramatically improve aircraft resilience to GPS spoofing and reinforce the value of Honeywell's IRS and AHRS as the trusted source of navigation. Honeywell is collaborating with aircraft manufacturers to make this technology available to all commercial platforms and continues to develop additional technology to stay ahead of GPS threats as they evolve.

References

1. Fernández-Hernández, I.; Walter, T.; Alexander, K.; Clark, B.; Châtre, E.; Hegarty, C.; Appel, M.; Meurer, M. Increasing International Civil Aviation Resilience: A Proposal for Nomenclature, Categorization and Treatment of New Interference Threats. Proceedings of the 2019 International Technical Meeting of The Institute of Navigation, Reston, Virginia; January 2019; pp. 389-407.
2. Ward, P. W.; Betz, J. W., Hegarty, C. GNSS Disruptions. In Understanding GPS/GNSS Principles and Applications - Kaplan, Hegarty (eds) - Third Edition; Artech House, 2017; pp. 549-617.
3. Humphreys, T. Interference In Handbook of Global Navigation Satellite Systems; Teunissen, P.; Montenbruck, O.; eds.; Springer, 2017; pp. 469-504.
4. International Civil Aviation Organization. International Standards and Recommended Practices - Annex 10 - Aeronautical Telecommunications - Vol 1 - Radio Navigation Aids - Sixth Edition - No. 91; ICAO publications; 2018.
5. RTCA SC-159. Minimum Operational Performance Standards for Global Positioning System - Wide Area augmentation System Airborne Equipment - DO229E; 2016.

6. EUROCAE. Minimum Operational Performance Standards for Dual-Frequency Multi-Constellation Satellite-based Augmentation System Airborne Equipment, ED-259A draft; EUROCAE Working Group 62 “Galileo”; 2023.
7. RTCA. Minimum Operational Performance Standard (MOPS) for GNSS Aided Inertial Systems, DO-384; December 17, 2020.
8. SAE ITC. GNSS Sensor ARINC Characteristic 743A-5; May 2009.
9. Wu, Z.; Zhang, Y.; Yang, Y.; Liang C.; Liu, V. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. In IEEE Access, vol. 8; pp. 165444-165496; 2020.