The FAA's Center of Excellence for UAS Research
ASSURE
Alliance for System Safety of UAS through Research Excellence

A11L.UAS.86 - A44 Mitigating GPS and ADS-B Risks for UAS

Task 3: Planning the Testing and Demonstration of Mitigations

October 14, 2022

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

LEGAL DISCLAIMER

The information provided herein may include content supplied by third parties. Although the data and information contained herein has been produced or processed from sources believed to be reliable, the Federal Aviation Administration makes no warranty, expressed or implied, regarding the accuracy, adequacy, completeness, legality, reliability or usefulness of any information, conclusions or recommendations provided herein. Distribution of the information contained herein does not constitute an endorsement or warranty of the data or information provided herein by the Federal Aviation Administration or the U.S. Department of Transportation. Neither the Federal Aviation Administration nor the U.S. Department of Transportation shall be held liable for any improper or incorrect use of the information contained herein and assumes no responsibility for anyone’s use of the information. The Federal Aviation Administration and U.S. Department of Transportation shall not be liable for any claim for any loss, harm, or other damages arising from access to or use of data or information, including without limitation any direct, indirect, incidental, exemplary, special or consequential damages, even if advised of the possibility of such damages. The Federal Aviation Administration shall not be liable to anyone for any decision made or action taken, or not taken, in reliance on the information contained herein.

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No.
A11L.UAS.86

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
A11L.UAS.86 - A44 Mitigating GPS and ADS-B Risks for UAS
Task 2: Planning the Testing and Demonstration of Mitigations

5. Report Date
October 14, 2022

6. Performing Organization Code

7. Author(s)

University of North Dakota
William Semke, william.semke@und.edu
Prakash Ranganathan, prakash.ranganathan@und.edu
Kansas State University
Randall Nichols, profrknichols@ksu.edu
Embry-Riddle Aeronautical University
Hever Moncayo, moncayoh@erau.edu
Oregon State University
Jihye Park, jihye.park@oregonstate.edu

8. Performing Organization Report No.

9. Performing Organization Name and Address
University of North Dakota
243 Centennial Dr.
Grand Forks, ND 58202

10. Work Unit No.

11. Contract or Grant No.

12. Sponsoring Agency Name and Address
FAA

13. Type of Report and Period Covered

14. Sponsoring Agency Code
5401

15. Supplementary Notes

16. Abstract

This Planning the Testing and Demonstration of Mitigations report fulfills Task 3 for the A44 ASSURE project. It prioritizes the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable. It places particular emphasis on prioritizing mitigations that support sUAS operations that will be tested in Task 4. The plans include the use of simulated flight data as a significant source of test data for evaluation.

17. Key Words
GPS, ADS-B, signal dropouts, erroneous data, jamming, spoofing

18. Distribution Statement
No restrictions. This document is available through the National Technical Information Service, Springfield, VA 22161.

19. Security Classification (of this report)
Unclassified

20. Security Classification (of this page) Unclassified

21. No. of Pages
29

22. Price

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF ACRONYMS

ACUASI	Alaska Center for UAS Integration
ADS-B	Automatic Dependent Surveillance-Broadcast
ADCL	Advanced Dynamics and Control Lab
AGL	Above Ground Level
C2	Command and Control
CCC	Circular Cross Correlation
CD	Collective Detection
CTN	Course -Time Navigation
DAA	Detect and Avoid
ECD	Dr. Manuel Eichelberger’s advanced implementation of CD to detect and mitigate spoofing attacks on GPS or ADS-B signals (Eichelberger 2019)
ERAU	Embry-Riddle Aeronautical University
FAA	Federal Aviation Administration
GCS	Ground Control Station
GNAV	Geomagnetic based Navigation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HIL	Hardware in Loop
IMU	Inertial Measurement Unit
LOS	Loss Of Signal
NIC	Navigation Integrity Category
OFA	Optical Flow Algorithm
OFNAV	Optical Flow Navigation
OrSU	Oregon State University
PFRR	Poker Flat Research Range
PRN	Pseudo Random Noise
RF	Radio Frequency
ROS	Robot Operating System
RSSI	Received Signal Strength Indicator
SIL	Software in Loop
SNR	Signal to Noise Ratio
sUAS	Small Uncrewed Aircraft System
UAF	University of Alaska Fairbanks
UAS	Uncrewed Aircraft Systems
UAV	Uncrewed Aerial Vehicle
UND	University of North Dakota

EXECUTIVE SUMMARY

Unvalidated or unavailable Automatic Dependent Surveillance-Broadcast (ADS-B) and Global Position Systems (GPS) data poses security and safety risks to automated Uncrewed Aircraft Systems (UAS) navigation and to Detect and Avoid (DAA) operations. Erroneous, spoofed, jammed, or drop outs of GPS data may result in uncrewed aircraft position and navigation being incorrect. This may result in a fly away beyond radio control, flight into infrastructure, or flight into controlled airspace. Erroneous, spoofed, jammed, or drop outs of "ADS-B-In" data may result in automated uncrewed aircraft being unable to detect and avoid other aircraft or result in detecting and avoiding illusionary aircraft. For automated DAA, a false ADS-B track can potentially be used to corral the uncrewed aircraft to fly towards controlled airspace, structures, terrain, and so on. This research is necessary to enable safe and secure automated small UAS (sUAS) navigation and safe and secure automated sUAS DAA operations. Goals for the project include reports and recommendations useful for Federal Aviation Administration (FAA) policy development and UAS standards development. It is expected that this information will be used to better understand the risks and potential mitigations, and to help the FAA to reassess and refine FAA policy with respect to validation of ADS-B data.

The A44 team has completed the planning for the testing and demonstration of mitigations report which fulfills Task 3 for the A44 ASSURE project. Select mitigation strategies were chosen form the Task 2 report for flight and simulation testing. It prioritizes the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable. It places particular emphasis on prioritizing mitigations that support sUAS operations that will be tested in Task 4. The plans include the use of simulated flight data as a significant source of test data for evaluation.

The integrity of ADS-B and GPS navigation systems will be tested to detect threats to the integrity and/or reliability of the data. These risks include erroneous, spoofed, jammed, and dropped data from GPS and/or ADS-B systems. Several mitigation schemes are identified for flight and simulation testing based on their potential effectiveness in jamming and spoofing conditions. The mitigation schemes to be tested are optical flow, geomagnetic navigation, cellular signal navigation, and the Eichelberger's Collective Detection (ECD) method. Previous results from Task 2 indicate that these have an overall high effectiveness rating, while having varying effectiveness in the individual factors scored.

The test results obtained based on the test plans created in this report will be evaluated, assessed, and summarized in the A44 Task 4 Test, Analysis, and Demonstration Report.

1. INTRODUCTION AND BACKGROUND

The FAA position communicated to Radio Technical Commission for Aeronautics Special Committee 228 is that UAS DAA systems should validate “ADS-B In” data before it is used to conduct DAA. A risk assessment and exploration of potential solutions is needed to inform potential policy updates for different types of UAS and operations for both GPS validation and ADS-B In validation. Potential risks and/or mitigations examples considered at the onset of the project are listed below.

- Potential Risk: If GPS data drops out or is jammed, the UAS may not know exactly where it is located and may fly away without anyone’s knowledge of where it is. Note that sUAS are not tracked by Air Traffic Control radar. Potential mitigations include means to detect broad area GPS jamming or GPS dropouts. Examples: monitor the known GPS position of a fixed GPS receiver on a cell phone, ground control station, tower, and other UAS that is on the ground. Alternatively, have an independent means of temporary navigation and UAS tracking sufficient to cease operations safely. Examples: Inertial Measurement Unit (IMU) navigation, UAS beacons (Radio Frequency (RF) or optical), vision-based navigation, rough triangulation or signal direction finding from the ground using Command and Control (C2) Signal to Noise Ratio (SNR) or time of flight analysis, etc.
- Potential Risk: If GPS signals are spoofed, the UAS may think it is in one location when it is actually at another location. This may result in the UAS crossing airspace boundaries, flying beyond radio control, sudden climbing to avoid terrain referenced onboard digital terrain elevation maps, etc. Potential mitigations could include means to detect broad are GPS spoofing. Examples: monitor the known GPS position of a fixed GPS receiver on a cell phone, Ground Control Station, tower, or other UAS that is on the ground. Alternatively, have an independent means of temporary navigation sufficient to cease operations. Potential examples may include temporary IMU navigation, navigate by C2 signal strength, UAS beacons (RF or optical), vision-based navigation, etc.
- Potential Risk: “ADS-B In” signals drop out or are jammed. This prevents UAS from detecting and avoiding other aircraft that are transmitting “ADS-B Out”. Potential mitigations could include a means to detect ADS-B dropouts and jamming to cease UAS operations when jamming is detected. Example: monitor the signal from a fixed “ADS-B Out” source (potentially easy and low cost). Alternatively, potential mitigations could rely upon detecting jamming, have a means to safely cease DAA operations.
- Potential Risk: A false “ADS-B In” signal is detected that harasses the UAS. If the UAS is automated to avoid collisions with other aircraft, there is the potential for false signals to harass and corral an automated UAS thereby directing it where a malicious actor desire it to fly (fly into infrastructure, terrain, controlled airspace, etc.). Potential mitigations could include having a means to validate “ADS-B In” tracks or detect false tracks. Example solutions: rough triangulation or signal direction finding from the ground using SNR or time of flight analysis. Users should have an ability for overriding UAS automated collision avoidance on unvalidated “ADS-B In” tracks. Users should cease UAS operations when false “ADS-B In” tracks are detected.

This Planning the Testing and Demonstration of Mitigations report fulfills Task 3 for the A44 ASSURE project. It prioritizes the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable. Particular emphasis will be placed on prioritizing mitigations that support sUAS operations that will be tested in Task 4. The plans include the use of simulated flight data as a significant source of test data for evaluation.

This report contains test plan for UAS navigation anomalies including dropouts and erroneous data, GPS and ADS-B signal jamming, and GPS and ADS-B signal spoofing. The UAS anomalies section will focus of using ADS-B data sets to identify ADS-B anomalies that would result in ceasing operations and identify the scenarios that are most common. With this data the use of hybrid machine learning models will be explored. For the jamming section, the evaluation of the capabilities, advantages, and limitations of Optical Flow (OFNAV) and Geomagnetic based Navigation (GNAV) techniques are tested using both flight and simulated data. In addition, a test is developed to record and utilize nearby LTE/4G cellular signals to inform a Global Navigation Satellite System (GNSS)-independent positioning solution from a UAS-based receiver. For the spoofing section, the ECD method is used in a simulation environment that will produce data to assess its effectiveness.

2. UAS NAVIGATIONAL ANOMALIES – DROPOUTS AND ERRONEOUS DATA TESTING AND DEMONSTRATION OF MITIGATIONS

The University of North Dakota (UND) team plans to model the scenarios under which drone operation could be ceased based on several abnormal ADS-B parameters. Specific parameters include Navigation Integrity Check (NIC), Received Signal Strength Indicator (RSSI), altitude variations, clock drift, and clock skew. The team will create a database containing scenarios of injected or simulated ADS-B anomalies. This database will begin from historical Open Sky data with injected columns of several abnormal ADS-B parameters. These injections will be performed using a variety of mathematical functions that represent all combinations of anomalies (gradual rise or fall, levels, sudden spikes, or dips). Examples of functions include sigmoid, trapezoidal, missing data, randomization and automated insertion of spikes, and dips of varying duration. This data will act as a training/test set for designing and evaluating machine learning models. Additionally, UND has sought assistance from the University of Alaska Fairbanks (UAF) on additional test data on ADS-B parameters which will be used to validate the detection of ADS-B anomalies. Once detectable, these mitigation strategies are easily transferable to UAS environments and will enable drones to be signaled when operations become unsafe and need to be ceased.

Figure 1 illustrates the three tasks associated with the planned efforts for dropouts and erroneous data testing and the demonstration of the mitigations.

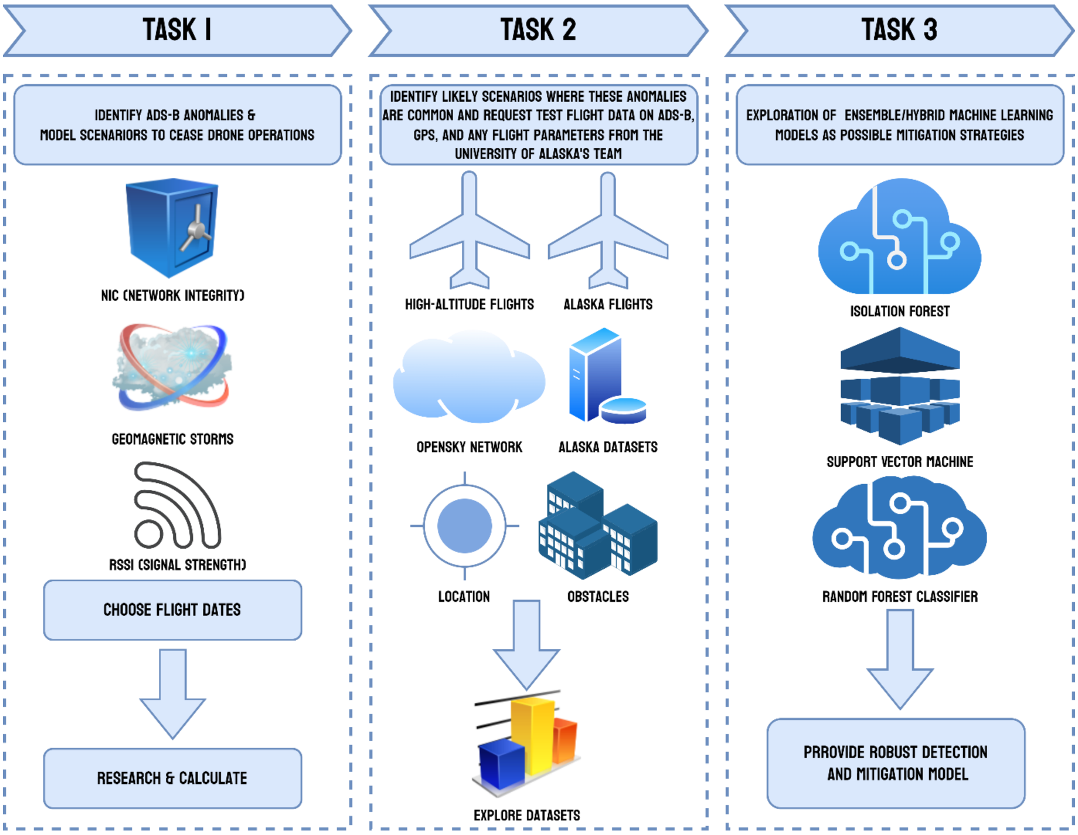
TASK I
TASK 2
TASK 3
IDENTIFY ADS-B ANOMALIES & MODEL SCENARIORS TO CEASE DRONE OPERATIONS
NIC (NETWORK INTEGRITY)
GEOMAGNETIC STORMS
RSSI (SIGNAL STRENGTH)
CHOOSE FLIGHT DATES
RESEARCH & CALCULATE
IDENTIFY LIKELY SCENARIOS WHERE THESE ANOMALIES ARE COMMON AND REQUEST TEST FLIGHT DATA ON ADS-B, GPS, AND ANY FLIGHT PARAMETERS FROM THE UNIVERSITY OF ALASKA'S TEAM
HIGH-ALTITUDE FLIGHTS
ALASKA FLIGHTS
OPENSKY NETWORK
ALASKA DATASETS
LOCATION
OBSTACLES
EXPLORE DATASETS
EXPLORATION OF ENSEMBLE/HYBRID MACHINE LEARNING MODELS AS POSSIBLE MITIGATION STRATEGIES
ISOLATION FOREST
SUPPORT VECTOR MACHINE
RANDOM FOREST CLASSIFIER
PRROVIDE ROBUST DETECTION AND MITIGATION MODEL

Figure 1. The three tasks associated with the planned efforts for dropouts and erroneous data testing and the demonstration of the mitigations.

2.1 Task 1: Identifying ADS-B anomalies and Modeling Scenarios to cease Drone Operations

The UND team will specifically investigate to model the following anomalies into a Commercial aircraft Database (e.g.., AIcrowd OpenSky, ADS-B Exchange). As there are limited or no ADS-B In/Out data available for sUAS aircrafts, the modeling techniques deployed for large aircraft will be similar and extensible for sUAS environments. For example, the UND team will design new and deploy existing mathematical representations for at least one or more type of anomalies listed: uncertain patterns or concept drifts such as rise, fall, levels in one or more parameters related to ADS-B data attribute will be investigated in this task.

a. *Clock Skew* – caused by the same clock signal arriving at different components at different times due to external factors (hardware differences, signal delays, etc.). In a Controller Area Network bus, clock skew is calculated by taking the difference between the actual received frame length from the nominal length in Equation 1 (Zhou et al. 2022).

$$Skew = \frac{NBS*n-S}{S} \qquad (1) \ \text{(Zhou et al. 2022)}$$

where NBT: Nominal Bit Time, S: measured length, n: number of bits.

b. *Clock Drift* – caused by the clock on the receiver not running at the same rate as the clock on the sender or reference clock (Semanjski et al. 2019).This may be caused by temperature and voltage (Marouani and Dagenais 2008), which may affect drones.

c. *Side Channel Attack* – these attacks typically target the cryptographic implemented algorithms and reveal unauthorized information. These attacks can lead to corruption or spoofing of the sensor readings. Some of the examples are IMU or GPS where the sensor readings can be intercepted and cause instability or crashing of drones. Author (Fei et al. 2018) proposed different types of side channel attacks on the Uncrewed Ariel Vehicles (UAVs) and proposed a framework model to protect against such attacks. Similarly, Son and colleagues (Son et al. 2015) used sound-based approach as side channel attack which affected the Micro-Electromechanical System gyroscope in the drone as the gyroscope are having resonant frequencies will degrade the accuracy.

d. *Received Signal Strength Indicator (RSSI)* – It is a measure of relative power measured at the receiving source of the signal. The monitoring of the RSSI is critical as this plays a vital role in the communication and when there is a loss in the communication leads to accidents. Environmental factors such as weather, or obstacles also play a role in the RSSI. In obstacle free environment, the RSSI of the received signal as follows (G. Liu et al. 2021):

$$\mathrm{RSSI} = 10\log\frac{\mathrm{Pr}}{\mathrm{Pt}} \qquad (2)$$

where Pr and Pt is the power of transmitted and received signals.

$$\mathrm{Pr} \propto \mathrm{Pt} \cdot \left(\frac{1}{\mathrm{d}}\right)^2 \qquad (3)$$

where d is the distance between the transmitter and receiver.

e. *Navigation Integrity Category (NIC)* – NIC is an uncertainty metric transmitted by the ADS-B, on a scale of 1 to 10. The higher the value of NIC, better the accuracy of the GPS fix. The acceptable values of NIC are between 7-10. Any value below 7 is indicative of a reduction in the accuracy of the GPS fix. This loss in GPS accuracy may be linked to interference events. A Loss in positional information for at least 10 seconds, followed by a drop in NIC from acceptable standards to 0, is an indication of an ADS-B dropout due to GPS inference activity. A drop in NIC would be indicative of GPS accuracy issues. The research team intends to create data and apply machine learning or rule-based approaches to detect this pattern, while also obtaining some important statistics on GPS interference.

f. The team will choose flights and dates to study. Flights and dates will be chosen by the changes in RSSI and NIC. Flights with higher variability in these features and high altitude will be chosen. All flights will take place within a five-day period.

f. The team will explore the dataset by plotting variables to discover relationships between them. This will inform which features to use for the machine learning models.

g. The UND Team will explore RSSI and NIC correlation across multiple flights. Data will be pulled from ADS-B Exchange via a manual download. Analysis will be done using Python and the libraries pandas, matplotlib, and plotly; relationships between variables will be found using the correlation. The correlation function that will be used is from the pandas library. This analysis will take place across multiple flights.

h. The team will explore the impact of geo magnetic storms on the NIC of Aircrafts. The team will find if there is a significance of geo magnetic storms on aircraft that experience a drop in NIC, by exploring distribution of NIC during quiet days, and days with geo magnetic disturbances.

i. The team will create a visual representation of areas around the US, where drops in NICs have occurred, to serve as a pre-warning for pilots.

2.2 Task 2: Identify likelihood scenarios where these anomalies are common and request test flight data on ADS-B, GPS, and any flight parameters from the University of Alaska's team.

UND requested the Alaska team to run their test flights for multiple scenarios that enable UND team to validate the created models. The team is looking for some data that needs to be collected under different scenarios. The team needs In data and GPS position information, RSSI, and NIC/ Navigation Accuracy Category Integrity Value of UAS dataset information on the following different scenarios:

a. Different Altitude ranges - low (below 200 ft.), medium (200 to 400 ft.), and high (above 400 ft.).

b. Data should be captured by testing in different scenarios in which materials or topography may cause the ADS-B to fail.

Once UND receives the test data, the UND team will integrate Alaska's data sets and use state-of-the-art machine learning platforms (Tensorflow, Python, Scikit learn) to run and evaluate the developed algorithms. In addition, the UND team will model some of the scenarios in a simulation setting.

This is done by injecting falsified data. This data will be injected into the RSSI and NIC parameters. These injections will be performed using a variety of statistical modification methods such as:

a. Sigmoid –

$$f(x) = \frac{1}{1-e^{-x}} \tag{4}$$

Where x = sample value, e = Euler's number

b. Trapezoidal Membership Function – Computes fuzzy membership values in Equation 5 (Mrabet 2022).

$$\mathrm{u}(\mathrm{x}, \alpha, \beta, \gamma, \delta) = \begin{cases} 0, \mathrm{x} < \alpha \\ \frac{\mathrm{x}-\alpha}{\beta-\alpha}, \alpha \leq \mathrm{x} \leq \beta \\ 1, \beta < \alpha \leq \gamma \\ \frac{\gamma-\mathrm{x}}{\gamma-\mathrm{y}}, \gamma < \mathrm{x} \leq \delta \\ 0, \ \mathrm{x} > \delta \end{cases} \tag{5}$$

c. Triangular/Tent Function – graph is shaped like a triangle Equation 6.

$$\mathrm{f(x)} = \begin{cases} 1-|\mathrm{x}|, \ |\mathrm{x}| < 1; \\ 0, \ otherwise \end{cases} \tag{6}$$

d. Missing Data – data removed at random times and intervals using Python and the Numpy package's np.random.rand function.

Once completed, this will comprise a training dataset on which machine learning will be used to detect these anomalies automatically and quickly.

2.3 Task 3: Exploration of Ensemble/Hybrid Machine Learning Models as Possible Mitigation Model

a. The team will apply several machine learning models to datasets with the purpose of detecting attacks:

  i. Random Forest Classifier – ensemble machine learning method for classification and regression which creates many decision trees at a time and selects the output chosen by the majority of trees.

  ii. Isolation Forest – creates many trees and measures the distance nodes are from each other, isolating anomalous data.

  iii. Support Vector Machine – SVMs are n-dimensional classification/regression algorithms.

  iv. The team will explore and develop hybrid models and use transfer learning to isolate anomalous data (Mrabet, Selvaraj, and Ranganathan 2019).

b. The team will provide a robust detection and mitigation model that is easy to deploy and cost effective.

c. Impacts of this study:

  i. Improved safety of drone operations in airport, military base, urban, and rural environments

  ii. Safe cancellation of drone operations when something goes wrong, or an anomaly is detected

  iii. Logging and analysis of attack/thread types for future determination of mitigation strategies and prevention

3. GPS AND ADS-B SIGNAL JAMMING TESTING AND DEMONSTRATION OF MITIGATIONS

The focus of Embry-Riddle Aeronautical University (ERAU) team until the end of the project is to evaluate the capabilities, advantages, and limitations of OFNAV and GNAV techniques as GPS mitigation strategies. For optical flow, Software-in-the-Loop (SIL) and flight testing will be designed and executed to analyze the performance of the approach at different conditions including lighting changes, terrain characteristics, and features. For GNAV, the approach will be only tested using SIL.

Several test cases will be designed to test the accuracy and performance on estimating position of both navigation approaches. The missions will include pre-set waypoint commands while flying on an altitude-hold mode in a package-delivery flight mode within an Urban Canyon. The OFNAV architecture shown in Figure 2 is currently being implemented as part of the SIL and includes the interaction of different modules and sensors including PXFLOW camera, range finder laser, a Kalman Filter sensor fusion, flight path, and control system.

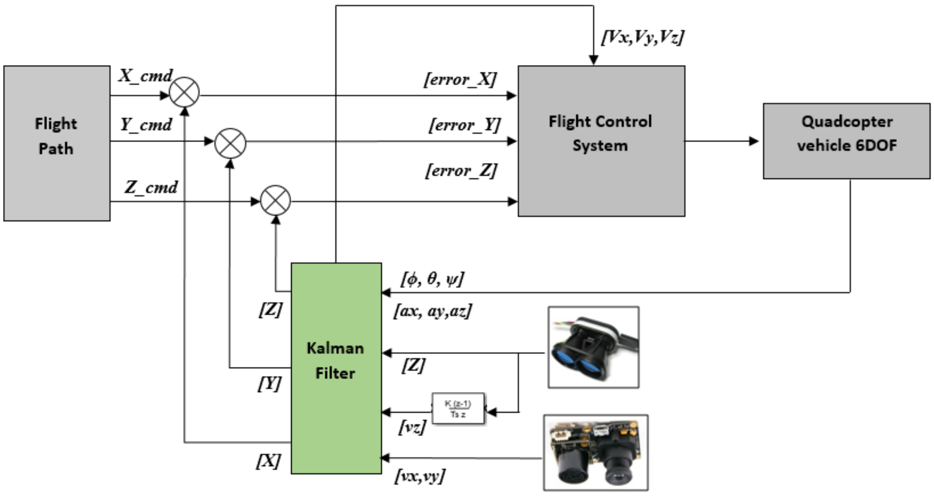

Figure 2. Optical-flow-based Autonomous Navigation Architecture.

The performance of both approaches will be analyzed by comparing the estimation accuracy against GPS Kalman filter based data. Based on preliminary results, it is expected that accurate results from OFNAV architecture will be obtained when there is a noticeable contrast or distinguishable features form part of the surface at which the camera is pointing. In this case, ERAU team is planning to evaluate the optical flow sensor limitations and the minimum conditions of light for increased accuracy. Both approaches will also be characterized and tested at higher altitudes in order to increase range for different applications. Different altitudes would translate into different allowable speed ranges, and maximum navigation speeds could be determined for different scenarios.

The ERAU testbed that will be used to test OFNAV approach capabilities is a 3DR X8 frame quadcopter. This low-cost testbed meets minimum requirements needed to implement OFNAV. This testbed uses eight motors "X8" configuration to provide extra lift capabilities. **Error! Reference source not found.** shows a close view of the testbed with the instrumentation onboard the vehicle.

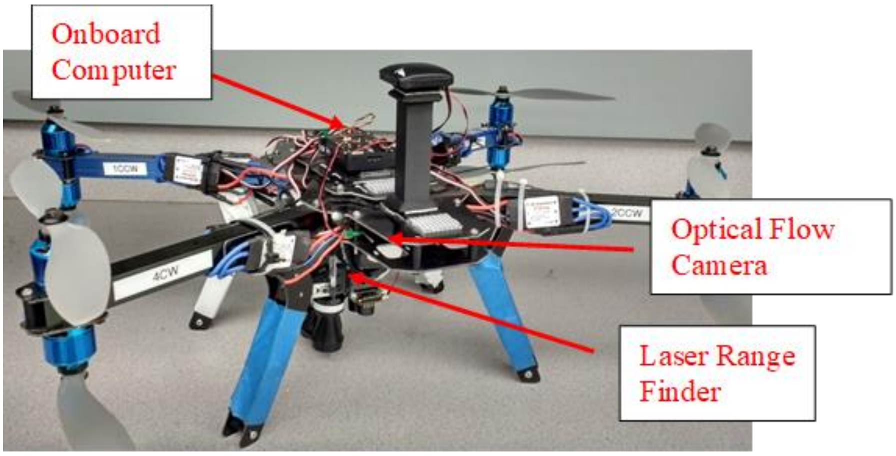

Figure 3. 3DR X8 Quadcopter Testbed with instrumentation.

ERAU is also coordinating with The Alaska Center for UAS Integration (ACUASI) at UAF to use video data obtained from one of the vehicles. This data will be processed by ERAU to evaluate performance of the developed OFNAV for estimating ground position and velocity. The ACUASI sensor flight suite includes integration and synchronization of inertial sensors (i.e., IMU) with GPS signals and infrared-based vision system. ACUASI's X6A is a heavy lift hexcopter that allows to accommodate large payloads and its extended flight enveloped will guarantee that several flight test data is generated at different but limited altitudes, velocities, and light-conditions.

Oregon State University (OrSU) testing plan will focus on Cellular Navigation. Current UAS navigation operations primarily rely on GNSS-informed positioning. In cases of GNSS receiver error or dropout due to interference or jamming, utilizing signals of opportunity can act as a backup or supplemental navigation source to allow the aircraft to complete an otherwise inhibited flight. Current cellular technology has established transmission infrastructure and range that allow for multiple overlapping signals in urban and agricultural settings, standing out as a possible candidate for UAS-based navigation.

This test intends to record and utilize nearby LTE/4G cellular signals from a UAS-based receiver and integrate with available GNSS signals to inform a positioning solution. The Cell/GNSS integrated solution will be obtained by applying the Extended Kalman filter. The accuracy of this method will be compared to the reliable GNSS-informed solution (e.g., relative positioning using nearby reference stations) and instructed flight trajectory waypoints to assess the viability of cellular signals as a navigational signal of opportunity for UAS operations.

OrSU is investigating this topic within Task 3 and Task 4, collaborating with UAF to complete flight testing, and managing equipment logistics. Collaboration may also include UAF's support gathering nearby cellular tower information relevant to logged cellular signals. OrSU will be responsible for post processing and accuracy assessment of acquired flight test data.

Flight Tests:

1. UAS Payload:
   a. GNSS receiver and antenna capable of collecting GPS and GLONASS constellations, with associated SNR measurements; sampling at 1 second interval, exported as standard RINEX observation files (version 2 or 3).
   b. Cellular receiver and antenna capable of logging received cellular signal power level (RSSI), band, tower CID at 1 second interval or more frequent. Needs to be able to log all received ambient cellular signals and RSSI. If band and CID are not possible to log within current resources and timeframe, alternate option will include a market-available specialized cellular scanner to fulfill the previously listed requirements as best as possible. Ideally, will also include built-in associated tower information (tower location and identification) sourced through a cellular tower database.
2. Flights:
   a. Waypoint-based trajectories (distance and time of flight variable based on flight timeframe and resource capabilities)
      i. Stationary at home location for 5 minutes
      ii. Straight trajectory from home location to set waypoint 300m away, and return to home location on same path. Altitude held constant until returned to home waypoint.
      iii. Diamond-like trajectory path with set waypoints guiding the aircraft in clock-wise motion starting from home, to three destinations ranging from 100-250m away, then returning to home location. Altitude held constant until returned to home waypoint.

c. Flying height (iterate above trajectories at each altitude):
    i. 200ft Above Ground Level (AGL)
    ii. 300ft AGL
    iii. 400ft AGL

GNSS and cellular data to be logged throughout above flight trajectory iterations, then processed in post by OrSU to develop position solutions for each test flight. A cellular-based solution will be derived from signal power (RSSI) to calculate distance from transmitting tower to receiver to inform a trilateration calculation. GNSS processing will utilize nearby GNSS reference station(s) to produce a real-time double difference solution. Solutions will be compared between the two technologies and in relation to the “truth” waypoint trajectory per flight.

Flight trajectories and flying height were chosen to act as simplistic analogs for different UAS commercial operation types (long linear infrastructure, precision agriculture, low-altitude surveillance, package delivery).

Due to timeframe of flight testing through UAF resources and OrSU equipment budget, the power-based signal positioning method is the most feasible approach for the A44 project. Other cellular localization methods to consider in future projects include time of arrival carrier phase positioning, or hybrid navigation systems utilizing GNSS and/or IMU solutions in tandem with cellular.

With flight testing resource timeframe and limited equipment budget considered, the cellular navigation mitigation scheme was chosen over Wi-Fi navigation for flight testing planning based off justifications investigated in Task 2, including:

a. Cellular infrastructure provides a higher bandwidth, and larger range than Wi-Fi signals of opportunity, broadening the applicability of cellular navigation as mitigation scheme across rural and urban UAS operations
b. Reliable Wi-Fi infrastructure is primarily constricted to dense urban environments, where more robust fingerprinting methods are needed to identify hotspots sources to utilize them in a positioning solution, which require regular care to remain up to date.
c. Vertical degradation of ground-based Wi-Fi hotspots can affect signal quality depending on flying height and UAS operation type.

Overall, results from Task 2 investigations presented cellular navigation methods as more broadly applicable than Wi-Fi navigation for flight operations included in the A44 project scope.

4. ECD, GPS AND ADS-B SIGNAL SPOOFING POTENTIAL MITIGATION ASSESSMENT

ECD, or *Eichelberger Collective Detection*, is a promising technology countermeasure to spoofing, which can detect, mitigate, and recover fake and genuine signals. A realistic and difficult simulation case was devised to perform a Proof of Concept for ECD spoofing effectiveness and to generate performance / key variable data for future flight operations studies described later in this section (R K Nichols et al. 2022).

Satellites present excellent Loss Of Signal (LOS) from a large part of the Earth's surface. They are highly susceptible to three kinds of hostile activity. Signals from satellites can be *intercepted*, strong hostile transmissions can *jam signals*, interfering with uplink or downlink signals to prevent proper reception, and *signals can be spoofed*, causing the satellite to interpret them as functional commands that are harmful or transmit useless positional data (Adamy 2021).

Any attack on a satellite link may involve single or multiple links. Each link is subject to transmission losses, including LOS, atmospheric, antenna misalignment, rain, and polarization losses.

A *spoofing link* goes from the hostile transmitter to a satellite link receiver. This receiver is generally on the satellite. The spoofing signal's purpose is to cause it to function improperly, but if the spoofer is in the Ground Control Station (GCS), the purpose is to invalidate the date – especially localization data (David Adamy 2015).

ECD has been discussed in detail in the A44 Task 1 and A44 Task 2 reports (Semke 2022a) (Semke 2022b, 2). ECD implementation and evaluation show that with some modifications, the robustness of Collective Detection (CD) can be exploited to mitigate spoofing attacks. (Eichelberger, 2019) shows that multiple locations, including the actual one, can be recovered from scenarios where several signals are present.

ECD does not track signals. It works with signal snapshots. It is suitable for snapshot receivers, a new low-power GPS receiver class (Eichelberger 2019; J. Liu et al. 2012).

ADS-B's high dependency on communication and navigation (GNSS) systems causes the system to inherit the vulnerabilities of those systems. This results in more opportunities (threats) to exploit those vulnerabilities. A vulnerability of ADS-B systems is their broadcast nature without security measures, which can easily be exploited to cause harm. It is important to understand that both GPS (part of the GNSS family) and ADS-B systems are vulnerable to spoofing attacks on both manned and unmanned aircraft. In general, GPS vulnerabilities translate down to the more specific ADS-B subset, which has its own vulnerabilities. In his book on *Robust Global Localization using GPS and Aircraft Signals*, Dr. Michael Eichelberger describes a functional tool known as CD to detect, mitigate and counter spoofing (and jamming) attacks on all stages of GPS (Eichelberger 2019).

Threats and weaknesses show that large damages (even fatal or catastrophic) can be caused by transmitting forged GPS signals. A GPS receiver computing its location wrongly or even failing to estimate any location at all can have different causes. Wrong localization solutions come from 1) a low SNR of the signal (examples: inside a building or below trees in a canyon), 2) reflected signals in multipath scenarios, or 3) deliberately spoofed signals. (Eichelberger, 2019) discusses mitigating low SNR and multipath reflected signals. Signal spoofing (#3) is the most difficult case since the attacker can freely choose the signal power and delays for each satellite individually (Eichelberger 2019; Randall K Nichols et al. 2020).

CD is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite but combines all the available information and decides only at the end of the computation. This technique is critical to the (Eichelberger, 2019) invention to mitigate spoofing attacks on GPS or ADS-B. CD can tolerate a few low-quality satellite signals and is more robust than Course -Time Navigation (CTN). CD requires much computational power. CD can be sped up by a branch and bound approach, which reduces the computational power per location fix to the order of one second, even for uncertainties of 100 km and a minute. CD improvements and research has been plentiful. (Eichelberger 2019; J. Liu et al. 2012; AXELRAD et al. 2011; Bissig, Eichelberger, and Wattenhofer 2017).

Dr. Manuel Eichelberger's *CD – Collective detection maximum likelihood localization approach* method (ECD) not only can *detect* spoofing attacks but also *mitigate* them. The ECD approach is a robust algorithm to mitigate spoofing. ECD can differentiate closer differences between the correct and spoofed locations than previously known approaches (Eichelberger 2019).

ECD solves even the toughest type of GPS spoofing attack consisting of spoofed signals with power levels similar to the authentic ones. (Eichelberger 2019) ECD approach uses only a few milliseconds of raw GPS signals, so-called snapshots, for each location fix. This enables offloading of the computation into the Cloud, which allows knowledge of observed attacks. Existing spoofing mitigation methods require a constant stream of GPS signals and tracking those signals over time. Computational load increases because fake signals must be detected, removed, or bypassed (Eichelberger 2019; Randall K Nichols et al. 2020).

4.1 ECD, GPS, AND ADS-B SIGNAL SPOOFING POTENTIAL MITIGATION ASSESSMENT /SIMULATION

The following Mitigation Plan for ECD using Simulation Datasets was chosen:

1. Establish a base case scenario in an urban location.

    A.) Scenario will be transporting vital organ delivery by UAS between hospitals during a 4-hour max transport time to be used for patient life support.

    B.) Organ & carry case weight 5 lbs

2. Establish a 3–5-mile route based on one satellite GPS dataset. Establish routing and performance characteristics for a successful delivery run.

3. Establish a Spoofing case where 2/3 of satellites send ghost signals that change GPS received signals to show / command UAS false route.

    A.) False Route change must be significant enough to cause Failure of Mission (perhaps 20% deviation) and measurable if real-time visual display.

4. Engage ECD as a countermeasure to

    A.) Detect/differentiate all three satellites. ECD must indicate the correct satellite and reject two false ghosts

    B.) Mitigate route deviation (return to correct mission route) to meet life mission time and delivery specs

C.) Recover correct signals and log the same.

5. Collect as much supplemental data from each interaction to perturb parameters and/or verify ECD performance to 4A-C above.

It is understood that datasets will be batch runs. The ERAU team will create the required signals and case datasets to send to Dr. Manuel Eichelberger to be run in his ECD models. Dr. Manuel Eichelberger will transmit results to the ERAU team for additional simulations and verification that ECD solved the 4) A-C goals. In addition to proof of concept, data should be collected to estimate in-flight, real-time use of ECD effectiveness in further studies (R K Nichols 2022).

4.2 ECD and Counter Spoofing Concepts Definitions

Acquisition – Acquisition is the process in a GPS receiver that finds the visible satellite signals and detects the delays of the Pseudo Random Noise (PRN) sequences and the Doppler shifts of the signals.

Circular Cross-Correlation (CCC) – In a GPS classical receiver, the circular cross-correlation is a similarity measure between two vectors of length N, circularly shifted by a given displacement d:

$$\text{Cxcorr}\ (a, b, d) = \sum_{I=0}^{N-1} a_i \text{ dot } b_I + d \bmod N$$

The two vectors are most similar at displacement d, where the sum (CCC value) is maximum. The vector of CCC values with all N displacements can be efficiently computed by a fast Fourier transform in Ớ (N log N) time (Eichelberger 2019).

Like classical GPS receivers, CTN is a snapshot receiver localization technique that measures sub-millisecond satellite ranges from correlation peaks (IS-GPS-200G 2013).

Collective Detection (CD) is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite but combines all the available information and decides only at the end of the computation. This technique is critical to the (Eichelberger, 2019) invention to mitigate spoofing attacks on GPS or ADS-B.

Coordinate System is a coordinate system uses an ordered list of coordinates to describe the location of points in space uniquely. The meaning of the coordinates is defined concerning some anchor points. The point with all coordinates being zero is called the origin. [Examples: terrestrial, Earth-centered, Earth-fixed, ellipsoid, equator, meridian longitude, latitude, geodetic latitude, geocentric latitude, and geoid.]

GCS - Ground Control Station

Localization is the process of determining an object's place concerning some reference, usually coordinate systems. [aka Positioning or Position Fix]

Navigation Data is the data transmitted from satellites, which includes orbit parameters to determine the satellite locations, timestamps of signal transmission, atmospheric delay estimations, and status information of the satellites and GPS as a whole, such as the accuracy and validity of the data (IS-GPS-200G 2013).

Pseudo-Random Noise (PRN) sequences are pseudo-random bit strings. Each GPS satellite uses a unique PRN sequence with a length of 1023 bits for its signal transmissions. Aka as Gold codes, they have a low cross-correlation with each other (IS-GPS-200G 2013).

Snapshot GPS Receiver is a snapshot receiver is a GPS receiver that captures one or a few milliseconds of raw GPS signal for a location fix (Diggelen 2009).

5. FACILITIES

There are several testing facilities that will be utilized by the A44 team and are briefly described in this section.

5.1 The Alaska Center for UAS Integration (ACUASI)

ACUASI at UAF is tasked with conducting a majority of the flight tests and demonstrations in this project. ACUASI has an assortment of unmanned aircraft, an engineering laboratory, and test ranges at our disposal. ACUASI employs pilots, engineers, and other personnel for flying UAVs, and building and testing payloads.

Several aircraft make of the fleet at ACUASI. The X6A is a heavy lift hexcopter. The flight times vary from 15-30 minutes depending on the weight of the payload. The maximum payload capacity is 15lbs, which allows for 15 minutes of flight time. With a 5lb payload, a 25 minute flight time can be expected. Payloads can be mounted either on the bottom of the aircraft or on the top utilizing 155mm rails. Power can be supplied by the aircraft.

The Skyfront P4 is a hybrid quadcopter that has a gas generator that drives electric motors. Flight times with an ultralight payload can reach 5 hours. The aircraft has an 8.8 lb payload limit that reduces flight time significantly to about 45 minutes. Payloads must be mounted beneath this aircraft. This aircraft is unable to provide power to the payload.

ACUASI is also able to utilize additional over the counter small UAVs such as EVO autels or various DJI UAVs. Intended usage of these UAVs should be indicated as soon as practicable should they be needed for testing on this project.

ACUASI operates at two primary test site locations in the Fairbanks area: Poker Flat Research Range (PFRR) and the UAF campus.

PFRR is located approximately 29 miles north of Fairbanks, Alaska. UAF is able to operate there up to 4000 ft AGL; however, UAF is still required to remain within visual line of sight, which restricts how high UAF can practically operate. Due to other equipment in the area, UAF is only able to fly within the red outlined area in the map in Figure 4.

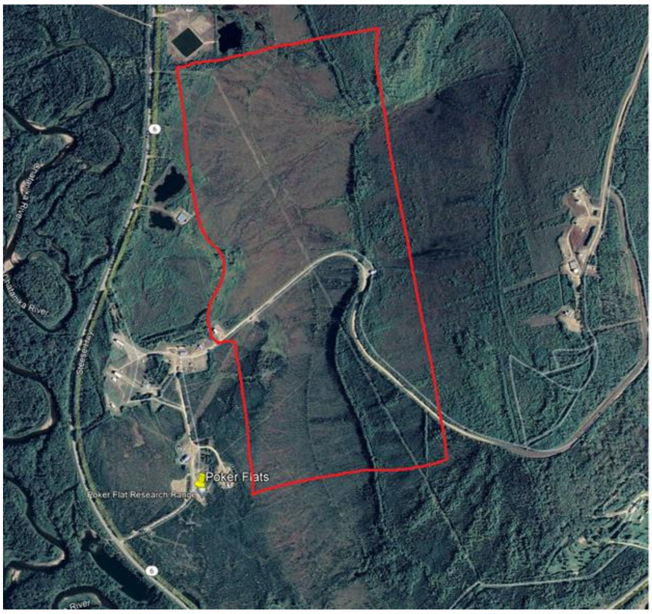

Figure 4. Map of Poker Flat Research Range.

UAF is also able to operate in two areas at the UAF campus. Researchers are limited to 500 ft AGL in the area outlined in red and limited to 1000 ft AGL in the area outlined in blue in Figure 5. Operations in both areas are restricted to visual line of sight operations. This significantly limits operations in the forested area.

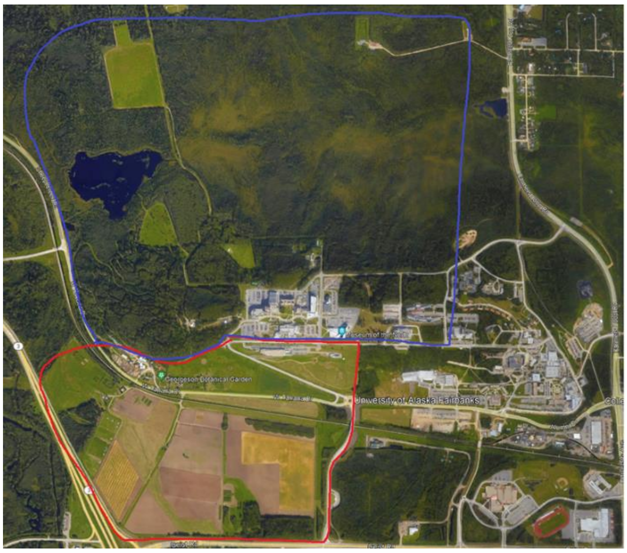

Figure 5. Map of UAF Campus.

5.2 ERAU – ADCL Facilities, Equipment, and Other Resources

The Advanced Dynamics and Control Lab (ADCL), where Dr. Moncayo is the director, is a research facility for the development and implementation of guidance, navigation, and control systems of a variety of aerospace vehicles, as well as research on a broad range of topics focused on flight dynamics. ADCL supports research activities aimed at advancing aviation and space technologies through the development of concepts, implementation of approaches, and demonstration of solutions with research efforts that span several areas.

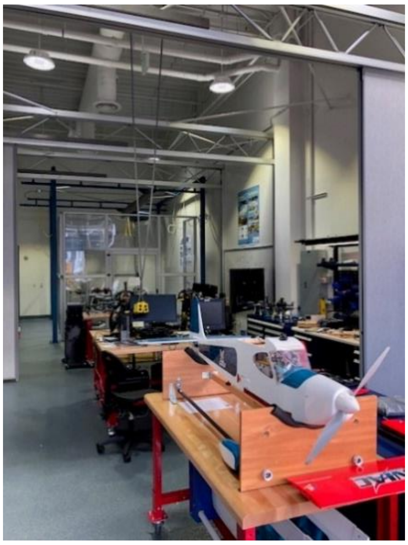

Figure 6. Advanced Dynamics and Control Lab.

The ADCL owns several unmanned research platforms as shown in Figures 6-9, including Hardware-in-the-Loop (HIL) UAS simulation platform, fixed-wing UAS platforms, quadrotors, autonomous mini-spacecraft systems, a mobile ground control station for UAS operations, robotic arms, sensor packages including LIDAR, 3D cameras for vision navigation, Inertial Measurement Systems, and on-board computers.

ADCL fleet consists of three ERAU 3DR quadcopters. PI Moncayo is a U.S. Commercial Drone Pilot and will conduct most of the UAV flying task for data collection under the regulation of FAA and the State laws. The 3DR quadcopter shown in Figure 7 has been instrumented by the research team using commercially low-cost hardware. It features a robust and open-source flight computer Pixhawk which is programmed to execute flight control laws required for stable flight and tracking. A PC104 type computer, Advantech PCM-3356, is programmed with artificial intelligence health monitoring, path planning, and decision-making algorithms. A PXFlow camera is also integrated with a range finder and IMU data to provide vision-aided navigation features.

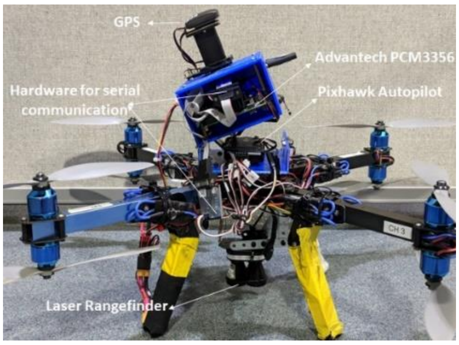

Figure 7. 3DR X8 UAV quadcopter components (opened box on top for visualization purposes).

ADCL fight operations utilize the ERAU Mobile UAS GCS which is an enclosed trailer that houses all necessary equipment for communication with the flight vehicle and monitoring data in real-time. The fundamental tasks of the ground station include receiving, processing, and recording telemetry data from the aircraft and displaying flight information to the pilot and flight test coordinator. The GCS can collect wind data using a Peet Bros weather station equipment which includes a ULTIMETER 2100 Keyboard/Display Unit, ULTIMETER PRO Anemometer/Wind Vane (w/40' cable), and an outdoor temperature sensor (w/25' cable). The station collects wind data at 2.9Hz with a wind speed accuracy of 0.9m/s and 5% for the 16-point magnetic direction sensing. The ground weather station setup is securely mounted on a pole close to the flight path approximately 7m above the ground. The GCS architecture is shown in Figure 8. The ground station architecture and its sub-systems are shown in Figure 9.

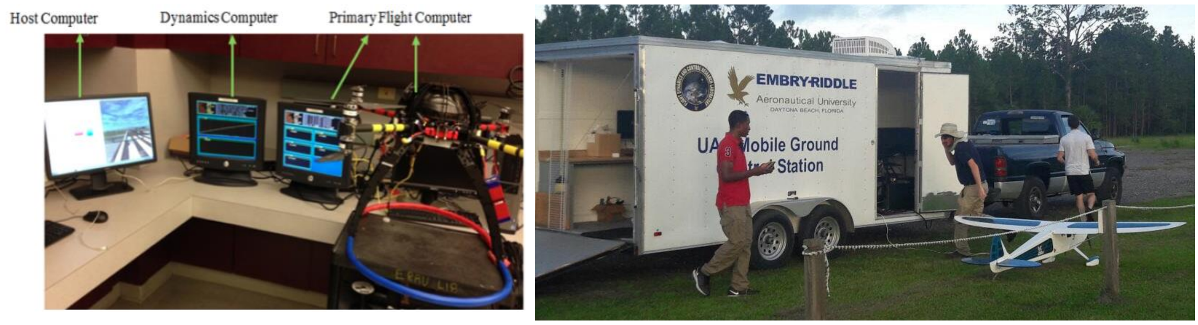

Figure 8. (a) Hardware-in-the-Loop UAS Simulation Platform; (b) Mobile Ground Control Station for UAS.

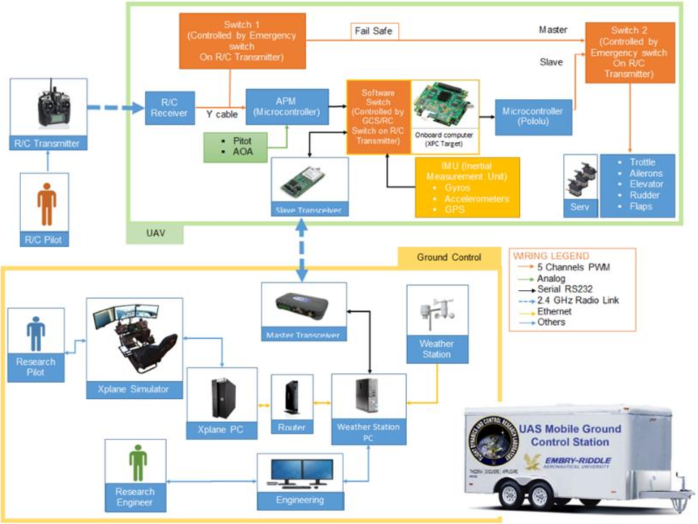

Figure 9. ERAU Mobile Ground Control Station Architecture.

Researchers at ADCL have also developed autonomous vehicle flight simulators, which provides the ability to design and test guidance, navigation, and control algorithms in SIL and HIL along with virtual environments using Gazebo open-source software.

Gazebo provides a synthetic environment that includes vehicle dynamics, sensor models, obstacle/maps with the flexibility required to be interfaced with other software such as Matlab/Simulink. Such interaction can be achieved using Robot Operating System (ROS) protocol, as shown in Figure 10. ROS allows an organized and fast-prototyping feature to move from SIL to HIL and flight testing of GNC algorithms. Within this architecture, the air vehicle model and the control laws are both run in real-time asynchronously at a clock speed of 0.002*ms*. The models are effectively synchronized using a flag sent from the aircraft model in Simulink to the primary module in Gazebo through ROS communication.

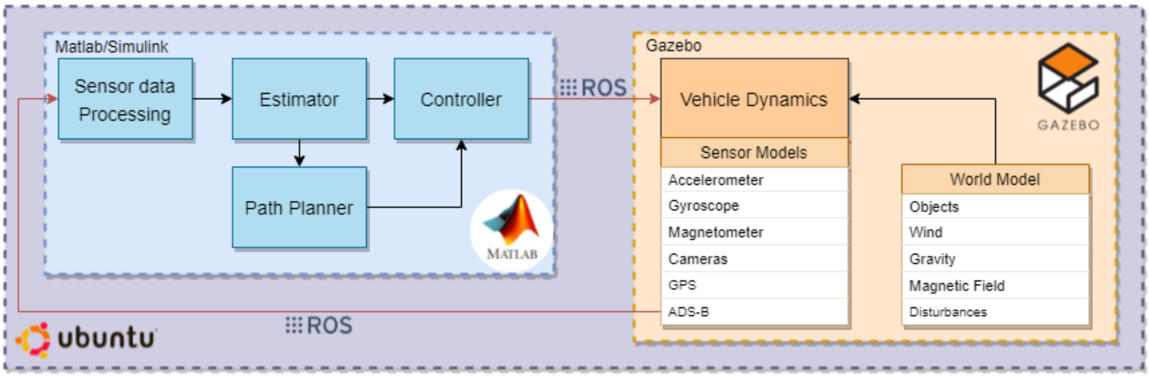

Figure 10. FlightGear Simulation for a Formation Flight Configuration.

The simulation environment also features different effects of GPS degradation that usually affect UAS operations in urban scenarios. This includes multi-path, obstruction or shadowing, drop-outs, and GPS signal distribution maps. Figure 11 shows an example of the virtual environment in Gazebo while distribution of GPS satellite signals is modeled in Simulink.

The simulation architecture also allows the evaluation and validation of developed GNC algorithms in SIL and HIL as a preparation of an experimental validation and demonstration through flight testing on an autonomous research platform proposed. The HIL simulation setup is used to integrate sensors required for a particular test mission with a flight computer and the dynamics model of the system. The SIL and HIL simulation is an important stage of testing algorithms before implementing and validating them in flight. For example, as shown in Figure 12, an integration of Optical Flow Algorithm (OFA) is possible through the implementation of a camera sensor onboard the vehicle flying within the virtual synthetic environment created in Gazebo. The same OFA can then directly be tested during flight onboard the actual vehicle.

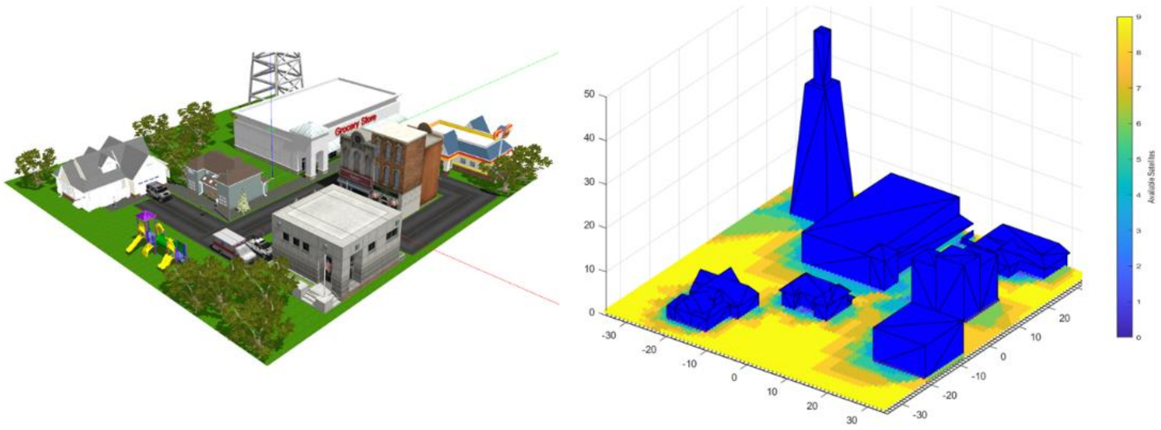

Figure 11. HIL Simulation Setup.

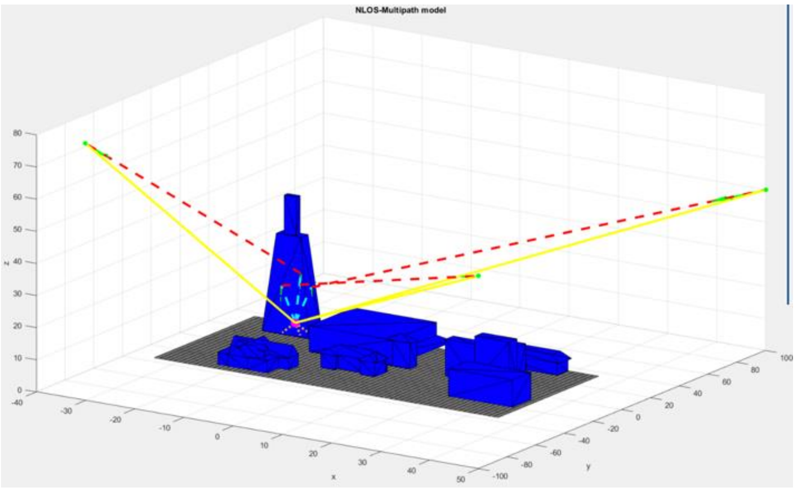

Figure 12. The Steps Taken by xPC Target to Compile Simulation onto Hardware.

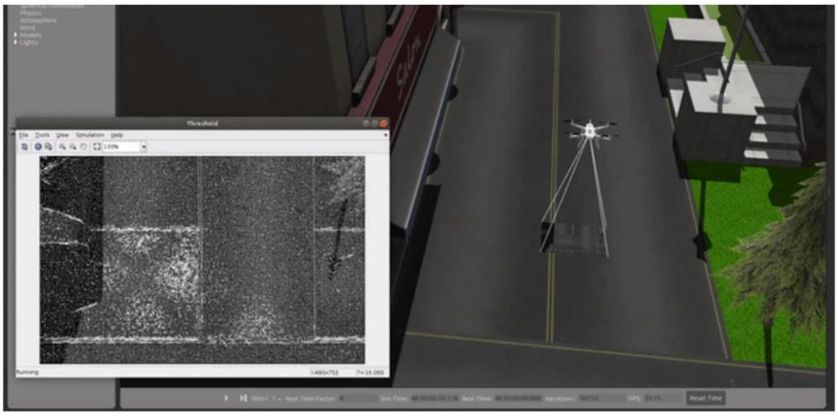

Figure 13. HIL Simulation Set.

The Academy of Model Aeronautics’ Daytona Beach field is used by ERAU team for flight testing programs. Approximately 1400 ft long and 1300 ft wide, the field has enough space to perform the necessary maneuvers. It has a single, hard-surface runway located on the east side. Figure 13 shows a satellite image of the field.

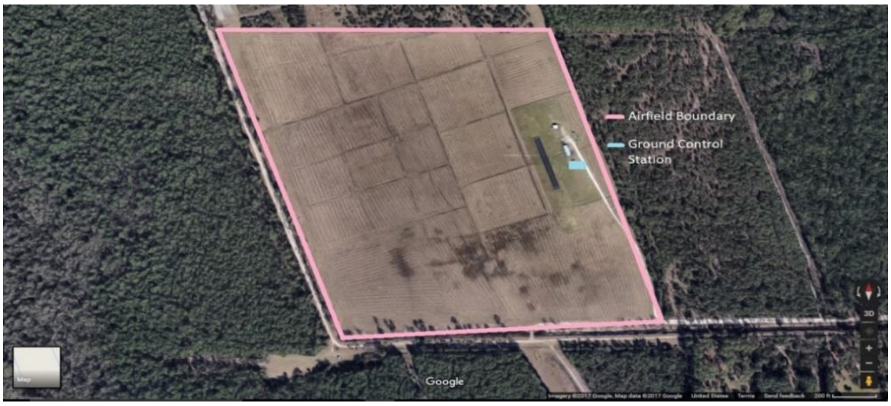

Figure 14. DBRC Field for Flight Testing.

5.3 UND Computational Resources

Dr. Prakash Ranganathan has a *Data Energy Cyber Systems Lab* with a maximum accommodation for thirteen students. This lab is equipped with a single unit High-Performance computing system (2TB SSD, 64GB RAM and 4X11GB GPU NVIDIA RTX 2080) smart grid equipment such as phasor measurement units/aggregators, battery units, relays, GPS, and wireless sensor motes. Dr. Ranganathan has access to software that includes SEL's SynchroWave software, AMPL, MATLAB, ETAP, *R*, *TensorFlow/PyTorch*, GPUs, and machine learning libraries. A swarm test bed that contains six UAS (DJI M100, M30, M300, M2EA, Mavic 3, Yuneec, Tarot), and custom test bed for a GPS spoofing station, thirteen desktops that have access to UND's high-performance computing and departmental virtualized servers. There are several clusters with state-of-the-art computers and peripheral equipment in the UND College of Engineering building.

UND has a high-performance computer to store and access data. UND has installed a 150-TB DDN AI400 40-GB/s Lustre-based storage appliance. It is online and tested with the base install with the Talon GPU nodes. UND will host all forecasting and data sets in a secured server. The HPC operates Hodor, a Linux HPC cluster comprised of 32 compute nodes, a single head node, and 110 TB of usable storage. Each computer node within Hodor is equipped with two quad-core 3.3-GHz Intel Sandy Bridge processors and 64 GB of RAM. Cluster communication is provided through a private 56 G-bit InfiniBand FDR interconnect. Four Nvidia Tesla K20 GPU accelerators and four Intel Xeon Phi 3120P co-processors have been installed in Hodor.

6. SUMMARY

This Planning the Testing and Demonstration of Mitigations report fulfills Task 3 for the A44 ASSURE project. It prioritizes the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable. It places particular emphasis on prioritizing mitigations that support sUAS operations that will be tested in Task 4. The use of simulated flight data is included as a significant source of test data for evaluation.

The report contains a test plan for UAS navigation anomalies including dropouts and erroneous data, GPS and ADS-B signal jamming, and GPS and ADS-B signal spoofing. The UAS anomalies chapter focused on using ADS-B data sets to identify ADS-B anomalies that would result in ceasing operations and to identify the scenarios that are most common. With this data the use of hybrid machine learning models will be explored. For the jamming chapter, the evaluation of the capabilities, advantages, and limitations of OPNAV and GNAV techniques will be tested using both flight and simulated data. In addition, a test is developed to record and utilize nearby LTE/4G cellular signals to inform a GNSS-independent positioning solution from a UAS-based receiver. For the spoofing chapter, the ECD method is used in a simulation environment that will produce data to assess its effectiveness in a challenging scenario.

With the test plan outlined in this Task 3 report for ASSURE A44, significant flight and simulator data will be acquired to best inform on the capabilities and weaknesses of GPS and ADS-B data.

7. REFERENCES

Adamy, David. 2021. *Space Electronic Warfare*. Artech House. https://us.artechhouse.com/EW-105-Space-Electronic-Warfare-P2178.aspx.

AXELRAD, PENINA, BEN K. BRADLEY, JAMES DONNA, MEGAN MITCHELL, and SHAN MOHIUDDIN. 2011. "Collective Detection and Direct Positioning Using Multiple GNSS Satellites." *NAVIGATION* 58 (4): 305–21. https://doi.org/10.1002/j.2161-4296.2011.tb02588.x.

Bissig, Pascal, Manuel Eichelberger, and Roger Wattenhofer. 2017. "Fast and Robust GPS Fix Using One Millisecond of Data." www.disco.ethz.ch.

David Adamy. 2015. *EW 104: Electronic Warfare Against a New Generation of Threats*. Artech. http://ieeexplore.ieee.org.ezproxy.library.und.edu/document/9100860.

Diggelen, F.S.T Van. 2009. *A-GPS: Assisted GPS, GNSS, and SBAS*. NYC: Artech House. https://us.artechhouse.com/A-GPS-Assisted-GPS-GNSS-and-SBAS-P1344.aspx.

Eichelberger, Manuel. 2019. "ETH Library Robust Global Localization Using GPS and Aircraft Signals." https://doi.org/10.3929/ethz-b-000379990.

Fei, Fan, Zhan Tu, Ruikun Yu, Taegyu Kim, Xiangyu Zhang, Dongyan Xu, and Xinyan Deng. 2018. "Cross-Layer Retrofitting of UAVs Against Cyber-Physical Attacks." In *2018 IEEE International Conference on Robotics and Automation (ICRA)*, 550–57. https://doi.org/10.1109/ICRA.2018.8462886.

IS-GPS-200G, Navstar. 2013. "IS-GPS-200H, GLOBAL POSITIONING SYSTEMS DIRECTORATE SYSTEMS ENGINEERING & INTEGRATION: INTERFACE SPECIFICATION IS-GPS-200 - NAVSTAR GPS SPACE SEGMENT/NAVIGATION USER INTERFACES (24-SEP-2013)." http://everyspec.com/MISC/IS-GPS-200H_53530/.

Liu, Gaoyang, Rui Zhang, Yang Yang, Chen Wang, and Ling Liu. 2021. "GPS Spoofed or Not? Exploiting RSSI and TSS in Crowdsourced Air Traffic Control Data." *Distributed and Parallel Databases* 39 (1): 231–57. https://doi.org/10.1007/s10619-020-07302-1.

Liu, Jie, Bodhi Priyantha, Ted Hart, Heitor S. Ramos, Antonio A. F. Loureiro, and Qiang Wang. 2012. "Energy Efficient GPS Sensing with Cloud Offloading." In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, 85–98. SenSys '12. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2426656.2426666.

Marouani, Hicham, and Michel R. Dagenais. 2008. "Internal Clock Drift Estimation in Computer Clusters." *Journal of Computer Networks and Communications* 2008 (May): e583162. https://doi.org/10.1155/2008/583162.

Mrabet, Zakaria El. 2022. “Real-Time Machine Learning Models To Detect Cyber And Physical Anomalies In Power Systems,” January, 147.

Mrabet, Zakaria El, Daisy Flora Selvaraj, and Prakash Ranganathan. 2019. “Adaptive Hoeffding Tree with Transfer Learning for Streaming Synchrophasor Data Sets.” In *2019 IEEE International Conference on Big Data (Big Data)*, 5697–5704. https://doi.org/10.1109/BigData47090.2019.9005720.

Nichols, R K, dir. 2022. *Meeting with ERAU Team Re Testing of ECD*.

Nichols, R K, M. Carter Candice, John Hood, Mark ; Jackson, M.J. Johnson Siny, Haley Larson, Wayne D. Lonstein, et al. 2022. *Space Systems: Emerging Technologies and Operations*.

Nichols, Randall K, Hans C Mumm, Wayne D Lonstein, Julie JCH Ryan, Candice Carter, and Julie Jch. 2020. “Counter Unmanned Aircraft Systems Technologies and Counter Unmanned Aircraft Systems Technologies and Operations Operations.” https://newprairiepress.org/ebooks.

Semanjski, Silvio, Alain Muls, Ivana Semanjski, and Wim De Wilde. 2019. “Use and Validation of Supervised Machine Learning Approach for Detection of GNSS Signal Spoofing.” In *2019 International Conference on Localization and GNSS (ICL-GNSS)*, 1–6. https://doi.org/10.1109/ICL-GNSS.2019.8752775.

Semke, William. 2022a. “Task 1 A11L.UAS.86 - A44 Mitigating GPS and ADS-B Risks for UAS - Literature Review. UND.”

Semke, William. 2022b. “Task 2 A11L.UAS.86 - A44 Mitigating GPS and ADS-B Risks for UAS. UND.”

Son, Yunmok, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors,” August, 17.

Zhou, Jia, Guoqi Xie, Haibo Zeng, Weizhe Zhang, Laurence T. Yang, Mamoun Alazab, and Renfa Li. 2022. “A Model-Based Method for Enabling Source Mapping and Intrusion Detection on Proprietary Can Bus.” *IEEE Transactions on Intelligent Transportation Systems*, 1–11. https://doi.org/10.1109/TITS.2022.3153718.