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

March 25, 2022

v 1.0

NOTICE

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. Enter the report number assigned by the sponsoring agency.	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle A44 Task 1 Literature Review for Mitigating GPS and ADS-B risks for UAS		**5. Report Date** March 25, 2022
		6. Performing Organization Code Enter any/all unique numbers assigned to the performing organization, if applicable.
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.** Enter any/all unique alphanumeric report numbers assigned by the performing organization, if applicable.
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** Task 1
		14. Sponsoring Agency Code code
15. Supplementary Notes		

16. Abstract

This literature review identifies the potential safety and security risks of relying on GPS and ADS-B data used for UAS operations based upon review of scholarly, government, and industry sources. The literature review assesses signal dropouts, erroneous data, jamming, spoofing, and other potential causes that may result in safety or security risks to UAS operations that rely on GPS and ADS-B data.

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. Enter any other agency mandated distribution statements. Remove NTIS statement if it does not apply.

19. Security Classification (of this report) Unclassified	**20. Security Classification (of this page)** Unclassified	**21. No. of Pages** 124	**22. Price**

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

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF ACRONYMS

1090ES	1090 Extended Squitter Data Link
a/c	Aircraft (Piloted or unmanned) also A/C
A/CFD	Aircraft Flood Denial jamming
ACAS	Airborne Collision Avoidance System
ADS - B	Automatic Dependent Surveillance – Broadcast systems
AOA	Angle of Arrival of signals to GPS receivers
ATC	Air Traffic Control / Air traffic Control Signals
ATCC	Air Traffic Control Center
ATM	Air Traffic Management
ATRAN	Automatic Terrain Recognition and Navigation System
ATS	Air Traffic Services
ATSAW	Air Traffic Situational Awareness
ATO	Air Traffic Organization
BVLOS	Beyond Visual Line-Of-Sight operations
C2	Command and Control
C /A	GPS Satellite Course Acquisition unique code, $ca_I(t)$ in Appendix A
C/No	Carrier to Noise ratio
CCC	Circular Cross-Correlation
CD	Collective Detection maximum likelihood localization approach (Eichelberger 2019)
CDMA	Code Division Multiple Access Protocol
CIA	Confidentiality, Integrity & Availability (standard INFOSEC paradigm)
CM	Countermeasure
CNPC	Control and Non-Payload links
COTS	Commercial Off-The-Shelf
CTN	Course -Time Navigation
DHS	Department of Homeland Security
DoS	Denial-of-Service
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
GNSS	Global Navigation Satellite System (GPS,GLONASS, Galileo, Beidou & other regional systems)
GNU	GNU / Linux Operating system
GPS	Global Positioning System
GS	Ground Station
GSFD	Ground Station Flood Denial jamming
HAPS UAVs	UAVs dedicated to HAPS service (example to communicate via CNPC links)
HAPS	High Altitude Platforms (generally for wireless communications enhancements)
HOW	Hand-Over-Word satellite data timestamp defined in (I.S.-G.P.S.-200G 2013)
ICAO	International Civil Aviation Organization
IMU	Inertial Measurement Unit
INFOSEC	Information Security

INS	Inertial Navigation System
ITE	Installation, Training & Expensive
ITP	In Trail Procedure
KSU	Kansas State University
LED	Light Emitting Diodes
LOS	Line-of-sight / Loss of Signal / Loss of Separation
LTE	Long-Term Evolution
MitM	Man-in-the-Middle
MLAT	Multilateration System
NASA	National Aeronautics and Space Administration
NDM	Navigation data modification spoofing attack
NLSO	Non-Line-Of-Sight
NMA	See Navigation Message Authentication
OrSU	Oregon State University
OTH	Over-The-Horizon
PEN	Probabilistic Environment Navigation
PMU	Phasor Measurement Unit
PRN	Pseudo-Random Noise
PSR	Primary Surveillance Radar
RF	Radio Frequency
RFID	Radio Frequency Identification (tags)
RN	Ryan-Nichols qualitative information security risk equations
RSS	Received Signal Strength.
SDR	Software Defined Radio.
SEN	Structured Environment Navigation
SIC	Successive Signal Interference Cancellation
SLAM	Simultaneous Localization and Mapping
SNR	Signal to Noise Ratio
SRMGSA	Safety Risk Management Guidance for System Acquisitions
SSLT	Seamless Satellite-Lock Takeover spoofing attack
SSR	Secondary Surveillance Radar
sUAS	Small Unmanned Aircraft System
TCAS	Traffic Collision Avoidance System
TDOA	Time Difference Of Arrival
TOA	Time of Arrival
ToF	Time of Flight
TTFF	Time To First Fix (latency)
UAF	University of Alaska, Fairbanks
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicle
UAT	Universal access transceiver
UND	University of North Dakota
USAF	United States Air force
UTM	Unmanned Traffic Management
VDL	VHF Data link
WAM	Wide Area Multilateration

EXECUTIVE SUMMARY

Unvalidated or unavailable Automatic Dependent Surveillance-Broadcast (ADS-B) and Global Position Systems (GPS) data poses security and safety risks to automated Unmanned Aircraft Systems (UAS) navigation and to Detect and Avoid (DAA) operations. Erroneous, spoofed, jammed, or drop outs of GPS data may result in unmanned 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 "ADSB-In" data may result in automated unmanned 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 unmanned 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 research may lead to new navigation requirements related to GPS as well.

The team conducted a literature review and meta-analysis that identified the potential safety and security risks of relying on GPS and ADS-B data used for UAS operations. It is divided into three areas of investigation: signal dropouts and erroneous data, jamming, and spoofing that may result in safety or security risks to UAS operations that rely on GPS and ADS-B data. The report also includes a safety and security risk assessment of potential UAS operations that rely on GPS and ADS-B data.

As expected, the analysis found that the only low risk situations occur with operations in the Part 107 conditions, the medium risk category contains primarily BVLOS conditions, and the high risk category contains primarily urban and near airport operations, which require significant mitigation schemes to reduce the risk to an acceptable level.

Going forward, based on the risk assessment in Task 1, the research team will conduct a market survey of market solutions to mitigate loss of GPS and loss of ADS-B data as part of Task 2. The work will focus on reducing the level of risk for medium risk operations, while also considering solutions for high risk operations. Mitigating BVLOS operations flying at low altitudes and conducting long linear infrastructure inspection, agriculture operations, package delivery, or aerial surveillance will be a focus area. The market solutions to mitigate unvalidated GPS and unvalidated ADS-B In data and will include estimated costs, ease of implementation, and a preliminary assessment of their effectiveness. The research team will explore and propose potential solutions for GPS mitigation strategies for denied and/or jammed environments, in addition to cybersecurity and counterintelligence measures. Finally, the team will examine the recorded ABS-B data to expose potential risks and provide guidance on mitigation schemes.

I. INTRODUCTION & BACKGROUND

The FAA position communicated to RTCA Special Committee 228 is that that UAS DAA systems should validate "ADS-B In" data before it is used to conduct Detect and Avoid (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. Example potential risks and mitigations that were 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 (ATC) 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 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 in 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 (GCS), 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 have a means to detect ADS-B dropouts and jamming and 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 desires 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 Signal to Noise ratio or time of flight analysis. Have an ability for overriding UAS automated collision avoidance on unvalidated "ADS-B In" tracks. Cease UAS operations when false (ADS-B In" tracks are detected.

This project is intended to assess the safety and security risks of unvalidated GPS and ADS-B In data used to support a variety of UAS operations to include primarily sUAS operations, while also

providing data to unmanned cargo transport and remotely piloted passenger transport operations where applicable. For sUAS operations, low cost and easy to implement mitigations commensurate with their safety and security risks is emphasized

The literature review presented in this document represents the initial step towards identifying potential safety and security risks of relying on GPS and ADS-B data used for UAS operations. It includes an initial description of potential causes that may result in safety or security risks to UAS operations that rely on GPS and ADS-B data. Much of the published work has a focus on mitigation schemes and do not produce a risk assessment. The research team worked to understand the situations and produce a risk assessment of the operational scenarios. Over 200 references are included in this literature review that contributed to the findings presented.

This report is organized into six major categories of ADS-B and GPS data safety and security risks: ADS-B Dropouts and Erroneous Data, GPS Dropouts and Erroneous Data, ADS-B Jamming, GPS Jamming, ADS-B Spooking, and GPS Spoofing. The research team has contributors in each area and the literature review findings will be presented. The findings are divided into four sections: Risk Assessment Overview, Dropouts and Erroneous Data Literature Review, Jamming Literature Review, Spoofing Literature Review, and Standards Bodies Literature Review.

The Risk Assessment Overview provided a high-level risk assessment summary of the findings that are broken into the six major categories in four different scenarios to assess the risk and illustrate a risk continuum depending on the environment in which the aircraft are operated. The next three sections each focus on one of the major categories and gives more depth into the past and present work in these areas.

II. RISK ASSESSMENT OVERVIEW

Risk assessments are needed to inform FAA policy decisions and to inform follow-on tasks in this research project that will explore potential low cost mitigations. The risk assessments presented here are preliminary and based on the expertise of the research team and the literature review. It is important to note that the likelihood of malicious acts impacting GPS and ADS-B have been increasing over time. This is in part due to the forward advancement of available technology and the decrease in technology cost over time. The risk assessments presented here use projected likelihoods based on current trends and the subject matter expertise of the research team for the 2025 to 2030 timeframe.

The FAA regulates drone operations to represent and protect the interests of third parties that might otherwise be negatively impacted by drone operations. Most drone rules and regulations are built around operators complying with the regulations during operations. Therefore, these drone risk assessments are intended to inform operational approvals and changes to the National Airspace System that would be applied to law abiding drone operators. Another primary purpose of the drone risk assessments is to represent third parties that may be adversely harmed by drone operations. This counter balances the drone industry's self-interests that may at times neglect the safety interests of third parties

A summary of the risk assessments is provided based on the literature review and subject matter expert discussions. The risk assessments were informed by Order 8040.6 which provides additional information to what is listed in Order 8040.4. The risk assessments were also informed by the Safety Management System (SMS) Air Traffic Organization (ATO) SMS Manual, and Safety Risk Management Guidance for System Acquisitions (SRMGSA) along with internal risk assessment measures. Order 8040.6 states that for operations above 400' above ground level (AGL) in class G airspace, the FAA follows the UAS Safety Risk Management (SRM) policy. Order 8040.6 provides the following tables and risk matrices to be used for drone operations in class G airspace below 400' AGL and for operations below the ATO Facility Map Altitudes.

Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Negligible safety effect	– Physical discomfort to persons – Slight damage to aircraft/vehicle	– Physical distress or injuries to persons – Substantial damage to aircraft/vehicle	Multiple serious injuries; fatal injury to a relatively small number of persons (one or two); or a hull loss without fatalities	Multiple fatalities (or fatality to all on board) usually with the loss of aircraft/ vehicle

* Excludes vehicles, crew, and participants of commercial space flight.

Fig. 1 FAA Order 8040.6 Severity Definitions

For Fig. 1 Order 8040.6 Severity Definitions, it is often interpreted that the severity that is of most interest is the severity experienced by people and systems external to the drone and its remote pilot. This includes people on the ground, people in other aircraft, damage to other aircraft, and so forth.

	Qualitative	Quantitative – Time/Calendar-based Occurrences Domain-wide/System-wide
Frequent A	Expected to occur routinely	Expected to occur more than 100 times per year (or more than approximately 10 times a month)
Probable B	Expected to occur often	Expected to occur between 10 and 100 times per year (or approximately 1-10 times a month)
Remote C	Expected to occur infrequently	Expected to occur one time every 1 month to 1 year
Extremely Remote D	Expected to occur rarely	Expected to occur one time every 1 to 10 years
Extremely Improbable E	Unlikely to occur, but not impossible	Expected to occur less than one time every 10 years

Fig. 2 FAA Order 8040.6 Likelihood definitions for general aviation operations for small aircraft and rotorcraft.

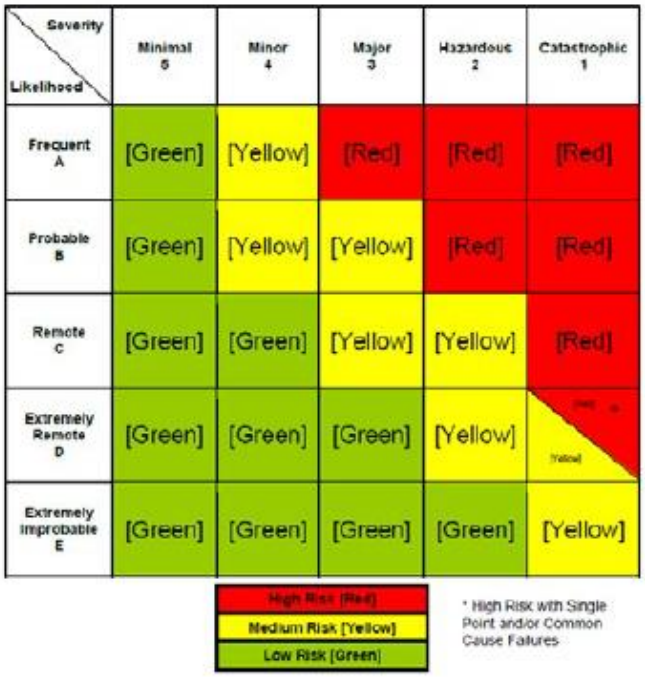

Fig. 3. Order 8040.6 risk matrix for general aviation operations for small aircraft and rotorcraft.

The FAA ATO SMS manual provides guidelines to assess the severity and likelihood of identified risks under the domain of the FAA ATO. This includes drone operations above 400' AGL in class G airspace, operations above the ATO Facility Map Altitudes, and operations in all other airspace. For flight operations, the research team used the SMS severity classifications for UAS shown in Figure 4. In addition to these severity classifications and additional security classifications for security risks was developed, as shown in Figure 2.

Severity Classifications for Unmanned Aircraft Systems

Effect On	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
▼	Conditions resulting in any one of the following:				
Unmanned Aircraft Systems	Discomfort to those on the ground Loss of separation leading to a Measure of Compliance greater than or equal to 66 percent	Low Risk Analysis Event severity, two or fewer indicators fail Non-serious injury to three or fewer people on the ground	Medium Risk Analysis Event severity, three indicators fail Non-serious injury to more than three people on the ground A reduced ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins Manned aircraft making an evasive maneuver, but proximity from Unmanned Aircraft remains greater than 500 feet	High Risk Analysis Event severity, four indicators fail Incapacitation to Unmanned Aircraft System crew Proximity of less than 500 feet to a manned aircraft Serious injury to persons other than the Unmanned Aircraft System crew	A collision with a manned aircraft Fatality or fatal injury to persons other than the Unmanned Aircraft System crew

Fig. 4. Severity Classifications of flight operations for Unmanned Aircraft Systems from the Safety Management System ATO SMS Manual.

The SMS qualitative likelihood table used for both flight operations and security threats under the domain of the FAA ATO is shown in Figure 5.

Likelihood Table — Qualitative

Note: This table only applies if the proposed NAS change or existing safety issue affects all ATO operations in a particular air traffic domain. Therefore, it cannot be used for site-specific changes or issues.

	Operations: Expected Occurrence Rate (Calendar-based) Qualitative (Domain-wide: NAS-wide, Terminal, or En Route)
A Frequent	Equal to or more than once per week
B Probable	Less than once per week and equal to or more than once per three months
C Remote	Less than once per three months and equal to or more than once per three years
D Extremely Remote	Less than once per three years and equal to or more than once per 30 years
E Extremely Improbable	Less than once per 30 years

Fig. 5. Qualitative Likelihood Table for Unmanned Aircraft Systems from the Safety Management System ATO SMS Manual.

As noted in Figure 5 of the ATO SMS Manual and in Figure 2 of order 8040.6, the FAA likelihood criteria only applies to proposed NAS wide changes that affect all similar operations in a particular air traffic domain. FAA likelihood tables are intended to assess the safety of wide scale changes and new types of operations applied across the NAS. For a given severity assignment, the associated likelihood tables refer to all events across all similar drone operations throughout the NAS. The FAA likelihood tables are not for a single drone and its specific operation. For example, there is a large difference between the likelihood of a specific drone and its operation experiencing a certain severity rating every 3 years and the likelihood of any drone throughout the entire NAS

that is operating in a similar manner experiencing the same severity rating every 3 years. Using these definitions, the risk matrix and associated classifications under the domain of the FAA ATO are shown in Figure 6.

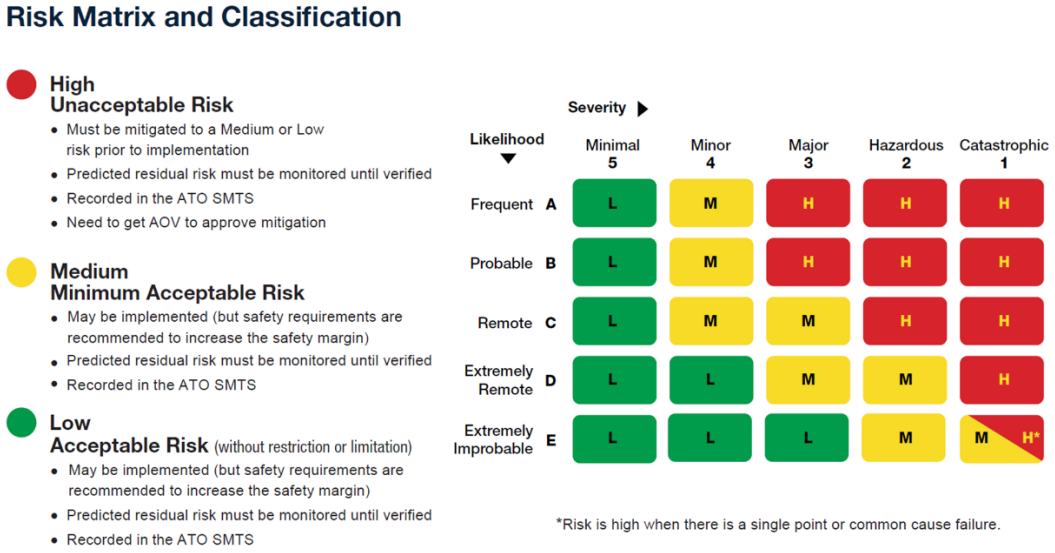

Fig. 6. Risk Assessment and Classifications for Unmanned Aircraft Systems from the Safety Management System ATO SMS Manual.

In order to use the likelihood tables, the risk assessment assumes a 2025-2030 timeframe. It assumes that there are many tens of thousands of BVLOS drone operations throughout the NAS over rural areas, over urban areas, and also near airports.

Many drones receive GPS signals for navigation. This risk assessment will examine the potential severity and likelihood of outcomes for drone operations where GPS is the sole means of navigating beyond visual line of sight (BVLOS). Risk assessments will include events traced to GPS dropouts and erroneous GPS signals derived from non-malicious causes. In addition, this risk assessment will also examine the risks of cyber attacks that jam or spoof GPS signals used for drone navigation.

This risk assessment will also investigate the potential severity and likelihood of outcomes for drone operations where the drone uses “ADS-B In” as the sole means of detecting other aircraft transmitting “ADS-B Out”. This risk assessment assumes that all other aircraft are equipped with “ADS-B Out” and that the drone does not have additional surveillance capabilities to detect approaching aircraft. The purpose of this risk assessment is to focus on potential risks that may occur under these theoretical assumptions and conditions. The risk assessment can then be leveraged when considering future changes to the NAS to enable wider drone operations. One such theoretical concept includes mandating ADS-B equipage on crewed aircraft that are operating at low altitudes in order to provide a low cost and easy way for drones to detect and avoid them. This risk assessment will inform discussions on the potential risks of over reliance on ADS-B as a means for aircraft detection under these hypothetical scenarios.

By focusing only on the avoidance of other aircraft equipped with "ADS-B Out", the risk assessment will also inform DAA standards and DAA architectures that intend to operate in the National Airspace System as it exists today. A concern that has been expressed by the small UAS DAA industry is that the cost and complexities of independent validation of ADS-B messages can be high and overly burdensome. By focusing the risk assessment only on interactions between the drone and ADS-B equipped aircraft, this risk assessment can also inform those discussions.

Many DAA architectures for small drones that operate Beyond Visual Line of Sight (BVLOS) use received ADS-B signals transmitted from other aircraft in order to Detect and Avoid (DAA) them. This risk assessment will examine the potential severity and likelihood of outcomes if the ADS-B information is not received by the drone due to signal drop outs or if the information in them is erroneous from non-malicious causes. In addition, this risk assessment will also examine the risks of cyber attacks that jam or spoof ADS-B signals used by the drone for detecting and avoiding other aircraft. The risk assessment will assume that the drone only encounters other aircraft that are equipped with ADS-B Out transmitters. It will also assume that ADS-B receivers are the sole sensors that the drone has for detecting and avoiding these ADS-B Out transmitting aircraft (e.g. there are not other Detect and Avoid sensors such as radar and cameras). This isolate the operational risks related directly to relying solely on received ADS-B signals for drone avoidance of ADS-B Out transmitting aircraft to inform the degree that mitigations may be needed. Because the information contained within transmitted ADS-B signals is derived from the transmitting aircraft's GPS positional data, if the aircraft transmitting ADS-B messages to the drone experiences a GPS dropout, that will in turn impact the usability of the ADS-B message to be used by the drone for Detect and Avoid. Hence, the risks associated with using received ADS-B signals for Detect and Avoid are impacted by the GPS signals that other aircraft rely on for creating ADS-B messages. A wide area GPS drop out or jamming event will not only impact the drone's ability to navigate but also the drone's ability to Detect and Avoid aircraft.

Another assumption in this risk assessment is that there are not obstructions between ADS-B transmitters and ADS-B receivers. It is assumed that adequate ADS-B surveillance coverage has already been obtained for the drone operation. There are generally two ways in which ADS-B messages are received for use in a low altitude Detect and Avoid (DAA) system. The first is directly from the transmitting aircraft to the drone operation using an ADS-B In receiver that is part of the drone DAA system. This is often the preferred approach because it has the best coverage for the drone operation with the least amount of latency. The second approach is via a subscription to an external network where the signal was received by an ADS-B In receiver owned by another entity and then relayed to the drone operation and its DAA system. This second approach often results in limited low altitude coverage due to earth curvature and radio line of sight obstructions caused by the surrounding terrain and structures. Whatever approach is used, this risk assessment assumes that the transmitting aircraft are within the surveillance coverage area of the ADS-B In receiver.

The six major categories of ADS-B and GPS data safety and security risks: ADS-B Dropouts and Erroneous Data, GPS Dropouts and Erroneous Data, ADS-B Jamming, GPS Jamming, ADS-B Spoofing, and GPS Spoofing are broken into smaller operation types. Further definition of the Risk Assessment is required to provide a clear and informative overview, the mission operation types are broken into four classifications: Part 107 Operations, Beyond Visual Line Of Sight

(BVLOS) over rural areas BVLOS Operations over Urban Areas, and BVLOS operations Near Airports in class B, Class C, or Class D airspace or airports which have Facility Map Altitude limitations. For BVLOS operations near airports, the drone operation under evaluation is intended to remain under the facility map altitudes and the risk assessment will also consider events that may result in the drone crossing facility map altitudes in addition to other risks. For each category, the severity and likelihood probability and associated references is presented.

Part 107 Operations will serve as the base reference. BVLOS operations over rural areas is the next category as it is crucial for many UAS operations and is of great importance to the UAS community. BVLOS operations over urban areas represent a unique case due to signal interruptions and other artifacts along with the density of humans and infrastructure. BVLOS operations near airports operations represent another unique situation due to the air traffic density and potential impacts to commercial airline traffic.

The team used a qualitative approach to risk assessment as there is a void in literature in regard to an appropriate quantitative scale. The risk levels are chosen by the ASSURE subject matter experts involved in this project in all the categories reviewed. They are based on an extensive literature review on the topics and use the most up-to-date and comprehensive studies that are available.

2-1 ADS-B Dropout and Erroneous Data Risk Classes

A typical ADS-B system broadcasts an unencrypted message including the aircraft velocity, position, direction, and other Air Traffic Management (ATM) and control related information to nearby aircraft and ground station over radio transmission links on a regular basis. Usually, the update rate is about one message per second. However, the unencrypted nature of the ADS-B messages along with their transmission over wireless networks make them exposed to several anomalies, including the dropout and erroneous data. Dropout of ADS-B data in this risk assessment refers to any discontinuation in the update rate of greater than the nominal one second interval that results in a sufficient duration to impact the ability for the information to be used to detect and avoid an aircraft that is transmitting ADS-B Out. ADS-B dropouts have various causes. They may occur due to error by an onboard pilot in using their ADS-B Out equipage, malfunctioning onboard equipment, loss of GPS signals that are used to form ADS-B messages, and many other potential causes. During periods when no ADS-B signals are being received in the region, it may not always be known whether this is due to a lack of local air traffic or due to a dropout condition.

ADS-B dropouts and erroneous ADS-B information that occur somewhere within the NAS are expected to occur regularly and with a likelihood assignment of Frequent. However, the likelihood that there is a dropout that occurs simultaneously to the data being needed for a drone to detect and avoid the aircraft transmitting the ADS-B information is expected to be much less that. Hence the likelihoods associated with severity outcomes is expected to be less than frequent even though dropouts and erroneous data received by drones across the NAS may be frequent.

(Tabassum and Semke 2018; Tabassum 2017; Semke et al. 2017). On the other hand, erroneous data implies all errors induced into the ADS-B data that comprise communication integrity (Kinowski and Skorupski 2016).

2.1.1 ADS-B Dropouts and Part 107 operations

Severity = 5 (Minimal) and Likelihood = D Extremely Remote Risk Level **LOW**

Small unmanned aircraft systems operating under Part 107 have to obey a certain set of rules, including avoiding manned aircraft, keeping the drone within sight, altitude restrictions, flying safely, not pose a hazard, avoiding potential collisions, and abiding by certain operational limitations. Part 107 operations are also limited to drones weighing less than 55 lbs. However, it is likely that certain external anomalies, related to the environment and cyberattacks, or internal anomalies, related to the system itself, could still impact the flying experience which are addressed in the jamming and spoofing sections of this report. Part 107 operators may choose to supplement their visual operation with a device that allows them to receive ADS-B information for greater airspace awareness. This may be received directly from the transmitting aircraft or through a network service that relays information from a ground station to the Part 107 operator. Multipath reflection and RF interference are examples of external threats. Multipath, spoofing, natural disaster, and ionospheric scintillations at high and low latitudes are also major factors in inducing erroneous data into the ADS-B messages and compromising communication integrity. Part 107 operations are based on visual separation of the drone with crewed aircraft (see Part 107.31). Part 107 operations are often limited to very low altitudes below 400 feet above ground level (AGL) (see Part 107.51) which reduces the likelihood of mid-air collisions. There is an option to request a waiver to operate at higher altitudes, and when within 400 feet of a ground based structure, the sUA may operate at any AGL altitude compliant with 107.31. For example, the sUA may fly at 1000'agl if within 400 feet of a radio tower and if the operation meets 107.31. Use of generally, or just saying the regulation with a few exeptions (reference the reg IE 107.51B) etc. Part 107 operations may optionally leverage received ADS-B messages for enhanced airspace situational awareness. Because Part 107 operations require visual means of separation and are not solely reliant on ADS-B messages for keeping the drone separated from ADS-B equipped aircraft, an interruption of ADS-B messages does not result in a critical failure for keeping the drone separated from other aircraft. Part 107 operators are not required to receive ADS-B information, and hence the impact of ADS-B dropouts or errant ADS-B information is minimal. Because most Part 107 operators do not use ADS-B information, the likelihood that ADS-B drop outs will impact Part 107 operations even in a minimal way when the information may be useful for enhanced situational awareness is estimated to be Extremely Remote. This qualitative likelihood is a combination of the number of Part 107 operations that may optionally choose to receive ADS-B information and the simultaneous chance that the drone encounters a manned aircraft and that there is also an ADS-B dropout.

It should be noted that the FAA tables are intended to be used by the FAA when considering changes to the NAS. Since Part 107 operations are already part of the regulatory structure these drone operations are not a change to the NAS. Part 107 operations occur regularly every day. However, this Part 107 risk assessment was conducted anyway as a reference baseline when considering future BVLOS operations.

Associated References: (Tabassum 2017; B. S. Ali et al. 2014; Kinowski and Skorupski 2016), (Aquino et al. 2009), (Park et al. 2017)

2.1.2 ADS-B Dropouts and Beyond Visual line of sight (BVLOS) Operations in Rural Areas Below 400' AGL

Severity = 2 Hazardous and Likelihood = D Extremely Remote Risk Level **MEDIUM**

Operating BVLOS introduces additional risks as compared to operating within visual line of sight (VLOS) resulting in a higher level of risk. For Part 107 operations, ADS-B messages provide an additional situational awareness safety enhancement to the baseline visual operations. In most rural areas, manned aircraft are not required to be equipped with ADS-B Out. These non-equipped aircraft are not part of this risk analysis. For our treatment of BVLOS operations, ADS-B is assumed to be the sole means of detecting other aircraft and that all the aircraft that the drone encounters are equipped with ADS-B Out transmitters. The isolation of risks related directly to ADS-B will then inform whether additional mitigations may be needed with respect to avoiding ADS-B intruders such as track validation, having a backup means of detection using sensors that can detect aircraft that are not transmitting ADS-B Out. We know that not all aircraft that the drone may encounter will be equipped with ADS-B Out, but this risk assessment is focused on aircraft with ADS-B equipage in order to directly inform the risks related to using ADS-B for Detect and Avoid. Because in this risk assessment we assume that received ADS-B messages are the sole means of detecting the ADS-B Out equipped aircraft, an ADS-B dropout of significant duration (e.g. one minute or less) therefore results in a complete loss of ability to Detect and Avoid. This may result in a mid-air collision with the ADS-B Out equipped aircraft. While BVLOS drones are not restricted to weighing less than 55 lbs as required in Part 107.3, for our assessment we assume that our BVLOS drones weigh just under 55 lbs. The drone weight and the collision speeds are important variables when assessing damage to a manned aircraft. Using the risk tables in 8040.6, the severity rating depends on whether a collision is more likely to result in one or two fatalities (Hazardous) or multiple fatalities (Catastrophic). For mid-air collisions in rural areas below 400' AGL, the most likely number of people to be onboard the aircraft was assumed to be limited to one or two persons in the vast majority of cases. Hence, a Hazardous severity rating is used to represent the most likely severity outcome of a mid-air collision while noting that there may be certain cases where more than two people might be onboard a low altitude aircraft in flying over a rural area (e.g. EMS Helicopter). The frequency of a Hazardous event occurring anywhere across the NAS when considering wide scale drone operations depends on the likelihood of ADS-B dropouts and the likelihood of non-malicious erroneous ADS-B data contributing to a collision. This is a combination of these ADS-B drop out events occurring along with the likelihood that one drone among many tens of thousands of BVLOS drones in the NAS flying in rural areas below 400' AGL, encounter a manned aircraft on a collision course. Using the end of the 2025-2030 timeframe, we make the assumption that there are many tens of thousands of BVLOS drones flying in the NAS on any given day. If we assume 100 BVLOS drones each day flying in rural areas in the NAS encounter a manned aircraft while there is simultaneously an ADS-B dropout or significantly erroneous ADS-B position data, that prevents the drone from performing detect and avoid, then we can estimate the unmitigated likelihood of collision given an encounter. Leveraging likelihood estimates by the ASSURE A47 project and from MIT Lincoln Laboratory analysis, the unmitigated probability of a drone colliding with a manned aircraft when there is an encounter depends on the definition of encounter used, the size of the drone, relative aircraft speeds, and assumptions about the randomness of encounter geometries. It comprises the product of the unmitigated probability of mid-air collision given a near mid-air collision (roughly 1 in 150) and the unmitigated probability of near mid-air collision given an encounter (roughly 1 in 250). Hence, the likelihood of an unmitigated mid-air collision given an encounter is estimated to be within an order of magnitude of 1 in 37,500. When multiplied by 100 drone encounters a day with simultaneous ADS-B dropouts or significant ADS-B errors, a rough order of magnitude estimate

results in a collision in the NAS to occur slightly less than once every year. This is on the border between likelihood definitions, but if it occurs on average less than once every year then in the 8040.6 risk tables this equates to an extremely remote probability. A change in the above assumptions could push the likelihood into a different category. This assessment assumes that there are not additional mitigations to avoid the approaching aircraft such as other sensors. Even though estimated values were used to help inform the likelihood, this is a qualitative assessment rather than a quantitative assessment. This is due to assumptions and unquantified uncertainties about the value of 100 BVLOS drone encounters a day in rural areas of the NAS where there is a simultaneous ADS-B dropout or significant ADS-B error.

Associated References: (Kinowski and Skorupski 2016; Tabassum 2017; Riahi Manesh and Kaabouch 2017; Martin Strohmeier, Lenders, and Martinovic 2014), (La Cour-Harbo, 2017), (Dolph et al. 2017)

2.1.3 ADS-B Dropouts and BVLOS Operation in Urban Areas Below 400' AGL

Severity = 1 Catastrophic and Likelihood = Extremely Remote Risk Level **MEDIUM**

Urban areas are characterized by an abundance of buildings, vehicles, trees, and other infrastructure that directly contribute to factors such as multipath reflection and obstruction that attenuate GPS signals, create interference, and which may impact the ADS-B data reliability. For the risk assessment we assume that ADS-B receivers have adequate field of regard surveillance coverage with direct line of sight to detect approaching aircraft that are transmitting ADS-B messages, even though multipath, wires, and other objects may interfere with or attenuate those signals.

Based on regulation 14 CFR Part 91.119, it is expected that the most common aircraft that the drone may encounter at low altitudes include helicopter operators performing emergency medical services, news gathering, police operations, or helicopter tours. It is assumed that on average, aircraft flying at or below 400' AGL over urban areas are more likely to have 3 or more people on board rather than just one or two. For example, it seems reasonable to expect that in cases involving air ambulance there are often multiple people onboard such as a pilot, emergency medical technician, and a patient. While a drone could encounter an air ambulance in a rural area, the assumption is that encounters with these aircraft are much more common when flying in urban areas where most hospitals are located. A hard landing of a helicopter in an urban area is also more likely to result in ground fatalities than in a rural area due to ground population densities. It is assumed that there is likely to be more fatalities that result from a drone collision when flying over an urban area as compared to a rural area. Because it is expected that there could be multiple fatalities that result from a drone collision when flying over urban areas, the severity assignment is Catastrophic.

A significant ADS-B dropout removes the ability for the drone to detect and avoid an approaching aircraft. Significantly erroneous ADS-B information also may prevent the drone from avoiding an approaching aircraft. Because urban areas are expected to create greater opportunities for multipath and unintentional interference with ADS-B messages, the likelihood of experiencing erroneous ADS-B information in urban areas is somewhat greater than in rural areas. It is also assumed that the concentration of manned aircraft activity and future drone operations will be higher over urban areas than over rural areas. This increases the likelihood of there simultaneously

being a drone encounter with a manned aircraft and also there either being an ADS-B dropout or significantly erroneous ADS-B information. The same likelihood justification and rationale for BVLOS operations over rural areas will be used, but the likelihood will be increased by one rating to account for the increased likelihood of collision due to increase traffic densities and greater opportunity for interference. Hence, the likelihood assignment without additional mitigations is Remote.
Associated References: (Morales and Kassas 2021; Lykou, Moustakas, and Gritzalis 2020; Lagkas et al. 2018; Gupta, Jain, and Vaszkun 2016), (Couturier and Akhloufi 2020), (Špánik et al., 2017), (Tongleamnak & Nagai, 2017), (Heng et al., 2015), (Bijjahalli et al. 2019)

2.1.4 ADS-B Dropouts and BVLOS Operation in Airspace Near Airports and under the Facility Map Altitudes

Severity = 1 Catastrophic and Likelihood = C (Remote) Risk Level **HIGH** **on ATO SMS Risk Matrix**

This risk assessment applies to BVLOS operations Near Airports in class B, Class C, or Class D airspace or which have Facility Map Altitude limitations that result in the use of the ATO SMS Risk Matrix. BVLOS drone operations near airports may include infrastructure inspection, package delivery from a distribution hub next to the airport, airport perimeter monitoring and security, and other operations. Drone flights near airports are likely to encounter aircraft with multiple passengers onboard. A collision resulting from an inability to detect and avoid because of ADS-B dropouts is assigned a Catastrophic severity rating. Airports are areas of concentrated traffic. Flying below 400 feet AGL and flying below the Facility Map Altitudes helps to keep BVLOS drones separated from manned air traffic. The Facility Map Altitudes help to constrain drone encounters in this high air traffic airspace. While the rate of encounters when operating near airports is expected to be higher than when operating over urban areas due to increased traffic, the Likelihood rating is assumed to remain within the same order of magnitude as with operations over urban areas. Hence a likelihood rating of Remote is assigned without additional mitigations beyond the Facility Map Altitudes.

Important to the ADS-B dropout assessment is an assumption that an ADS-B dropout event may go unnoticed. The drone may not be able to tell the cause of not receiving ADS-B information which could be that there is no proximate traffic, or that there is an ADS-B dropout that prevents detecting local traffic which may be a result of various causes such as pilot error, malfunctioning transmitter equipment, local radio obstruction such as a hill, and so forth.

Associated References: (Sedjelmaci, Senouci, and Messous 2016; Sedjelmaci, Senouci, and Ansari 2017; Cui et al. 2016; Morales and Kassas 2021; Souli, Kolios, and Ellinas 2020), (Li, 2009), (Aquino et al. 2009), (Park et al. 2017)

2-2 GPS Dropout and Erroneous Data Risk Classes

A formal definition for dropout of GPS data is not identified in scholarly literature, but for the purposes of this analysis, any circumstance that makes it conducive for GPS data to be degraded (poor or intermittent reception) or denied (unavailability of data for definite periods of time) can be classified as a factor contributing to dropped GPS data (Silvagni et al. 2017; Goforth and Lucey 2019). Erroneous data implies all errors induced into the ADS-B/GPS data, intentionally or

unintentionally, and attempts to comprise communication integrity (Kinowski and Skorupski 2016).

The quality and strength of received GPS signals can be significantly affected by terrestrial factors or causes beyond the earth's atmosphere which can lead. Two of these factors are multipath reflection and ionospheric scintillation which can lead to erroneous and dropped GPS data respectively. Multipath reflections are a significant source of error that particularly affects receivers that use differential GPS (DGPS) technology. Though the occurrence of the ionospheric scintillations and its effects is less likely, it can cause GPS data can be dropped because the GPS receiver on the sUAS can lose lock depending on the strength of magnetic storms

For this risk assessment it is assumed that GPS data is the sole means of long distance and long duration navigation. Many drones may be able to temporarily navigate for a short duration without a GPS update or with a temporary degradation in positional accuracy for a few seconds without significant impact on the performance or DAA. This risk assessment considers non-intentional and non-malicious GPS dropouts and GPS degradation that is significant enough to contribute to the severity outcomes listed in FAA severity tables. Many drones that use GPS for navigation are robust to a few missed GPS updates or a temporary change in GPS accuracy. However when operating near terrain or structures, the sensitivity to drop outs and GPS errors increases. GPS data is not only used for drone navigation, but it is also important for the drone to avoid manned aircraft that are transmitting ADS-B Out messages. Manned aircraft use GPS to create ADS-B Out messages containing their position that a drone can receive for detecting and avoiding the manned aircraft. GPS data is also received by the drone and used when forming the avoidance decisions for how the drone will safely avoid the manned aircraft that is transmitting ADS-B Out. GPS dropouts and erroneous GPS information that may impact a drone operating somewhere in the NAS is expected to occur frequently. However, frequent GPS dropouts does not result in drones causing frequent harm to other people on the ground or in other aircraft. For most GPS dropout events, no harm will occur. The below risk assessments leverage the FAA severity tables and determine the likelihood of those end outcomes listed on the severity tables. This results in a risk assignment for different categories of operations related to frequent GPS dropouts and erroneous GPS data.

2.2.1 GPS Dropouts and Part 107 operations

Severity = Various and Likelihood = Various All Risk Levels are **LOW**

Small unmanned aerial vehicles subject to Part 107 have operating requirements such as direct line of sight to the remote pilot in command (RPIC) unaided by any vision-assistive devices, a minimum weather visibility of 3 miles from the operator, altitude restrictions, weight limitations, restrictions for flight over people (see Part 107.39), an anti-collision lighting to make them more conspicuous at night, and many other operating rules.

Based on ASSURE project A50 drone statistics the most commonly flown drones are under 2 kg. While some Part 107 drone operations can be flown using GPS waypoints, it is assumed that the majority of Part 107 drones can also be flown manually. This combined with visual monitoring of the drone and the many operating restrictions placed on Part 107 operations serve to mitigate the potential effects of a GPS dropout and erroneous GPS information. Some Part 107 drones also have features that will cause the drone to hover/orbit until GPS is reacquired or becomes usable

again. Other Part 107 drones may perform an emergency landing. For Part 107 drones that can only be flown by waypoint and do not have these emergency features, the drone could potentially wander until it is flying over people and then potentially fall on them if other variables like loss of power come into play. This severity may be minor, major, or hazardous depending on the size and flight hours of the Part 107 drone. A hazardous severity is expected to be less common since heavier drones operated under Part 107 are not as common as lighter drones. . There are also additional requirements for heavier drones (drones over 55 lbs) to operate over people contained in the FAA's "Operations of Small Unmanned Aircraft Systems Over People" final rule. It is important to note that BVLOS drones are likely to be larger and heavier than most of the small drones sold. Commercial BVLOS drones will often have longer flight times, might have additional payloads, etc. than Part 107 operations (which include both commercial and personal drones). All combinations of severity and likelihood based on drone weight are expected to result in a LOW risk rating (hazardous and extremely improbable, major and extremely remote, minor and remote.

Most Part 107 drones can support flight times less than one hour due to their limited size. This limits the exposure time that a Part 107 drone without any manual controls and solely reliant on waypoint navigation may continue to fly/hover in the event of a GPS dropout. The likelihood that a GPS dropout or errant GPS information will cause a Part 107 drone operation to wander into the path of an oncoming aircraft is considered extremely improbable. For most Part 107 drones, the collision severity will be major or less based on the size of the Part 107 drone. Larger drones with a hazardous severity rating are less common and so their likelihood is also less at extremely improbable when flown with the intent to follow Part 107 rules. This rating is informed from an examination of historical drone collisions with conventional manned aircraft conducted by ASSURE project A47. This also assumes that there are no manual controls for the remote pilot to manually fly the drone, and that the drone does not perform an emergency landing when GPS is lost or becomes unusable. The various severity and likelihood combinations for this risk of a drone colliding with a manned aircraft due to GPS dropouts or errant GPS information is given a risk rating of LOW.

It should be noted that the FAA tables are intended to be used by the FAA when considering changes to the NAS. Since Part 107 operations are already part of the regulatory structure these drone operations are not a change to the NAS. Part 107 operations occur regularly every day. However, this Part 107 risk assessment was performed as a reference baseline when considering future BVLOS operations.

Associated References: (Kos et al. 2010), (Seo, Walter, and Enge 2011)

2.2.2 GPS Dropouts and Beyond Visual line of sight (BVLOS) in rural areas

Severity = 2 Hazardous and Likelihood = D Extremely Remote Risk Level **MEDIUM**

Beyond visual line of sight (BVLOS) operations are becoming increasingly common and are as they allow the UAS operator to cover greater distances, reduce human presence in otherwise dangerous areas, and allow for more cost effective and fewer deployments. However, not having a LOS to the drone can increase circumstantial risks that can easily disrupt operations such as deployment in remote areas, obstructions, and cyber threats. Larger distances and the presence of obstructions or multipath reflections between the UA and its operator can deteriorate the communication link, lead to propagation delays or complete loss of link, and ultimately lead to

dropped GPS data. Additionally, these consequences can lead to a cascading effect where there is reduced situational awareness (SA) for the unmanned agent (UA) and its operator.

Depending on the system design, drones operated Beyond Visual Line of Sight over rural areas that experience a significant GPS dropout or degradation of GPS information without another means of navigation may fly into terrain, collide with structures, hover or orbit, perform an emergency landing, or experience a fly away event. Positional accuracy can change based on the movement of satellites, multipath, radio line of sight obstructions, atmospherics, and other causes. The risk of collision with terrain and structures is greatest for drones that are operating beyond visual line of sight and in close proximity to terrain and structures such as those that are doing power line, bridge, or tower inspections.

Loss or significant degradation of drone position will also impact the drone's ability to determine its own position relative to aircraft transmitting their position via ADS-B messages. A loss or degradation of drone GPS position is expected to also result in either a large degradation or an entire loss of capability to avoid ADS-B aircraft if ADS-B receivers are the sole means of aircraft detection. ADS-B data contains geometric altitude, latitude, longitude, and barometric pressure information. A loss of GPS positional information frustrates the ability to self-separate based on geometric altitude, latitude, and longitude. However, some amount of altitude separation may still be possible based on the barometric information. The ability to self-separate vertically is limited for drone flight at low altitudes below 400' AGL due to barometric altitude uncertainties of the terrain and ground structures, and the barometric uncertainties associated with the drone's own altitude and of the intruder aircraft's altitude.

Loss or significant degradation of drone GPS data is assessed as being within the same order of magnitude of severity and likelihood as a loss or significant degradation of ADS-B information. Hence the risk for BVLOS operations in rural areas is assigned a severity rating of Hazardous and a likelihood rating of Extremely Remote, for an aggregate risk assignment of Medium.

Associated References: (Kamienski and Semanek 2015), (Politi et al. 2021).

2.2.3 GPS Dropouts and BVLOS Operation in Urban Areas

Severity = 1 Catastrophic and Likelihood= C (Remote) Risk Level **HIGH**

Urban areas are characterized by an abundance of buildings, vehicles, trees, and other infrastructure that directly contribute to factors such as multipath reflection and obstruction that attenuate GPS signals and cause GPS dropouts.

GPS interference is a common and probable problem that GNSS can suffer, and various reports of incidents of this type are available for consulting. Operations within urban environments take place in concentrated RF environments with high levels of noise, degraded signals, signal reflection, and other RF issues that could impact navigational operations reliant on GPS signaling. Once a GPS satellite signal reaches earth, the signal loses strength, making it susceptible to high-power external signals. GPS availability rates in urban environments range from 30% to 50% due to obstacles such as buildings that can partially block or reflect the GPS signal before is received by the UAS. This creates high potential for signal degradation related to multipath, significant signal

attenuation, masking and can add significant errors to the expected GNSS measurements that are difficult to account for in real time.

BVLOS drone operations in urban areas are expected to include operations such as package delivery and various forms of inspection surveillance. Package delivery operations often include a phase of the flight where the drone either lands or operates in close proximity to the ground to deliver the package. It is likely that there are people on the ground at the delivery point. The delivery phase may include flight in close proximity to trees, buildings, poles, wires, and other collision hazards. The potential for radio line of sight obstruction to satellites is also increased in this phase of flight. During transit at altitude, the drone may also need to navigate around tall structures such as radio frequency towers. Collision with a structure while in flight may also induce a risk to people on the ground.

GPS dropouts and significant GPS position errors are expected to be Frequent occurrences when considering all BVLOS drone operations over urban areas in the NAS. The likelihood that they will occur and result in a collision with terrain, wires, or ground structures is given a likelihood of Probable. Some drone parachute systems do not have sufficient altitude to deploy when colliding with low altitude structures. The likelihood that a BVLOS drone collision in the NAS operating over urban areas navigating solely by GPS without additional mitigations collides with an obstacle and then injures a person on the ground either directly or indirectly (e.g. falling on a road and becoming a road hazard) is given a likelihood of Remote and a severity of either Major or Hazardous depending on the size of the drone and its ability to reduce its descent velocity and impact energy.

Loss or significant degradation of GPS will also result in loss or significant degradation of the drone to use received ADS-B messages for detect and avoid. This will impact the ability for the drone to avoid low flying helicopters that may operate over urban areas. Low flying helicopters include operations such as emergency medical services and helicopter tours that may have multiple people onboard. For helicopter operations over urban areas, there are fewer places to have an emergency hard landing that does not endanger others. Without mitigations to address the risk, the likelihood of a drone collision in the NAS with other aircraft due to a loss or significant degradation of GPS while in transit is considered to be within the same order of magnitude as the risk category dealing with loss or significant degradation of ADS-B information for drone BVLOS operations over urban areas. The severity is Catastrophic due to the potential for multiple fatalities and the likelihood is Remote, for an overall aggregate risk assignment of High.

Associated References: (Morales and Kassas 2021; Lykou, Moustakas, and Gritzalis 2020; Lagkas et al. 2018; Gupta, Jain, and Vaszkun 2016), (Couturier and Akhloufi 2020), (Špánik et al., 2017), (Tongleamnak & Nagai, 2017), (Heng et al., 2015), (Bijjahalli et al. 2019)

2.2.4 GPS Dropouts and BVLOS Operation in Airspace Near Airports

Severity = 1 Catastrophic and Probability = C (Remote) using the ATO SMS Manual Risk Level **HIGH on ATO SMS Risk Matrix**

BVLOS flight near airports below 400’ AGL and under the Facility Map Altitudes is likely to include flight over people. Operations may include infrastructure inspection, package delivery

from a distribution hub next to the airport, airport perimeter monitoring and security, and other operations.

Quantifying a Catastrophic severity outcome largely depends on several factors such as the type/size of aircraft, number of people onboard, and distance to/from the airport location (rural vs. urban). For example, manned aircraft operating near airports located in urban areas will have a Catastrophic outcome both onboard as well as on the ground. On the other hand, for airports located away from densely populated areas, the ground fatalities are lesser. A collision with a manned aircraft is therefore assumed to be Catastrophic.

The event likelihood of a BVLOS drone flying near an airport experiencing a loss of GPS or significant degradation of GPS signals is expected to be Frequent when considering all similar operations across the NAS. Air traffic density near airports is also higher than in other portions of the NAS. Drones that use GPS information for navigation can often detect when there is a dropout or when there is reduced positional accuracy due to fewer satellite signals being received. Common mitigations may be to hover, descend to a lower altitude based on the best position information available, perform an emergency landing, or have the remote pilot take manual control and fly using camera imagery if available. Because this risk assessment assumes that GPS might be the sole means of navigation in order to assess the risk and determine navigation requirements, this risk assessment assumes that camera imagery may not always be available for ad hoc emergency navigation.

For conditions where the drone remains airborne when experiencing a GPS dropout or significantly erroneous position information, the likelihood is expected to be on the same order of magnitude as the associated ADS-B risk category for BVLOS operations near airports. The likelihood for this is Remote.

If the drone solely navigates using received GPS signals and there is a dropout or significant degradation in the accuracy of position signals without mitigations, then the drone may wander into areas that are no longer under the UAS Facility Map Altitudes. The drone would no longer be wholly contained within the UAS Facility Map Altitudes which would then trigger the use of the ATO SMS Manual instead of the risk tables in 8040.6. In this case the severity would remain as Catastrophic and the Likelihood is estimated to be Remote when considering all similar BVLOS operations across the NAS. It should be noted that a Catastrophic and Remote assignment using the ATO SMS Manual is deeper into the Red High section of a risk matrix, than the same Catastrophic and Remote assignment using risk matrix found in the appendix to Order 8040.6.

Associated References: (Sedjelmaci, Senouci, and Messous 2016; Sedjelmaci, Senouci, and Ansari 2017; Cui et al. 2016; Morales and Kassas 2021; Souli, Kolios, and Ellinas 2020), (Li, 2009), (Aquino et al. 2009), (Park et al. 2017)

2-3 ADS-B Signal Jamming Risk Classes

Unintentional and non-malicious interference is covered under the dropout and erroneous data risk assessments for both GPS and ADS-B risk focus areas. For the ADS-B signal Jamming Risk Classes, jamming is defined as the intentional and illegal process of interfering and blocking radio

communications using frequency transmitting devices at the same working frequency as the target device. Both GPS and ADS-B technology functionalities are based on RF transmission, making these devices vulnerable to jamming effects. A jamming intervention may introduce noise to the main signal which can introduce inaccuracies, or even block and replace the desired data with the jamming signal. (Yu et al. 2012) (Leonardi and Piracci 2018).

Devices utilizing ADS-B In receive information about the transmitting aircraft's location. If one component is jammed, the effect can compound onto the other. Examples include: (McCallie et al. 2011)

This section focuses on the risks of ADS-B jamming, while acknowledging the relationship between GPS and ADS-B signals, when applicable.

2.3.1 ADS-B Jamming of Part 107 operations

Severity = 5 (Minimal) and Probability = E Extremely Improbable Risk Level **LOW**

Part 107 operations are not solely reliant on ADS-B messages to keep the drone separated from ADS-B Out equipped aircrafts, since a visual line of sight is required with the UAS. Therefore, the successful jamming of ADS-B messages does not guarantee the conditions for a critical failure or collision to occur. In addition, Part 107 operators are not required to receive ADS-B information, and hence the impact of ADS-B jamming that results in dropouts or errant information is extremely improbable. Because most Part 107 operators do not use ADS-B information, the likelihood that ADS-B jamming will impact Part 107 operations even in a minimal way is estimated to be Extremely Improbable which is one rating below ADS-B dropouts. ADS-B jamming is expected to be significantly more rare than ADS-B dropouts.

The primary negative impact that is expected to occur is a potentially temporary and soft distraction from monitoring the airspace if the Remote Pilot attempts to troubleshoot their ADS-B receiver. The Part 107 operator is required to visually monitor the airspace regardless of whether their ADS-B receiver may be experiencing difficulties in tracking aircraft. This qualitative likelihood is a combination of the number of Part 107 operations that may optionally choose to receive ADS-B information and the simultaneous chance that the drone encounters a manned aircraft and that there is also an ADS-B jamming event.

It should be noted that the FAA tables are intended to be used by the FAA when considering changes to the NAS. Since Part 107 operations are already part of the regulatory structure these drone operations are not a change to the NAS. Part 107 operations occur regularly every day. However, this Part 107 risk assessment was performed as a reference baseline when considering future BVLOS operations.

2.3.2 ADS-B Jamming of Beyond Visual line of sight (BVLOS) over Rural Areas

Severity = Hazardous and Probability = E Extremely Improbable Risk Level **LOW**

ADS-B technology has an air-to-air component and an air-to-ground aspect. Both depend on GPS availability, meaning that any problem presented in the GPS system of an airborne unit (manned aviation or drone) will be propagated via the ADS-B signal. ADS-B technology uses GPS data for

self-localization of the airborne unit, which is then broadcasted (ADS-B OUT) to other airspace receivers (ADS-B IN) for traffic information, and also to ground stations to feed into the airspace sitation servers (proprietary systems or public dashboards as Flightradar24). For this risk assessment we assume that the GPS signals are authentic, but that the ADS-B signals are being jammed. The treatment of jammed GPS signals is a separate focus area.

The historical data from manned aircraft operations indicate a very low risk for potential jamming of ADS-B signals to occur whereas ADS-B signal dropout is more commonly caused by environmental or infrastructure interference than jamming. However, the severity of an intentional ADS-B Jamming event may vary based on the malicious motivation. At the extreme it may contribute to a mid-air collision.

While there is the potential for a jamming event to result in the drone colliding with a manned aircraft, the conditions for a mid-air collision geometry would first need to exist before the jamming event. Due to remote possibility of these conditions, the likelihood of ADS-B Jamming contributing to a collision is considered extremely improbable. It is also assigned this likelihood rating because ADS-B Jamming events are expected to be much rarer than naturally occurring ADS-B dropouts.

Associated References: (Purton et al. 2010)

2.3.3 ADS-B Jamming of BVLOS Operations over Urban Areas

Severity = Catastrophic and Likelihood = Extremely Improbable Risk Level **MEDIUM**

The same rational used to assign the severity for ADS-B jamming events is used for both rural and urban areas. However the severity increases from Hazardous to Catastrophic to account for the increased severity of a mid-air collision due to the increased chance that multiple people are onboard the aircraft.

Jamming the ADS-B signal will interfere with the ability for drones to detect and avoid manned aircraft thereby causing drone operations to cease if detected. It may also create unsafe conditions for manned aircraft to operate until the airspace has been cleared of BVLOS drones, if ADS-B signals are their sole surveillance source for drones to detect other aircraft.

Urban environments are likely to have greater concentrations of both manned and unmanned aircraft than rural areas. They are also likely to be more attractive targets for malicious actors. Hence, the likelihood for ADS-B jamming in urban areas is assigned one rating higher than ADS-B jamming over rural areas. The likelihood assignment is still considered Extremely Improbable since the chances that an ADS-B jamming event would occur simultaneously with aircraft being on a collision trajectory.

Associated References: (Purton et al. 2010), (Schäfer, Lenders, and Martinovic 2013).

2.3.4 ADS-B Jamming of BVLOS Operations Near Airports

Severity = Catastrophic 1 and Likelihood = Extremely Remote Risk Level **HIGH** **on ATO SMS Risk Matrix**

Airports operate under rigorous security precautions where tracking each individual object within or near airspace is standard and essential to prevent any type of fatal failure. Since airports often provide an architecture for ADS-B communication with strong levels of security, a jamming attack or occurrence in close vicinities of airports is assumed to be rare. Operations of UAVs near airports can be dangerous and pose a high risk, due to the higher density of airspace utilization. ADS-B jamming incidents may cause unintentional navigation failures that could impact both manned and unmanned aviation in the area.

BVLOS drone operations near airports may include infrastructure inspection, package delivery from a distribution hub next to the airport, airport perimeter monitoring and security, and other operations. Drone flights near airports are likely to encounter aircrafts with multiple passengers onboard. A collision resulting from an inability to detect and avoid because of ADS-B jamming is assigned a Catastrophic severity rating. Airports are areas of concentrated traffic. Flying below 400 feet AGL and flying below the Facility Map Altitudes helps to keep BVLOS drones separated from manned air traffic. The Facility Map Altitudes help to constrain drone encounters in this high air traffic airspace. While the rate of encounters when operating near airports is expected to be higher than when operating over urban areas due to increased traffic, the Likelihood rating is assumed to remain within the same order of magnitude as with operations over urban areas. Hence a likelihood rating of Extremely Remote is assigned without additional mitigations beyond the Facility Map Altitudes.

Based on the legal ramifications as a deterrance to jamming ADS-B signals near an airport, the likelihood is Extremely Remote. The same severity as other jamming events for drone operations in urban and rural environments is used and is assigned a rating of Major. While an ADS-B Jamming event would likely impact operations at the airport independent of the drone BVLOS operation and be assigned a Hazardous rating due to disruption of airport operations, this risk assessment is focused on severity outcomes that involve the drone.

Associated References: (Darabseh, Bitsikas, and Tedongmo 2019)

2-4 GPS Signal Jamming Risk Classes

Jamming is the process of interfering and blocking radio communications using frequency transmitting devices at the same working frequency as the target device. The jamming transmission introduces interference noise to the target signal which can introduce inaccuracies or cause the signal to dropout entirely. GPS functionality is based on RF transmission, making UAV operations vulnerable to jamming effects. (Yu et al. 2012) (Leonardi and Piracci 2018).

GPS jamming methods are low-cost and increasingly accessible to the general public, introducing increased potential for jamming occurrences to impact GPS-informed navigation in UAV operations. For instance, UAV operations within urban areas take place in concentrated RF environments with high levels of noise, degraded signals, signal reflection, and other RF issues, disrupting operations relying on location and position determination using GPS signaling, and therefore impacting ADS-B effectiveness.

GPS jamming events that impact one or more drone operations in the NAS is expected to be a frequent event. However, this does not mean that the outcomes listed in the severity tables will be experienced frequently, but at a likelihood less than frequent.

2.4.1 GPS Jamming of Part 107 operations

Severity = Various and Likelihood = Various Risk Level **LOW**

Part 107 operations represent a regulated and controlled flight environment. However, diverse types of failures are possible, including jamming events. For example, waypoint navigation, which relies on GPS functionality, is a common piloting mode in Part 107 operations. Certain GPS signal jamming events may occur in controlled scenarios for research purposes, and uncontrolled cases such as magnetic interference with high-power infrastructures, if present. However, jamming events represent a minimum risk in this type of environment since there exists a visual line of sight with the aircraft and commonlyan ability to manually control the aircraft in the case of a jamming event.

Based on ASSURE project A50 drone statistics the most commonly flown drones are under 2 kg. While some Part 107 drone operations can be flown using GPS waypoints, it is assumed that the majority of Part 107 drones can also be flown manually. This combined with visual monitoring of the drone and the many operating restrictions placed on Part 107 operations serve to mitigate the potential effects of a GPS dropout and erroneous GPS information. Some Part 107 drones also have features that will cause the drone to hover/orbit until GPS is reacquired or becomes usable again. Other Part 107 drones may perform an emergency landing. For Part 107 drones that can only be flown by waypoint and do not have these emergency features, the drone could potentially wander until it is flying over people and then potentially fall on them if other variables like loss of power come into play. This severity may be minor, major, or hazardous depending on the size of the Part 107 drone. A hazardous severity is expected to be less common since heavier drones operated under Part 107 are not as common as lighter drones. There are also additional requirements for heavier drones to operate over people contained in the FAA's "Operations of Small Unmanned Aircraft Systems Over People" final rule. All combinations of severity and likelihood based on drone weight are expected to result in a LOW risk rating (hazardous and extremely remote, major and remote, minor and probable.

Most Part 107 drones can support flight times less than one hour due to their limited size. This limits the exposure time that a Part 107 drone without any manual controls and solely reliant on waypoint navigation may continue to fly/hover in the event of a GPS dropout. The likelihood that a GPS dropout or errant GPS information will cause a Part 107 drone operation to wander into the path of an oncoming aircraft is considered extremely improbable. For most Part 107 drones, the collision severity will be major or less based on the size of the Part 107 drone. Larger drones with a hazardous severity rating are less common and so their likelihood is also less at extremely improbable when flown with the intent to follow Part 107 rules. This rating is informed from an examination of historical drone collisions with conventional manned aircraft conducted by ASSURE project A47. This also assumes that there are no manual controls for the remote pilot to manually fly the drone, and that the drone does not perform an emergency landing when GPS is lost or becomes unusable. All combinations of severity and likelihood based on drone weight are

expected to result in a LOW risk rating (hazardous and extremely improbable, major and extremely remote, minor and remote.

It should be noted that the FAA tables are intended to be used by the FAA when considering changes to the NAS. Since Part 107 operations are already part of the regulatory structure these drone operations are not a change to the NAS. Part 107 operations occur regularly every day. However, this Part 107 risk assessment was performed as a reference baseline when considering future BVLOS operations.

Associated References: (Kerns et al. 2014), (Yu et al. 2012), (Leonardi and Piracci 2018), (Darabseh, Bitsikas, and Tedongmo 2019), (Cuntz et al. 2012), (Fadaei, 2016), (Aghadadashfam et al., 2020), (Li 2009), (Medina et al., 2019)

2.4.2 GPS Jamming of Beyond Visual line of sight (BVLOS) over rural areas

Severity = 2 Hazardous and Likelihood = D Extremely Improbable Risk Level **LOW**

The risk involved in the loss of control of UAS due to GPS signal jamming increases in BVLOS operating conditions, and is dependent on the surrounding environment of flight operations.

Depending on the system design, drones operated Beyond Visual Line of Sight over rural areas that experience GPS jamming without another means of navigation may fly into terrain, collide with structures, hover or orbit, perform an emergency landing, or experience a fly away event. The risk of collision with terrain and structures is greatest for drones that are operating beyond visual line of sight and in close proximity to terrain and structures such as those that are doing power line, bridge, or tower inspections.

Many of these end outcomes that may destroy the drone but do not injure 3rd parties are not listed in the FAA 8040.6 severity table. However that does not mean that they aren't significant. Title 49 of the Code of Federal Regulations (CFR) Part 830.2 defines an unmanned aircraft accident as one that results in death, serious injury, or where the aircraft has a maximum gross takeoff weight of 300 pounds or greater and sustains substantial damage. FAA order 8020.11D includes a definition of aircraft accident that is specific to small unmanned aircraft where a small unmanned aircraft accident is defined by serious injury or greater harm or damage to property other than the small unmanned aircraft that exceeds $500.

Jamming GPS signals will also impact the drone's ability to determine its own position relative to aircraft transmitting their position via ADS-B messages. A loss or degradation of drone GPS position is expected to also result in either a large degradation or an entire loss of capability to avoid ADS-B aircraft if ADS-B receivers are the sole means of aircraft detection. ADS-B data contains geometric altitude, latitude, longitude, and barometric pressure information. A loss of GPS positional information frustrates the ability to self-separate based on geometric altitude, latitude, and longitude. However, some amount of altitude separation may still be possible based on the barometric information. The ability to self-separate vertically is limited for drone flight at low altitudes below 400' AGL due to barometric altitude uncertainties of the terrain and ground structures, and the barometric uncertainties associated with the drone's own altitude and of the intruder aircraft's altitude.

While there is the potential for a GPS jamming event to contribute to a drone colliding with a manned aircraft, GPS jamming by itself does not cause a mid-air collision. Jamming removes a mitigation layer that helps to prevent mid-air collisions. The chance conditions that lead to a mid-air collision also need to exist to include an encounter between aircraft that are on a collision geometry. For a localized area of operations below 400 feet AGL in a rural environment, the chance that a drone and a manned aircraft are on a collision trajectory is expected to often be less than once in 100,000 flight hours. This presents few opportunities for a malicious actor to jam local GPS signals at the right moment in order to create the conditions that lead to a mid-air collision.

GPS jamming that impacts drone operations is assessed as being significantly less frequent than an unintentional loss or significant degradation of GPS information. Hence the GPS jamming risk for BVLOS operations in rural areas is assigned a severity rating of Hazardous and a likelihood rating of Extremely Improbable, for an aggregate risk assignment of Low.

Associated References: (Strümpfel et al. 2020), (L. T. Hsu 2018), (Costin and Francillon 2014), (Yu et al. 2012), (Leonardi and Piracci 2018), (I. I. Alexeev et al. 2001), (Igor I. Alexeev et al. 2003), (La Cour-Harbo, 2017), (Dolph et al. 2017)

2.4.3 GPS Jamming of BVLOS Operations over Urban Areas

Severity = 1 Catastrophic and Likelihood = C Extremely Remote Risk Level **MEDIUM - HIGH**

BVLOS drone operations in urban areas are expected to include operations such as package delivery and various forms of inspection surveillance. Package delivery operations often include a phase of the flight where the drone either lands or operates in close proximity to the ground to deliver the package. It is likely that there are people on the ground at the delivery point. The delivery phase may include flight in close proximity to trees, buildings, poles, wires, and other collision hazards. The potential for radio line of sight obstruction to satellites is also increased in this phase of flight. During transit at altitude, the drone may also need to navigate around tall structures such as radio frequency towers. Collision with a structure while in flight may also induce a risk to people on the ground.

GPS jamming events are expected to be Frequent occurrences when considering all BVLOS drone operations over urban areas in the NAS. The likelihood that one of the tens of thousands of urban BVLOS drones will experience a jamming event that causes it to collide with terrain, wires, or ground structures is given a likelihood of Extremely Remote which is one rating less than GPS dropouts which are likely to be more frequent than jamming events.

Some drone parachute systems do not have sufficient altitude to deploy when colliding with low altitude structures. The likelihood that a BVLOS drone collision in the NAS operating over urban areas navigating solely by GPS without additional mitigations collides with an obstacle and then injures a person on the ground either directly or indirectly (e.g. falling on a road and becoming a road hazard) is given a likelihood of Extremely Remote and a severity of either Major or Hazardous depending on the size of the drone and its ability to reduce its descent velocity and impact energy.

GPS jamming will also result in loss or significant degradation of the drone to use received ADS-B messages for detect and avoid. This will impact the ability for the drone to avoid low flying helicopters that may operate over urban areas. Low flying helicopters include operations such as emergency medical services and helicopter tours that may have multiple people onboard. For helicopter operations over urban areas, there are fewer places to have an emergency hard landing that does not endanger others. Without mitigations to address the risk of the drone losing its ability to detect and avoid, the likelihood of a drone collision in the NAS with other aircraft due to GPS jamming while in transit is considered to be less likely than the risks dealing with non-malicious GPS dropouts and errant GPS positional information. The severity is Catastrophic due to the potential for multiple fatalities if a collision occurs and the likelihood that a collision occurs is Extremely Remote, for an overall aggregate risk assignment of Medium-High.

Associated References: (L. T. Hsu 2018), (Costin and Francillon 2014), (Yu et al. 2012), (Leonardi and Piracci 2018), (Rufa and Atkins 2016), (Balamurugan, Valarmathi, and Naidu 2017), (Chao, Gu, and Napolitano 2013), (Rhudy et al. 2015), (Causa, Fasano, and Grassi 2018), (Fadaei, 2016), (Aghadadashfam et al., 2020), (Li 2009), (Medina et al., 2019), (Van den Bergh and Pollin, 2019)

2.4.4 GPS Jamming of BVLOS Operations Near Airports

Severity = 1 Catastrophic and Likelihood = (D Extremely Remote) Risk Level **HIGH on ATO SMS Table**

Airports operate under rigorous security precautions and provide the required infrastructure for systems like ADS-B to work properly, as well as facilitating the GPS communication links between vehicles and satellites. This reduces the probability of occurrence of such events in an environment that represents elevated risk.

Intentional interference causes GNSS signal interference or jamming that are either deliberately coordinated attacks or people using personal radio jammers, known as Personal Privacy Devices (PPDs). Jamming incidents using PPD are more frequent and common than the coordinated attacks. Hundreds of jamming events have occurred at Newark Airport using PPDs since 2009. According to experimental research by Stanisak et al. (2016), there were hundreds of interference events detected near Braunschweig airport, and 14% of the detected events were high-priority, high-signal-power events leading significant impact on GNSS receivers. Although airports equipped with terrestrial navigation infrastructure (VOR/DEM, ILS) may not be affected by the GNSS interferences for their operation, more research and technical measures are recommended to minimize the risk on air and land transport operation and critical infrastructure. Still, although many studies state that the impact of GNSS jamming to ATC operations in the airport area is minor because of the ADS-B and other guidance systems, it is this team's opinion that they are not generally in situations where sUAS operations disrupt airport operations.

BVLOS flight near airports below 400' AGL and under the Facility Map Altitudes is likely to include flight over people. Operations may include infrastructure inspection, package delivery from a distribution hub next to the airport, airport perimeter monitoring and security, and other operations.

Manned aircraft operating near airports are likely to have multiple persons on board. A collision with a manned aircraft is therefore assumed to be Catastrophic.

The event likelihood of a BVLOS drone flying near an airport experiencing a loss of GPS or significant degradation of GPS signals is expected to be Frequent when considering all similar operations across the NAS. Air traffic density near airports is also higher than in other portions of the NAS. Many drones can detect when GPS signals are lost or degraded. If they do not have an alternate means of navigation, they may hover or perform an emergency landing if they are able to do so. For conditions where the drone remains airborne when experiencing a GPS jamming event, the frequency of event is expected to be less than the rate at which non-malicious GPS dropouts and significantly errant GPS position data occur. A likelihood of Extremely Remote is assigned to the simultaneous occurrence of a GPS jamming event where there is a collision trajectory with a manned aircraft and the drone remains airborne or experiences a fly away rather than descending to a lower altitude or landing and the remote pilot does not have the capability to manually fly the drone remotely with the aid of cameras or other means of navigation.

If the drone solely navigates using received GPS signals and there is a dropout or significant degradation in the accuracy of position signals without mitigations, then the drone may wander into areas that are no longer under the UAS Facility Map Altitudes. If GPS signals are jammed, then the drone may not have the information to be able to form avoidance decisions that involve lateral avoidance maneuvers. If the drone wanders, it may no longer be wholly contained within the UAS Facility Map Altitudes which would then trigger the use of the ATO SMS Manual instead of the risk tables in 8040.6. The severity is Catastrophic and the Likelihood is estimated to be Extremely Remote when considering all similar BVLOS operations across the NAS. Extremely Remote is also one likelihood rating less than GPS dropouts from non-malicious causes. GPS jamming is expected to occur much less often than GPS dropouts. It should be noted that a Catastrophic and Extremely Remote assignment using the ATO SMS Manual is deeper into the Red High section of a risk matrix, than the same Catastrophic and Extremely Remote assignment using risk matrix found in the appendix to Order 8040.6.

BVLOS drone operations near airports may include infrastructure inspection, package delivery from a distribution hub next to the airport, airport perimeter monitoring and security, and other operations. Drone flights near airports are likely to encounter aircraft with multiple passengers onboard. A collision resulting from an inability to detect and avoid because of ADS-B jamming is assigned a Catastrophic severity rating. Airports are areas of concentrated traffic. Flying below 400 feet AGL and flying below the Facility Map Altitudes helps to keep BVLOS drones separated from manned air traffic. The Facility Map Altitudes help to constrain drone encounters in this high air traffic airspace. While the rate of encounters when operating near airports is expected to be higher than when operating over urban areas due to increased traffic, the Likelihood rating is assumed to remain within the same order of magnitude as with operations over urban areas. Hence a likelihood rating of Remote is assigned without additional mitigations beyond the Facility Map Altitudes.

Based on deterrance for jamming ADS-B signals, the likelihood is Remote. The same severity as other jamming events for drone operations in urban and rural environments is used and is assigned

a rating of Major. While an ADS-B Jamming event would likely impact operations at the airport independent of the drone BVLOS operation and be assigned a Hazardous rating due to disruption of airport operations, this risk assessment is focused on severity outcomes that involve the drone.

Associated References: (L. T. Hsu 2018), (Costin and Francillon 2014), (Yu et al. 2012), (Leonardi and Piracci 2018), (Rufa and Atkins 2016), (Balamurugan, Valarmathi, and Naidu 2017), (Chao, Gu, and Napolitano 2013), (Rhudy et al. 2015), (Causa, Fasano, and Grassi 2018), (Andrej Novak et al., 2020), (Stanisak et al., 2016), (Novák et al., 2019), (Li, 2009)

2-5 ADS-B Signal Spoofing Risk Classes

The definition of spoofing is a cyber-weapon attack that generates false signals to replace valid ones. Spoofing is intentionally malicious. It requires greater sophistication and technical capability than Jamming. Hence, spoofing also requires greater dedication and likely involves greater malicious intent than jamming. Spoofing may be paired with other cyber attacks and other malicious acts to achieve the goals of the bad actor. Spoofing is an attempt to disrupt aircraft operations or cause the drone to behave in a certain way. Spoofing attacks may be associated with forms of cyber hijacking to attempt to force avoidance maneuvers to control the drone for malicious purposes which may be catastrophic in nature. Spoofing attacks may also saturate the air picture with false targets thereby disrupting drone operations or causing unintended aircraft avoidance behavior. This risk assessment assumes that ADS-B is the sole technology used for drones to detect and avoid ADS-B equipped aircraft when operating BVLOS. Drones do not have an onboard pilot to counter act spoofed ADS-B signals by using see-and-avoid. RTCA industry standards require that large drone Detect and Avoid systems have a means to validate ADS-B signals to detect potential false ADS-B targets. Industry standards for smaller drones to validate ADS-B signals do not yet exist and a focus of this research effort is to determine whether ADS-B validation is needed as a means to counter ADS-B spoofing attacks and if so, the degree of mitigation that may be acceptable.

An ASTM industry BVLOS group created a whitepaper suggesting that ADS-B validation is not needed because of the reduced risk that small drones pose as compared to larger drones addressed in RTCA standards. Important to note is that highly automated small drones may be more susceptible to ADS-B spoofing attacks than drones flown with a pilot in the loop who can monitor system behavior and oddities in the air picture. Large swarms of small drones that are under an ADS-B spoofing attack may also present larger severity outcomes than if there is a ratio of one small drone to one remote pilot. It is assumed that a bad actor that can spoof ADS-B signals also has the technical capacity to perform wide area ADS-B jamming, or jam the signals associated with a specific aircraft.

Section 2-5 deals with the direct spoofing of ADS-B messages and ADS-B frequencies rather than indirect spoofing via GPS signals and frequencies. ADS-B is dependent on GPS signals for location information. The spoofing of GPS signals is covered in Section 2-6 and that section covers the secondary effects that spoofed GPS signals may have on ADS-B messages.

Associated References: (Humphrees and e 2008)(Tippenhauer and etal 2011) (Tippenhauer & et.al, 2011)

2.5.1 Spoofing ADS-B used in Part 107 operations (Represents Best Case Scenario with low Severity levels for spoofing threats)

Severity = 5 Minimal and Likelihood = E Extremely Improbable Risk Level **LOW**

Because of limited airspace operations and licensing requirements, spoofing threats primarily occur via researcher experimentation, amateur and testing labs. Spoofing attacks are usually single sourced and may use Software Defined Radio (SDR) implementations. (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) There is little at stake since the operator is in direct contact and control of aircraft if a spoofing event occurred. Part 107 operations represent low risk (Minimum Acceptable Risk). Normal safety precautions are recommended.

Because Part 107 operations require visual means of separation and are not solely reliant on ADS-B messages for keeping the drone separated from ADS-B equipped aircraft, the intentional spoofing of ADS-B messages does not result in a critical failure for keeping the drone separated from other aircraft. Part 107 operators are not required to receive ADS-B information, and hence the impact of ADS-B spoofing that results in dropouts or errant information is minimal. Because most Part 107 operators do not use ADS-B information, the likelihood that ADS-B spoofing will impact Part 107 operations even in a minimal way when the information may be useful for enhanced situational awareness is estimated to not be significant. The primary negative impact that is expected to occur is a potentially temporary and soft distraction from monitoring the airspace if the Remote Pilot attempts to troubleshoot their ADS-B receiver. The Part 107 operator is required to visually monitor the airspace regardless of whether their ADS-B receiver may be experiencing difficulties in tracking aircraft. This qualitative likelihood is a combination of the number of Part 107 operations that may optionally choose to receive ADS-B information and the simultaneous chance that the drone encounters a manned aircraft and that there is also an ADS-B spoofing event.

It should be noted that the FAA tables are intended to be used by the FAA when considering changes to the NAS. Since Part 107 operations are already part of the regulatory structure these drone operations are not a change to the NAS. Part 107 operations occur regularly every day. However, this Part 107 risk assessment was performed as a reference baseline when considering future BVLOS operations.

Associated References: (R. Nichols and al. 2020; M. L. Psiaki and Humphreys 2016; Randall K. Nichols et al. 2019; Ochin and Lrmieszewski 2021; Ng and Gao 2016; Warner and Johnson 2002)

2.5.2 Spoofing ADS-B for Drone BVLOS Operations over Rural Areas (Represents increase spoofing threats and higher Severity risk level without loss of life)

Severity = HAZARDOUS and Likelihood = Extremely Remote Risk Level **MEDIUM**

Because the UAS is not limited to a specified flying space and may cross beyond the visual horizon, BVLOS represents an elevated UAS spoofing threat and risk. Severity varies depending on the malicious actors intentions.

If the drone is solely reliant on received ADS-B messages to detect and avoid other aircraft, then false ADS-B signals could be used to influence the drone's flight by forcing avoidance maneuvers. This may cause the drone to fly above crowds until its power reserves are exhausted, fly towards urban areas and airports, fly into sensitive critical infrastructure, or any number of malicious acts. The worst credible/reasonable outcome is assessed as aligning with a Hazardous severity rating. It is expected that many BVLOS systems will have geofencing and keepout zones that make it difficult for the drone to cause multiple fatalities required for a Catastrophic rating.

Another potential threat is to law enforcement and emergency response operations. Effective spoofing in this class causes civil, emergency response, or law enforcement drones to *disrupt law enforcement and emergency response missions.*

Associated References: (Khan, Mohsin, and Iqbal 2021; Randall K. Nichols et al. 2020; 2019; Ochin and Lrmieszewski 2021; Moncayo, Yanke, and Yuetong 2020; Eichelberger 2019; I.C.A.O. 2021; Schmidt and al 2016; Ng and Gao 2016)

2.5.3 Spoofing ADS-B for Drone BVLOS Operations over Urban Areas (Represents a difficult case for mitigating spoofing threats with increased potential of harm)

Severity = Catastrophic and Probability = Extremely Improbable Risk Level **MEDIUM/HIGH**

Urban area operations represent increased severity of consequences. Humans and equipment are at risk. Spoofing incidents present serious difficulties in detection of the single or multiple spoofer antennas. The worst credible/reasonable outcomes includes a spoofing attack that forces the drone to avoid illusionary targets. Severity outcomes may include damage to property, failure of law enforcement and emergency responder missions, and multiple fatalities. False ADS-B targets may cause the drone to perform false avoidance maneuvers and create the conditions of a potential mid-air collision with low flying aircraft with multiple persons onboard. Hence, the severity rating is catastrophic.

Another potential threat is to law enforcement and emergency response operations. Effective spoofing in this class causes civil, emergency response, or law enforcement drones to *disrupt law enforcement and emergency response missions.*

Associated References: (Khan, Mohsin, and Iqbal 2021; Jovanovic and Botteron 2014; e a Ali 2014; Closas and al. 2007; Warner and Johnston 2003; Eichelberger 2019; Eichelberger and Tanner 2017; Bissig and Wattenhoffer 2017; M. Psiaki and al. 2013; Randall K. Nichols et al. 2020)

2.5.4 Spoofing ADS-B for Drone BVLOS Operations Near Airports (Represents the Worst-Case spoofing scenario with highest Severity and potential loss of life)

Severity = 1 Catastrophic) and Probability = Extremely Remote Risk Level **HIGH on ATO SMS Risk Matrix**

Near airports represents the worst-case scenario with the highest severity and likelihood probability among ADS-B spoofing events. Likelihood is higher than other ADS-B spoofing scenarios because of potential as a prime target for terrorist activities if there are not adequate ADS-B spoofing mitigations. . These present serious risk / consequences to human life and death with the potential for multiple fatalities. All of the potential severity outcomes associated with the ADS-B spoofing over urban areas are also present with operations near airports.

ADS-B spoofing may cause the drone to fly towards other low flying aircraft with multiple people on board. Successful spoofing incidents near airports represent unacceptable risk and must be mitigated to medium or low to prevent aircraft disasters and heavy equipment damage. Further, research and global tracking of terrorist activities suggest that airports are prime targets for cyber-attacks. These spoofing attacks are generally quite sophisticated. They can be launched from multiple sources, mobile carriers, coordinated power levels and timing based on publicly available data and Commercial Off-The- Shelf (COTS) devices. They are generally preceded by jamming to disrupt the normal signal differentiation. Floating landing strips (aircraft carriers) represent an interesting and particularly rich target for spoofing navigation and control systems, which are beyond the scope of the current project, but may offer helpful information and insight. Civilian airport operations show a similar threat trajectory. At stake are passenger aircraft, tower facilities, ground personnel. Spoofing drones near airports carries with it serious consequences and liability.

Another potential threat is to law enforcement and emergency response operations. Effective spoofing in this class causes civil, emergency response, or law enforcement drones to *disrupt law enforcement and emergency response missions.*

Associated References: (Eichelberger 2019; Randall K. Nichols et al. 2020; Bissig and Wattenhoffer 2017; Haider and Khalid 2016; Madhani and al. 2003; Kuhn 2015)

2-6 GPS Signal Spoofing Risk Classes

GPS spoofing is an attack to provide false information to GPS receivers by broadcasting counterfeit signals similar to original GPS signal or by recording original GPS signal captured somewhere else in some other time and then retransmitting the signal. The spoofing attack causes GPS receivers to provide the wrong information about position and time.

Near airports represents the worst-case scenario with the highest severity and likelihood probability. There are significant globally reports of UAS and other aircraft spoofing incidents. These present serious risk / consequences to human life and death. Successful spoofing incidents near airports represent unacceptable risk and must be mitigated to medium or low to prevent aircraft disasters and heavy equipment damage. Further, research and global tracking of terrorist activities suggest that airports are prime targets for cyber-attacks. These spoofing attacks are generally quite sophisticated. They can be launched from multiple sources, mobile carriers, coordinated power levels and timing based on publicly available data and Commercial Off-The-

Shelf (COTS) devices. They are generally preceded by jamming to disrupt the normal signal differentiation. Floating landing strips (aircraft carriers) represent an interesting and particularly rich target for spoofing navigation and control systems, which are beyond the scope of the current project, but may offer helpful information and insight. Civilian airport operations show a similar threat trajectory. At stake are passenger aircraft, tower facilities, ground personnel. Spoofing drones near airports carries with it serious consequences and liability.

A bad actor that has the ability to spoof GPS signals also has the technical capacity to perform wide area GPS jamming. They may also have the technical capacity to perform localized jamming or spoofing on a specific aircraft. Successful spoofing of GPS signals is considered more technically challenging than spoofing of ADS-B signals. However, due to the availability of GPS jammers and spoofers, and the number of non-aviation systems that can be affected by GPS spoofing as compared to ADS-B spoofing that only affects aviation systems, GPS spoofing is more prevalent in the literature and is reported more often than ADS-B spoofing.

A drone that is solely reliant on GPS signals for navigation is susceptible to GPS spoofing. False GPS signals may cause a loss of ability for the remote pilot to navigate the aircraft. False GPS positions may cause the drone to cross geofence boundaries, fly into keep out zones, fly over groups of people, fly towards critical infrastructure, fly towards other air traffic, and so on.

Because an aircraft's GPS position is used to create an ADS-B Out message, spoofed GPS position data on a manned aircraft will make its way into the ADS-B messages that are transmitted. Other airspace users (including drones) that receive the transmitted ADS-B message will have false position information on the manned aircraft.

Associated References: (Humphrees and e 2008)(Tippenhauer and etal 2011) (Tippenhauer & et.al, 2011)

2.6.1 Spoofing GPS used in Part 107 operations (Represents Best Case Scenario with low Severity levels for spoofing threats)

Severity = Various and Likelihood = Various Risk Level **LOW**

For Part 107 operations, the operator is in direct visual contact and control of the aircraft. . Many part 107 operations that are flown by GPS waypoint also can be flown manually. Part 107 operations represent low risk. It is unlikely that a Part 107 drone operation would be the primary target of a GPS spoofing attack since other higher value and potentially softer targets that are not under direct visual contact exist such as drones operated BVLOS. (Minimum Acceptable Risk). Normal safety precautions are recommended.

It should be noted that the FAA tables are intended to be used by the FAA when considering changes to the NAS. Since Part 107 operations are already part of the regulatory structure these drone operations are not a change to the NAS. Part 107 operations occur regularly every day. However, this Part 107 risk assessment was performed as a reference baseline when considering other types of future operations.

Associated References: (R. Nichols and al. 2020; M. L. Psiaki and Humphreys 2016; Randall K. Nichols et al. 2019; Ochin and Lrmieszewski 2021; Ng and Gao 2016; Warner and Johnson 2002)

2.6.2 Spoofing GPS for BVLOS Drone Operations over Rural Areas (Represents increase spoofing threats and higher Severity risk level without loss of life)

Severity = Hazardous to Catastrophic and Likelihood = Extremely Remote Risk Level **MEDIUM** to **MEDIUM/HIGH**

If the drone is solely reliant on GPS for navigation, then false GPS signals could be used to influence the drone's flight to include causing it to cross protective geofence boundaries. This may cause the drone to fly above crowds until its power reserves are exhausted, fly towards urban areas and airports, fly into sensitive critical infrastructure, or any number of malicious acts. The worst credible/reasonable outcome is assessed as aligning with a Hazardous to Catastrophic severity rating depending on the malicious intent of the bad actor and their opportunity to cause multiple fatalities.

Because GPS spoofing occurs more frequently than ADS-B spoofing in the literature, the likelihood of GPS spoofing is assumed to be one likelihood rating greater than ADS-B spoofing and a likelihood rating of Extremely Remote is used.

Another potential threat is to law enforcement and emergency response operations. Effective spoofing in this class causes civil, emergency response, or law enforcement drones to *disrupt law enforcement and emergency response missions.*

Associated References: (Khan, Mohsin, and Iqbal 2021; Randall K. Nichols et al. 2020; 2019; Ochin and Lrmieszewski 2021; Moncayo, Yanke, and Yuetong 2020; Eichelberger 2019; I.C.A.O. 2021; Schmidt and al 2016; Ng and Gao 2016)

2.6.3 Spoofing GPS Drone BVLOS Operations over Urban Areas (Represents a difficult case for mitigating spoofing threats with increased potential of harm)

Severity = Catastrophic and Likelihood = Extremely Remote Risk Level **MEDIUM/HIGH**

Urban area operations represent an increased severity of consequences. Urban areas present difficulty to enact countermeasures to mitigate the impact of a spoofing attack. Humans and equipment are at risk. Spoofing incidents present serious difficulties in detection of the single or multiple spoofer antennas.

If the drone is solely reliant on GPS for navigation, then false GPS signals could be used to influence the drone's flight to include causing it to cross protective geofence boundaries. This may cause the drone to fly above crowds until its power reserves are exhausted, fly towards airports, fly into sensitive critical infrastructure, or any number of malicious acts. The worst credible/reasonable outcome is assessed as Catastrophic due to a malicious actor having the opportunity to cause multiple fatalities.

Because GPS spoofing occurs more frequently than ADS-B spoofing in the literature, the likelihood of GPS spoofing is assumed to be one likelihood rating greater than ADS-B spoofing and a likelihood rating of Extremely Remote is used.

Associated References: (Khan, Mohsin, and Iqbal 2021; Jovanovic and Botteron 2014; e a Ali 2014; Closas and al. 2007; Warner and Johnston 2003; Eichelberger 2019; Eichelberger and Tanner 2017; Bissig and Wattenhoffer 2017; M. Psiaki and al. 2013; Randall K. Nichols et al. 2020)

2.6.4 Spoofing GPS BVLOS Operations Near Airports (Represents the Worst-Case spoofing scenario with highest Severity and potential loss of life)

Severity = Catastophic and Probability = Extremely Remote Risk Level **HIGH** **on ATO SMS Risk Matrix**

If the drone is solely reliant on GPS for navigation, then false GPS signals could be used to influence the drone's flight to include causing it to cross protective geofence boundaries. This may cause the drone to fly above crowds until its power reserves are exhausted, fly towards urban areas and airports, fly into sensitive critical infrastructure, or any number of malicious acts. The worst credible/reasonable outcome is assessed as Catastrophic due to a malicious actor having the opportunity to cause multiple fatalities.

Because GPS spoofing occurs more frequently than ADS-B spoofing in the literature, the likelihood of GPS spoofing is assumed to be one likelihood rating greater than ADS-B spoofing and a likelihood rating of Extremely Remote is used. Because of the operation near airports and the potential to cross the lines of the facility map altitudes, the ATO SMS Manual risk matrix is used.

Another potential threat is to law enforcement and emergency response operations. Effective spoofing in this class causes civil, emergency response, or law enforcement drones to *disrupt law enforcement and emergency response missions.*

Associated References: (Eichelberger 2019; Randall K. Nichols et al. 2020; Bissig and Wattenhoffer 2017; Haider and Khalid 2016; Madhani and al. 2003; Kuhn 2015)

2.7 Risk Assessment Summary

Reviewing the risk assessments conducted by the subject matter experts, a summary of the risk levels are:

LOW RISK	ADS-B Dropout and Erroneous Data Risks - Part 107 Operations
	GPS Dropout and Erroneous Data Risks - Part 107 Operations
	ADS-B data Signal Jamming Risks - Part 107 Operations
	ADS-B data Signal Jamming Risks- Rural BVLOS Operations
	GPS data Signal Jamming Risks - Part 107 Operations
	GPS data Signal Jamming Risks- Rural BVLOS Operations
	ADS-B data Signal Spoofing Risks – Part 107 Operations
	GPS data Signal Spoofing Risks – Part 107 Operations
MEDIUM RISK	ADS-B Dropout and Erroneous Data Risks - BVLOS Operations
	GPS Dropout and Erroneous Data Risks - BVLOS Operations
	ADS-B Dropout and Erroneous Data Risks - Urban BVLOS Operations
	ADS-B data Signal Jamming Risks- Urban BVLOS Operations
	ADS-B data Signal Spoofing Risks – Rural BVLOS Operations
MED/HIGH RISK	GPS data Signal Jamming Risks- Urban BVLOS Operations
	GPS data Signal Spoofing Risks – Rural BVLOS Operations
	ADS-B data Signal Spoofing Risks- Urban BVLOS Operations
	GPS data Signal Spoofing Risks – Urban BVLOS Operations
HIGH RISK	ADS-B Dropout and Erroneous Data Risks – BVLOS Operations Near Airports
	GPS Dropout and Erroneous Data Risks – BVLOS Operations Near Airports
	GPS Dropout and Erroneous Data Risks – BVLOS Operations in Urban Areas
	ADS-B data Signal Jamming Risks – BVLOS Operations Near Airports
	GPS data Signal Jamming Risks – BVLOS Operations Near Airports
	ADS-B data Signal Spoofing Risks – BVLOS Operations Near Airports
	GPS data Signal Spoofing Risks – BVLOS Operations Near Airports

Table 1 is a summary of the risk levels for the 6 classes and 4 classifications of operations in a table format to illustrate continuum of risk levels in the various combinations.

Table 1. Summary of the risk levels for the 6 classes and 4 classifications of operations.

Risk	Part 107	Rural BVLOS	Urban BVLOS	Near Airport BVLOS
ADS-B Dropout	LOW	MEDIUM	MEDIUM	HIGH
GPS Dropout	LOW	MEDIUM	HIGH	HIGH
ADS-B Signal Jamming	LOW	LOW	MEDIUM	HIGH
GPS Signal Jamming	LOW	LOW	MED/HIGH	HIGH
ADS-B Signal Spoofing	LOW	MEDIUM	MED/HIGH	HIGH
GPS Signal Spoofing	LOW	MED/HIGH	MED/HIGH	HIGH

From this analysis it is evident that the only low risk situations occur with operations in the Part 107 conditions. This was expected due to the nature of Part 107 and the current operability allowed by the FAA. In the medium risk category, most of the conditions are either in the BVOS or urban area conditions. This is also expected since in both cases the FAA has demonstrated the authority to deviate from certain regulations in the form of a waiver if included in the effective rule, "authorizing" operations or exemptions to certain regulations per 14 CFR part 11 to allow operations in these areas. The waiver and potentially other situations may be mitigated using additional processes, procedures, and technology to reduce the risk to a lower acceptable level. The high-risk category contains only urban and near airport operations. These areas result in high-risk operations and significant mitigation schemes are needed to reduce the risk to an acceptable level.

Additional and significant details of the complete literature review are included in the following sections: III. UAS Navigational Anomalies – GPS Dropouts and Erroneous Data, IV. GPS and ADS-B Data Signal Jamming, V. GPS and ADS-B Data Signal Spoofing, and VI. Standards Bodies Review. Each of these sections is led by a subject matter expert in their respective areas that is part of the A44 project.

III. UAS Navigational Anomalies – Dropouts and Erroneous Data Literature Review

According to the Centre for Unmanned Aircraft Systems in Public Safety and the FAA, a sUAS is "a small version of an unmanned aircraft system weighing less than 55 pounds (including the onboard systems)" (Centre for Unmanned Aircraft Systems in Public Safety 2021) with a maximum allowable altitude of 400 feet above ground (Federal Aviation Administration 2020). See Figure 7 for class-wise requirements for manned and unmanned aircraft as mandated by the FAA. The FAA obligates that ~~all~~ certain aircraft in the national US airspace to be equipped by an ADS-B) by January 2020. The ADS-B is an ATM/ATC surveillance system that is intended to replace traditional radar-based systems and become a key component in the Next Generation Air Transportation System (NextGen systems). The GPS receiver obtains data such as position and altitude and provides it to ADS-B which broadcasts this information and other data to other aircraft and ground stations.

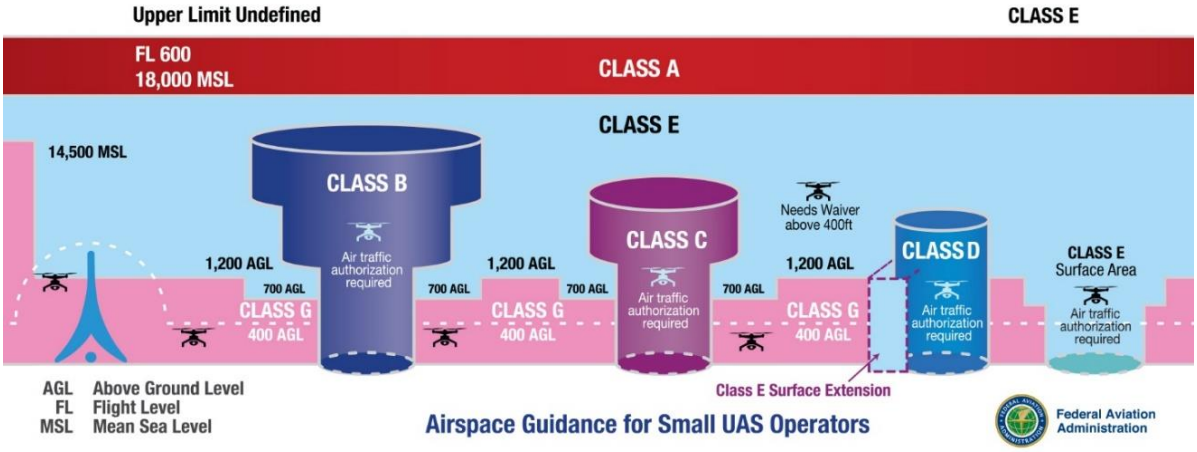

Figure **7**. FAA specified operating altitudes for UAVs based on classes (Federal Aviation Administration 2018).

sUAS rely on GNSS infrastructure that is deployed in space for their positioning and navigation. State-owned systems such as the GPS by the US, Galileo by Europe, and GLONASS by Russia use the GNSS framework to provide PNT information for GNSS-enabled hardware (Transportation, n.d.). This reliance of sUAS on GPS satellite systems for their operation brings forward the critical discussion on what factors could affect the QoS. For the purposes of this review, consider the GPS constellation which is provided by the U.S. to its user segment and upon which relies systems such as ADS-B which periodically and automatically broadcast information that improves situational awareness and provides assurance of airborne separation in regulated airspace.

There are two types of ADS-B systems: the ADS-B IN and the ADS-B IN/OUT. The ADS-B IN receives ADS-B signals from other aircraft and ground stations and does not transmit. The ADS-B IN/OUT receives signals from other aircraft and ground station and transmits its own data stream. The ADS-B OUT broadcasts a data stream that is in plain text, unencrypted, and error-

code protected over radio transmission links, including the velocity, ID, and other ATM/ATC related information, approximately one message per second. The message will be intercepted by ATC on the ground and nearby aircrafts if equipped with the ADS-B IN system (Tabassum and Semke 2018). The ground station, on the other hand provides automatic dependent surveillance-rebroadcast (ADS-R) and traffic information service-broadcast (TIS-B). ADS-R systems monitor if there are other aircraft nearby with different ADS-B links and then rebroadcast surveillance information received on one link to aircraft on the other link (Tabassum and Semke 2018). Such information along with others transmitted via ADS-B OUT, ADS-R, and TIS-B messages are received and decoded by the ADS-B IN system (Tabassum and Semke 2018). ADS-B IN assists in increasing the pilot's situational awareness and self-separation (Tabassum and Semke 2018). ADS-B IN/OUT messages are dependent on the GPS (Figure 8) as the "position and velocity vectors are derived from the Global Positioning System (GPS)" (F.A.A. 2020) and requires GPS receivers that are capable of handling wide area multilaterate (WAM) or multilaterate (MLAT) requirements (Niles et al. 2012).

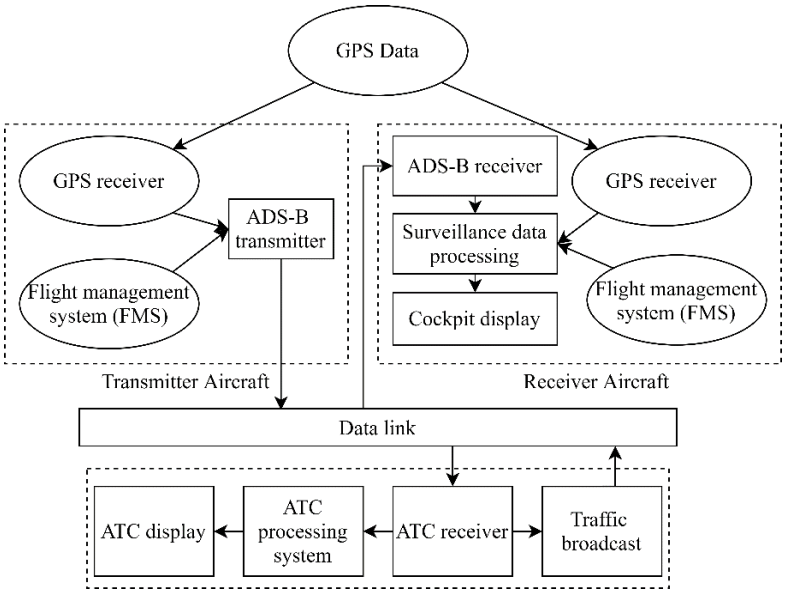

Figure 8. ADS-B system's components.

GPS signals deliver three distinct elements to their receivers: pseudorandom code (satellite identifier), ephemeris (satellite health, data, and time), and almanac (position of the satellite at any point in time) data. These data are transmitted on two carrier frequency bands known as L1 and L2 bands. The L1 band is centered at a frequency of 1575.42 MHz and is used for military, civilian, and aviation applications while the L2 band is centered at 1227.6 MHz Developments by the US government have now led to the use of L2C (1227.6 MHz), L5 (1176.45 MHz), and L1C (1575.42 MHz) in addition to L1 and L2, all of which can be used for civilian applications. This was made possible by deploying satellites from the Block II-F (follow-up), II-R (replenishment), and the latest Block III generations which have extended operating lifespans, higher accuracy atomic clocks, and faster onboard processors (GPS.GOV 2021). However, signals from these satellites are subject to degradation (dropped or erroneous data) depending on terrestrial or extraterrestrial

factors that degraded the quality of data received by standalone GPS receivers in the user segment (ground-based) or aircraft systems relying on ADS-B technology.

For this review, the researchers have classified the anomalies in ADS-B/GPS systems based on two overarching categories of dropped and erroneous data. These categories are further subclassified into their respective causes based on factors due to operating environment, system-related functions, and voluntary intervention due to cyber-attacks. See Figure 9 for an overview of the subsequent details that are covered in these categories.

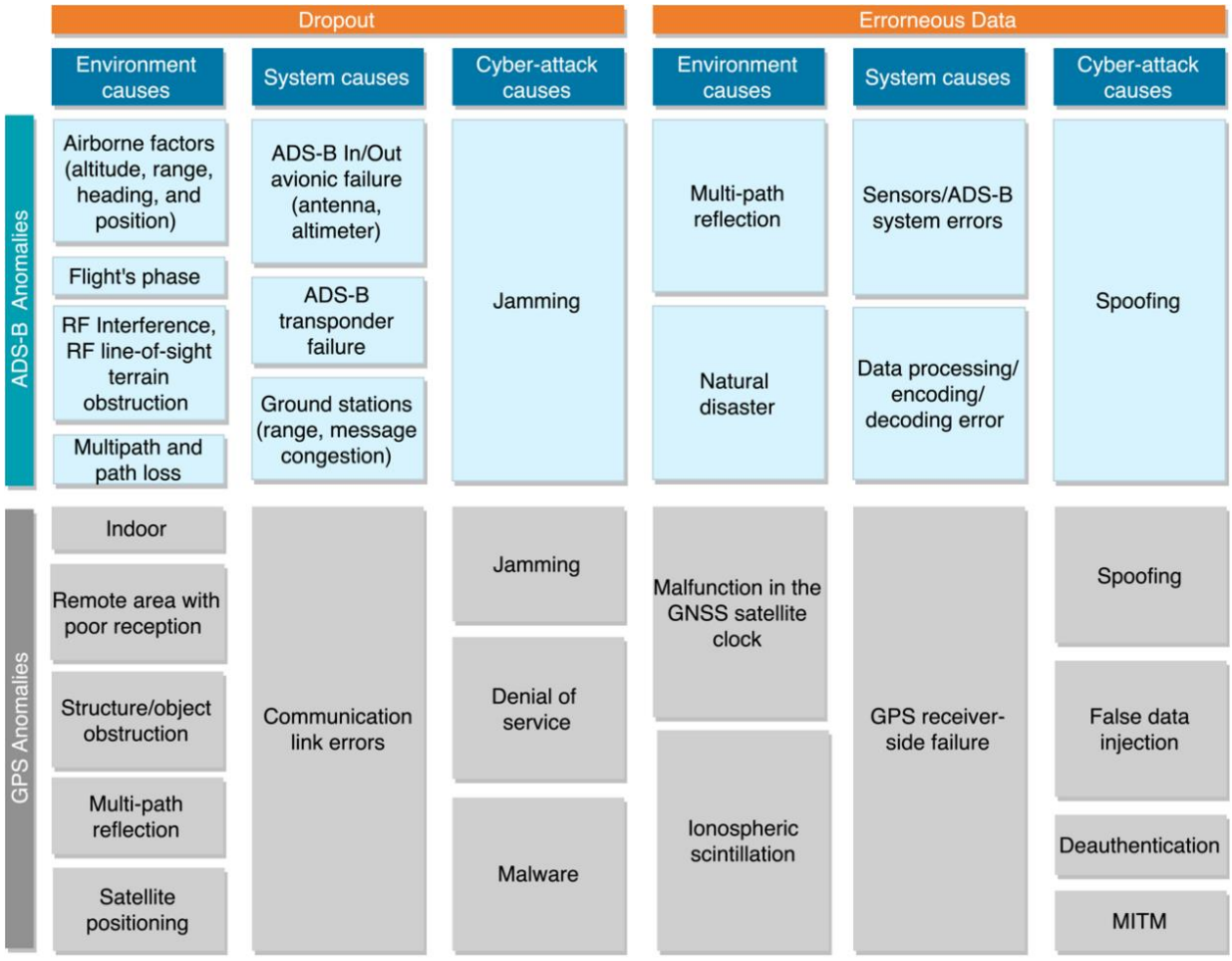

Fig. 9. Taxonomy of anomalies in ADS-B and GPS systems.

3.1 DROPOUT DATA

A typical ADS-B is designed to broadcast an update once per second. ADS-B Dropout is referred to the discontinuation of an update within one second (Tabassum 2017),(Sahawneh et al. 2015) ,(Semke et al. 2017), (Tabassum and Semke 2018). A formal definition for dropout of GPS data is not identified in scholarly literature but for the purposes of this analysis, any circumstance that makes it conducive for GPS data to be degraded (poor or intermittent reception) or denied (unavailability of data for definite periods of time) can be classified as a factor contributing to

dropped GPS data (Silvagni et al. 2017; Goforth and Lucey 2019). In this section, the various factors that affect the dropout, particularly those related to the environment, system, and cyber-attacks will be investigated.

3.1.1 ADS-B

3.1.1.1Environment causes (Airborne Factors)

Authors in (Tabassum 2017) have conducted four experimental studies to investigate the effect of airborne factors on the dropout frequency. These factors include, the altitude, range, heading and position. In their first study, four different flight levels were chosen; in the first region, the altitude was less than 4000 feet; in the second one, the altitude was between 4000 and 8000 feet; the altitude in region three was ranging between 18000 and 12000 feet; and the last one's altitude was between 12000 and 18000 feet. The reported experiment results showed that the dropout frequency was high in the first, third, and forth regions while low in the second region; concluding that flying in an altitude of 4000-8000 feet was the optimal altitude in terms for reducing the ADS-B message dropout. This hypothesis has been proved in another study (B. S. Ali, Ochieng, and Zainudin 2017) where the authors found a positive correlation between the aircraft flight level and the ADS-B message update rate as this latter increases when the flight level increases. Based on the second and third experiments' findings, the range and aircraft heading do not have a significant impact on the dropout frequency. Conversely, authors (B. S. Ali, Ochieng, and Zainudin 2017) have found out that the aircraft range, which represents the distance between the aircraft position and the ADS-B message received station using ellipsoid distance formula, has an influence on the updating rate as it increases when the flight altitude increases. The fourth experiment indicated that some positions may increase the dropout frequency with longer duration, especially in dense traffic areas, such as terminals.

Authors in (B. S. Ali, Ochieng, and Zainudin 2017) have conducted an experimental study for analyzing the performance of ADS-B message broadcast rate from aircraft to the ADS-B ground station in London Maneuvering Area. Specifically, a correlation analysis has been conducted to determine the actual effect of flight's phase on the dropout. Based on the reported findings, the ADS-B message updating performance is poor during the cruising phase at higher levels ranging between 30,000 and 40,000 feet, and relatively high performance during the climbing and descent phases. Thus, the phase of flight has an impact on the ADS-B message updating rate, which may be due to small distance between ADS-B antenna mounting on the aircraft and the ground station location.

There are other potential external factors that impact the ADS-B message updating rate. For instance, interference with radio frequencies or electromagnetic fields can impact the ADS-B message updating rate. In dense traffic area, aircraft signal interference is high likely to happen causing ADS-B signal loss. Authors in (Arteaga et al. 2018) have found out that signal drop out may also occur during RF line-of-sight terrain obstruction and aircraft maneuvers. Additionally, heavy electronic system and Distance Measuring Equipment (DME) located near the ground receiver may create electromagnetic interference (Tabassum 2017) (B. S. Ali et al. 2014). Path loss is another phenomenon where the signal power decreases as the distance between the transmitter and receiver increases (Tabassum 2017). The ADS-B signal can also be affected by distance leading to dropout.

3.1.1.2 System causes

In addition to some environmental related causes, such as multipath, interference, and path loss, the cyclic redundancy checks (CRC) is another potential cause that effects the ADS-B message updating rate. CRC is a mechanism used by ADS-B to check the accuracy of the received message and any message with bit error is discarded at reception (Tabassum 2017). Such mechanism would increase the dropout frequency at the ground receiver level if faulty data has been accidently injected into the message.

In the same study conducted in (B. S. Ali, Ochieng, and Zainudin 2017), a correlation has been found between the aircraft model and the ADS-B message updating rate as the reported results indicated that an A319 provides the optimal performance with 87.35% of the message update rate within 2s, followed by an A321 with 82.32%, and a B777-200 with 80.55%, then a B744 with 72.24%. This performance degradation was due to the different avionic use models including GPS, transponder, and FMS. Another experimental study (Syd Ali et al. 2016) discussed the potential effect of avionic types (i.e., GPS model) on the ADS-B message updating rate. The GPS latitude and longitude were provided every 4s for The B747-400 Rockwell Collins GLU920 MMR, and 2s for the B767-300 using Honeywell Mercury Card-equipped EGPWC MkV (system causes). Other ADS-B OUT avionic failure mode that could lead to dropout has been listed in (B. S. Ali et al. 2014). The GPS receiver malfunctioning would result in the loss of situational awareness of the aircraft. Since this information is not provided to the ADS-B the data is not transmitted to other aircraft as well. Altimeter malfunctioning failure could prevent ADS-B emitters from receiving altitude data. Failure of connection between navigation source and transponder may cause loss of ADS-B positional data. Unstable sensitivity of the ground sensor may cause disruption in the ADS-B message update. Failure of ADS-B ground station power supply may cause unexpected loss of ADS-B data. Failure of data links between the ADS-B ground station and controller working position may cause abrupt loss of ADS-B data. In addition, there are several ADS-B IN failure that could cause dropout (B. S. Ali et al. 2014). For instance, the ADS-B IN receiving antenna malfunction may cause sudden loss of ADS-B data to ADS-B IN application. Also, the failure of ADS-B IN receiver on the aircraft may result in a sudden loss of ADS-B data affecting ADS-B IN application.

3.1.1.3 Cyber-attack causes

The relevant operating status information shared by aircraft make them potential targets for attackers. Cyberattacks have a significant impact on the ADS-B message updating rate and could lead to message dropouts or even a denial-of-service situation. Jamming is considered one of these main cyberattacks. In a typical jamming attack, the jammer bombards the communication channel with random data to disturb or even prevent other legitimates users from using the available channel. It is considered a potential threat in all wireless communication networks. With ADS-B systems particularly, jamming may be classified into ground station flood denial attacks and aircraft flood denial attacks (Riahi Manesh and Kaabouch 2017). Although both attack types interrupt the surveillance network by disrupting and blocking communication channels, the first is easier to conduct as the jammer can get closer to its target, the ground station, and send a low power jamming signal. On the contrary, the second attack type requires forging a very high-powered jamming signal in order to reach the targeted aircraft.

3.1.2 GPS

3.1.2.1 Environmental causes

Depending on the environment a UAS is operating in, it can experience missing or low confidence (degraded) GPS data due to enclosed spaces, remote areas with poor signal reception, objects that obstruct received signal path, multi-path reflection, or poor satellite positioning (Figure 10). Some research also suggests that riverine ambiences (water bodies) also affect the quality of the signal received by the UAS (Sobers, Chowdhary, and Johnson 2009).

Navigation may be degraded due to factors such as interference, signal blockage, or poor signal reception. One way to mitigate degraded navigation is through visual odometry. External reference points that serve as markers can also help in localizing the vehicle and to help the UAV to navigate autonomously. For instance, Nahangi et al. (Nahangi et al. 2018) show the feasibility of fiducial markers (also known as visual tags) and a camera system to localize the vehicle to the visual tag's coordinate frame. Once the onboard hardware computes the 3D translational and rotational vectors, the computed locations are compared to hardcoded ground truth locations that are identified by a distinct "indoor positioning system".

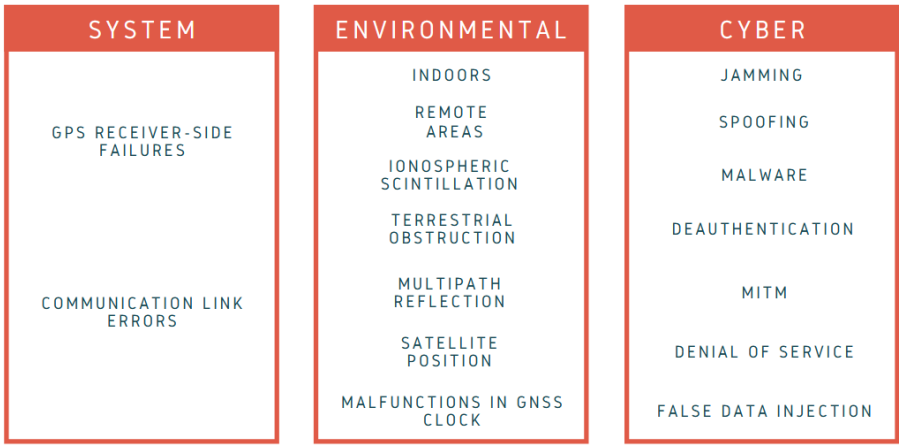

Fig. 10. Categorization for causes of dropped and erroneous GPS data.

Ionospheric scintillation is another cause for GPS receivers on UAVs to be unable to lock onto signals provided by the satellite. This is a broadly-defined term for any disturbances experienced by the electromagnetic waves propagating from the satellite at the ionosphere (Kintner, Ledvina, and De Paula 2007). This effect is observed particularly when the ionosphere (which starts at about 46 miles above sea level and is part of the thermosphere) experiences non-uniformity due to magnetic disturbances such as those caused by solar winds. This leads to a situation known as "loss of lock" where GPS receivers are unable to lock onto a satellite signal.

Obstructions from buildings, trees, vehicles, and other infrastructure (particularly in urban areas) lead to degraded or unavailability of GPS data though its effect might be temporary. This might be less of an issue for sUAS operations that are above 400 ft. in altitude (which is higher than most structures) but for requirements under this threshold, there might be a temporary drop in GPS data (Gebre-Egziabher and Taylor 2012). A related but distinct consequence of obstructions is multipath reflections which lead to multiple wavefronts received by the GPS receiver. If the

multipath reflections are too dense, the GPS receiver will be unable to detect the transmitted data and this can cause periods of intermittent data reception (Isaacs et al. 2014).

According to (GPS.GOV 2021), the position of the satellite directly affects the QoS of relayed GPS data to the user segment such as sUAS. This is because a minimum of 3 satellites are required to determine the position of a user, but 4 satellites are ideal to have a precise determination for the GPS receiver. Though the deployed GPS satellites orbit the earth twice a day (two 12-hour periods), not all locations have sufficient accuracy to effectively operate UAS.

For all these causes, it's important to identify mitigation solutions that can address the need based on the factor causing the dropout. For instance, receiver-side clock correction can be used to increase the accuracy of the data provided by GPS satellites which are subject to clock errors. Figure 11 categorizes the most commonly used elements in a localization solution based on hardware and software.

Fig. 11. Mitigation solutions for GPS denied environments (Ling 2020).

In order to reconstruct the GPS data payload in such situations where there is a loss of lock, an integrated INS/GPS solution with a correction mechanism such as the Kalman Filter (Kissai and Smith 2019) can help in localizing the sUAS. In onboard systems that lack such a correction mechanism, dead reckoning (which is the use of previously calculated PNT data to predict current and future parameters) can be a reasonable option; it has to be noted, however, that integration drift in the INS can cause errors in each calculated step to be cumulative and can ultimately produce data that is highly deviant from the ground truth.

Table 2 shows a comparison of the mitigation tactics and their reliance on GPS data as a secondary system for aided UAV localization. "Application Type" specifies the environment in which the respective mitigation tactic was designed to work in. Outdoor and indoor application types can potentially work when the UAS experiences GPS dropout due to the factors listed in Fig. 7. "GPS

Reliance" indicates the degree to which the solution requires current or historical GPS data. "Vehicle Type" lists the rotor specification and the size of the UAV used in terms of altitude, rotor span, and maximum takeoff weight. Micro UAVs have rotor spans under 0.49 ft, altitude under 100 ft above ground level (AGL), and a take-off weight under 0.22 lbs. Miniature UAVs have rotor spans under 2.6 ft, altitude under 500 ft AGL, and a takeoff weight under 6.6 lbs., and the small tactical UAV has a rotor span of 6.2 ft, and a maximum takeoff weight between 22 – 55 lbs.

Table 2. Current mitigation methods based on sUAS vehicle types.

Mitigation Tactic	**Application Type**	**GPS Reliance**	**Vehicle Type***	**Operating Altitude (ft)**	**References**
Laser SLAM, visual odometry, and sensor fusion	Indoor	Medium	Miniature Hexarotor	-	(Bi et al. 2019)
Dual laser scanners, IMU, Robust and Precise Tracking (RPT)	Indoor	Low	Miniature Quadrotor	-	(F. Wang et al. 2014)
Google Maps, HOG, OP/PF	Outdoor	High	Miniature Quadrotor	< 265	(Shan et al. 2015)
Homography using IMU, monocular camera, compass, EKF	Indoor/Outdoor	Low	Miniature Quadrotor	-	(Zhao et al. 2016)
Robust and Precise Tracking (RPT) control law for stability, laser odometry, graph SLAM	Outdoor	Low	Miniature Quadrotor	-	(Cui et al. 2016)
GPS/IMU, monocular and stereo cameras	Outdoor	High	Small Tactical Helicopter	-	(Andert et al. 2014)

Relative Navigation (RN) frontend and global backend	Indoor/Outdoor	Low	Miniature Hexacopter	-	(Wheeler et al. 2020) (Horri and Palmer 2013)
Radio SLAM using Signals of Opportunity	Outdoor	Low	Miniature Quadrotor	-	(Morales and Kassas 2021)
Relative Visual Localization (RVL) using IMU and monocular camera	Outdoor	Low	Micro-Miniature Quadrotor	< 500	(Couturier and Akhloufi 2020)

*****Based on the classification criteria by Cai et al. (Cai, Dias, and Seneviratne 2014)

3.1.2.2 System causes

When considering system-related factors that can contribute to GPS dropout data, it is imperative to first discuss the types of wireless technologies used in a UAS. The performance of the GPS can be affected by available wireless communication links within the UAS (onboard sensors/subsystems) and external to the UAS environment (ground station). For example, while the processor inside UAS needs to rely on wireless links for seamless data transport among IMUs and other sensors, there may be advanced scenarios where additional positional information may be required from external UAS environment (ground station) during GPS dropout conditions. In the latter scenario, GPS information needs to be uplinked back to the UAS with updated positional information. According to Lagkas and colleagues (Lagkas et al. 2018), technologies such as Zigbee, WiFi 802.11 a/b/g/n, LoRa, and LTE (4G) can be categorized into wireless personal area network (WPAN), wireless local area network (WLAN), low-power wide-area network (LPWAN), and cellular mediums respectively and are the most common technologies used for communication in a UAS. Before further discussion on the importance of quality of service in UAS communication, it might help to categorize the subsystems of a UAS depending on their primary functions. Similar to a classification framework for motor vehicles and based on a UAV's onboard sensors such as laser, electro-optical, IMU, etc. that gather precise data, stabilized or automated control of the UAV which are forms of UA piloting, and a wireless link between the UAV operator and the UAV that makes piloting possible, it can be said that a UAS operates in the sensing, communication, and control categories respectively and based on a framework used for the automotive industry (El-Rewini et al. 2020) (Figure 12). The primary focus will be in the communication layer that handles a full duplex communication, implements technologies mentioned earlier to make wireless communication possible, and inter-UAV communication (in the special case of UAV swarms).

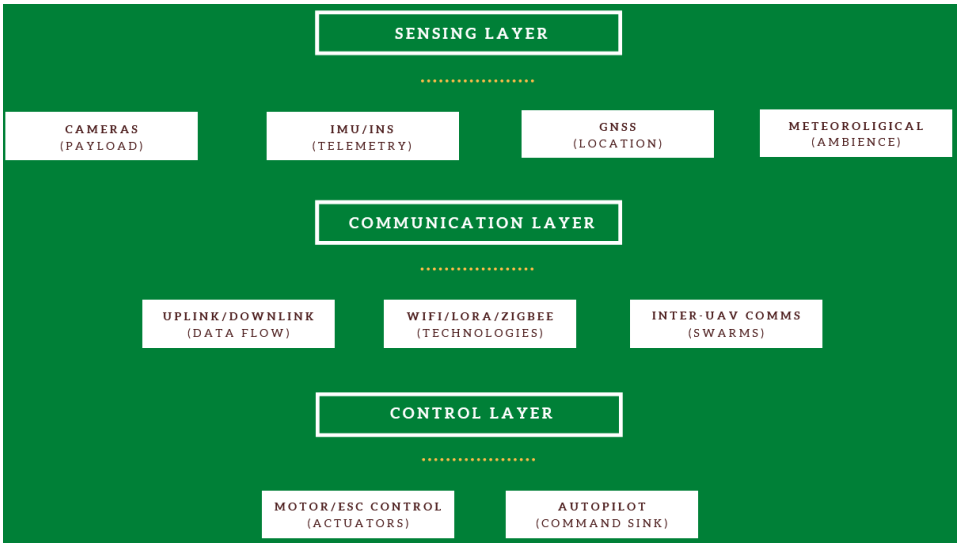

Fig. 12. Operating framework for a UAS.

Communication link errors can be controlled if the topology of the UAS network can be identified and implemented before deployment. For instance, it is stated by Gupta and Jain (Gupta, Jain, and Vaszkun 2016) that star networks have higher latency and delays in transmission because the distance between the downlink distances (distance between the node and the GCS) for each UAV in the system is greater than the inter-UAV distance. As the GCS handles all the communication data from each node in the star network, every node in the UAV will not have reliable data if the GCS experiences downtime (Hentati and Fourati 2020). However, both these networks are still susceptible to communication link failures/errors (contributing to dropped GPS data) due to factors such as interference and mobility. One mitigation strategy to regain a functional link is through self-organization of the UAVs in the swarm but there are other considerations that can be investigated.

Considering multi-UAV systems such as those in swarms, much deliberation has to go into the application, topology, unit mobility, network configuration, and the dynamicity of the unit's movements. Gupta and Jain (Gupta, Jain, and Vaszkun 2016) state that mesh networks are more reliable and offer better performance in terms of data links as each node is interconnected and has more than one direct link to communicate the data it receives. For COTS components, design considerations such as the data rate required for the application is a crucial characteristic that needs to be deliberated as it is usually specified by the manufacturer. It is encouraged for UAS to work with a range of data rates depending on channel (transmission medium) conditions. Additionally, parameters that are affected by the channel such as the multi-input multi-output (MIMO) antennae (Matolak 2015), antenna directivity (power of radio signal in a specified direction), antenna altitude, antenna polarization (matching polarization between the receiving and transmitting antennae promises optimal power transfer), and antenna beamwidth (signal coverage) (H. Wang et al. 2018) will ensure that the inevitable negative effects of environmental factors stated in the previous section can be minimized and while being resource-efficient. More recently, a radio access technique called nonorthogonal multiple access (NOMA) with successive interference cancellation (SIC) (Higuchi and Benjebbour 2015)(Liu et al. 2019) can be considered to mitigate

the effects of interference and degraded communication links. However, there are inherent challenges in implementing some of these solutions like MIMO for UAS. For instance, directional mmWave communications utilize MIMO technology but due to the highly dynamic and mobile nature of UAVs, it will be challenging to achieve synchronized transmitter and receiver beam alignment (Zeng, Zhang, and Lim 2016).

3.1.2.3 Cyber-attack causes

The navigation framework on which GPS is based, the GNSS, is susceptible to cyber-attacks that can contribute to GPS data that is dropped or missed (Ly and Ly 2021). Yagdereli and colleagues (Yağdereli, Gemci, and Aktaş 2015) state that it is possible for attackers to "interrupt or corrupt communications between control system components." Mitigation solutions used by the military in such cases include the selective availability anti spoofing module (SAASM) which is a GPS security architecture that provides GPS receivers the ability to encrypt and decrypt received signals (Program and Air Force Program 2012), military code (M-code) encryption or M-code GPS user equipment (MGUE), a sensor fusion approach called receiver autonomous integrity monitoring (RAIM), and GPS receivers that can track multiple state-owned satellite constellations such as GPS, GLONASS, Beidou, or Galileo. GPS receivers in all these cases could be used in ground instruments, weapons systems, or UAVs. Commercial uses, however, require low-cost but efficient solutions to counter cyber threats. Although the GCS and the UAV are vulnerable to attacks such as man-in-the-middle (MitM) (Ly and Ly 2021), DoS (Gudla, Rana, and Sung 2018), keylogging (Hartmann and Steup 2013), spoofing, malware, etc., it has been identified that GPS spoofing followed by GPS jamming are the two most common cyber-attacks identified with lesser research on deauthentication, malware, and keylogging attacks (Leela Krishna and Murphy 2018).

Before listing the attacks that contribute to dropped, degraded, or denied GPS data, it might be helpful to describe which aspect of the confidentiality, integrity, and availability (CIA) triad that our primary concern (dropped GPS data) maps to. According to NIST, availability is "ensuring timely and reliable access to and use of information" and that a "loss of availability is the disruption of access to or use of information or an information system" (National Institute of Standards and Technology (NIST) 2004). By this definition, it can be said that the availability of a system is compromised when it experiences dropped, degraded, or denied GPS data. Keeping this is mind, the two key points of focus when identifying cyber-attacks that cause dropped and erroneous GPS data will be to identify cyber threats that primarily compromise the availability (unavailable data when they are required) and integrity (data that are modified/destroyed) respectively though they might also compromise the confidentiality of the data.

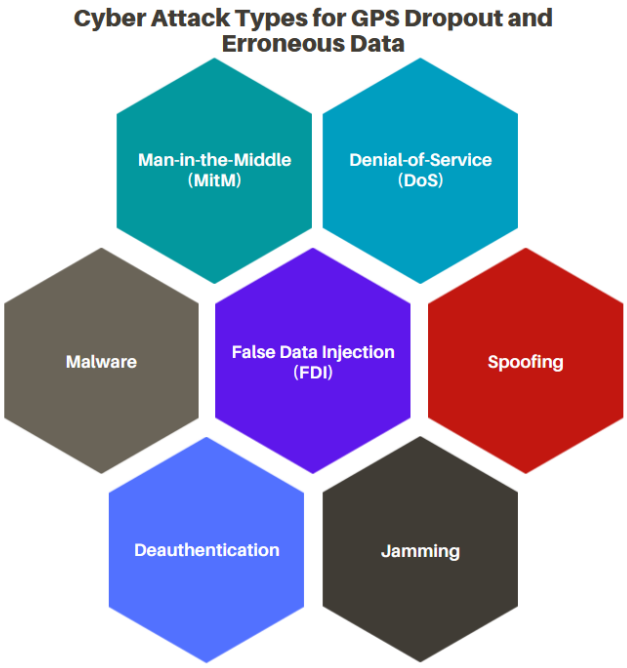

Fig. 13. Cyber-attacks that compromise the availability and integrity of UAV GPS data.

As stated by Haque and Chowdhury (Vidal and Choo 2018), one way to classify the attack surfaces is by categorizing attack vectors three distinct groups that can be used to attack the UAV: hardware, wireless, and sensor spoofing. However, for the purposes of this paper, the team will address seven cyber-attacks (Figure 13) that have been consistently identified in literature (Yaacoub et al. 2020)(Jain et al. 2020)(Sallam 2016) and pose a threat to UAV nodes and their GCSs as well as contribute to dropped and erroneous GPS data. For instance, attacks such as DoS, MiTM, false data injection, deauthentication, malware can passively monitor communication or actively intervene to modify or compromise the availability of the data.

Though there are variations to jamming attacks, they work on the underlying premise that legitimate GPS signals can be overshadowed by an external malicious agent through the use of hardware that emits a high-power signal that overpowers the legitimate signal. Jamming attacks can pave the way for other attacks such as spoofing so the attacker can trick the UAV into localizing itself with false coordinates (Sedjelmaci, Senouci, and Ansari 2017).

Similarly, a malicious agent can identify a vulnerability in a UAV's communication link to significantly degrade the quality of data sent to the GCS. This is known as a logic-based DoS attack that can be carried out due to software flaws or the lack of proper packet filtering mechanisms (Vasconcelos et al. 2016) and crucial data received by the UAV (such as GPS frames) no longer retains their quality when they are forwarded to the main operator. DoS attacks can also be the ultimate goal before other attacks such as malware-based exploitations are carried out (Garg et al. 2019).

Malware for UAVs can be packaged as exploits that can act as a proxy to listen in on the inter-sensor communication onboard UAVs (GPS, IMU, magnetometer, etc.) based on open ports and

forward falsified data or drop traffic altogether when communicating with the GCS (Shashok 2017)(Sung et al. 2020). It can also be deployed at the GCS level to modify critical software discreetly and passively record sensitive information or take complete control of the system (L. Li, Qu, and Lin 2020) and the possibility of this attack to eventually lead to the completely unavailability of the system (DoS) is considered (Garg et al. 2019).

One way to mitigate dropped data is by using a multi-antenna system. Flysher and colleagues (Flysher, Yozevitch, and Ben-Moshe 2017) implement a COTS solution to recover from dropped GPS data using a GPS receiver, four antennas that were pointed in each direction, and a microcontroller (MCU) to act as a switch between the four antennas which are all connected to the receiver. The MCU was also crucial for synchronizing the data received by the GPS receiver and the antenna that was routed to that receiver at that time period. SNR measurements were taken for each directional antenna and scored after which a threshold was calculated. Any satellite below this threshold raises a "spoofer alarm". A more advanced version was also presented where previous scoring histories were recorded and then analyzed for anomalies to detect the attacker and disregard any data from this source. Though the authors targeted this as a measure to primarily counter spoofing attacks, attacks such as tampering or MitM that can modify GPS data before being seamlessly sent to a given GPS receiver can also be mitigated.

3.2 ERRONEOUS DATA

Erroneous data implies all errors induced into the ADS-B/GPS data, intentionally or unintentionally, and attempt to comprise the communication integrity (Kinowski and Skorupski 2016).

3.2.1 ADS-B

3.2.1.1 Environmental related causes

Authors in (Kinowski and Skorupski 2016) have conducted an analysis study on the potential causes of occurrence of incorrect data in ADS-B systems. The study concluded to two categories of threats: unintentional and intentional. Among the unintentional threats, the authors discussed the unforeseen coincidence of event (i.e., natural disaster) and its role in inducing accidently erroneous data into the ADS-B message. The multipath is another environmental major error source that could compromise the ADS-B data integrity due to the reflection and diffraction of satellite signal by the tall buildings and skyscrapers (L.-T. Hsu 2017).

3.2.1.2 System related causes

Authors in (Tabassum 2017) have identified two main sources of errors that compromise the integrity of the data: one from the sensors and one from the ADS-B system itself. The sensor errors related causes are due to any potential malfunction in pitot tube, which could ultimately lead to erroneous altitude value. The ADS-B system related causes are mainly due to rounding the altitude value which is encoded in a 25-foot resolution. Other system related errors including the unchecked source code and undeveloped procedure were discussed in (Kinowski and Skorupski 2016). Authors in (Martin Strohmeier et al. 2014) have listed multiple erroneous data causes that could occur either at the ADS-B OUT level or at the ground station level. At the ADS-B OUT level and as the ADS-B relies on the GPS system, any temporary unavailability of the GPS signal may result in an error in the message. Furthermore, bugs in the module, bugs in the data processing,

and encoding errors may introduce fault in the ADS-B message. At the ground receiver level, there are multiple reasons behind the failure in receiving or decoding the message.

3.1.2.3 Cyber-attack related causes

A spoofing attack is considered as illicit way to alter the message content and compromise its integrity. Authors in (Riahi Manesh and Kaabouch 2017) discussed three methods to conduct such an attack: overshadowing, bit flipping, and combining message deletion and injection. Unlike jamming attacks where the entire communication channel is flooded, overshadowing consists of sending a high-power signal to alter a legitimate message fully or partially; Bit flipping, as its name states, aims to superimpose a signal that changes multiple 0 into 1, or vice versa. The last attack type attempts to delete the legitimate message and send a new one. The first two spoofing attacks are more critical as the legitimate messages are altered during transit and the receiver considered them to be legitimate (Riahi Manesh and Kaabouch 2017; Martin Strohmeier, Lenders, and Martinovic 2014; Pöpper et al. 2011; Wilhelm, Schmitt, and Lenders 2012).

3.2.2 GPS

3.2.2.1Environmental related causes

According to Bendea and colleagues (Bendea et al. 2008), since the selective availability (SA) scheme was stopped by the US government in the year 2000, one of the causes of erroneous data now is due to ionospheric interference. All satellite-based positioning devices rely on the precision and quality of the hardware onboard the satellite providing the PNT data. Though the satellite clock itself may be highly stable and deliver consistent readings, there is a high likelihood that the data will have errors when comparing it to the GPS system time (Bidikar et al. 2014). Though the GPS clock is designed to be kept within a certain range of marginal error (about 1 μS), satellite clocks are subjects to higher drift errors which will affect the quality of data received by the user segment. Other potential sources of erroneous GPS data are terrestrial obstructions and satellite position/geometry.

3.2.2.2 System related causes

Limitations in hardware design (Stamatescu et al. 2015) can contribute to erroneous GPS data i.e., COTS components which are economical may not necessarily offer better quality of GPS data. GPS receiver-side clocks and their inability to stabilize the PNT data received by GPS constellation satellites makes it necessary for an estimation mechanism to be put in place so the data received can be precisely estimated at regular intervals. Depending on the application and the precision of GPS positioning data required for optimal operation, high sensitivity GPS receivers can be used to track GPS signals with a high signal-to-noise ratio (SNR). Additionally, subsystems like IMU/INS that are commonly integrated with GPS as aiding sensors are known to have drift errors (Nagai et al. 2008).

3.2.2.3 Cyber related causes

Cyber-attacks that contribute to erroneous GPS data are highlighted by Abbaspour et al. (Abbaspour et al. 2016). False Data Injection (FDI) is an attack that compromises the integrity of a system and makes it possible to append invalid/erroneous data which collide with legitimate GPS

data. Spoofing attacks can target various subsystems onboard a UAV, so it is possible for the incorrect data to be targeted at the GPS receiver. The difference between spoofing and FDI lies in their definitions: spoofing attacks first establish a communication link with the UAV, making it think that it is a legitimate and authorized source when it is not whereas an FDI is carried out by an attacker who does not intend to fake a valid and authorized identity and instead proceeds to actively intervene in sabotaging the asset(s).

Man-in-the-Middle (MitM) attacks can be carried out on UAV networks either actively or passively for reconnaissance, data export, or data modification but typically compromise the integrity of the data relayed or received by the UA agent (Dahiya and Garg 2019). Deauthentication (feasible only on WiFi networks) enables an attacker to scan for wireless Access Points (APs) put out by an operating UAV and continuously transmit deauthentication packets to trick the UAV into thinking the legitimate GCS has disconnected. The attacker then reconnects to the UAV as its operator. As with other cyber-attacks mentioned in Section 2, deauthentication makes it easier to cascade and compound the effects of other attacks to modify data received by the UA (Guo, Wang, and Weng 2020; Mamchenko 2021). Some attacks such as keylogging and WiFi-based attacks that are not mentioned in this list are variations of the types mentioned; keylogging software can be considered a form of malware while any WiFi-based attack that overloads the communication buffer (like TCP three-way handshake-based attacks) or actively eavesdrops on data can be variations of DoS and MitM respectively. Therefore, for systems solely reliant on GPS data for effective navigation, these attacks may pose a risk.

Implementing an Intrusion Detection System (IDS) for identifying cyber-attacks such as spoofing and FDI in UAV networks is not uncommon and has been explored. For instance, Sedjelmaci et al. (Sedjelmaci, Senouci, and Ansari 2017; Sedjelmaci, Senouci, and Messous 2016) deploy an IDS running at the node (UAV) level and at the GCS level to detect spoofing, jamming, and FDI attacks. This solution works well particularly in UAV swarms where multiple UAVs can act as broadcast nodes for information using “promiscuous mode” communication where all neighboring UAVs within radio range broadcast real-time information. In the situation where a malicious agent attempts to inject false data, a UAV can compare these data to those broadcasted by neighboring UAVs. If a system utilizes only one UAV, the GCS can verify the data based on historical UAV data collection and decide if the UAV is malicious or not.

Hu and colleagues (Hu, Chang, and Tomlin 2016) deploy a state estimation and a Kalman Filter based approach to mitigate MiTM and spoofing attacks. State estimation problems seek to determine the dynamic state of a functional cyber physical system based on faulty or compromised inputs while making as few assumptions of the malicious agent as possible. This is done to improve the performance of the estimator in real-world situations which are bound to follow a high degree of unpredictability. An interesting assumption based by the authors is using measurements from a closed loop, hardwired system such as IMU/INS that is secure from any attacks and provides ground truth measurements for error correction.

Table 3 shows the overview of potential causes and their respective descriptions for ADS-B/GPS anomalies of dropout and erroneous data.

Table 3. Dropout and Erroneous data in ADS-B systems.

Anomaly	Potential causes	Description	Impacted aircraft model		References
			Type	Altitude	
Dropout	Heading and range	Dropouts could be caused by an aircraft leaving the range of other ADS-B transmitters ~~ground station's range~~	sUAS	<400 ft AGL	(B. S. Ali, Ochieng, and Zainudin 2017)(Snyder et al. 2016)
	Flight altitude and position	The ADS-B message updating rate increases with the flight level	Large UAS	12000-18000 ft	(Tabassum 2017)
	Flight's phase	The updating performance is poor when the aircraft is isolated from other ADS-B systems	Large UAS	30000 – 40000 ft	(B. S. Ali, Ochieng, and Zainudin 2017)
	RF interference, RF line-of-sight terrain obstruction	-	sUAS	<400 ft AGL	(Tabassum 2017; Arteaga et al. 2018)
	Path loss	-	sUAS	<400 ft AGL	(Tabassum 2017)
	Cyclic redundancy checks (CRC)	CRC could increase the dropout frequency at the ground receiver level if faulty data has been accidently injected into the message.	sUAS	<400 ft AGL	(Tabassum 2017; Tabassum and Semke 2018)
	GPS clock	Missing time information were found in the GPS time data without any deterministic patterns.	B777-200 and B747-400 using the Rockwell Collins GLU920 MMR	30000 – 40000 ft	(Syd Ali et al. 2016)
	GPS, transponder models, and flight management system (FMS)	-	Large UAS	30000 – 40000 ft	(B. S. Ali, Ochieng, and Zainudin 2017)
	ADS-B transceiver failure	-	sUAS	<400 ft AGL	(Sahawneh et al. 2015)
	ADS-B OUT avionic failure (Altimeter, GPS receiver)	ADS-B OUT avionic malfunctioning failure could prevent ADS-B emitter from receive altitude and position data	Large UAS	<400 ft AGL	(B. S. Ali et al. 2014)

	ADS-B IN failure (antenna, receiver)	Failure of ADS-B IN receiver or antenna on may result in a sudden loss of ADS-B data	Large UAS	30000 – 40000 ft	(B. S. Ali et al. 2014)
	Message congestion at ground station	Message congestions could occur at the ground station leading to dropouts	Large UAS	30000 – 40000 ft	(B. S. Ali, Ochieng, and Zainudin 2017)
	ADS-B ground station power supply	Failure of ADS-B ground station power supply may cause unexpected loss of ADS-B data if no other ADS-B aircraft are present	Large UAS	30000 – 40000 ft	(B. S. Ali et al. 2014)
	Jamming	Ground station flood denial attacks or aircraft flood denial attacks could disrupt the communication channel	sUAS and large UAS	<400 ft AGL and 30000 – 40000 ft	(Riahi Manesh and Kaabouch 2017)(C. Li and Wang 2017)
	Remote Areas	Canyon areas may have little to no reception	sUAS UAS	<400 ft AGL	(Ling 2020)
	Ionospheric Scintillation	Magnetic storms in the upper atmosphere causes relayed GPS data to attenuate and drop	sUAS and large UAS	<400 ft AGL and over 16, 000 ft	(Bendea et al. 2008)
	Satellite Position	A minimum of 3 satellites are required (4 satellites give higher precision) for trilateration but the QoS depends on how closely or far apart the satellites are spaced when broadcasting to the user segment	sUAS and large UAS	<400 ft AGL and over 16, 000 ft	(GPS.GOV 2021)
	Denial of Service	Targeting flooding of data packets to the node (UAV) can lead to dropped GPS data	sUAS	<400 ft AGL	(Flysher, Yozevitch, and Ben-Moshe 2017)
	Sub-optimal Communication Links (Link Errors)	Network topology (in the case of swarms) affects the latency and delay of relayed GPS data.	sUAS	<400 ft AGL	(Gupta, Jain, and Vaszkun 2016)
	Indoor Environments	Indoor UAV operations such as for logistics and surveillance are	sUAS	<400 ft AGL	(Khosiawan and Nielsen 2016)

		prone to errors in GPS data			
	Malware	Deployment of malicious software can lead to system lockout that can temporarily prevent GPS data from being received or relayed	sUAS	<400 ft AGL	(Sung et al. 2020).
Erroneous data	Natural disaster	-	sUAS and large UAS	<400 ft AGL and 30000 – 40000 ft	(Kinowski and Skorupski 2016)
	Multipath	-	sUAS	<400 ft AGL	(Tabassum 2017)
	Terrestrial Obstructions	-	sUAS and large UAS	<400 ft AGL and over 16, 000 ft	(Johnson and Dewberry 2011)
	GPS receiver-side Failures	Depending on the hardware used for GNSS receivers, tracking sensitivity and data correction will affect quality of received GPS data	sUAS	< 400 ft AGL	(Jumaah et al. 2021)(Lin and Wei 2020)
	Man-in-the-middle (MitM), false data injection (FDI), and deauthentication attacks	Integrity and confidentiality of data is compromised, an implication of which is modification of received GPS data	sUAS and large UAS	<400 ft AGL and over 16, 000 ft	(Abbaspour et al. 2017; Dahiya and Garg 2019)
	Sensors/ADS-B system errors	Any malfunctioning in the sensors, such as pitot tube, could compromise ADS-B data integrity.	sUAS and large UAS	<400 ft AGL and 30000 – 40000 ft	(Tabassum 2017)
	ADS-B OUT/Ground station errors	Bugs in the module and data processing/encoding /Decoding may introduce error in the ADS-B message	sUAS and large UAS	<400 ft AGL and 30000 – 40000 ft	(Martin Strohmeier et al. 2014)
	Spoofing attack (overshadowing, bit flipping, and combining message deletion and injection)	Compromising illicitly the integrity of the message could impact the ADS-B message updating rate	sUAS and large UAS	<400 ft AGL and 30000 – 40000 ft	(Riahi Manesh and Kaabouch 2017; Martin Strohmeier, Lenders, and Martinovic 2014; Pöpper et al. 2011;

					Wilhelm, Schmitt, and Lenders 2012)(Qiao, Zhang, and Du 2018)

IV. GPS and ADS-B Signal Jamming Literature Review

Security and safety implications of relying on GPS and ADS-B

Autonomous vehicles require high accuracy and precision from the measurements provided by GNSS and signals ADS-B systems. During operation, these devices provide critical position information needed to maintain safe distances from civilians, obstacles, flight traffic and restrictive areas. However, there exist persistent limitations in the use of ADS-B and GPS along with their signal integrity (Pollack and Ranganathan 2018). Signal integrity problems include both data anomalies and data dropouts, therefore, consequent security challenges must be considered. (Hunter and Wei 2019).

Since the mandated use of ADS-B in 2020 for some aircraft type operations in Europe and U.S.A, advancement in lighter, smaller, and low-cost electronics has been made. By using ADS-B receivers each aircraft obtains its coordinates from global navigation satellites and messages are transmitted to the ground-based receivers over the 1090MHz band. ADS-B messages contain coordinates, velocity, a unique identifier (ICAO) and other ATC related data (Darabseh, Bitsikas, and Tedongmo 2019). This technology has also been tested on UAS demonstrating over 20 nmi (nautical miles) range (Hunter and Wei 2019), making ADS-B a promising technology for UAS and DAA applications. However, dependent surveillance has limitations and challenges. For instance, signals may degrade due to terrain, structures, and multipath. Additionally, since ADS-B designs do not have a robust model of deficiency and lack authentication and encryption, making it vulnerable to a range of cyber-attacks (Sidorov et al. 2017). The susceptibility of the protocol allows hackers to interfere with the communication signals, resulting in a threat in the safety of the aerial system as it could lead to collisions and further damage. In (Costin and Francillon 2014), the authors investigated the lack of security with respect to the protocol used in the communication and how it is vulnerable to attacks. In the same work, the authors described one major drawback of ADS-B associated to the dependence on line-of-sight availability and a solid ground-based transceiver infrastructure to work properly.

According to (International Civil Aviation Organisation 2013), ADS-B data may be used in combination with data obtained by other means of surveillance (such as radar, flight plan track, ADS-C) for the application of separation provided appropriate minima as determined by the state are applied. For the localization and positioning for an ADS-B device, the native GNSS receiver (for airplane, helicopter or sUAS) is used as source of truth. So, without further validation, this process is susceptible to errors or interference, where compromised GNSS data poses a single point of failure, leading to cascading negative effects. Henceforth, a lot of the pertinent literature concentrates on the security and integrity of GNSS data as means of navigation and separation.

Relevant results have also been indicated in the study (Langejan et al. 2016), where it was found that increasing ADS-B transmission range also increased signal interference, which in turn lowered safety. For example, if multiple ADS-B messages are received simultaneously at a receiver, it may not be possible to decode the received messages depending on the degree of overlap. It was suggested that the degrading effect of ADS-B signal interference should be considered in future airborne Conflict Detection and Resolution (CD&R) research, particularly for high traffic densities. Another concluding remark from this study is that the quality of an ADS-B message is affected by truncation, state accuracy and latency. Truncation is related to the digit significance in

the latitude and longitude locations. The accuracy of the on-board sensors affects the location precision, and the latency is related to the offset in location due to the travel time of signals.

GNSS such as the GPS represents one of the most reliable solutions for position and navigation. However, operations in urban environments are often referred to as GNSS-challenged environments due to limited availability and deteriorated navigation performance. This also may include isolated environments with lack of signal reachability. As described in (Pollack and Ranganathan 2018), GPS systems are highly vulnerable to large scale failures, hackers' attacks usually such as jamming and spoofing, and interferences of natural phenomena as geological locations and weather conditions. For instance, jamming attacks can adversely affect the precision of received GPS signals and is considered a DoS type attack that can cause erroneous navigation system information, as mentioned in the study performed by (Darabseh, Bitsikas, and Tedongmo 2019). On this study, a GPS jamming detection model is addressed, based on ADS-B quality metrics. Numerous jamming detection schemes are presented in this work to explore real world GPS jamming incidents on air traffic data. As a matter of fact, the authors proposed a scheme where each sensor is able to determine possible jamming attacks based on the distribution of its received data in a specific time period. For this purpose, the time history of transmissions for each aircraft was analyzed to obtain possible patterns and investigate suspicious signals that deviate from normal transmissions. The following types of jamming attacks were considered on the study: Constant Jamming, Deceptive Jamming, Adapting Jamming, Channel-hopping Jamming, and Smart Jamming. Despite the promising results, further experiments need to be performed utilizing more advanced statistical techniques given the complexity of jamming attacks.

According to (Rufa and Atkins 2016), past research has shown that GPS availability rates in urban environments range from 30% to 50% at ground level, and that this signal degradation is related to factors such as multipath, significant signal attenuation, masking, or even intentional acts such as jamming, denial, or deception. Some of these types of malicious interventions like jamming and spoofing attacks are described by (Yu et al. 2012). In jamming attacks, significant RF noise is transmitted so the receiver can no longer acquire satellite signal. On the other hand, in spoofing attacks, GPS counterfeit signals are generated causing the receiver to have incorrect position and data. However, in both interventions the attacks are not on the receiver software itself. A deeper analysis of modeling and characterization of GPS spoofing is developed by (Larcom and Liu 2013). In this work, attack models are described in diverse scenarios to analyze possible vulnerable aspects of civilian GPS. In a similar work presented by (Kerns et al. 2014), the authors investigated through modeling the sufficient conditions needed to successfully spoof and capture an autonomous drone, and demonstrated with field tests the capturing of a simple UAS via civilian based GPS spoofing. Using simulation environments, the authors showed that by subjecting GPS receivers, if the spoofer’s estimation errors of the UAS position and velocity are below 50 m and 10 m/s, respectively, the spoofer is capable of reliable and covert capture of the target drone’s control. The coupled dynamics of the UAS and spoofer showed that a GPS spoofing attack can force a UAS to unknowingly follow a trajectory imposed by the attacker and counterfeit signal. The feasibility of these conditions and spoofing attacks were field demonstrated and confirmed.

In a recent work sponsored by NASA(Ippolito et al. 2019), a set of assumptions, concepts of operations, challenges and design requirements were investigated to characterize flight-operations of emerging small UAS in heavily populated urban centers. One of the goals of this effort, named

NASA Safe Autonomous Flight Environment for the Last 50 Feet (SAFE50) project, is to investigate the challenges of integrating and enabling access of small UAS to low-altitude high-density urban environments through advanced onboard autonomy. One of the main concerns discussed in the paper is the flight operations to be developed in degraded or denied GNSS/GPS conditions. For example, the authors pointed out that urban canyon environments are not reliable to utilize satellite-based communication for over-the-horizon (OTH) communication. In consequence, operations near urban canyons will result in disruptions to wireless communication, degraded air-ground communication, satellite-based communication, line-of-site blockage, and signal reflections. Additionally, risk and hazard analysis were performed, and the actors involved in the development of UAS operations were identified as: the general public, supplemental service data providers, regulatory agencies, insurance companies, other aircraft, dynamic ground objects, and static ground objects.

Causes and Potential Mitigation Strategies

Operations within urban environments take place in concentrated RF environments with high levels of noise, degraded signals, and RF issues such as signal reflection, causing impact over operations relying on GPS signal. As mentioned by (Strümpfel et al. 2020), potential causes for GNSS unavailability or sparsely availability may be caused due to shadowing effects due to the presence of objects and buildings or deteriorated positioning performance due to multipath and poor available satellite geometry. Studies have been performed to analyze the relationship between predicted receiver position, satellite constellation, and object database to calculate and proof the LOS to available satellites.

As previously mentioned, natural phenomena may affect the GPS reliability. These include space weather effects such as solar radio burst, scintillation and geomagnetic storms, atmospheric refractions and delays, and equatorial regions. As described by (Comberiate et al. 2012) for example, solar flare eruption produces radio waves that reduces the signal to noise ratio of relative weak GPS signals and interferes with frequency channels used by GPS. In conjunction with solar flares, magnetic storms, very well studied by (I. I. Alexeev et al. 2001) (Igor I. Alexeev et al. 2003), cause denominated scintillations in GPS signals that arise from spatial temporal variations in the ionosphere. Along with this phenomenon, atmospheric effects as ionic concentration, temperature, pressure, and humidity at the tropospheric layer causes delay in the communication due to refraction of the signal entering the Earth.

Non-line-of-sight (NLOS) conditions can severely affect the accuracy of the measurements and the performance of the autonomous drone during operation. NLSO conditions are common within urbanized cities where the GNSS signals are partially blocked, jammed, or reflected by buildings surround the drone. These reflections and disruptions can add significant errors to the expected GNSS measurements and are difficult to account for since these reflections can bounce along various pathways before being received and processed by the drone. (L. T. Hsu 2018) investigated the modeling and severity of NLOS for small UASs in an urban environment. The GNSS modeling was compared to controlled field tests to access the modelling accuracy and a mitigation process to reduce the noise and error created by the NLOS reflections.

From the cyber-security perspective, since GPS localization relies on active communication, signals are transmitted and received between different nodes, exposing itself to external intervention. As presented by (Yu et al. 2012), there exist weaknesses to be detected on the

software of GPS manufacturers. Although security measurements have been taken to overcome this problem, as for example validation algorithms in the communication protocols, filters, attack detectors, satellite identification codes, timing comparison and counter check with IMU or sensor data, as reported in (Haider and Khalid 2016), the constant innovation in technology also allows for new jamming and spoofing techniques that exploit hardware and software weak spots.

Another effect, similar to jamming attacks that affects GPS and ADS-B sensors, is obtained through garbling which also generates the superimposing of signals coming from different sources. A method to mitigate these effects has been studied using a multichannel ADS-B receiver and implementing techniques such as Blind Source Separation (BSS) and Principal Component Analysis (PCA), as presented in (Leonardi and Piracci 2018). For instance, according to the authors, using a multi-channel/multi-antenna receiver, it is possible to exploit the different signal sources to estimate and extract the original signals. However, a drawback from this method is that it requires a multi-channel antenna and receiver, which increases the costs of the ADS-B receiver. In the literature, multi-channel receivers for ADS-B signals have been widely analyzed to overcome the problem of overlapping signals coming from different aircraft.

Machine learning techniques have also been studied to mitigate jamming attacks on ADS-B devices. In (Manesh et al. 2019) the authors performed a comparison analysis of machine learning based techniques to increase detection rates of cyber-attacks, particularly jamming attacks to the ground station or to the aircraft. In particular, the study noted that ground stations are more prone to jamming attacks, as the attack requires less power. In contrast, an aircraft jamming attack would require more power, more money, and more difficult to make equipment. However, they also note that other nearby aircraft can easily jam others such as in the case of drones. The authors in this study compared different techniques from the literature proposed to monitor and detect jamming attacks. These include support vector machine, k-nearest neighbor, artificial neural network (NN), and decision tree. Features used to detect jamming using these techniques include bit error rate, bad packet ratio, and energy statistic of received signal. The study found that the most acceptable performance in detecting jamming attacks, with high detection rate and relatively low false alarms, was obtained with the neural network approach. With NN, the detection rate and false alarms were 90.3%, and 30.9%, respectively. All the studied techniques, however, showed high percentage of false alarm that exceeded 24%, which would be unacceptable in real scenarios.

ADS-B signal validation strategies using vision-aided detection systems have been also proposed in the literature as alternative approach to mitigate signal degradation. According to (Carrio et al. 2017), kinds of sensing technologies can be deployed onboard UASs to detect flying obstacles. In particular, the authors demonstrated a low-powered ADS-B system integrated with a Thermal Infrared (TIR) camera to evaluate the effectiveness of the combined sensors for obstacle and aircraft detection. This complimentary system was compared to an ADS-B coupled with an RGB camera. These systems were prototyped and integrated on a UAS platform within a laboratory environment to develop and test image processing algorithms and sensor fusion techniques. TIR imaging proved to be effective for vision-based conflict detection systems, allowing visual detections under extreme illumination conditions such as direct sun exposure or during the night, at real-time frame rates. *“Experimental results report a detection accuracy of 100 % in all cases and an average recall rate of 65.94 %, acquiring images and processing them at 30Hz, with detection ranges between 3 to 5 Km.”*

In recent years, there has been a significant interest on investigating compensation strategies for GPS degradation or absents in the navigation procedures and countermeasures for cyber-attacks that can disrupt the normal course of action. According to (Strümpfel et al. 2020), to enable operation of small UAS at any time in any environment, a navigation capability is required that is robust enough and not solely dependent on GNSS. The problem of deteriorated and sometimes unavailable GNSS has motivated the study of potential mitigation strategies ranging from GPS only to trajectory optimization, and complementary multisensory fusion using inertial sensors, priori urban maps, and ground-based navigation. With the use of these strategies, it is expected that, as soon as the GNSS is affected, the technology must assess what alternative positioning strategy is available and switch to a different navigation method. A widely studied alternative is IMU. The advantage of using IMU resides on the use of only inertial acceleration measurements which are not affected by disruptions to wireless communication or degraded air-ground communication. However, a significant disadvantage is that such measurements used to approximate position and attitude suffers drift over time.

For GPS-denied environments, modern alternative approaches utilize visual odometry, and more specifically SLAM techniques. An extensive survey of these technologies for GPS denied navigation have been performed by (Balamurugan, Valarmathi, and Naidu 2017). SLAM algorithms allow the mobile system to construct a live map of the surroundings by information obtained from IMU, onboard cameras and additional sensors. This methodology allows the vehicle to navigate in environments with even no GPS access.

Laser-based solutions have also been investigated along with hybrid approaches that utilize the observation of features in the environment using laser range scanners and imagery. According to (Strümpfel et al. 2020) challenging environments are divided into structured and unstructured environments. The Structured Environment Navigation (SEN) is characterized by well-defined boundaries such as predictable heights, shapes/sizes, room/corridors and building materials. Unstructured environment navigation, also known as Probabilistic Environment Navigation (PEN), is characterized by irregular dimensions and rough surfaces. One of the advantages of using vision type sensors, as discussed by (Rufa and Atkins 2016), is that they do not depend on any man-made electromagnetic transmission to work properly, which makes them a suitable and complementary sensor to GPS.

Additional techniques that rely on visual odometry include optical flow or feature detection/localization. In particular, optical flow can be applied to small UAS operating in proximity to urban canyons or buildings. Using a camera with acceptable resolution, this technique calculates the apparent local velocities of adjacent features (e.g., buildings or the street below) to estimate the relative position within a pre-defined reference frame. Numerical simulations and flight tests have shown that vehicles equipped with combined optical flow-stereo sensors can also navigate 90 degree turns in simulated urban canyons without relying totally on GPS (Chao, Gu, and Napolitano 2013); (Rhudy et al. 2015). Feature detection/localization uses vanishing points to measure aircraft pitch and roll angles which can be used to reset the error in the IMU attitude angle estimate. In addition to supporting navigation, laser and camera data may also be used to support detect and avoid functions to assess the risk of collisions.

Long-term evolution cellular network has also been reported as an alternative concept that could increase navigation accuracy of small UASs in urban centers. Since urban environments usually

have large number of towers, the accuracy of localization navigation estimation can be improved as a function of the number of towers available. This concept, however, it is still an active area of research (Khalife, Bhattacharya, and Kassas 2018).

Network navigation-based techniques that use trajectory optimization of multiple small UASs have been initially studied as a novel solution for GPS-denied navigation. In the work presented by (Causa, Fasano, and Grassi 2018), an optimization algorithm is developed for flying trajectories of multi-UAS missions, associating a vehicle not susceptible to GNSS signal corruption, referred as" father'' vehicle, to support autonomous navigation of a" son'' vehicle operating in complex environments. The challenging zones are defined as areas where GNSS satellites are not available, and in those areas, the number of father vehicles depends on the available GNSS information and alternative mitigation sensors.

Light Detection and Ranging (LIDAR) is another potential navigation sensor solution for small UAS navigation operating in urban canyons. These sensors can operate in GPS and weather degraded conditions. According to (Rufa and Atkins 2016), this sensor can increase urban canyon navigation accuracy by an order of magnitude compared with the traditional GPS/IMU/Odometry. However, the only drawback of using this sensor is the associated high cost for small UASs.

Additionally, (Rufa and Atkins 2016) performed a comprehensive study regarding sensor accuracy and availability as a function of environment characteristics. The authors investigated alternative signals to GPS, including cellular network, television, wireless fidelity (Wi-Fi), and signals from other satellites to determine if any of these available technologies would be a viable solution for GPS independent navigation. They concluded that although LIDAR sensor allow mapping the environment, complementary solutions such as Wi-Fi and cellular network could provide a long-term evolution (LTE) technology to support inertial navigation in GPS denied urban environments.

Figure 14 shows a diagram of the possible sensors and existing urban navigation solutions. Table 4 shows the measured states provided by each type of sensor, based on the states for a rigid-body fixed-wing UAS: north position N; east position XE; altitude h; ground speed VT; angle of attack α; angle of sideslip β; the following Euler orientation angles of roll angle ϕ, pitch angle θ, and yaw angle ψ; and the body-fixed angular velocities of roll rate p, pitch rate q, and yaw rate r.

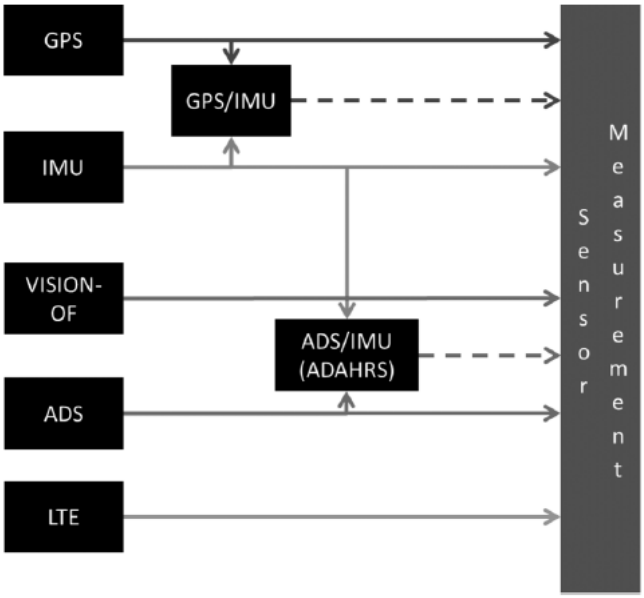

Figure 14. Sensor System Diagram. Taken from (Rufa and Atkins 2016).

Table 4. UAS Sensor Information. Taken from (Rufa and Atkins 2016).

Sensor	Measured states
GPS	X_N, X_E, h, V_T
AHRS	ϕ , θ, ψ, p , q , r
Vision	V_T
ADS	h, V_T, α, β
LTE	X_N, X_E
GPS/IMU	X_N, X_E, h, V_T, ϕ , θ, ψ, p , q , r
ADS/IMU	V_T, α, β, ϕ , θ, ψ, p , q , r

Alongside the additional hardware selected for each approach, a variety of guidance algorithms can be integrated as part of a robust navigation solution to address external disturbances and dropouts. These guidance algorithms can enhance the accuracy of the localization and different hybrid solutions have been studied. As presented in Table 5, possible navigation solutions and combination of different techniques have been reported in the literature to overcome GPS unavailability (Balamurugan, Valarmathi, and Naidu 2017).

One more promising solution for navigation in GPS-denied environments includes nonconventional approaches such as geomagnetic navigation, that combined with machine

learning techniques could represent a potential navigation solution. The United States Air force (USAF) and NASA with the National Oceanic and Atmospheric Administration have been investigating the use of the Earth's geomagnetic field for navigation for over two decades (Canciani and Raquet 2017)(Sabaka et al. 2020). This alternative navigation technique, proposed even before the GPS era, provides terrain navigation based on map contours. In1940, Goodyear Aircraft Corporation started developing the Automatic Terrain Recognition and Navigation System (ATRAN), a radar-map matching system capable of correcting the flight path deviation by correlating measurements from a radar scanning antenna with a series of maps on board a missile. Later in 1958, this was successfully demonstrated at Holloman AFB by using a three-axis precision magnetometer attached to a plane and finding the best fit between the geomagnetic profile measured during the flight and the corresponding profile in a stored map. With these initiatives, a foundation for modern geomagnetic navigation was established (Goldenberg 2006).

Geomagnetic based methodology, however, is also affected by the solar winds and magnetic storms. Currently, machine learning techniques are used to provide support in the forecasting of key magnetic storm indicators for real-time applications, including navigation (Cuenca and Moncayo 2021).

Table 5. Visual Navigation Solutions for GPS-denied Scenarios from (Balamurugan, Valarmathi, and Naidu 2017)

No	Type of Vehicle	Strategy	Sensors Used	Year
1	AscTec Pelican Quadrotor	Visual Odometry	Stereo camera	2015
2	Quadrotor (GTQ)	Visual SLAM and Laser SLAM with EKF	IMU, Sonar, Scanning laser and Camera	2014
3	Hexacopter	Visual SLAM with EKF	IMU, Monocular camera	2014
4	Mikrokopter	EKF	IMU, Monocular camera, GPS, Barometric altimeter	2014
5	Six Wheeled UGV	Bayesian Information Filter (EKF)	IMU and Stereo Camera	2013
6	AsTec Pelican MAV	VO and SLAM	Stereo camera	2013
7	Simulator with flight data	UKF	IMU, GPS and Camera	2013
8	Quadrotor	Invariant EKF	IMU and RGBD Odometry (Kinect)	2013
9	Astec Pelican Quadrotor	UKF	IMU, Monocular camera	2013
10	Astec Firefly MAV	EKF	IMU, Pressure sensor and Monocular camera	2013
11	Quadrotor	Visual SLAM with KF	IMU with Monocular camera	2013
12	Hexacopter	Visual SLAM with EKF	IMU and WVGA Monocular camera	2012
13	Simulator with data	EKF	IMU, Monocular camera	2012
14	Multi-Stereo Helmet tracking system	EKF	IMU and Monocular camera	2012
15	Test bed which is gas-powered radio-controlled model helicopter	Visual SLAM with EKF	IMU, Monocular camera	2012

No	Type of Vehicle	Strategy	Sensors Used	Year
16	Quadcopter	Visual SLAM with EKF	IMU, Pressure Sensor, USB Firefly Monocular camera	2011
17	Gas-powered radio-controlled model helicopter	Visual Odometry with EKF	IMU, Monocular camera	2011
18	Scout B1-100 Helicopter	Using Pre-Existing Maps	IMU and Monocular camera	2011
19	Six-Legged Crawler	Visual Odometry	IMU with Stereo camera	2011
20	Simulator with Flight Data	Image Registration using GIS Data	IMU, GPS, Camera and GIS Data	2010
21	Simulator with Flight Data	Visual SLAM	Camera	2010
22	Quadrotor	Visual SLAM with EKF	IMU, Stereo camera, Monocular Color Camera with Laser finder	2010
23	HMAV	EKF	IMU and Wi-Fi camera	2009
24	Quadcopter	KF	IMU and VGA camera	2009
25	Yamaha RMAX Helicopter	KF with Image Registration	IMU, GPS, Camera and Satellite Images	2008
26	Simulator with Vehicle data	Kalman Filter	IMU with Laser scanner	2008
27	Simulator with synthetic MAV flight data	UKF Framework utilizing epipolar constraint	IMU and Stereo Camera	2008
28	Simulator with MAV flight data	Iterative Registration method, UKF	IMU with Monocular camera	2007
29	Simulator with MAV flight data	Visual Odometry with EKF	IMU with Monocular camera	2007
30	Acrobatic 23cc helicopter	Non-Linear observer	IMU and Webcam	2007
31	Simulator with Vehicle data	EKF	IMU with Camera	2007

V. ECD, GPS and ADS-B Signal Spoofing Literature Review

Three main topics are included in this section of the literature review: 1) GPS spoofing detection and mitigation for GNSS / GPS using the ECD algorithm; 2) GPS spoofing of ADS-B systems, and 3) indoor localization with aircraft signals.[i] Recognize that ADS-B is a subset of the larger receiver localization problem. Solutions that apply to the larger vector space, GNSS / GPS also are valid for the subset, ADS-B, if computational hardware is available.

GPS spoofing is a reasonably well researched topic. Many methods have been proposed to detect and mitigate spoofing. The majority of the research focuses on detection of spoofing attacks. Methods of spoofing mitigation are often specialized or computationally burdensome. Civilian COTS anti spoofing countermeasures are rare. This report highlights the brilliant additive research by Dr Manuel Eichelberger on mitigation and recovery of GPS spoofing. (Eichelberger 2019) ECD implementation and evaluation shows 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 in which several signals are present. Experiments based on the TEXBAT database show that a wide variety of attacks can be mitigated. In the TEXBAT scenarios, an attacker can introduce a maximum error of 222 m and a median error under 19 m. [ii]This is less than a sixth of the maximum unnoticed location offset reported in previous work that only detects spoofing attacks. (Ranganathan and al. 2016).

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

ADS-B high dependency on communication and navigation (GNSS) systems causes the system to inherit the vulnerabilities of those systems. This results in more opportunities to exploit those vulnerabilities. In general, advancements in computers, connectivity, storage, hardware, software, and apps are major aids to malicious parties who wish to carry out the spoofing and other threats by exploiting the vulnerabilities of ADS-B. Another main vulnerability of ADS-B systems is its broadcast nature without security measures, which can easily be exploited to cause harm.

Qualitative Risk Assessment Opinion based on FAA SRM Reference Guidelines (F.A.A. 2018; 2019; 2021)**.**
After reviewing data, papers, and reports regarding the Severity, Likelihood, and Risks associated with spoofing GNSS/ GPS signals, there are two schools of thought. Before 2015, transmitting fake GNSS/GPS signals was both a qualitative - unlikely [Table 3-C *Remote*] (F.A.A. 2018) risk and a niche issue. After 2015, the world changed considerably. Low-cost SDR RF signal generators combined with awareness that spoofing was a powerful disruption technique, and availability of COTs precipitated a sharp increase in incidents ranging from amateur, to researcher generated, to professional crook, to nation-state. The Ling and Qing demonstration of SDR signal spoofer at DEFCON 2015 plus the 2013 spoofing of the 213' motor yacht White Rose of Drachs, by Humphreys' team set the stage for significant spoofing incidents to follow. (Humphrees and e 2008).

There are two organizations which report the spoofing risks quite differently: the FAA and US Navy. The FAA is concerned with the safe operation of aircraft, including UAS, in the NAS.

Using the FAA SRM definitions the maximum severity of signal spoofing threat is *Major* [Table 2 -3] (F.A.A. 2018). This is because the threat would most likely result in substantial damage to the aircraft vehicle and physical distress or injuries to persons *without loss of life*. Depending on circumstances, the FAA SRM definitions result in the maximum likelihood as *Probable* - especially for UAS. [Table 4-B]. (F.A.A. 2018)

The US Navy sees the spoofing threat quite differently. It considered the spate of incidents in 2016 in Moscow, Black Sea in 2017, Port of Shanghai in 2019 and the loss of 20 sailors in the South China Seas in 2017 involving incidents with the USS McCain and USS Fitzgerald colliding with commercial vessels Alnic MC and ACX. The US Navy sees the spoofing severity as *Catastrophic* [Table 2-1] because of multiple fatalities, loss, and/or severe damage to ships and defensive aircraft. Further, the US Navy view appears to be that the likelihood is *Probable* [Table 3-B]. (F.A.A. 2018) Depending on the view, spoofing can be considered at Risk Levels *Yellow or Red* [*Medium to High*], i.e., medium acceptable risk to unacceptable risk. This bears out based on the number of researchers and analysts studying / reporting / conventions on GNSS/GPS spoofing countermeasures since 2018.

Using FAA SRM Guidelines, signal spoofing on UAS /ADS-B systems is above average likelihood (*probable -> frequent*) and severity [*Yellow bordering on Red or in terms of the severity qualitative scale 3*-> 2]. (F.A.A. 2019; 2018) As such, it is definitely not negligible and further investigation is warranted. Further, ECD countermeasure methodology appears to be the superior solution for outdoor localization. Simulation of ECD by ERAU is recommended.

In addition, the European Union Aviation Safety Agency's (EASA) Opinion No 03/2021 regarding *Management of Information Security Risks* offers some relevant information. (E.A.S.A. 2021) SME Discussion is found in the end notes. [iii] [iv] (R. Nichols and Ryan 2000) [v] [vi]

ASSURE A44

The ASSURE A44 project requires further definition of the Risk Assessment for spoofing threats into four classifications: *Part 107 Operations, BVLOS, Urban Areas, and Near Airports*. Tables 1-3 show the Severity and Likelihood Probability, Associated References, and Mitigation Schemes associated with the increasing Risk Profile for these classes. Because of federal guidelines and licensing requirements, Part 107 Operations specifies a near pristine Risk level, or The Best-Case Scenario. Because the UAS is not limited to a specified space and may cross the visual horizon, BVLOS represents an elevated UAS spoofing threat and risk. Urban area operations represent a difficult case for spoofing with increased Severity of consequences. Urban areas present difficulty to enact countermeasure to a spoofing attack. Humans and equipment are at risk. Near Airports represents the Worst-Case scenario with the highest Severity and Likelihood Probability. There are globally reported UAS – aircraft and UAS – ship spoofing incidents that present serious consequences to human life. In all four classifications, spoofing is probable. Both FAA and USN consider spoofing a real and escalating threat. It no longer represents a remote or niche possibility (Khan, Mohsin, and Iqbal 2021; R. Nichols and Ryan 2000; M. L. Psiaki and Humphreys 2016).

DISCLAIMERS / ASSUMPTIONS

Readers are assumed to have a reasonable knowledge of GNSS / GPS and ADS-B "IN" and "OUT" systems. For those that need a refresher, (Moncayo, Yanke, and Yuetong 2020) gives a good discussion of ADS-B "IN" vulnerabilities against jamming and spoofing threats. The FAA defines the scope of ADS-B "OUT" in its 2018 Edition on the subject. (F.A.A. 2018) Chapter 4 of (Busyairah 2019) gives a detailed view of Aircraft Surveillance Systems and the Radar limitations, advantages, disadvantages, infrastructure, and applicable standards for a complete ADS-B system. Chapter 6 discusses the security considerations of ADS-B systems. (Busyairah 2019) UAS and C-UAS Cybersecurity considerations for GPS and ADS-B systems are effectively detailed in (R.K. Nichols and a 2020), (Randall K. Nichols et al. 2019) and (D.H.S. 2018). GPS systems and message formats are described in both (Eichelberger 2019) and (Wikipedia 2021).

Jamming attacks are briefly covered in this report. However, the ECD/CD method described in (Eichelberger 2019) is an effective countermeasure to jamming attacks on GPS and ADS-B systems.

History of spoofing countermeasures is covered up through 2016 with sole reference to (Haider and Khalid 2016)

Intersecting Vulnerabilities [vii]

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 vulnerabilities in its own right. This report will cover in detail the brilliant work of Dr. Michael Eichelberger on *Robust Global Localization using GPS and Aircraft Signals*. He describes a functional tool known as CD to detect, mitigate and counter spoofing (and jamming) attacks on all stages of GPS. (Eichelberger 2019)

GPS is ubiquitous and is incorporated into so many applications (aircraft, ship, car /truck navigation; train routing and control; cellular network, stock market, and power grid synchronization) that it makes a "rich" target for spoofing a receiver's perceived location or time. Wrong information in time or space can have severe consequences.

ATC is partially transitioning from radar to a scheme in which aircraft (A/C) transmit their current location twice per second, through ADS-B messages. This system is mandated in Europe and well under way in US since 2020. The A/C determine their own location using GPS. If a wrong location is estimated by the on-board GPS receiver due to spoofing, wrong routing instructions will be delivered due to a wrong reported A/C location, leading to an A/C crash.

Ships depend heavily on GPS. They have few reference points to localize themselves apart from GPS. Wrong location indication can strand a ship, cause a collision, push off course into dangerous waters, ground a ship, or turn a ship into a ghost or a missile. 2017 incidents in the Black Sea and South China Seas have been documented. (Burgess 2017; Randall K. Nichols et al. 2019)

While planes and ships suffer spoofing attacks in the domain of location, an attacker may also try to change the perceived time of a GPS receiver. Cellular networks rely on accurate time synchronization for exchanging communication data packets between ground antennas and mobile handsets in the same network cell. Also, all neighboring cells of the network need to be time

synchronized for seamless call handoffs of handsets switching cells and coordinating data transmissions in overlapping coverage areas. Since most cellular ground stations get their timing information from GPS, a signal spoofing attacker could decouple cells from the common network time. Overlapping cells might send data at the same time and frequencies, leading to message collisions and losses. (Anonymous 2014) Failing communications networks can disrupt emergency services and businesses. (Eichelberger 2019)

SPOOFING

Threats and weaknesses show that large damages (even fatal or catastrophic) can be caused by transmitting forged GPS signals. False signal generators may cost only a few hundred dollars of software and hardware.

A GPS receiver computing its location incorrectly or even failing to estimate any location at all can have different causes. Wrong localization solutions come from 1) a low signal-to-noise ratio (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 is the most difficult case since the attacker can freely choose the signal power and delays for each satellite individually. (Eichelberger 2019)

Before discussing ECD – Collective detection maximum likelihood localization approach, (Eichelberger 2019) it is best to step back and briefly discuss GPS signals, classical GPS receivers, A-GPS, and snapshot receivers. Then the ECD approach to spoofing will show some real power by comparison. Power is defined as both enhanced spoofing detection and mitigation capabilities. [viii]

GPS SIGNAL

The GPS system consists of a control segment, space segment, and user segment. The space segment contains the 24 orbiting satellites. The network monitor stations, and GCS and their antennas make up the control segment. The third and most important are the receivers which make up the user segment. (U.S.G.P.O. 2021)

Satellites transmit signals in different frequency bands. These include the L1 and L2 frequency bands at 1.57542 GHz and 1.2276 GHz. (DoD 2008) Signals from different satellites may be distinguished and extracted from background noise using code division multiple access protocol (CDMA).(DoD 2008) Each satellite has a unique course / acquisition code (C/A) of 1023 bits. The C/A codes are PRN sequences transmitted at 10.23 MHz which means it repeats every millisecond. The C /A code is merged using an XOR before being with the L1 or L2 carrier. The data broadcast has a timestamp called HOW which is used to compute the location of the satellite when the packet was transmitted. The receiver needs accurate orbital information (aka ephemeris) about the satellite which changes over time. The timestamp is broadcast every six seconds, the ephemeris data can only be received if the receiver can decode at least 30 seconds of signal. (Eichelberger 2019)[ix]

CLASSIC RECEIVERS

Classical GPS receivers use three stages when obtaining a location fix: acquisition, tracking, and localization.

Acquisition. The relative speed between satellite and receiver introduces a significant Doppler shift to the carrier frequency. [x] GPS receiver locates the set of available satellites. This is achieved by correlating the received signal with the known C /A codes from satellites. Since satellites move at considerable speeds. The signal frequency is affected by a Doppler shift. So, the receiver must correlate the received signal with C/ A codes with different Doppler shifts. (Eichelberger 2019)[xi]

Tracking. After a set of satellites has been acquired, the data contained in the broadcast signal is decoded. Doppler shifts and C /A code phase are tracked using tracking loops. After the receiver obtained the ephemeris data and HOW timestamps from at least four satellites, it can start to compute its location. (Eichelberger 2019)[xii]

Localization. Localization in GPS is achieved using signal time of flight (ToF) measurements. ToFs are the difference between the arrival times of the HOW timestamps decoded in the tracking stage of the receiver and those signal transmission timestamps themselves. [xiii] The local time at the receiver is unknown and the localization is done using pseudo-ranges. The receiver location is usually found using least-squares optimization. (Eichelberger 2019; Wikipedia 2021)[xiv]

A main disadvantage of GPS is the low bit rate of the navigation data encoded in the signals transmitted by the satellites. The minimal data necessary to compute a location fix, which includes the ephemerides of the satellites, repeats only every 30 seconds. [xv]

A-GPS (ASSISTED GPS) – REDUCING THE START-UP TIME

Assisted GPS (A-GPS) drastically reduces the start-up time by fetching the navigation data over the internet, commonly by connecting via a cellular network. Data transmission over cellular networks is faster than decoding the GPS signals and normally only takes a few seconds. The ephemeris data is valid for 30 minutes. Using that data, the acquisition time can be reduced since the available satellites can be estimated along with their expected Doppler shifts. With A-GPS, the receiver still needs to extract the HOW timestamps from the signal. However, these timestamps are transmitted every six seconds, which translates to how much time it takes the A-GPS receiver to compute a location fix. (Eichelberger 2019)[xvi]

COARSE – TIME NAVIGATION

Coarse -Time Navigation (CTN) is an A-GPS technique which drops the requirement to decode the HOW timestamps from the GPS signals. (Diggelen 2009) The only information used from the GPS signals are the phases of the C/A code sequences which are detected by a matched filter. Those C/A code arrival times are directly related to the sub-milliseconds unambiguously, the deviation may be no more than 150 km from the correct values. [xvii] [xviii] Since the PRN sequences repeat every millisecond, without considering navigation data flips in the signal, CTN can, in theory, compute a location from one millisecond of the sampled signal. [xix] Noise can be an issue with such short signal recordings because it cannot be filtered out the same way with longer recordings of several seconds. The big advantage is that signal processing is fast and power-efficient and reduces latency of the first fix. Since no metadata is extracted from the GPS signal, CTN can often compute a location even in the presence of noise or attenuation (Diggelen 2009).

SNAPSHOT RECEIVERS

Snapshot receivers aim at the remaining latency that results from transmission of timestamps from satellites every six seconds. Snapshot receivers can determine the ranges to the satellite modulo 1 ms, which corresponds to 300 km.

COLLECTIVE DETECTION

Collective Detection (CD) is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite, but rather combine all the available information and decide only at the end of the computation. [xx] 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 CTN. CD requires a lot of 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 and etal 2012; Axelrod and al 2011; Bissag and M 2017)

ECD

Returning to the spoofing attack discussion, Dr Manuel Eichelberger's *CD – Collective detection maximum likelihood localization approach*, his method 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, Robust Global Localization using GPS and Aircraft Signals, 2019) COTS have little spoofing integrated defenses. Military receivers use symmetrically encrypted GPS signals which are subject to a "replay" attack with a small delay to confuse receivers.

ECD solves even the toughest type of GPS spoofing attack which consists of spoofed signals with power levels similar to the authentic signals. (Eichelberger 2019) ECD achieves median errors under 19 m on the TEXBAT dataset, which is the de facto reference dataset for testing GPS anti-spoofing algorithms. (Ranganathan and al. 2016; Wesson 2014) The ECD approach uses only a few milliseconds worth of raw GPS signals, so called snapshots, for each location fix. This enables offloading the computation into the Cloud, which allows knowledge of observed attacks. [xxi] Existing spoofing mitigation methods require a constant stream of GPS signals and track those signals over time. Computational load is increased because fake signals have to be detected, removed, or bypassed. (Eichelberger 2019)

RESEARCH TO 2016: SURVEY OF EFFECTIVE GPS SPOOFING COUNTERMEASURES

Because of the overwhelming dependence on GPS in every sector, ranging from civilian to military, researchers have been trying to desperately find a complete solution to meet spoofing threat. To understand that ECD (following sections) is a brilliant departure from the past efforts, it is necessary to briefly cover the prevailing common wisdom. Haider and Khalid in 2016 published an adequate survey of spoofing countermeasures up through the end of 2016. (Haider and Khalid 2016)

SPOOFING TECHNIQUES

According to (Haider and Khalid 2016) there are three common GPS Spoofing techniques with different sophistication levels: simplistic, intermediate, and sophisticated (Humphreys and al. 2008).

The *simplistic spoofing attack* is the most commonly used technique to spoof GPS receivers. It only requires a COTS GPS signal simulator, amplifier, and antenna to broadcast signals towards the GPS receiver. It was performed successfully by Los Alamos National Laboratory in 2002. (Warner and Johnston 2003) Simplistic spoofing attacks can be expensive as the GPS simulator can cost $400K and be heavy (not mobile). Simulator signals are not synchronized by the available GPS signal and detection is easy.

In the *intermediate spoofing attack*, the spoofing component consists of GPS receiver to receiver genuine GPS signal and spoofing device to transmit a fake GPS signal. The idea is to estimate the target receiver antenna position and velocity and then broadcast a fake signal relative to the genuine GPS signal. This type of spoofing attack is difficult to detect and can be partially prevented by use of an IMU. (Humphreys and al. 2008)

In *sophisticated spoofing attacks*, multiple receiver-spoofer devices target the GPS receiver from different angles and directions. The angle-of-attack defense against GPS spoofing in which the angle of reception is monitored to detect spoofing, fails in this scenario. The only known defense successful against such attack is cryptographic authentication. (Humphreys and al. 2008) [xxii]

Note that prior research on spoofing was to *exclude* the fake signals and focus on a single satellite. ECD (next section) *includes* the fake signal on a minimum of four satellites, and then progressively / selectively eliminates their effect until the real *weaker* GPS signals become apparent. (Eichelberger 2019)

According to (Haider and Khalid 2016), there have been six innovative research papers that cover spoofing countermeasures.

A. Multi-test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers (Jovanovic and Botteron 2014)

The CM presented in this paper relies on statistical properties of the GPS signal, signal power level, Doppler frequency offset, and carrier to noise ratio. [xxiii] The method monitors the above statistical properties and checks for inconsistencies to detect the presence of a GPS spoofer signal. The test results show that the proposed CMs can successfully detect the presence of the GPS fake signal with a low probability of false alarm. The method offers a protection module (once the spoofed signal is detected) where the tracking history is further evaluated to re-establish the lock on correct signal. This method only works against simplistic spoofer attacks. However, it is cost-effective as it requires only changes to the classic GNSS receiver, not the whole GPS infrastructure. (Jovanovic and Botteron 2014)

B. GPS Spoofing Countermeasures (Warner and Johnston 2003)

The Warner and Johnson paper is good material for anyone interested in learning about GPS spoofing CMs, but the techniques discussed were general not specific. The effectiveness of the approaches and strategies to defend against spoofing mentioned cannot be measured because no

tests were performed to evaluate the methods presented. None of the presented methods were implemented in the field. The majority of strategies discussed were based on the monitoring of signal properties. (Haider and Khalid 2016)

C. An Asymmetric Security Mechanism for Navigation Signals (Kuhn 2015)

The method described in Kuhn is based on cross-correlation and short-term information processing.[xxiv] It is proposed that each satellite transmitter will transmit a signal known as a hidden mark signal at regular intervals of time with a power level lower than receiver noise level. After each mark signal transmission, a signed (encrypted) data signal is transmitted with a power level above the receiver noise level. The hidden mark signal can only be assessed by GPS receivers after receiving the signed data signal. This approach is best for a spoofed -replayed attack. The crystal oscillators inside classic GPS receivers can easily measure the delay between the data signal and the hidden mark signal despite being less than accurate as compared to onboard atomic clocks of the satellite. The method fails for multiple spoofer antennas. (Kuhn 2015)

D. A Cross layer defense mechanism against GPS spoofing attacks on PMUs in Smart Grid (Fan and al. 2015)

The CM described is a method to protect the electrical grid PMUs from possible GPS spoofing attacks. The protection method consists of cross layer protection. The first layer (physical) receives signals from hybrid antennas, and then measure the AOA of the signals of all the GPS receivers. AOA will be the same to GPS receiver if sourced at the same satellite. Spoofed signals will have a different AOA. The second layer (upper layer) receives input from the physical layer then processes using state-based estimation techniques to detect bad data. The technique is feasible and only requires additional GPS receiver and antenna. The method works against simple and intermediate attacks. (Fan and al. 2015)

E. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing (Magiera and Katulski 2015)

This paper focuses on a CM that uses spatial processing. It tests well for both detection and reducing the impact of spoofed receivers. The method uses multiple antennas for reception and combines with the AOA approach. The phase delay measurement is used distinguish the fake and authentic signals. The accuracy of the CM was tested when 4-8 spoofed signals were in play. Accuracy prediction was 99% when carrier to noise ratio was at least 46 dBHz (Magiera and Katulski 2015).

F. GPS Spoofing Detection via Dual- Receiver Correlation of Military Signals (M. Psiaki and al. 2013)

The authors proposed a cross-layer detection mechanism to detect multiple spoofing attacks against the smart grid. In the physical layer, an AOA based mechanism is employed. The distribution of the normal to spoofed standard deviation of the difference of the C/No from different antennas is calculated. The prior probability of spoofing is calculated then fed into the upper layer for further detection. In the upper layer, a Kalman filter is applied to estimate the state of the power system and use the measurement error to calculate the trustworthiness value of being

spoofed. The information is all combined and correlated / integrated into the cross-layer mechanism. Results have posted well but computation time is high (M. Psiaki and al. 2013).

A-F ANALYSIS (Haider and Khalid 2016)

Table 6, reprinted from (Haider and Khalid 2016), shows the criteria used to evaluate each technique to find the most effective GPS spoofing CM. Table 7, reprinted from (Haider and Khalid 2016), presents an analysis of A-F with respect to criteria set forth in Table 11.

From Table 7, it can be discerned that almost all the techniques can offer protection against a simplistic spoofing attack (Kuhn 2015; Jovanovic and Botteron 2014; Fan and al. 2015; Magiera and Katulski 2015; M. Psiaki and al. 2013). Only two techniques can offer protection against sophisticated types of attacks (Kuhn 2015; M. Psiaki and al. 2013). This represents a reasonable look at the state-of-the-art in GPS spoofing CMs in 2016.

Table 6. GPS spoofing effectiveness criteria.

Criteria	Definition	Possible Values
Quick Implementation	Ability to apply the technique quickly and as soon as possible	Yes / No
Cost effective	Cost should be low and affordable to apply the technique either in small scale or large number of production	Yes/ No
Prevent Simplistic Attack	Ability to detect simplistic attack	Yes/ No
Prevent Intermediate Attack	Ability to detect intermediate type of attack	Yes/ No
Prevent Sophisticated Attack	Ability to detect sophisticated and advanced types of attacks	Yes/ No
Requires Changes to satellite transmitters	Requires changes to satellite transmitters for implementation of technique	Yes/ No
Requires changes to receiver side	Requires changes to receiver for implementation of technique	Yes/ No
Validation	How easy to test	Yes/ No
Interoperability	Machine Independence	Yes/ No
Requires External Hardware	Does the technique require	Yes/ No

Table 7. Analysis of spoofing technologies with respect to effectiveness criteria.

S.No	Technique	Quick Implementation	Cost effective	Prevent Simplistic Attack	Prevent Intermediate Attack	Prevent Sophisticated Attack	Changes to satellite transmitters	changes to receiver side	Validation	Interoperability	Requires External Hardware
1	Multi-test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	No
2	An Asymmetric Security Mechanism for Navigation Signals	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No
3	A Cross-Layer Defense Mechanism against GPS Spoofing Attacks on PMUs in Smart Grid	Yes	Yes	Yes	Yes	No	No	No	Yes	No	Yes
4	Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing	No	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes
5	GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals	No	No	Yes	Yes	Yes	No	No	Yes	No	Yes

GPS SPOOFING RESEARCH: OUT OF THE BOX BRILLIANCE TO ECD DEFENSE

Three tracks of research are most relevant to ECD / CD**:** Maximum Likelihood Localization, Spoofing Mitigation algorithms, and Successive Signal Interference Cancellation (SIC). Note that historical spoofing research focusses primarily on detection on singular SPS source attacks. The focus on mitigation, correction, and recovery attending to multiple spoofing signals on multiple satellite attack surface is the hallmark of ECD.

Maximum Likelihood Localization

CD is a maximum likelihood GPS localization technique. It was proposed it 1996 but considered computational infeasible at that time. (Spilker 1996) CD was first implemented by Axelrod et al. in 2011 (Axelrod and al 2011). The search space contained millions or more location hypotheses. Improvements in the computational burden were found using various heuristics (Cheong and al. 2011; Jia 2016). A breakthrough came with the proposal of a branch-and-bound algorithm that finds the optimal solution within ten seconds running on a single CPU thread. (Bissag and M 2017)

Spoofing Mitigation

GPS spoofing defenses have been intensively studied. Most of the defenses focus on detecting spoofing attacks. There is a paucity of prior research for spoofing mitigation and recovering from successful attacks by finding and authenticating the correct signals (M. L. Psiaki and Humphreys 2016). In contrast to the vast research on GPS spoofing, there is a lack of commercial, civil receivers with anti-spoofing capabilities (Eichelberger 2019). ECD inherently mitigates spoofing attacks. The tide will turn.[xxv]

Spoofing hardware performing a sophisticated seamless satellite-lock takeover attack has been built (Humphreys and al. 2008). Challenges associated with spoofing are matching the spoofed and authentic signal's amplitudes at the receiver, which might not be in LOS and moving (Schmidt and al 2016).

It is practically feasible for a spoofer to erase the authentic signals at a 180-degree phase offset (M. L. Psiaki and Humphreys 2016). This is one of the strongest attacks that can only be detected with multiple receiver antennas or by a moving receiver (M. L. Psiaki and Humphreys 2016). For signal erasure to be feasible, the spoofer needs to know the receiver location more accurately than the GPS L1 wavelength, which is 19 cm. Receivers with only a single antenna cannot withstand such an erasure attack. ECD targets single-antenna receivers and does not deal with signal erasure (Eichelberger 2019). In all other types of spoofing attacks, including signal replay and multiple transmission antenna implementations, the original signals are still present and ECD remains robust (Eichelberger 2019). Detecting multi-antenna receivers and differentiating signal timing consistencies is covered in (Tippenhauer and etal 2011).

The GPS anti-spoofing work most relevant to ECD is based on joint processing of satellite signals and the maximum likelihood localization. One method is able to mitigate a limited number of spoofed signals by vector tracking of all satellite signals (Jafarnia-Jahromi and al. 2012). A similar technique is shown to be robust against jamming and signal replay (Ng and Gao 2016).

Successive Signal Interference Cancellation [xxvi]

ECD uses an iterative signal damping technique with spoofing signals similar to SIC. SIC removes the strongest received signals one by one in order to find the weaker signals and have been used with GPS signals before (Lopez-Risueno and Seco-Granados 2005; Madhani and al. 2003). That work is based on a classical receiver architecture which only keeps a signal's timing, amplitude, and phase. The ECD has its own snapshot receiver based on CD, which directly operates in the localization domain and does not identify individual signals in an intermediate stage. It is impossible to differentiate between authentic and spoofed signal, *a priori*, ECD does not remove signals from the sample data. Otherwise, the localization algorithm might lose the information from authentic signals. Instead, ECD dampens strong signals by 60% to reveal weaker signals. This can reveal localization solutions with lower CD likelihood. (Eichelberger 2019)

GPS Signal Jamming

The easiest way to prevent a receiver from finding a GPS location is jamming the GPS frequency band. GPS signals are weak and require sophisticated processing to be found. Satellite signal jamming considerably worsens the signal to noise ratio (SNR) of the satellite signal acquisition results. ECD algorithms achieve a better SNR than classical receivers and are able to tolerate more noise or stronger jamming (Eichelberger 2019).

A jammed receiver is less likely to detect spoofing since the original signals cannot be accurately determined. The receiver tries to acquire any satellite signals it can find. The attacker only needs to send a set of valid GPS satellite signals stronger than the noise floor, without any synchronization with the authentic signals [xxvii] (Eichelberger 2019).

There is a more powerful and subtle attack on top of the jammed signal. The spoofer can send a set of satellite signals with adjusted power levels and synchronized to the authentic signals to successfully spoof the receiver (Eichelberger 2019). So even if the receiver has countermeasures to differentiate the jamming, the spoofer signals will be accepted as authentic (R. Nichols and al. 2020).

Two Robust GPS Signal Spoofing Attacks and ECD

Two of the most powerful GPS signal spoofing attacks are: Seamless Satellite-Lock Takeover (SSLT) and Navigation Data Modification (NDM). How does ECD perform against these?

Seamless Satellite-Lock Takeover (SSLT)

The most powerful attack is a seamless satellite-lock takeover. In such attack, the original and counterfeit signals are nearly identical with respect to the satellite code, navigation data, code phase, transmission frequency, and received power. This requires the attacker to know the location of the spoofed device precisely, so that ToF and power losses over a distance can be factored in. After matching the spoofed signals with the authentic ones, the spoofer can send its own signals with a small power advantage to trick the receiver into tracking those instead of the authentic signals. A classical receiver without spoofing countermeasures, like tracking multiple peaks, is unable to mitigate or detect the SSLT attack, and there is no indication of interruption of the receiver's signal tracking. (Eichelberger 2019)

Navigation Data Modification (NDM)

An attacker basically has two attack vectors: modifying the signals code phase or altering the navigation data. The former changes the signal arrival time measurements. The latter affects the perceived satellite locations. Both influence the calculated receiver location. ECD works with snapshot GPS receivers and are not vulnerable to NDM changes as they fetch information from other sources like the Internet. ECD deals with modified, wireless GPS signals.

ECD ALGORITHM DESIGN

ECD is aimed at single-antenna receivers. Its spoofing mitigation algorithm object is to identify all likely localization solutions. It is based on CD because 1) CD has improved noise tolerance compared to classical receivers, 2) CD is suitable for snapshot receivers, 3) CD is not susceptible to navigation data modifications, and 4) CD computes a location likelihood distribution which can reveal all likely receiver locations including the actual location, independent of the number of spoofed and multipath signals. ECD avoids all the spoofing pitfalls and signal selection problems by joining and transforming all signals into a location likelihood distribution. Therefore, it defeats the top two GPS spoofing signal attacks (Eichelberger 2019).

Relating to the fourth point, spoofing and multi-path signals are actually similar from a receiver's perspective. Both result in several observed signals from the same satellite. The difference is that multipath signals have a delay dependent on the environment while spoofing signals can be crafted to yield consistent localization solution at the receiver. In order to detect spoofing and multipath signals, classical receivers can be modified to track an arbitrary number of signals per satellite, instead of only one (S.A.Shaukat and al. 2016). In such a receiver, the set of authentic signals – one signal from each satellite – would have to be correctly identified. Any selection of signals can be checked for consistency by verification that the resulting residual error of the localization algorithm is very small. This is a combinatorically difficult problem. For **n** satellites and **m** transmitted sets of spoofed signals, there are $\mathbf{(m+1)^n}$ **possibilities** for the receiver to select a set of signals. Only **m + 1** of those will result in a consistent localization solution, which represents the actual location and **m** spoofed locations. ECD avoids this signal selection problem by joining and transforming all signals into a location likelihood distribution (Eichelberger 2019).

ECD only shows consistent signals, since just a few signals overlapping (synced) for some location hypotheses do not accumulate a significant likelihood. All plausible receiver locations – given the observed signals - have a high likelihood. Finding these locations in four dimensions, space, and time, is computationally expensive (Bissig and Wattenhoffer 2017).

Branch and Bound

To reduce the computational load comparing to exhaustively enumerating all the location hypotheses in the search space, a fast CD leveraging branch and bound algorithm is employed. (Eichelberger 2019) describes the modifications to the B&B algorithm for ECD in copious detail in Chapter 6. Eichelberger also discusses acquisition, receiver implementation and experiments using the TEXBAT database. [xxviii] [xxix]

One of the key points under the receiver implementation concerns correlation of C/A codes. [xxx]

The highest correlation is theoretically achieved when the C/A code in the received signal is aligned with the reference C/A code. Due to the pseudo-random nature of the C/A codes, a shift

larger than one code chip from the correct location results in a low correlation value. Since one code chip has a duration of 1/1023 ms, the width of the peaks found in the acquisition vector is less than 2% of the total vector size. ECD reduces the maximum peak by 60% in each vector. A detection for partially overlapping peaks prevents changes to those peaks. Reducing the signal rather than eliminating it has little negative impact on the accuracy. Before using these vectors in the next iteration of the algorithm, the acquisition result vectors are normalized again. This reduces the search space based on the prior iteration (Eichelberger 2019).

ADS-B SECURITY

A subset problem, namely ADS-B systems on aircraft both manned and unmanned needs to be explored. ADS-B ubiquitously uses GPS location and signal receiver technologies. ADS-B has a very high dependency on communication and navigation (GNSS) systems. This is a fundamental cause of insecurity in the ADS-B system. It inherits the vulnerabilities of those systems and results in increased Risk and additional threats. (R.K. Nichols and a 2020; Randall K. Nichols et al. 2019)[xxxi] Another vulnerability of the ADS-B system is its broadcast nature without security measures. These can easily be exploited to cause other threats such as eavesdropping aircraft movement with the intention to harm, message deletion and modification. The systems dependency on the on-board transponder is also considered a major vulnerability, which is shared by the SSR. This vulnerability can be exploited by aircraft hijackers to make the aircraft movements invisible (Busyairah 2019).

ADS-B Standards

ICAO has stressed including provisions for the protection of critical information and communication technology systems against cyberattacks and interference as stated in the Aviation Security Manual Document 8973/8 (I.C.A.O. 2021). This was further emphasized in ATM Security Manual Document 9985 AN/492 to protect ATMs against cyberattacks (I.C.A.O. 2021).

ADS-B Security Requirements [xxxii]

Strohmeier, et al. (M. Strohmeier 2015) and Nichols, et al. (Randall K. Nichols et al. 2019) have both outlined a set of security requirements for piloted aircraft and unmanned aircraft, respectively. The combined security requirements for the ADS-B system in sync with the standard information security paradigm of CIA are as follows:

- Data integrity [xxxiii]
    - The system security should be able to ensure that ADS-B data received by the ground station or other aircraft (a/c) or UAS (if equipped) are the exact message transmitted by the a/c. It should also be able to detect any malicious modification to the data during the broadcast.
- Source integrity
    - The system security should be able to verify that the ADS-B message received is sent by the actual owner (correct a/c) of the message.
- Data origin (location / position fix) authentication
    - The system security should be able to verify that the positioning information in the ADS-B message received is the original position of the a/c at the time of transmission.

- Low impact on current operations
    - The system security hardware / software should be compatible with the current ADS-B installation and standards.
- Sufficiently quick and correct detection of incidents
- Secure against DOS attacks against computing power
- System security functions need to be scalable irrespective of traffic density.
- Robustness to packet loss

Vulnerabilities in ADS-B system

Vulnerability in this section refers to the Ryan Nichols (RN) equations for information Risk determination. A vulnerability is a weakness in the system that makes it susceptible to exploitation via a threat or various types of threats (Randall K. Nichols et al. 2019). ADS-B system is vulnerable to security threats.

Broadcast Nature of RF Communications

ADS-B principle of operation, system components, integration and operational environment are adequately discussed in Chapter 4 of (Busyairah 2019). The ADS-B system broadcasts ADS-B messages containing a/c state vector information and identity information via RF communication links such as 1090ES, UAT, or VDL Mode 4. The broadcast nature of the wireless networks without additional security measures is the main vulnerability in the system. (R.K. Nichols and Lekkas 2002) [xxxiv]

No Cryptographic Mechanisms

Neither ADS-B messages are encrypted by the sender at the point of origin, nor the transmission links. There are no authentication mechanisms based on robust cryptographic security protocols. The ICAO (Airport's authority of India 2014) has verified that there is no cryptographic mechanism implemented in the ADS-B protocol (ADDIN ZOTERO_ITEM CSL_CITATION {"ci.[xxxv]

ADS-B COTS

ADS-B receivers are available in COTS at affordable prices. The receiver can be used to track ADS-B capable a/c flying within a specific range of the receiver. The number of ADS-B tracking gadgets for all kinds of media is growing every year. They can be used to hack the systems on UAS (Randall K. Nichols et al. 2019).

Shared Data

As a results of COTS availability of ADS-B receivers, various parties, both private and public, are sharing real-time air traffic information on a/c on the internet. There are a number of websites on the internet that provide digitized live ADS-B traffic data to the public, e.g., flightradar24.com, radarvirtuel.com, and Flightaware. The available of the data and the capability to track individual a/c movements open the door to malicious parties to perform undesired acts that may have safety implications (Busyairah 2019).

ASTERIX Data Format

All-purpose Structured EUROCONTROL Surveillance Information eXchange (ASTERIX) is a binary format for information exchange in aviation (ADDIN ZOTERO_ITEM CSL_CITATION Surveillance Data Exchange - Part 1" 2016). ADS-B data is encoded into ASTERIX CAT 21 format and transmitted by ADS-B equipped a/c to ADS_B ground stations and decoded into usable form for ATC use. The ASTERIX format decoding guidance, source code and tools are widely available in the public domain.

Dependency On the On-Board Transponder

ADS-B encoding, and broadcast are performed by either the transponder (for 1090ES) or an emitter (for UAT/ VDL Mode 4) on board the a/c. Therefore, the ADS-B aircraft surveillance is dependent on the on-board equipment. There is a vulnerability (not cyber or spoofing) whereby the transponder or emitter can be turned off inside the cockpit. Obviously, the a/c becomes invisible and SSR and TCAS operation integrity is affected.

Complex System Architecture and Pass-through of GNSS Vulnerabilities

ADS-B is an integrated system, dependent on an on-board navigation system to obtain information about the state of the a/c as well as a communication data link to broadcast the information to ATC on the ground and other ADS-B equipped a/c. The system interacts with external elements such as human, (controllers and pilots) and environmental factors. The integrated nature of the system increases the systems vulnerability. The vulnerabilities of the GNSS on which the system relies to obtain a/c positioning information are inherited by the system. Vulnerabilities of the communications links are also inherited by the ADS-B system (Eichelberger 2019; *The Royal Academy of Engineering* 2011).

Threats in ADS-B system

Threats in this section refers to the Ryan Nichols (RN) equations for information risk determination. A threat is an action exploiting a vulnerability in the system to cause damage or harm specifically to a/c and generally to the Air Traffic Services (ATS), intentionally or unintentionally (Randall K. Nichols et al. 2019). The ADS-B system is vulnerable to security threats.

Eavesdropping

The broadcast nature of ADS-B RF communication links without additional security measures (cryptographic mechanisms) enables the act of eavesdropping into the transmission. While ADS-B information is meant to be shared with others top provide traffic information, eavesdropping can lead to serious threats such as targeting specific a/c movement information with intention to harm the a/c. This can be done with more sophisticated traffic and signal analysis using available sources such as Mode S and ASDS-B capable open-source GNU Radio modules or SDR. Eavesdropping is a violation of confidentiality and compromises system security (Busyairah 2019).

Data-Link Jamming

Data-link jamming is an act of deliberate/non-deliberate blocking, jamming, or causing interference in wireless communications (R.K. Nichols and Lekkas 2002). Deliberate jamming using a radio jammer device aims to disrupt information flow (message sending/receiving)

between users within a wireless network. Jammer devices can be easily obtained as COTS devices (M. Strohmeier 2015; R.K. Nichols and Lekkas 2002). Using the Ryan Nichols equations, the impact is severe in aviation due to the large coverage area (airspace) which is impossible to control. It involves safety critical data; hence the computed Risk / lethality level is high (R.K. Nichols and Lekkas 2002) (Busyairah 2019). The INFOSEC quality affected is availability because jamming stops the a/c or ground stations or multiple users within a specific area from communicating.

Jamming is performed on ADS-B frequencies, e.g., 1090MHz. Targeted jamming attack would disable ATS at any airport using ATCC. Jamming a moving a/c is difficult but feasible (M. Strohmeier 2015).

ADS-B system transmitting on 1090ES is prone to unintentional signal jamming due to the use of the same frequency (Mode S 1090 MHz) by many systems such as SSR, TCAS, MLAT and ADS-B, particularly in dense space (Busyairah 2019).[xxxvi] Not only is ADS-B prone to jamming, so is SSR (Adamy 2001, 2).[xxxvii]

Two Types of Jamming Threats for ADS-B

Apart from GNSS (positioning source for ADS-B) jamming, the main jamming threats for the ADS-B system include GS Flood Denial and A/C Flood Denial.

Ground Station Flood Denial (GSFD)

The GSFD blocks 1090 MHz transmissions at the ADS-B ground station. There is no difficulty in gaining close proximity to a ground station. Jamming can be performed using a low-power jamming device to block ADS-B signals from A/C to the ground station. The threat does not target individual a/c. It blocks ADS-B signals from all A/C within the range of the ground station.

Aircraft Flood Denial (A/C FD)

A/CFD blocks signal transmission to the a/c. This threat disables the reception of ADS-B IN messages, TCAS, and interrogation from WAM/MLAT and SSR. It is very difficult to gain close proximity to a moving A/C. The attacker needs to use a high-powered jamming device. According to (McCallie and a 2011) these devices are not easy to obtain.[xxxviii] It is true is the jamming function will be ineffective as soon as the a/c moves out of the specific range of the jamming device. Actually, better attempts can be made from within the a/c. [xxxix]

ADS-B SIGNAL SPOOFING

ADS-B signal spoofing attempts to deceive an ADS-B receiver by broadcasting fake ADS-B signals, structured to resemble a set of normal ADS-B signals or by re-broadcasting genuine signals captured elsewhere or at a different time. Spoofing an ADS-B system is also known as message injection because fake (ghost) a/c are introduced into the air traffic. The vulnerability of the system – having no authentication measures implemented at the systems data link layer – enables this threat. Spoofing is a hit on the security goal of Integrity. This leads to undesired operational decisions by controllers or surveillance operations in air or on ground. The threat affects both ADS-B IN and OUT systems (Busyairah 2019). Spoofing threats are of two basic varieties: Ground Station Target Ghost Injection / Flooding and Ground Station Target Ghost Injection / Flooding.

Ground Station Target Ghost Injection / Flooding

Ground Station Target Ghost Injection / Flooding is performed by injecting ADS-B signals from a single a/c or multiple fake (ghost) a/c into a ground station. This will cause single /multiple fake (ghost) a/c to appear on the controller's working position (radar screen). [xl]

Aircraft Target Ghost Injection / Flooding

Aircraft Target Ghost Injection / Flooding is performed by injecting ADS-B signals from a single a/c or multiple fake (ghost) a/c into an airplane in flight. This will cause ghost a/c to appear on the TCAS and CDTI screens in the cockpit to perform erratically. Making the situation even worse, the fake data will also be used by airborne operations such as ACAS, ATSAW, ITP and others for aiding a/c navigation operations. (Busyairah 2019)

ADS-B message deletion

An a/c can be made to look like it has vanished from the ADS-B based air traffic by deleting ADS-B message broadcast from the a/c. This can be done by two methods: destructive interference and constructive interference. Destructive interference is performed by transmitting an inverse of an actual ADS-B signal to an ADS-B receiver. Constructive interference is performed by transmitting a duplicate of the ADS-B signal and adding the two signal waves (original and duplicate). The two signal waves must be of the same frequency, phase and travelling in the same direction. Both approaches will be result in discarded by the ADS-B receiver as corrupt (Busyairah 2019).

ADS-B message modification

ADS-B message modification is feasible on the physical layer during transmission via datalinks using two methods: Signal Overshadowing and Bit-flipping. Signal overshadowing is done by sending a stronger signal to the ADS-B receiver, whereby only the stronger of the two colliding signals is received. This method will replace either the whole target message or part of it. Bit flipping is an algorithmic manipulation of bits. The attacker changes bits from 1 to 0 or vice versa. This will modify the ADS-B message and is a clear violation of the security goal of integrity (M. Strohmeier 2015). This attack will disrupt ATC operations or a/c navigation.

Circling back to ECD

Note that all of the ADS-B vulnerabilities and threats above are amenable to ECD mitigation if sufficient computing horsepower is available. For an a/c or ground station, this condition bodes well. For a UAS or sUAS, the ability for sufficient computational performance is limited.

INDOOR LOCALIZATION WITH AIRCRAFT SIGNALS USING ECD VS COMPETITIVE TECHNOLOGIES

GPS does not work well indoors due to the low signal strength. GPS satellite gets its energy from a dual solar array, which generates about 400-2900 W of power (depending on the satellite generation).[xli] With an altitude of about 12,427 miles, this relatively weak signal barely makes it to earth. (Accuracy 2021) The free space path loss is on the order of 180 dB (anonomous 2021) (Eichelberger and Tanner 2017).

Airplanes and other aircraft fly at an altitude below 8.5 miles. They also have ample power leaving for communications.[xlii] For safety reasons, airplanes and helicopters repeatedly transmit their location (like GPS satellites). These ADS-B signals are strong enough to be received indoors, even with cheap hardware. However, the question is if these ATC signals precise enough to not only

locate the aircraft but any mobile device. ATC signals have not been designed for indoor localization. Three challenges are present: (Eichelberger and Tanner 2017)

1) Aircraft do not fly in an orbit. Aircraft do not have accurate predetermined flight paths and unexpected changes to their route are always possible (i.e., holding pattern, weather, crowded airport).
2) Aircraft are not uniformly distributed in the sky. GPS satellites cover the sky in a regular pattern to maximize use position fixing (localization).
3) Aircraft position signals are not precise. An aircraft has an unpredictable delay between learning its position from the GPS satellites and retransmitting this position (LII. 2021). [xliii] Unlike GPS satellites with their atomic clocks, aircraft transmissions may not include complete time information; some aircraft do not even include precise position information.

There are key differences in "accuracy" and "precision" and "absolute" and "relative" accuracy when it comes to discussions of GNSS/ GPS position fixing, mapping, and surveying. Schaefer devotes Chapter 19 Accuracy and Precision of GNSS in the field, in his book, *GPS and GNSS Technology in Geosciences* (2021) (Schaefer and Pearson 2021) .

Eichelberger points out a few mitigating factors. Aircraft do not fly in orbits, but passengers and crew certainly do not appreciate abrupt flight path changes. Aircraft positions are not optimized for ground user-localization, but rather for air traffic safety. In urban areas there are more aircraft available than satellites. This increases the number of signals and reduces statistical uncertainty in position estimation from noisy measurements (item 3) (Eichelberger and Tanner 2017) . However, at night, frequency of received A/C signals is substantially lower than during the daytime.

Therefore, the question is if the mitigations above outweigh the communications issues using just aircraft signals to retransmit the GPS signals to ground stations and users. The answer is no as Eichelberger presents a indoor localization method using ECD. It requires only a network of receivers, [ground stations]; a receiver whose position should be determined [handset]; and a server which connects the handset. His entire approach, mathematics, field tests, and conclusions may be found in the publication by Eichelberger and Tanner (Eichelberger and Tanner 2017).

ECD vs minimum US government GPS standards

The GPS Performance Standard the US government currently lists a worse-case horizontal accuracy better than 17 meters (~55.8 ft) in 95% of all cases (U.S.G.P.O. 2020). Depending on the quality of the receiver and available correction methods, the horizontal can be substantially better, on the order of 3-7 meters (~9.8 - 23 ft).[xliv] Usually, indoor localization methods attempt to be more accurate, as for instance military targeting or user in large mall.

ECD cannot compete with other indoor localization methods. ECD prototype implementation has a median error of about 25 m (82 ft). On the plus side, ECD works very well for both outdoors and marginally for indoor localization. For purposes of this research, ECD does not report well for indoor localization operations. Rather than describe the indoor ECD implementation, prototype methods, simulations, and details results, the reader is guided to the primary paper for further discussion (Eichelberger 2019).

Related Work

Much research on indoor localization focuses on providing accurate position fixes (localization)--for instance room level or sub-meter accuracy. The cost factors are **ITE**:

1. **I**nstallation of dedicated infrastructure like beacons in each building or room (ex., hospital neo-natal or heart surgery recovery),
2. **T**raining or initialization phase to gather data, which is necessary for subsequent localization,
3. Usage of **E**xpensive user equipment (Eichelberger and Tanner 2017).

Most methods do not suffer all three drawbacks. However, lower cost is a trade-off for less accuracy. Liu et al. provide an overview of indoor localization methods. They differ by fundamental measurements, which are received signal strength (RSS), time of arrival (TOA), time difference of arrival (TDOA),[xlv] or angle of arrival (AOA). = (G. Li et al. 2007). Below are briefly listed the main ECD competitors with ITE drawbacks in brackets.

WiFi [T]

WiFi signals are popular for indoor localization because of the wide use of WiFi hotspots. No dedicated infrastructure like beacons are needed. WiFi based approaches generally have an accuracy of a few meters ("few" x 3.280 = ft). WiFi localization methods require a training phase in which positions or fingerprints of the access points are determined at different locations. Infrastructure changes have to be detected and database needs to be updated regularly (G. Li et al. 2007).

Ultrasound [I]

Ultrasound based methods require dedicated hardware. Cheap equipment with excellent results. Ultrasound systems have proven to be very accurate achieving centimeter-level accuracy. (1 cm= 0.393 in) The drawbacks are limited effective distance, prone to ambient noise (Oberholzer and etal 2011).

Light [T, E]

The most accurate results are achieved by laser- and camera – based methods. The best system in 2016 achieved an accuracy of 5 cm (1.968 in) using two lasers and multi high-end cameras. It costs a quarter million dollars. (Microsoft 2016) LEDS and miniaturization has opened up the visible light spectrum to communication and localization techniques. Pathak et al. give an extensive overview of current methods (Pathak and al 2015).

Bluetooth [T, I]

Bluetooth like WiFi uses 2.4 GHz frequency band. WiFi may take tens of seconds to identify base stations, faster response times can be achieved with Bluetooth (Mair 2012). Bluetooth pairing presents a delay before users can exchange information. Accuracy of Bluetooth methods approaches 3 m (9 ft).

RFID [I]

RFID systems are either active or passive. They have limited capacity, energy and require many units to communicate over short distances. Bouet and Dos Santos explore RFID localization systems (Bouet 2008) .

Sensor Fusion

Sensor assisted localization methods are favored in smartphone applications, because all these devices feature an inertial measurement unit (IMU) comprising an accelerometer, a gyroscope, and a compass (Ye and al 2012). Accuracy ranges are dependent on local conditions, tower availability, 4 or 5G / LTE available networks.

HAPS

Of special interest to this reviewer is the possibility of using High Altitude UAS Platforms for wireless communications (HAPS) to replace the aircraft in retransmitting GPS signals and acting as the primary agent for indoor and outdoor localization procedures. Two important references detail the advantages and disadvantages of HAPS for communication systems and localization use (Alejandro Aragon-Zavala 2008). Nichols, et. al provides an especially strong analysis of HAPS capabilities compared to terrestrial and satellite systems for telecommunications, HAPS platform advanced telecommunications services in various stages of engineering and development, HAPS link budgets, and characteristics of terrestrial, satellite and haps systems (Randall K. Nichols et al. 2019).

Security of GNSS (Shrivastava 2021) (Ochin and Lrmieszewski 2021)

In 2021, (Ochin and Lrmieszewski 2021) Ochin & Lemieszewski penned an excellent update to the spoofing threat covering air, land and sea operations in Europe and Asia. Some of the interesting topics covered were self-spoofing or limpet spoofing technologies; DIY GNSS spoofers; [xlvi] GNSS interference modalities; complementary countermeasures like INS; [xlvii] GNSS jamming techniques; GNSS meaconing; and detailed sections on cloud based GNSS positioning. Modern satellite navigation is based on the use of NO-Request range measurements between navigation satellite and the user. It means that the information about the satellites' coordinates given to the user is included into the navigation signal. The way of range measurement is based on the calculation of the receiving signal time delay compared with the signals generated by the user's equipment (Ochin and Lrmieszewski 2021)**.** Chapter 3 divides cloud based spoofing detection into four classes and proceeds to mathematically define the antenna distances and navigation modes based on those classes. All of these detection modes are based on a single antenna spoofer and do not consider mitigation and recovery steps. This is in comparison to ECD which does all three steps in the security solution.

Ochin & Lemieszewski (Ochin and Lrmieszewski 2021) present a fascinating picture of the history of anti-spoofing from 1942 patent to fight the American radio-controlled sea-based torpedoes with a radio jamming of German boats and submarines. (US Patent 1942) They continue with a European view of security measures for the six satellite constellations. They conclude with a Postscript on the drama behind the taking by Iran of the US RQ-170 Sentinel and how they did it! (Goward 2020) The Ochin & Lemieszewski chapter supports the risk opinions presented earlier. "The risk of losing GNSS signal (to spoofing) is growing every day. The accessories necessary for the manufacture of systems for GNSS "jamming" and / or "spoofing" are now widely available,

and this type of attack can be taken advantage of by not only the military but also by terrorists" (Ochin and Lrmieszewski 2021).

Acronyms [xlviii] Spoofing - A Cyber-weapon attack that generates false signals to replace valid ones. GPS Spoofing is an attack to provide false information to GPS receivers by broadcasting counterfeit signals similar to original GPS signal or by recording original GPS signal captured somewhere else in some other time and then retransmitting the signal. The Spoofing attack causes GPS receivers to provide the wrong information about position and time (Humphrees and e 2008; Tippenhauer and etal 2011).

Definitions [xlix]

Acquisition – Acquisition is the process in a GPS receiver that finds the visible satellite signals and detects the delays of the 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:

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

The two vectors are most similar at the 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 (FFT) in Ó (N log N) time. [l] (Eichelberger 2019)

Coarse-Time Navigation (CTN) is a snapshot receiver localization technique measuring sub-millisecond satellite ranges from correlation peaks, like classical GPS receivers. (IS-GPS-200G, 2013) [See also expanded definition.]

Collective Detection (CD) is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite, but rather combine all the available information and decide 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 – A coordinate system uses an ordered list of coordinates, to uniquely describe the location of points in space. The meaning of the coordinates is defined with respect to some anchor points. The point with all coordinates being zero is called the origin. [Examples: terrestrial, Earth-centered, Earth - fixed, poles, ellipsoid, equator, meridian longitude, latitude, geodetic latitude, geocentric latitude, and geoid. [li]

Localization – Process of determining an object's place with respect to 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 accuracy and validity of the data. (I.S.-G.P.S.-200G 2013) [lii]

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. (I.S.-G.P.S.-200G 2013)

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

CYBER RISK ASSESSMENT - RYAN - NICHOLS EQUATIONS

Standards

Some globally renowned risk frameworks and standards include OCTAVE (Carnegie Mellon), NIST Risk Management Framework (800-53, 800-60,800-37), AS/NZS 4360, ISO 31000:2009 Risk Management Standard, COSO ERM, RiskIT, and Safety Management System (SMS) Air Traffic Organization (ATO) SMS Manual and Safety Risk Management Guidance for System Acquisitions (SRMGSA) along with internal risk assessment measures. (Morana, 2015) Although well-known throughout the globe, many of these frameworks lack the technical specificity to provide an actionable implementation of effective countermeasures or controls during the remediation phase of the risk management process.

Cybersecurity

Cybersecurity generally refers to the ability to control access to computer-networked systems and their information. Cyber information may be stored or in transit between systems. Where Cyber security controls (countermeasures) are effective, cyberspace is a reliable, trustworthy, and resilient digital infrastructure. Where cyber security controls are absent, compromised, incomplete, ineffective, delayed, or poorly designed, cyberspace is the treasure of hackers, crackers, terrorists, spies, and thieves. Whether a system is a physical facility or a collection of cyberspace components, the role of the Cybersecurity professional is to plan for a potential attack, identify threats, prepare for consequences, calculate Impact, and identify/deploy appropriate countermeasures (controls). (Nichols R. K.-P., 2019)

Role of UAS/ UAVs

UAS/UAVs are advanced technology, unmanned vehicles deployed within cyberspace for global multiple hybrid missions: intelligence, military, and commercial. They come in all sizes, deploy in four different FAA levels of airspace, and carry a wide variety of special equipment instrumentation controlled by SCADA systems. They are essential assets of National Critical Infrastructure. They use computer networking for critical control systems, communications, navigation, payload delivery, and intelligence coordination from various land, sea, air, and satellite platforms. The larger threat is that a terrorist organization will interfere or take command of the SCADA or information control systems in a UAS and *turn* the payload or down the aircraft. [The T.V. series "24" actually happened in real life - Iran seized control of an RQ-170 UAV drone in December 2011. It bragged that it had done so by cyber warfare and reengineered the critical intelligence components.] (Nichols R. K.-P., 2019)

Cyber Attack Taxonomy

Chapter 3: *Understanding Hostile Use and Cyber-Vulnerabilities of UAS: Components, Autonomy v Automation, Sensors, SAA, SCADA, and Cyber Attack Taxonomy* in (Nichols R. K.-P., 2019) provides the most detailed and extensive look at the Cyber Theater of Operations and the relationship to Unmanned Aircraft Systems. The taxonomy has been updated and extended further to include IoT and artificial intelligence in (R. K. Barnhart, 2021) Chapter 18: *Cybersecurity Counter Unmanned Aircraft Systems and Artificial Intelligence.*

Traditional risk assessment efforts within a risk management practice are inherently *qualitative.* This is opposed to *quantitative* risk analysis, which concentrates on probability and business impact values and financial losses. Traditional risk formula encompasses the following variables for Risk: Impact (or consequence), Threat (or attack), and Vulnerability. (Morana, 2015)

Unmitigated Risk can be thought of as the intersection of three vector sets:

1) Attack complexity which includes the ease of vulnerability exploitation and probability of attacker successfully executing,
2) Consequence which is Impact if the information (cyber) asset is compromised and the probability of various impact scenarios, and
3) Ease of Exploitation is the ability to exploit vulnerability(ies) and the probability of successful exploitation.

Ryan - Nichols Information Risk Assessment Framework (RN) and Equations

The Ryan - Nichols Risk Assessment Framework (RN) was initially developed as an application threat model in 2000 (Nichols & Ryan, 2000). It is based on the scholastic works of Dr. Julie JCH Ryan and Dr. Dan J. Ryan (Ryan J. J., 2006), (Ryan & Ryan, Proportional Hazards in Information Security, 2005) and (Ryan J. J., An Exploration of Information Security Aspects in the Thirty Elements of Systems Engineering, 1998). The RN framework was designed to assist the DoD, DHS, and DTRA plus commercial organizations to

1) Identify unique threat scenarios,
2) Incorporate business objectives,
3) Improve on probability calculations and predictions by establishing probability ranges,
4) Performing attack exploits to simulate real-life risk scenarios,
5) Incorporate countermeasures and mitigation steps to reduce the overall Risk by reducing threats to the system. (Nichols R. K.-P., 2019) (Nichols R. K., 2020) (Morana, 2015)

This last element was the key to adopting this framework to other fields – specifically Counter-Terrorism, UAS, and UUV. See: (Nichols & Sincavage, Disruptive Technologies with Applications in Airline, Marine, and Defense Industries, 2021), (Nichols & al., Unmanned Vehicle Systems and Operations on Air, Sea, and Land, 2020) and (Nichols R. K.-P., 2019)

A *qualitative* view of information risk (also a measure of cyber-attack lethality) in a system such as ADS-B, SAA, or any computer networked communications affecting navigation, control, or signals may be expressed as (Nichols & Ryan, 2000)

RISK = THREATS X VULNERABILITIES X IMPACT / COUNTERMEASURES

Where: THREATs are real, act on a system, and represent the possibility that the attack vectors become accessible for exploitation. (The attacker has the necessary time and resources to conduct the exploit.) VULNERABILITIES are inherent weaknesses in the information system and represent the vulnerabilities becoming successfully exploited. IMPACT is the business value of a successful exploit. COUNTERMEASURES represent the technical mitigations/solutions or probability that a particular mix of counter-technologies will reduce the active THREATS on a system. The above equation is used to calculate the Initial Risk Assessment (IRA) before any perturbation by Threats.

At time state = 0, we note that Vulnerabilities are constant and always present, and Impact is just a "delta number" and a constant. Threats and Countermeasures are independent variables; Risk is the dependent variable. Using calculus, both Vulnerabilities and Impact drop out of the IRA equation to give a compressed form:

RISK = THREATS / COUNTERMEASURES

This well-designed equation is used to calculate the absolute value (plus or minus) changes away from the IRA and to account for differences (or levels of Risk) based on the scenario. If the IRA is the Normal case (or Base case), then the compressed RN equation helps calculate the Worst- and Best-Case Scenarios. A detailed discussion of the variables, constants, probabilities, use, and procedures for the RN model is found in Chapter 2: *Wireless Information Warfare* (R.K. Nichols & Lekkas, 2002). The RN framework uses a Legend to classify changes in levels of Risk. An example of a team-defined Lethality Matrix is shown in the figure below. Risk probabilities are always positive, and changes can be visualized linearly. See a partial example from a recent assessment of a potential terrorist incident involving UAS assets against an Air Defense System (ADS).

Figures 15-17 show only a small part of the detailed analysis that the Ryan Nichols Risk Assessment Framework requires. RN equations have been used effectively to assess risk changes and required mitigation funding for Nuclear war calculations, Suicide Bombers, Piracy, Kidnapping, attacks on National Critical Infrastructure Systems, ADS, malware analysis / affects, INFOSEC, network security, Unmanned Aircraft Systems and Unmanned Underwater Systems (robots), signals spoofing, communications networks, ADS-B and GNSS navigation data systems. (R.K. Nichols, 2020) The most recent example of the RN approach used is determining the intelligence Threats due to satellite imagery being spoofed by "deep fakes."

RN Equation Legend: Team Defined Risk Analysis Probabilities

Qualitative Measure	Quantitative Value
High	>75%
Medium - High	61-75%
Medium	31-60%
Low	16-30%
Very Low	1-15%

Fig. 13. RN equation risk analysis probabilities. (Redetzke, 2021)

DEFENSE BOOST - RISK PROBABILITY

Threat	Vulnerability	Impact	Countermeasure	Risk
RDD Swarm Attack	Iron Dome Saturation	Mass panic and fear – Economic and Food	Iron Dome, Response Plan, Diplomacy, EMP, Pre-emptive, Swarm, Comms	
15% - Low to Medium	20% - Low to Medium	75% Medium to High	85% High	.03 Very Low

Overall Risk with Defense Boost 3% Very Low

Fig. 14 Defense boost risk probabilities. (Redetzke, 2021)

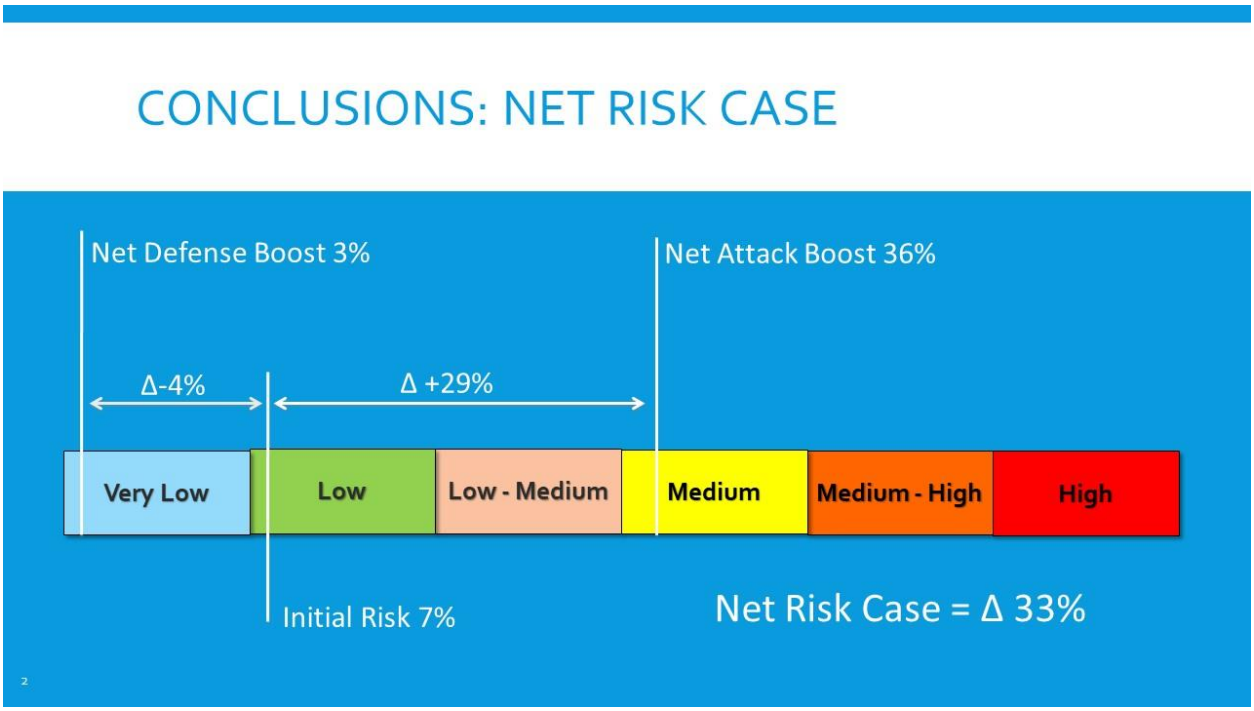

Fig. 15 Final net risk case. (Redetzke, 2021)

VI. Standards Bodies Literature Review

Below is a list and synopsis of updates from several external organizations and working groups that were deemed important and pertinent by the FAA. Weight was placed on staying up to date with RTCA SC-228. Significant work was done regarding reviewing all SC-228 meeting minutes, phases of work, and all released and published documents for information applicable to this project. All other organizations, sub committees, and working groups have been investigated for applicability of previous, current, and upcoming work and deliverables. Some of the areas reviewed are not directly associated with ADS-B and GPS, but are related and assessed on the potential impact on these systems. Throughout the period of performance of the project, the researchers will continue to stay up to date with all organizations to inform the project.

RTCA SC-228 Detect and Avoid standards

- SC-228 of RTCA is meant to work closely with the UAS community to develop the Minimum operational Performance Standards (MOPS) for DAA equipment and the Performance Standards for the C2 Data Link.
- SC-228 deliverables include several performance standards documents which have been reviewed in their entirety for applicability to this effort. All documents have a disclaimer mentioning applicability only to Part 91 aircraft and operations and not Part 107 sUAS. Only DO-365 and DO-381 specifically mentioned ADS-B and GPS.
    - DO-362A – Command and Control Data Link Minimum Operational Perf. Standards (MOPS)
        - The main focus of this MOPS is the technical standards describing how CNPC Data Link Systems can compatibly share the spectrum that has been allocated for their use, yet remain waveform agnostic (i.e., unspecified). There are no interoperability requirements, as these are internal UAS interfaces. Rather, this MOPS provides required electromagnetic compatibility that permits simultaneous operation of federated designs in common spectrum.
    - DO-365A – MOPS for DAA Systems
        - The DAA system for UAS flight was developed to assist the PIC with his/her duties of operating an aircraft safely in the NAS.
        - All aircraft flying in the NAS must comply with the operating rules of Title 14 of the Code of Federal Regulations (14 CFR). Specifically, Part 91, .3, .111, .113(b), .115, .123 and .181(b), which address see and avoid, collision avoidance, and right-of-way rules. These operating regulations assumed that a pilot would be onboard the aircraft, so he/she would be able to exercise his/her authority to fully comply with these rules.
        - This document contains Phase 1 MOPS for DAA systems used in aircraft transitioning to and from Class A or special use airspace (higher than 500’ AGL), traversing Class D, E, and G airspace in the NAS. It does not apply to small UAS operating in low-level environments (below 500’) or other segmented areas. Likewise, it does not apply to operations in the Visual Flight Rules (VFR) traffic pattern of an airport.
        - Applicability:
            - DO-365 talks through ideal and safe performance standards that OEMs should meet for the safest and most efficient operations and

walks through several con-ops that could apply to GPS/ADS-B DAA

- DO-366A – MOPS for Air-to-Air Radar for Traffic Surveillance
  - This document contains the first update to the MOPS for the air-to-air radar for traffic surveillance.
  - The intended application is supporting DAA operations including collision avoidance to detect intruders below 10,000' Mean Sea Level (MSL). These standards specify the radar system characteristics that should be useful for designers, manufacturers, installers and users of the equipment.
- DO-377 – Minimum Aviation Safety Performance Standards (MASPS) for C2 link systems supporting operations of unmanned aircraft systems in US Airspace
  - This document contains the MASPS for a C2 Link System connecting a Control Station (CS) and an UAS.
  - It covers UA operations requiring a C2 Link System that allows the UA to operate within line of sight and beyond the line-of-sight of a CS. This MASPS contains the standards which specify system characteristics, i.e., it is design independent, that should be useful to UAS operators, 701 OEM, and equipment manufacturers1 plus the FAA, as UAS operate within the U.S. airspace.
- DO-381 – MOPS for Ground Based Surveillance System (GBSS) for Traffic Surveillance
  - This document contains MOPS for GBSS used for air traffic surveillance in support of DAA operations for unmanned aircraft. The primary applications will be used in terminal, transit, or extended operational areas in the NAS as defined in RTCA Document 365A (DO 365A), Minimum Operational Performance Standards for Detect and Avoid Systems.
  - These standards specify the GBSS characteristics that should be useful for designers, manufacturers, installers and users of the equipment. Note that in this context, surveillance "systems" includes one or more networked non-cooperative sensors (e.g., radar and lidar), Electro-Optical/Infrared (EO/IR), etc.) needed to meet these MOPS.
  - Applicability:
    - DO-381 addresses several performance standards including but not limited to false track, latency, range, weather and environmental impacts and effect. It should be further investigated for exact applicability to A44.

RTCA SC-147 Traffic Alert and Collision Avoidance System

- SC-147, since it was established in 1980, has produced and maintained MOPS for Collision Avoidance Systems (CAS) and surveillance techniques required to meet desired levels of performance and safety.
- Since 2013, SC-147 has worked with EUROCAE WG75 to develop a new generation of collision avoidance systems called ACAS X
- Recently, SC-147 has also worked closely with SC-228 on standards to ensure interoperability between all existing and future CAS and DAA systems (DO-382) and

variants of ACAS X for UAS and Vertical Take-off and Landing (VTOL) aircraft that are compliant and integrated with DAA standards published in versions of DO-365

- In December 2020, SC-147 published the ACAS Xu MOPS (DO-386) which is a DAA/CA system for fully equipped (Transponder and ADS-B Out) aircraft flying in controlled airspace and receiving ATC services.
    - DO-386 – This defines the minimum operational performance standards (Vol I) and Algorithm Design Descriptions (Vol II) for the Airborne Collision Avoidance System Xu (ACAS Xu) equipment, designed for platforms with a wide range of surveillance technologies and performance characteristics such as UAS.

RTCA SC-186 Automatic Dependent Surveillance Broadcast (ADS-B)

- The purpose of SC-186 is to codify requirements based upon the airborne and ground user needs for an ADS-B system.
- MOPS published by SC-186 are intended to be used by the FAA and other civil aviation authorities (CAA's) as an acceptable means of certifying ADS-B equipment for civil aircraft.
- Deliverables are intended to result in revised Technical Standard Orders for manufacturers of ADS-B equipment.
- In 2009, SC-186 published DO-282B – MOPS for Universal Access Transceiver (UAT) ADS-B. This document is scheduled to be updated and delivered by March 2022 as DO-282C. This will ultimately mean a higher degree of applicability to the A44 project.

Effort is also being made to become up to speed with ASTM F38 and the following standards:

ASTM F38 WK16285 New Spec for Design and Performance of UAS Class 1320
ASTM F38 WK27055 New Practice for UAS Remote ID
ASTM F38 WK53964 Design, Construct, and Test of VTOL
ASTM F38 WK62670 New Standard Large UAS Design and Construction
ASTM F38 WK62668 Detect and Avoid Performance Requirements
ASTM F38 WK62669 Detect and Avoid Test Methods
ASTM F38 WK28019 New Practice for selecting sUAS Launch and Recovery
ASTM F38 WK59317 Vertiport Design
ASTM F38 WK63418 Service Provided under UAS Traffic Management (UTM)
ASTM F38 WK62344 BVLOS Package Delivery sUAS Operations
ASTM F38 WK11425 New Practice for Private UAS Pilot Practical Test Standards for UAS
ASTM F38 WK62730 UAS Operator Audit Programs
ASTM F38 WK62733 Training and Development of Training Manuals for UAS Operator
ASTM F38 WK63407 Required Product Information to be provided with an sUAS
ASTM F38 WK69690 Surveillance UTM Supplemental Data Service Provider (SDSP)

VII. Summary and Conclusions

This Literature Review Report fulfills Task 1 for the A44 ASSURE project. It provides a literature review and meta-analysis that identified the potential safety and security risks of relying on GPS and ADS-B data used for UAS operations. It is divided into three areas of investigation, signal dropouts and erroneous data, jamming, and spoofing that may result in safety or security risks to UAS operations that rely on GPS and ADS-B data. Based on the information gathered, a safety and security risk assessments of potential UAS operations that rely on GPS and ADS-B data is presented.

A summary of the risk assessments is provided using the Safety Management System (SMS) Air Traffic Organization (ATO) SMS Manual and Safety Risk Management Guidance for System Acquisitions (SRMGSA). This manual provides guidelines to assess the severity and likelihood of identified risks. The risk assessment is broken into four classifications: Part 107 Operations, Beyond Visual Line Of Sight (BVLOS), Urban Areas, and Near Airports. For each category, the severity and likelihood probability, associated references, and mitigation schemes associated with the increasing risk profile is presented. Part 107 Operations specifies a near pristine risk level, or the best-case scenario and will serve as the base reference for the increasing risks in the other environments. BVLOS is the next category as it is a crucial for many UAS operations and is of great importance to the UAS community. Urban area operations represent a unique case due to signal interruptions and other artifacts along with the density of humans and infrastructure. Near airports operations represents another unique situation due to the air traffic density and potential impacts to commercial airline traffic.

From this analysis it is evident that the only low risk situations occur with operations in the Part 107 conditions. This was expected due to the nature of Part 107 and the current operability allowed by the FAA. In the medium risk category, most of the operating environments are in the BVLOS operations. This is also expected since both cases can be allowed by using a FAA waiver process to allow operations in these areas. The waiver and potentially other situations may be mitigated using additional processes, procedures, and technology to reduce the risk to a lower acceptable level. The high risk category contains mainly urban and near airport operations. These areas result in high risk operations and significant mitigation schemes are needed to reduce the risk to an acceptable level.

BVLOS operations are of special interest as these are in great demand from operators and industry. Mitigating BVLOS operations flying at low altitudes and conducting long linear infrastructure inspection, agriculture operations, package delivery, or aerial surveillance are focus areas. As mitigation strategies are found and evaluated the impact of them as well as the costs associated will be assessed. There is a desire to minimize cost and weight while still providing a high level of safety. These operations do have significant potential for adverse outcomes, however several mitigation techniques show promise as tools to be used in conjunction with regulatory requirements.

Based on the risk assessment in Task 1, a market survey of market solutions to mitigate loss of GPS and loss of ADS-B data will be conducted as part of Task 2. The work will focus on reducing those medium risk operations to an acceptable level. However, these and other mitigations found may also offer solutions to the high risk operations. The commercial market solutions to mitigate unvalidated GPS and unvalidated ADS-B In data and will include estimated costs, ease of

implementation, and a preliminary assessment of the effectiveness of market solutions to mitigate the various risks identified in Task 1. An assessment of whether there are other potential methods, operational mitigations, strategic mitigations, or other means for addressing potential safety and security risks will be completed. GPS mitigation strategies for denied and/or jammed environments will be explored and potential solution proposed. Cybersecurity and counterintelligence measures will also be explored to decrease the risk of disruption or takeover. Examination of recorded ABS-B data will be conducted to expose potential risks and provide guidance on mitigation schemes will also be included.

VIII. References

"49 CFR Part 1542 -- Airport Security." n.d. Accessed September 25, 2021. https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-C/part-1542.

Abbaspour, Alireza, Kang K. Yen, Shirin Noei, and Arman Sargolzaei. 2016. "Detection of Fault Data Injection Attack on Uav Using Adaptive Neural Network." Procedia Computer Science 95: 193–200.

Abbaspour, Alireza, Michael Sanchez, Arman Sargolzaei, Kang K. Yen, and Nalat Sornkhampan. 2017. "Adaptive Neural Network Based Fault Detection Design for Unmanned Quadrotor under Faults and Cyber Attacks." In ICSEng, 77–84.

Accuracy, G.G.-G. 2021. "Official U.S. Government Information about the Global Positioning System (GPS) and Related Topics." https://www.gps.gov/:

Adamy, D. 2001. EW 101: A First Course in Electronic Warfare. Boston: Artech House.

Aghadadashfam, M., Mosavi, M.R., Rezaei, M.J., 2020. A new post-correlation anti-jamming technique for GPS receivers 24, 89. https://doi.org/10.1007/s10291-020-01004-y

"Airports Authority of India." 2014. In ICAO. Hong Kong. China: ICAO.

Alejandro Aragon-Zavala, J.L.-R.-P. 2008. High-Altitude Platforms for Wireless Communications. Chichester, West Sussex, UK: John Wiley & Sons.

Alexeev, I. I., V. V. Kalegaev, E. S. Belenkaya, S. Y. Bobrovnikov, Ya I. Feldstein, and L. I. Gromova. 2001. "Dynamic Model of the Magnetosphere: Case Study for January 9-12, 1997." Journal of Geophysical Research: Space Physics 106 (A11): 25683–93. https://doi.org/10.1029/2001ja900057.

Alexeev, Igor I., Elena S. Belenkaya, Sergey Yu Bobrovnikov, and Vladimir V. Kalegaev. 2003. "Modelling of the Electromagnetic Field in the Interplanetary Space and in the Earth's Magnetosphere." Space Science Reviews 107 (1–2): 7–26. https://doi.org/10.1023/A:1025542915800.

Ali, Busyairah Syd, Washington Ochieng, Arnab Majumdar, Wolfgang Schuster, and Thiam Kian Chiew. 2014. "ADS-B System Failure Modes and Models." The Journal of Navigation 67 (6): 995–1017.

Ali, Busyairah Syd, Washington Yotto Ochieng, and Rozaimah Zainudin. 2017. "An Analysis and Model for Automatic Dependent Surveillance Broadcast (ADS-B) Continuity." GPS Solutions 21 (4): 1841–54. https://doi.org/10.1007/s10291-017-0657-y.

Ali, Busyairah Syd, Washington Yotto Ochieng, Wolfgang Schuster, Arnab Majumdar, and Thiam Kian Chiew. 2015. "A Safety Assessment Framework for the Automatic Dependent Surveillance Broadcast (ADS-B) System." Safety Science 78 (October): 91–100. https://doi.org/10.1016/j.ssci.2015.04.011.

Ali, e a. 2014. "ADS-B system failure modes and models." The Journal of Navigation 67: 995–1017.

Andert, Franz, Nikolaus Ammann, Jan Puschel, and Jorg Dittrich. 2014. “On the Safe Navigation Problem for Unmanned Aircraft: Visual Odometry and Alignment Optimizations for UAV Positioning.” 2014 International Conference on Unmanned Aircraft Systems, ICUAS 2014 - Conference Proceedings, 734–43. https://doi.org/10.1109/ICUAS.2014.6842318.

anonomous. 2021. “GPS Newsgroup.” http://gpsinformation.net/main/gpspower.htm:

Anonymous. 2014. “Timing & Synchronization for LTE-TDD & LTE-Advanced Mobile Networks.” Technical Report,. Microsemi. https://www.microsemi.com/document-portal/doc_download/133615-timing-sync-for-lte-tdd-lte-a-mobile-networks.

Arteaga, Ricardo A., Kraettli Epperson, Mohammed Dandachy, Arun Aruljothi, Hong Truong, and Mihir Vedantam. 2018. “MADS-B Detect and Avoid Flight Tests on Phantom 4 Unmanned Aircraft System.” In 2018 AIAA Information Systems-AIAA Infotech@ Aerospace, 2014.

Axelrod, P., and e al. 2011. “Collective Detection and Direct Positioning Using Multiple GNSS Satellites.” Navigation, Pp 58 (4): 305–21.

Balamurugan, G., J. Valarmathi, and V. P.S. Naidu. 2017. “Survey on UAV Navigation in GPS Denied Environments.” International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES 2016 - Proceedings, 198–204. https://doi.org/10.1109/SCOPES.2016.7955787.

Barnhart, RK, DM Marshall, and E Shappee. 2021. Introduction to Unmanned Aircraft Systems. https://books.google.com/books?hl=en&lr=&id=N_AeEAAAQBAJ&oi=fnd&pg=PT5&dq=Introduction+to+Unmanned+Systems+barnhart&ots=LqBIQ3P7tB&sig=wvFhmAmRu4cj-SCc4jaWZrrXEEo.

“Beamforming: a versatile approach to spatial filtering.” 1988. IEEE ASSP Magazine ID: 22880273. https://doi.org/10.1109/53.665Corpus.

Bendea, H, P Boccardo, S Dequal, F Giulio Tonolo, D Marenchino, and M Piras. 2008. “Low Cost UAV for Post-Disaster Assessment.” Proceedings of The XXI Congress of the International Society for Photogrammetry and Remote Sensing Beijing China 311 July 2008 XXXVII: 1373–80.

Bi, Yingcai, Menglu Lan, Jiaxin Li, Shupeng Lai, and Ben M. Chen. 2019. “A Lightweight Autonomous MAV for Indoor Search and Rescue.” Asian Journal of Control 21 (4): 1732–44. https://doi.org/10.1002/asjc.2162.

Bidikar, Bharati, Gottapu Sasibhushana Rao, Laveti Ganesh, and MNVS Santosh Kumar. 2014. “Satellite Clock Error and Orbital Solution Error Estimation for Precise Navigation Applications.” Positioning 2014.

Bissag, P., and E. M. 2017. “Fast and Robust GPS Fix Using One Millisecond of Data.” In Proc of the 16th ACM /IEEE International Conference on Information Processing in IPSN, 223–34.

Bissig, P., and M.E. Wattenhoffer. 2017. “Fast & Robust GPS Fix Using 1 Millisecond of Data.” In 16 ACM / IEEE Int Conf on Information Processing in Sensor Networks, 223–34. Pittsburg, PA: IPSN.

Bouet, M. 2008. “RFID Tags: Position Principles and localization techniques.” In IEEE 1st IFIP Wireless Days, 1–5.

Bougard, B. et al., CIGALA: Challenging the Solar Maximum in Brazil with PolaRxS, Proc. ION GNSS Conference, Portland, Sept. 2011

Burgess, M. 2017. “When a Tanker Vanishes, All Evidence Points to Russia.” https://www.wired.co.uk/:

Busyairah, S.A. 2019. Aircraft Surveillance Systems: Radar Limitations and the Advent of the Automatic Dependent Surveillance Broadcast. New York: Routledge.

Cai, Guowei, Jorge Dias, and Lakmal Seneviratne. 2014. “A Survey of Small-Scale Unmanned Aerial Vehicles: Recent Advances and Future Development Trends.” Unmanned Systems 2 (2): 175–99. https://doi.org/10.1142/S2301385014300017.

Canciani, Aaron, and John Raquet. 2017. “Airborne Magnetic Anomaly Navigation.” IEEE Transactions on Aerospace and Electronic Systems 53 (1): 67–80. https://doi.org/10.1109/TAES.2017.2649238.

Capozza, P.T., Holland, B.J., Hopkinson, T.M., Li, C., Moulin, D., Pacheco, P., Rifkin, R., 1999. Measured Effects of a Narrowband Interference Suppressor on GPS Receivers, in: Proceedings of the 55th Annual Meeting of The Institute of Navigation. Cambridge, MA, pp. 645–651.

Carrio, Adrian, Yucong Lin, Srikanth Saripalli, and Pascual Campoy. 2017. “Obstacle Detection System for Small UAVs Using ADS-B and Thermal Imaging.” Journal of Intelligent and Robotic Systems: Theory and Applications 88 (2–4): 583–95. https://doi.org/10.1007/s10846-017-0529-2.

Causa, Flavia, Giancarmine Fasano, and Michele Grassi. 2018. “Multi-UAV Path Planning for Autonomous Missions in Mixed GNSS Coverage Scenarios.” Sensors (Switzerland) 18 (12). https://doi.org/10.3390/s18124188.

Centre for Unmanned Aircraft Systems in Public Safety. 2021. “What Is UAS?”

Chao, Haiyang, Yu Gu, and Marcello Napolitano. 2013. “A Survey of Optical Flow Techniques for UAV Navigation Applications.” In 2013 International Conference on Unmanned Aircraft Systems, ICUAS 2013 - Conference Proceedings, 710–16. https://doi.org/10.1109/ICUAS.2013.6564752.

Chen, Y., Zheng, H., Wang, Y., 2011. Adaptive bandwidth PLL design based on fuzzy logic control, in: 2011 4th IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, MAPE 2011. IEEE, Beijing, China, pp. 645–648. https://doi.org/10.1109/MAPE.2011.6156324.

Cheong, J., and e al. 2011. “Efficient Implementation of Collective Dection.” In IGNSS Symposium, 15–17.

Closas, P., and e al. 2007. “Maximum Likelyhood Estimation of Position in GNSS.” IEEE Signal Processing Letters (Pp 14 (5): 359–62.

Comberiate, Joe, Michael Kelly, Lars Dyrud, and Gregory Weaver. 2012. “Space Weather Effects on GPS Systems.”

Conker, R. S., El-Arini M. B., Hegarty, C. J., and Hsiao, T., “Modeling the Effects of Ionospheric Scintillation on GPS/satellite-based Augmentation System Availability,” Radio Science, Vol. 38, No. 1, 2003, p. 1001.

Cortés, I., Merwe, J.R. van der, Nurmi, J., Rügamer, A., Felber, W., 2021. Evaluation of Adaptive Loop-Bandwidth Tracking Techniques in GNSS Receivers. Sensors (Basel). 21, 1–40. https://doi.org/10.3390/S21020502

Costin, Andrei, and Aurélien Francillon. 2014. “Ghost in the Air(Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices.” In Network and Security DepartmentEURECOM.

Couturier, Andy, and Moulay A. Akhloufi. 2019. “UAV Navigation in GPS-Denied Environment Using Particle Filtered RVL.” In Situation Awareness in Degraded Environments 2019, 11019:110190N. International Society for Optics and Photonics.

Couturier, Andy, and Moulay Akhloufi. 2020. “Conditional Probabilistic Relative Visual Localization for Unmanned Aerial Vehicles.” Canadian Conference on Electrical and Computer Engineering 2020-Augus. https://doi.org/10.1109/CCECE47787.2020.9255691.

Cuenca, Andrei, and Hever Moncayo. 2021. “A Geomagnetic-Based Integrated Architecture for Dead-Reckoning Navigation.” AIAA Scitech 2021 Forum 1 PartF (January): 1–14. https://doi.org/10.2514/6.2021-1227.

Cui, Jin Q., Shupeng Lai, Xiangxu Dong, and Ben M. Chen. 2016. “Autonomous Navigation of UAV in Foliage Environment.” Journal of Intelligent & Robotic Systems 84 (1): 259–76.

Cuntz, Manuel, Andriy Konovaltsev, Achim Dreher, and Michael Meurer. 2012. “Jamming and Spoofing in GPS/GNSS Based Applications and Services - Threats and Countermeasures.” Communications in Computer and Information Science 318 CCIS: 196–99. https://doi.org/10.1007/978-3-642-33161-9_29.

D.H.S. 2018. “Cybersecurity Risks Posed by Unmanned Aircraft Systems.” https://www.eisac.com/:

Dahiya, Susheela, and Manik Garg. 2019. “Unmanned Aerial Vehicles: Vulnerability to Cyber Attacks.” In International Conference on Unmanned Aerial System in Geomatics, 201–11. Springer, Cham.

Darabseh, Ala’, Evangelos Bitsikas, and Brice Tedongmo. 2019. “Detecting Gps Jamming Incidents in Opensky Data.” EPiC Series in Computing 67: 97–108. https://doi.org/10.29007/1mmw.

Diggelen, FST Van. 2009. A-Gps: Assisted Gps, Gnss, and Sbas. https://books.google.com/books?hl=en&lr=&id=stTSHdFhrFUC&oi=fnd&pg=PR13&dq=A-GPS:+Assisted+GPS,+GNSS,+and+SBAS&ots=zaMc1ClcUs&sig=aC5HIPjRXw0z2B7eMPnWR3ExB-k.DoD. 2008. “Global Positioning System Performance Standard.” Washington, DC: DoD.

E.A.S.A. 2021. Opinion No 03 /2021 Management of Information Security Risks. Geneva: EASA.

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

Eichelberger, Manuel, Kevin Luchsinger, Eth Zürich, Simon Tanner, Roger Wattenhofer, and Roger Wat. 2017. "Indoor Localization with Aircraft Signals." Dl.Acm.Org 2017-January (November). https://doi.org/10.1145/3131672.3131698

Eichelberger, Manuel, Eth Zurich, Ferdinand Von, Hagen Eth Zurich, Roger Wattenhofer, and Ferdinand Von Hagen. 2019. "Multi-Year Gps Tracking Using a Coin Cell." Dl.Acm.Org, February, 141–46. https://doi.org/10.1145/3301293.3302367.

El-Rewini, Zeinab, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. 2020. "Cybersecurity Attacks in Vehicular Sensors." IEEE Sensors Journal 20 (22): 13752–67. https://doi.org/10.1109/JSEN.2020.3004275.

Elghamrawy, H., Karaim, M., Tamazin, M., Noureldin, A., 2020. Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers. Appl. Sci. 2020, Vol. 10, Page 4240 10, 4240. https://doi.org/10.3390/APP10124240

"EUROCONTROL Specification for Surveillance Data Exchange - Part 1." 2016. https://www.eurocontrol.int/sites/default/files/2019-06/part_1_-_eurocontrol_specification_asterix_spec-149_ed_2.4.pdf.

F.A.A. 2018. "FAA Safety Management." https://www.faa.gov/:

———. 2019. "ATO-SMS-Manual." https://www.faa.gov/:

———. 2020. "Fact Sheet – Small Unmanned Aircraft Systems (UAS) Regulations (Part 107)." 2020. https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615.

———. 2020. "Ins and Outs." Template. January 2, 2020. https://www.faa.gov/nextgen/equipadsb/capabilities/ins_outs/.

———. 2021. SRM Safety Management Quick Reference Guide. Washington: FAA Manual Sections.

———. 2021. "What Is GPS."

Fadaei, N., 2016. Detection, Characterization and Mitigation of GNSS Jamming Interference Using Pre-Correlation Methods. University of Calgary, Canada, Calgary, Alberta.

Fan, Y., and e al. 2015. "A Cross Layer Defense Mechanism against GPS Spoofing Attacks on PMUs in Smart Grid." IEEE Trans on Smart Grid 6 (6).

Fante, R.L., Vaccaro, J.J., 2002. Evaluation of Adaptive Space-Time-Polarization Cancellation of Broadband Interference, in: 2002 IEEE Position Location and Navigation Symposium. Palm Springs, CA, USA, pp. 1–3.

Federal Aviation Administration. 2018. "Airspace 101 – Rules of the Sky." Unmanned Aircraft Systems. 2018. https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_101/.

Flysher, Nir, Roi Yozevitch, and Boaz Ben-Moshe. 2017. "GNSS Denial of Service and the Preparation for Tomorrow's Threats." 2016 IEEE International Conference on the Science of Electrical Engineering, ICSEE 2016. https://doi.org/10.1109/ICSEE.2016.7806081.

Garg, Sahil, Gagangeet Singh Aujla, Neeraj Kumar, and Shalini Batra. 2019. “Tree-Based Attack–Defense Model for Risk Assessment in Multi-UAV Networks.” IEEE Consumer Electronics Magazine 8 (6): 35–41.

Gebre-Egziabher, Demoz, and Brian Taylor. 2012. “Impact and Mitigation of GPS-Unavailability on Small UAV Navigation, Guidance and Control, Univ. of MN UAV Laboratory.” Dep’t of Aerospace Eng. & Mech.

Goforth, Hunter, and Simon Lucey. 2019. “GPS-Denied UAV Localization Using Pre-Existing Satellite Imagery.” In 2019 International Conference on Robotics and Automation (ICRA), 2974–80. IEEE.

Goldenberg, Felix. 2006. “Geomagnetic Navigation beyond the Magnetic Compass.” Record - IEEE PLANS, Position Location and Navigation Symposium 2006: 684–94. https://doi.org/10.1109/PLANS.2006.1650662.

Goward, D. 2020. GPS Circle Spoofing Discovered in Iran. GPS World.

GPS.GOV. 2021. “Space Segment.” Systems. 2021. https://www.gps.gov/systems/gps/space/.

Gudla, Charan, Md Shohel Rana, and Andrew H Sung. 2018. “Defense Techniques against Cyber Attacks on Unmanned Aerial Vehicles.” Proceedings of the International Conference on Embedded Systems, Cyber-Physical Systems, and Applications (ESCS), 110–16.

Guo, Rongxiao, Buhong Wang, and Jiang Weng. 2020. “Vulnerabilities and Attacks of UAV Cyber Physical Systems.” In Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things, 8–12.

Gupta, Lav, Raj Jain, and Gabor Vaszkun. 2016. “Survey of Important Issues in UAV Communication Networks.” IEEE Communications Surveys and Tutorials 18 (2): 1123–52.

Haider, Zeeshan, and Shehzad Khalid. 2016. “Survey on Effective GPS Spoofing Countermeasures.” In 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 573–77. IEEE.

Hammer, Jonathan, G. Calgaris, and M. Llobet. 2007. “Safety Analysis Methodology for ADS-B Based Surveillance Applications.” In 7th USA/Europe Air Traffic Management R&D Seminar.

Hartmann, Kim, and Christoph Steup. 2013. “The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment.” International Conference on Cyber Conflict, CYCON.

Hentati, Aicha Idriss, and Lamia Chaari Fourati. 2020. “Comprehensive Survey of UAVs Communication Networks.” Computer Standards and Interfaces 72 (June): 103451. https://doi.org/10.1016/j.csi.2020.103451.

Higuchi, Kenichi, and Anass Benjebbour. 2015. “Non-Orthogonal Multiple Access (NOMA) with Successive Interference Cancellation for Future Radio Access.” IEICE Transactions on Communications E98B (3): 403–14. https://doi.org/10.1587/transcom.E98.B.403.

Horri, Nadjim, and Phil Palmer. 2013. “Relative Navigation.” Distributed Space Missions for Earth System Monitoring, no. August: 331–44. https://doi.org/10.1007/978-1-4614-4541-8_9.

Hsu, Li Ta. 2018. “Analysis and Modeling GPS NLOS Effect in Highly Urbanized Area.” GPS Solutions 22 (1). https://doi.org/10.1007/s10291-017-0667-9.

Hsu, Li-Ta. 2017. “GNSS Multipath Detection Using a Machine Learning Approach.” In 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), 1–6. https://doi.org/10.1109/ITSC.2017.8317700.

https://doi.org/10.1016/J.AST.2018.04.029.

Hu, Qie, Young Hwan Chang, and Claire J. Tomlin. 2016. “Secure Estimation for Unmanned Aerial Vehicles against Adversarial Cyber Attacks.” 30th Congress of the International Council of the Aeronautical Sciences, ICAS 2016, no. 1.

Humphrees, T.E. and e. 2008. “Assessing the Spoofing Threat: Development of a portable GPS Spoofing Civilian Spoofer.” In ION, 16–19. Savana, GA: ION.

Humphreys, T., and e al. 2008. “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer.” In Radionavigation Laboratory Conf. Proc.

Hunter, George and Peng Wei, and Peng Wei. 2019. “Service-Oriented Separation Assurance For Small UAS Traffic Management.” In : : IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS).

I.C.A.O. 2021. “Aviation Security Manual Document 8973/8.” https://www.icao.int/Security/:

I.S.-G.P.S.-200G. 2013. “IS-GPS-200H.” In 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/:

International Civil Aviation Organisation. 2013. “ADS-B Implementation and Operations Guidance Document,” no. June.

Ippolito, Corey A., Kalmanje Krishnakumar, Vahram Stepanyan, Anjan Chakrabarty, and Josh Baculi. 2019. “SAFE50 Reference Design Study for Large-Scale High-Density Low-Altitude UAS Operations in Urban Areas.” In AIAA Scitech 2019 Forum. American Institute of Aeronautics and Astronautics Inc, AIAA. https://doi.org/10.2514/6.2019-0687.

Isaacs, Jason T., Ceridwen Magee, Anantharaman Subbaraman, François Quitin, Kingsley Fregene, Andrew R. Teel, Upamanyu Madhow, and João P. Hespanha. 2014. “GPS-Optimal Micro Air Vehicle Navigation in Degraded Environments.” Proceedings of the American Control Conference, 1864–71. https://doi.org/10.1109/ACC.2014.6859336.

J.Liu and etal. 2012. “Energy Efficient GPS Sensing with Cloud Offloading.” In Proceedings of 10 ACM Conference on Embedded Networked Sensor Signals (SenSys, 85–89.

Jafarnia-Jahromi, A., and e al. 2012. Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver. ION ITM.

Jain, Kamal, Koroush Khoshelham, Xuan Zhu, and Anuj Tiwari. 2020. Unmanned Aerial System in Geomatics. Lecture Notes in Civil Engineering. Vol. 51. https://doi.org/10.1007/978-3-030-37393-1_23.

Jia, Z. 2016. “A Type of Collective Detection Scheme with Improved Pigeon-Inspired Optimization.” Inter. J. of Intelligent Computing and Cybernetics 9 (1): 105–23.

Johnson, Jeff, and Brandon Dewberry. 2011. “Ultra-Wideband Aiding of GPS for Quick Deployment of Anchors in a GPS-Denied Ad-Hoc Sensor Tracking and Communication System.” 24th International Technical Meeting of the Satellite Division of the Institute of Navigation 2011, ION GNSS 2011 5: 3959–66.

Jovanovic, A., and C. Botteron. 2014. “Multi-Test Detection and Protection Algorithm against Spoofing Attacks on GNSS Receivers.” In PLANS IEEE/ION Position, Location and Navigation Symposium, 5–8. May. Monterey, CA 5-8 May: IEEE/ION.

Jumaah, Huda Jamal, Bahareh Kalantar, Shattri Mansor, Alfian Abdul Halin, Naonori Ueda, and Sarah Jamal Jumaah. 2021. “Development of UAV-Based PM2. 5 Monitoring System.” Drones 5 (3): 60.

Kamienski, J, J Semanek - Procedia Manufacturing, and undefined 2015. n.d. “ATC Perspectives of UAS Integration in Controlled Airspace.” Elsevier. Accessed January 15, 2022. https://www.sciencedirect.com/science/article/pii/S2351978915001705.

Kerns, Andrew J., Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. 2014. “Unmanned Aircraft Capture and Control via GPS Spoofing.” Journal of Field Robotics 31 (4): 617–36. https://doi.org/10.1002/rob.21513.

Khalife, Joe J., Souradeep Bhattacharya, and Zaher M.Joe J. Kassas. 2018. “Centimeter-Accurate UAV Navigation with Cellular Signals.” In Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2018, 2321–31.

Khan, Shah Zahid, Mujahid Mohsin, and Waseem Iqbal. 2021. “On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions.” PeerJ Computer Science 7: e507.

Khosiawan, Yohanes, and Izabela Nielsen. 2016. “A System of UAV Application in Indoor Environment.” Production & Manufacturing Research 4 (1): 2–22.

Kinowski, Artur, and Jacek Skorupski. 2016. “THE PROCESSES OF ATM DATA PROCESSING AS THE SOURCE OF THREATS IN AIR TRAFFIC.”

Kintner, P. M., B. M. Ledvina, and E. R. De Paula. 2007. “GPS and Ionospheric Scintillations.” Space Weather 5 (9): 1–23. https://doi.org/10.1029/2006SW000260.

Kissai, Ali, and Milton Smith. 2019. “UAV Dead Reckoning with and without Using INS/GPS Integrated System in GPS Denied Polar Regions.” International Journal of Aeronautics and Aerospace Engineering 1 (2): 58–67. https://doi.org/10.18689/ijae-1000109.

Kos, T, I Markezic, J Pokrajcic - Proceedings ELMAR-2010, and Undefined 2010. 2010. “Effects of Multipath Reception on GPS Positioning Performance.” Ieeexplore.Ieee.Org. https://ieeexplore.ieee.org/abstract/document/5606130/.

Kuhn, M.G. 2015. “An Asymmetric Security Mechanism for Navigation Signals. 6th Info Hiding Workshop.” Toronto, CA: Univ of Cambridge. https://www.cl.cam.ac.uk/~mgk25/ih2004-navsec.pdf.

Lagkas, Thomas, Vasileios Argyriou, Stamatia Bibi, and Panagiotis Sarigiannidis. 2018. “UAV IoT Framework Views and Challenges: Towards Protecting Drones as ‘Things.’” Sensors 18 (11): 4015.

Langejan, Thom, Emmanuel Sunil, Joost Ellerbroek, and Jacco Hoekstra. 2016. “Effect of ADS-B Characteristics on Airborne Conflict Detection and Resolution.” In 6th SESAR Innovation Days, Hosted by Delft.

Larcom, Jonathan A., and Hong Liu. 2013. “Modeling and Characterization of GPS Spoofing.” 2013 IEEE International Conference on Technologies for Homeland Security, HST 2013, 729–34. https://doi.org/10.1109/THS.2013.6699094.

Leela Krishna, C. G., and Robin Murphy. 2018. “A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles.” Auvsi Xponential 2018, 0–5.

Leonardi, Mauro, and Emilio Giuseppe Piracci. 2018. “ADS-B Degarbling and Jamming Mitigation by the Use of Blind Source Separation.” AIAA/IEEE Digital Avionics Systems Conference - Proceedings 2018-September. https://doi.org/10.1109/DASC.2018.8569598.

Li, Chang, and Xudong Wang. 2017. “Jamming Research of the UAV GPS/INS Integrated Navigation System Based on Trajectory Cheating.” Proceedings - 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, CISP-BMEI 2016, no. 2: 1113–17. https://doi.org/10.1109/CISP-BMEI.2016.7852880.

Li, Guang, Chen Ching Liu, Chris Mattson, and Jacques Lawarrée. 2007. “Day-Ahead Electricity Price Forecasting in a Grid Environment.” IEEE Transactions on Power Systems 22 (1): 266–74. https://doi.org/10.1109/TPWRS.2006.887893.

Li, J., 2009. GPS Interference Mitigation for Small UAV Applications. MSc Thesis. The University of Adelaide, Australia.

Li, Li, Kangye Qu, and Kuo-Yi Lin. 2020. “A Survey on Attack Resilient of UAV Motion Planning.” In 2020 IEEE 16th International Conference on Control & Automation (ICCA), 558–63. IEEE.

LII., Cornell -. 2021. “ADS-B Law.” https://www.law.cornell.edu/:

Lin, Honglei, and Dong Wei. 2020. “A High Sensitivity Carrier Frequency Tracking Algorithm for Satellite Navigation Receiver.” In Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering, 302–6.

Ling, Samantha Poh En. 2020. “Literature Review on Remote Sensing, Aerial Manipulation, UAV Navigation and UAV Navigation in GPS Denied Environments,” 1–9.

Liu, Yuanwei, Zhijin Qin, Yunlong Cai, Yue Gao, Geoffrey Ye Li, and Arumugam Nallanathan. 2019. “UAV Communications Based on Non-Orthogonal Multiple Access.” IEEE Wireless Communications 26 (1): 52–57. https://doi.org/10.1109/MWC.2018.1800196.

Lopez-Risueno, G., and G. Seco-Granados. 2005. “Cn/Sub 0/ Estimation and near Far Mitigation for GNSS Indoor Receivers.” In 2005 IEEE 61st Vehiclar Technology Conf, V4:2624–28.

Ly, Bora, and Romny Ly. 2021. “Cybersecurity in Unmanned Aerial Vehicles (UAVs).” Journal of Cyber Security Technology 5 (2): 120–37. https://doi.org/10.1080/23742917.2020.1846307.

Lykou, Georgia, Dimitrios Moustakas, and Dimitris Gritzalis. 2020. “Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies.” Sensors 20 (12): 3537.

Madhani, P., and e al. 2003. “Application of Successive Interference Cancellation to the GPS Pseudolite near Far Problem.” IEEE Trans, on Aerospace & Elect. Systems 39 (2): 481–88.

Magiera, Jaroslaw, and Ryszard Katulski. 2015. “Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing.” Journal of Applied Research and Technology 13 (1): 45–57.

Mair, N. 2012. “A Collaborative Bluetooth- Based Approach to Localization of Mobile Devices.” In IEEE 8th Inter Conf. on Collaborative Computing :Networking, Applications and Worksharing, 363–71.

Mamchenko, M. V. 2021. “Analysis of Control Channel Cybersecurity of the Consumer-Grade UAV by the Example of DJI Tello.” In Journal of Physics: Conference Series, 1864:012127. IOP Publishing.

Manesh, Mohsen Riahi, Mahdi Saeedi Velashani, Elias Ghribi, and Naima Kaabouch. 2019. “Performance Comparison of Machine Learning Algorithms in Detecting Jamming Attacks on ADS-B0 Devices.” IEEE International Conference on Electro Information Technology 2019-May: 200–206. https://doi.org/10.1109/EIT.2019.8833789.

Mao, W.L., 2008. Novel SREKF-based recurrent neural predictor for narrowband/FM interference rejection in GPS. AEU - Int. J. Electron. Commun. 62, 216–222. https://doi.org/10.1016/J.AEUE.2007.04.002

Matolak, David W. 2015. “Unmanned Aerial Vehicles: Communications Challenges and Future Aerial Networking.” 2015 International Conference on Computing, Networking and Communications, ICNC 2015, 567–72. https://doi.org/10.1109/ICCNC.2015.7069407.

McCallie, D. and a. 2011. “Security Analysis of the ADS-B Implementation in the NEXT Generation Air Transport System.” Inter J. of Critical Infrastructure Protection 4: 78–87.

Medina, D., Lass, C., Marcos, E.P., Ziebold, R., Closas, P., García, J., 2019. On GNSS Jamming Threat from the Maritime Navigation Perspective, in: 2019 22th International Conference on Information Fusion (FUSION). IEEE, Ottawa, ON, Canada.

Microsoft. 2016. “Microsoft Indoor Localization Competition.” www.microsoft.com:

Moncayo, H., C. Yanke, and Li Yuetong. 2020. Embry-Riddle Aeronautical University Quarterly Report #1 Technical: A-44 Mitigating GPS and ADS-B Risk for UAS. Daytona Beach, FL: ERAU.

Morales, Joshua J., and Zaher M. Kassas. 2021. “Tightly Coupled Inertial Navigation System With Signals of Opportunity Aiding.” IEEE Transactions on Aerospace and Electronic Systems 57 (3): 1930–48.

Morana, T. U. (2015). Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. Hoboken, NJ: Wiley.

Mosavi, M.R., Pashaian, M., Rezaei, M.J., Mohammadi, K., 2015. Jamming mitigation in global positioning system receivers using wavelet packet coefficients thresholding. IET Signal Process. 9, 457–464. https://doi.org/10.1049/IET-SPR.2014.0280

Mosavi, M.R., Shafie, F., 2016. Narrowband interference suppression for GPS navigation using neural networks. GPS Solut. 20, 341–351. https://doi.org/10.1007/S10291-015-0442-8

Nagai, Masahiko, Tianen Chen, Afzal Ahmed, and Ryosuke Shibasaki. 2008. "UAV Borne Mapping by Multi Sensor Integration." Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci 37: 1215–21.

Nahangi, Mohammad, Adam Heins, Brenda McCabe, and Angela Schoellig. 2018. "Automated Localization of UAVs in GPS-Denied Indoor Construction Environments Using Fiducial Markers." ISARC 2018 - 35th International Symposium on Automation and Robotics in Construction and International AEC/FM Hackathon: The Future of Building Things, no. Isarc. https://doi.org/10.22260/isarc2018/0012.

National Institute of Standards and Technology (NIST). 2004. "Standards for Security Categorization of Federal Information and Information Systems." Federal Information Processing Standards Publication (FIPS PUB 199), no. February: 473–84. https://doi.org/10.1016/b978-159749116-7/50032-9.

Ng, Y., and G. Gao. 2016. "Mitigating Jamming & Meaconing Attacks Using Direct GPS Positioning." In Position, Location & Navigation Symposium (PLANS) IEEE/ION, 1021–26.

Nichols, Randall K, Hans C Mumm, and Wayne D Lonstein. 2020. "New Prairie Press Counter Unmanned Aircraft Systems Technologies and Operations."

Nichols, RK. 1998. "ICSA Guide to Cryptography." https://dl.acm.org/doi/abs/10.5555/552688.

Nichols, RK, P Lekkas, and PC Lekkas. 2001. Wireless Security. http://sutlib2.sut.ac.th/sut_contents/H106096.pdf.

Nichols, RK, H Mumm, WD Lonstein, and JJCH Ryan. 2020. "Unmanned Vehicle Systems & Operations on Air, Sea, Land." https://newprairiepress.org/ebooks/35/.

Nichols, RK, HC Mumm, W Lonstein, and S Sincavage. 2021. "Disruptive Technologies with Applications in Airline & Marine and Defense Industries." https://newprairiepress.org/ebooks/38/.

Nichols, RK, HC Mumm, WD Lonstein, and JJCH Ryan. 2019. Unmanned Aircraft Systems in the Cyber Domain. https://newprairiepress.org/ebooks/27/.

Nichols, RK, JJ Ryan, and DJ Ryan. 2000. "Defending Your Digital Assets against Hackers, Crackers, Spies, and Thieves." https://dl.acm.org/doi/abs/10.5555/555691.

Niles, Frederick A., Robert S. Conker, M. Bakry El-Arini, Daniel G. O'Laighlin, and Dmitri V. Baraban. 2012. "Wide Area Multilateration for Alternate Position, Navigation, and Timing (APNT)." MITRE-CAASD, Tech. Rep.

Oberholzer and etal. 2011. "Spiderbat: Augmenting Wireless Sensor Networks with Distance and Angle Information." In Proc of 10th ACM/IEEE Int Conf on Information Processing in Sensor Networks, 211–22.

Ochin, Evgeny, and Lukasz Lrmieszewski. 2021. "Security of GNSS." In GPS and GNSS Technology in Geosciences, 51–74. Elsevier.

Park, J., Sreeja, V., Aquino, M., Cesaroni, C., Spogli, L., Dodson, A., De Franceschi, G., 2016, Performance of ionospheric maps in support of long baseline GNSS kinematic positioning at low latitudes. Radio Sci., 51, https://doi.org/10.1002/2015RS005933.

Park, J., Veettil, S. V., Aquino, M., Yang, L., and Cesaroni, C., 2017, Mitigation of Ionospheric Effects on GNSS Positioning at Low Latitudes. J Inst Navig, 64: 67– 74. https://doi.org/10.1002/navi.177.

Park, K., Lee, D., Seo, J., 2018. Dual-polarized GPS antenna array algorithm to adaptively mitigate a large number of interference signals. Aerosp. Sci. Technol. 78, 387–396.

Pathak, H.P., and e al. 2015. "Visible light communication, networking and sensing: a survey, potential and challenges." IEEE Communications Surveys & Tutorials 4: 17,.

Politi, Elena, Ilias Panagiotopoulos, Iraklis Varlamis, and George Dimitrakopoulos. n.d. "A Survey of UAS Technologies to Enable Beyond Visual Line Of Sight (BVLOS) Operations." Scitepress.Org. Accessed January 15, 2022. https://doi.org/10.5220/0010446905050512.

Pollack, Jason, and Prakask Ranganathan. 2018. "Aviation Navigation Systems Security: ADS-B, GPS, IFF." International Conference on Security and Management (SAM), 129–35.

Program, Air Force, and Air Force Program. 2012. "Global Positioning System (GPS) Selective Availability Anti-Spoofing Module (SAASM)." Gps Saasm, 227–28.

Psiaki, M., and e al. 2013. "GPS Spoofing Detection via Dual- Receiver Correlation of Military Signals." IEEE Tran of Aerospace & Electrical Systems 49 (ue 4): 2250–60.

Psiaki, M.L., and T. Humphreys. 2016. "GNSS Spoofing and Detection." Proc. of the IEEE 104 (6): 1258–70.

Purton, L, H Abbass, S Alam - Australian, and undefined 2010. 2010. "Identification of ADS-B System Vulnerabilities and Threats." Australasiantransportresearchforum …. https://www.australasiantransportresearchforum.org.au/sites/default/files/2010_Purton_Abbass_Alam.pdf

Pöpper, Christina, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun. 2011. "Investigation of Signal and Message Manipulations on the Wireless Channel." In European Symposium on Research in Computer Security, 40–59. Springer.

Qiao, Yinrong, Yuxing Zhang, and Xiao Du. 2018. "A Vision-Based GPS-Spoofing Detection Method for Small UAVs." Proceedings - 13th International Conference on Computational Intelligence and Security, CIS 2017 2018-Janua: 312–16. https://doi.org/10.1109/CIS.2017.00074.

Ranganathan, A., and e al. 2016. "SPREE: A Spoofing Resistant GPS Receiver." In Proc. of the 22nd Ann Inter Conf. on Mobile Computing and Networking, ACM, 348–60.

Redetzke, J. &. (2021). Capt. Redetzke COT 680 Iron Dome JR Rev 3A RKN Rev 5A 07262021 PIF GRANTED. Salina, KS: KSU.

Ren, T., Petovello, M.G., 2017. A Stand-Alone Approach for High-Sensitivity GNSS Receivers in Signal-Challenged Environment. IEEE Trans. Aerosp. Electron. Syst. 53, 2438–2448. https://doi.org/10.1109/TAES.2017.2699539.

Reza, M., Javad, R., PashaianMatin, Salamat, M., 2017. A fast and accurate anti-jamming system based on wavelet packet transform for GPS receivers. GPS Solut. 21, 415–426. https://doi.org/10.1007/S10291-016-0535-Z

Rhudy, Matthew B., Yu Gu, Haiyang Chao, and Jason N. Gross. 2015. "Unmanned Aerial Vehicle Navigation Using Wide-Field Optical Flow and Inertial Sensors." Journal of Robotics 2015. https://doi.org/10.1155/2015/251379.

Riahi Manesh, Mohsen, and Naima Kaabouch. 2017. "Analysis of Vulnerabilities, Attacks, Countermeasures and Overall Risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) System." International Journal of Critical Infrastructure Protection 19 (December): 16–31. https://doi.org/10.1016/j.ijcip.2017.10.002.

Rufa, Justin R., and Ella M. Atkins. 2016. "Unmanned Aircraft System Navigation in the Urban Environment: A Systems Analysis." Journal of Aerospace Information Systems. American Institute of Aeronautics and Astronautics Inc. https://doi.org/10.2514/1.I010280.

Ryan, J. J. (1998). An Exploration of Information Security Aspects in the Thirty Elements of Systems Engineering. Washington: GWU EMGT Spring.

Ryan, J. J. (2006, November). Expected Benefits of Information Security Investments. Computers & Security , pp. Volume 25, Issue 8, Pages 579-588. Retrieved from Computers & Security : https://www.sciencedirect.com/science/article/pii/S0167404806001192

Ryan, J. J., & Ryan, &. D. (2005, May 8). Proportional Hazards in Information Security. Risk Analysis, p. 9.

S.A.Shaukat, and e al. 2016. "Robust Vehicle Localization with GPS Dropouts." In 6th Ann Inter Conf on Intelligent and Advanced Systems, 1–6. IEEE.

Sabaka, Terence J., Lars Tøffner-Clausen, Nils Olsen, and Christopher C. Finlay. 2020. "CM6: A Comprehensive Geomagnetic Field Model Derived from Both CHAMP and Swarm Satellite Observations." Earth, Planets and Space 72 (1). https://doi.org/10.1186/s40623-020-01210-5.

Sahawneh, Laith R., Matthew O. Duffield, Randal W. Beard, and Timothy W. McLain. 2015. "Detect and Avoid for Small Unmanned Aircraft Systems Using ADS-B." Air Traffic Control Quarterly 23 (2–3): 203–40. https://doi.org/10.2514/atcq.23.2-3.203.

Sallam, Marwan. 2016. "What Threats May Cyber Warfare Implicate on Unmanned Arial Vehicles (UAV)? Are Those Threats Taken Seriously by the US Government ? Marwan Sallam Student , AUC School of Business Abstract" 4 (4).

Schaefer, M., and A. Pearson. 2021. GPS and GNSS Technology in Geosciences. NYC: Elsevier.

Schmidt, D., and e al. 2016. "A Survey and Analysis of GNSS Spoofing Threat and Countermeasures." ACM Computing Surveys (CSUR 48 (4).

Schuster, Wolfgang, Jie Bai, Shaojun Feng, and Washington Ochieng. 2012. "Integrity Monitoring Algorithms for Airport Surface Movement." GPS Solutions 16 (1): 65–75. https://doi.org/10.1007/s10291-011-0209-9.

Schäfer, Matthias, Vincent Lenders, and Ivan Martinovic. 2013. "Experimental Analysis of Attacks on next Generation Air Traffic Communication." Lecture Notes in Computer Science

(Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7954 LNCS: 253–71. https://doi.org/10.1007/978-3-642-38980-1_16.

Sedjelmaci, Hichem, Sidi Mohammed Senouci, and Mohamed-Ayoub Messous. 2016. "How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?" In 2016 IEEE Global Communications Conference (GLOBECOM), 1–6. IEEE.

Sedjelmaci, Hichem, Sidi Mohammed Senouci, and Nirwan Ansari. 2017. "A Hierarchical Detection and Response System to Enhance Security against Lethal Cyber-Attacks in UAV Networks." IEEE Transactions on Systems, Man, and Cybernetics: Systems 48 (9): 1594–1606.

Semke, William, Nicholas Allen, Asma Tabassum, Matthew McCrink, Mohammad Moallemi, Kyle Snyder, Evan Arnold, Dawson Stott, and Michael G. Wing. 2017. "Analysis of Radar and ADS-B Influences on Aircraft Detect and Avoid (DAA) Systems." Aerospace 4 (3): 49. https://doi.org/10.3390/aerospace4030049.

Seo, Jiwon, Todd Walter, and Per Enge. 2011. "Availability Impact on GPS Aviation Due to Strong Ionospheric Scintillation." IEEE Transactions on Aerospace and Electronic Systems 47 (3): 1963–73. https://doi.org/10.1109/TAES.2011.5937276.

Shan, Mo, Fei Wang, Feng Lin, Zhi Gao, Ya Z. Tang, and Ben M. Chen. 2015. "Google Map Aided Visual Navigation for UAVs in GPS-Denied Environment." 2015 IEEE International Conference on Robotics and Biomimetics, IEEE-ROBIO 2015, 114–19. https://doi.org/10.1109/ROBIO.2015.7418753.

Shashok, Nikolas. 2017. "Analysis of Vulnerabilities in Modern Unmanned Aircraft Systems To The Community : Modern Drone Uses and Risks."

Shrivastava, G.P. 2021. GPS and GNSS Technology in the Geosciences. NYC: Elsevier.

Sidorov, Vasily, Wee Keong Ng, Kwok Yan Lam, and Mohamed Faisal Bin Mohamed Salleh. 2017. "Implications of Cyber Threats for the Design of Unmanned Air Traffic Management System." 2017 International Conference on Unmanned Aircraft Systems, ICUAS 2017, 1682–89. https://doi.org/10.1109/ICUAS.2017.7991429.

Silvagni, Mario, Andrea Tonoli, Enrico Zenerino, and Marcello Chiaberge. 2017. "Multipurpose UAV for Search and Rescue Operations in Mountain Avalanche Events." Geomatics, Natural Hazards and Risk 8 (1): 18–33.

Singh, H., Jha, R.M., 2012. Trends in adaptive array processing. Int. J. Antennas Propag. 2012. https://doi.org/10.1155/2012/361768.

Skone, S., Lachapelle, G., Yao, D., Yu, W., Watson, R., 2005. Investigating the Impact of Ionospheric Scintillation Using a GPS Software Receiver, in: Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005). Long Beach, CA, pp. 1126–1137.

Snyder, Kyle, William Semke, Jim Gregory, Michael Wing, Mohammad Moallemi, and J. W. Bruce. 2016. "UAS Surveillance Criticality."

Sobers, D. Michael, Girish Chowdhary, and Eric N. Johnson. 2009. “Indoor Navigation for Unmanned Aerial Vehicles.” AIAA Guidance, Navigation, and Control Conference and Exhibit, no. August. https://doi.org/10.2514/6.2009-5658.

Souli, Nicolas, Panayiotis Kolios, and Georgios Ellinas. 2020. “Relative Positioning of Autonomous Systems Using Signals of Opportunity.” In 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 1–6. IEEE.

Spilker, J. 1996. “Fundamentals of Signal Tracking Theory.” Prog in Astronautics & Aeronautics 163: 245–328.

Sreeja, V., Aquino, M., Elmas, Z. G., and Forte, B., 2012. Correlation Analysis Between Ionospheric Scintillation Levels and Receiver Tracking Performance, Space Weather, Vol. 10, No. 6, 2012, p. S06005.

Stamatescu, Grigore, Iulia Stamatescu, Dan Popescu, and Cristian Mateescu. 2015. “Sensor Fusion Method for Altitude Estimation in Mini-UAV Applications.” In 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), SSS-39. IEEE.

Strohmeier, M. 2015. “On the security of automatic dependent surveillance- broadcast protocol.” IEEE communications Surveys & Tutorials 17: 1066–87.

Strohmeier, Martin, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. 2014. “Realities and Challenges of Nextgen Air Traffic Management: The Case of ADS-B.” IEEE Communications Magazine 52 (5): 111–18.

Strohmeier, Martin, Vincent Lenders, and Ivan Martinovic. 2014. “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol.” IEEE Communications Surveys & Tutorials 17 (2): 1066–87.

Strümpfel, Christoph, Eric Schuster, Svenja Huschbeck, Christian Berth, and Maarten Uijt de Haag. 2020. “Assured Multi-Mode Navigation for Urban Operations of Small Uas.” In AIAA Scitech 2020 Forum. Vol. 1 PartF. American Institute of Aeronautics and Astronautics Inc, AIAA. https://doi.org/10.2514/6.2020-1945.

Sun, K., Jin, T., Yang, D., 2015. An Improved Time-Frequency Analysis Method in Interference Detection for GNSS Receivers. Sensors (Basel). 15, 9404. https://doi.org/10.3390/S150409404

Sung, Yunsick, Sejun Jang, Young Sik Jeong, and Jong Hyuk (James J.). Park. 2020. “Malware Classification Algorithm Using Advanced Word2vec-Based Bi-LSTM for Ground Control Stations.” Computer Communications 153 (December 2019): 342–48. https://doi.org/10.1016/j.comcom.2020.02.005.

Syd Ali, Busyairah, Wolfgang Schuster, Washington Ochieng, and Arnab Majumdar. 2016. “Analysis of Anomalies in ADS-B and Its GPS Data.” GPS Solutions 20 (3): 429–38. https://doi.org/10.1007/s10291-015-0453-5.

Tabassum, Asma, and William Semke. 2018. “UAT ADS-B Data Anomalies and the Effect of Flight Parameters on Dropout Occurrences.” Data 3 (2): 19.

Tabassum, Asma. 2017. Performance Analysis of Automatic Dependent Surveillance-Broadcast (ADS-B) and Breakdown of Anomalies. The University of North Dakota.

Thayaparan, T. (2000). Linear and Quadratic Time-Frequency Representations. Defence Research Establishment Ottawa. https://apps.dtic.mil/sti/pdfs/ADA385576.pdf

The Royal Academy of Engineering. 2011. London: The Royal Academy of Engineering.

Tippenhauer, N. and etal. 2011. “On the Requirements for Successful Spoofing Attacks.” In Proc. of the 18th ACM Conf. on Computing and Communications Security (CCS, 75–86.

Transporation, U.S. Department of. n.d. “What Is Positioning, Navigation and Timing (PNT)?” https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt.

U.S.G.P.O. 2020. “Global Positioning System (GPS) Standard Positioning Service (SPS.” https://www.gps.gov/technical/ps/:

US Patent. 1942. 2,292,387, issued 1942.

Vasconcelos, Gabriel, Gabriel Carrijo, Rodrigo Miani, Jefferson Souza, and Vitor Guizilini. 2016. “The Impact of DoS Attacks on the AR.Drone 2.0.” Proceedings - 13th Latin American Robotics Symposium and 4th Brazilian Symposium on Robotics, LARS/SBR 2016, 127–32. https://doi.org/10.1109/LARS-SBR.2016.28.

Vidal, Chaz, and Kim Kwang Raymond Choo. 2018. Situational Crime Prevention and the Mitigation of Cloud Computing Threats. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. Vol. 239. https://doi.org/10.1007/978-3-319-78816-6_16.

Wang, Fei, Kangli Wang, Shupeng Lai, Swee King Phang, Ben M. Chen, and Tong H. Lee. 2014. “An Efficient UAV Navigation Solution for Confined but Partially Known Indoor Environments.” IEEE International Conference on Control and Automation, ICCA, 1351–56. https://doi.org/10.1109/ICCA.2014.6871120.

Wang, Haichao, Jinlong Wang, Jin Chen, Yuping Gong, and Guoru Ding. 2018. “Network-Connected UAV Communications: Potentials and Challenges.” China Communications 15 (12): 111–21.

Wang, J., Amin, M.G., 2008. Multiple Interference Cancellation Performance for GPS Receivers with Dual-Polarized Antenna Arrays. EURASIP J. Adv. Signal Process. 597613, 13. https://doi.org/10.1155/2008/597613.

Warner, and Johnson. 2002. “A Simple Demonstration That the System (GPS) Is Vulnerable to Spoofing.” J. of Security Administration. https://the-eye.eu/public/Books/Electronic%20Archive/GPS-Spoofing-2002-2003.pdf.

Warner, J.S., and R. Johnston. 2003. “GPS Spoofing Countermeasures.” Journ of Security Administration. https://www.semanticscholar.org/paper/GPS-Spoofing-Countermeasures-Warner-Johnston/36e17f723bff8d429aca4714abe54500a9edaa49.

Wesson, K. 2014. “Secure Navigation and Timing without Local Storage of Secret Keys.” PhD Thesis.

Wheeler, David O., Daniel P. Koch, James S. Jackson, Gary J. Ellingson, Paul W. Nyholm, Timothy W. McLain, and Randal W. Beard. 2020. “Relative Navigation of Autonomous GPS-Degraded Micro Air Vehicles.” Autonomous Robots, 1–20.

Wikipedia. 2021. “Global Positioning System.” https://en.wikipedia.org/wiki/:

Wilhelm, Matthias, Jens B. Schmitt, and Vincent Lenders. 2012. “Practical Message Manipulation Attacks in IEEE 802.15. 4 Wireless Networks.” In MMB & DFT 2012 Workshop Proceedings, 29–31.

Yaacoub, Jean-Paul, Hassan Noura, Ola Salman, and Ali Chehab. 2020. “Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations.” Internet of Things 11: 100218. https://doi.org/10.1016/j.iot.2020.100218.

Yan, J., Laflamme, S., Singh, P., Sadhu, A., Dodson, J., 2020. A Comparison of Time-Frequency Methods for Real-Time Application to High-Rate Dynamic Systems. Vibration 3, 204–216. https://doi.org/10.3390/VIBRATION3030016

Yağdereli, Eray, Cemal Gemci, and A. Ziya Aktaş. 2015. “A Study on Cyber-Security of Autonomous and Unmanned Vehicles.” Journal of Defense Modeling and Simulation 12 (4): 369–81. https://doi.org/10.1177/1548512915575803.

Ye, H., and e al. 2012. “FTrack: Infrastructure-Free Floor Localization via Mobile Phone Sensing.” IEEE Inter Conf. on Pervasive Computing and Communications, 2–10.

Yu, Ting, Audit Association for Computing Machinery. Special Interest Group on Security, National Science Foundation (U.S.), Association for Computing Machinery, and ACM Digital Library. 2012. “GPS Software Attacks,” 1070.

Yuchao, M., Weiming, Y., Haoxiang, H., Kai, W., 2014. Damage detection based on cross-term extraction from bilinear time-frequency distributions. Math. Probl. Eng. 2014. https://doi.org/10.1155/2014/986050

Zeng, Yong, Rui Zhang, and Teng Joon Lim. 2016. “Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges.” IEEE Communications Magazine 54 (5): 36–42. https://doi.org/10.1109/MCOM.2016.7470933.

Zhao, Shiyu, Feng Lin, Kemao Peng, Xiangxu Dong, Ben M. Chen, and Tong H. Lee. 2016. “Vision-Aided Estimation of Attitude, Velocity, and Inertial Measurement Bias for UAV Stabilization.” Journal of Intelligent and Robotic Systems: Theory and Applications 81 (3–4): 531–49. https://doi.org/10.1007/s10846-015-0206-2.

Zoltowski, M.D., Gecan, A.S., 1995. Advanced adaptive null steering concepts for GPS. Proc. - IEEE Mil. Commun. Conf. MILCOM 3, 1214–1218. https://doi.org/10.1109/MILCOM.1995.483688

[i] Aircraft signal transfer is not the only means to localize indoor signals. HAPs, WiFi, Ultrasound, Light, Bluetooth, RFID. Sensor fusion and GSM all have a place in the decision-making process.

[ii] The results are defined and graphically presented in (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) p87-ff.

[iii] "Hi Randy, based on your findings of FAA and US Navy spoofing risk assessment, I did some research about the status here in Europe. EASA is currently looking at jamming/spoofing as a general threat for manned aviation, there is currently no UAS-focused consideration about this. The main docs I found are listed below:
https://www.easa.europa.eu/sites/default/files/dfu/EASA-REP-RESEA-2016-1-v0.2-cln.pdf
https://www.easa.europa.eu/sites/default/files/dfu/easa_opinion_no_03-2021.pdf
https://www.easa.europa.eu/download/etso/ETSO-C146e_CS-ETSO_13.pdf,
Kind regards, Chris" (Sep 7, 2021, at 11:27)

[iv] "Chris, on page 15/41 in this complex rule making document (Opinion #03/2021) under applicability to operators of UAS, there are three key exclusions: 1) Operators of UAS in "Open" & "Specific" categories. 2) Operators in "Certified" category. Both are Excluded from the regulation. # 2) will be addressed in a future RMT .0230
& 3) Third country Operators required under EU #452/2014 Also excluded under scope of proposed regulations
Page 27/41 discusses the rule and information risk assessment and treatment. It is standard practice guidance.
Page 33/41 mentions cybersecurity and incorrectly lumps it into IS category which applies to subjects like networking and cloud storage not cyber risks like spoofing and SCADA attacks. It gives no specific coverage other than EU 2015/1998 and 'similar' by requiring "consistency among other organizations and rules". The most one can say positive about this document is that it a General / Legal attempt to harmonize among all actors / participants (EU) in their collection and use of Information Risk Events in the Aviation System. It requires support of AMC (acceptable means of compliance) and GM (guidance material) and industry standards. The list of organizations that are affected are listed on page 11/41. You are correct it does not specify any cybersecurity risk. It leaves it to the member organizations within guidance found in Part-IS.AR &. OR standards. The most useful information is found on page 23/41 regarding Part-IS.AR standards (Authority requirements) IS.AR.100-235 and
Part-IS. OR (Organization Requirements) IS.OR.100-260. These are the same normal IS Protect-Detect-Correct; Response, Recovery, Training, Policy functions discussed in many Information Risk Textbooks. My co-authors and I wrote a best- seller about these IS security processes in Nichols, R.K, Ryan, D.J, & Ryan, J.C.H. (2000) Defending Your Digital Assets against Hackers, Crackers, Spies and Thieves, San Francisco: McGraw Hill, RSA Press. It contained: {Part 1: Digital Espionage, Warfare, and Information Security (INFOSEC); Part 2: Information Concepts; Part 4: Enterprise Continuity Planning; Part 5: Appendices C, D, E on Enacted legislation, Policy Initiatives and International - 35 Countries and Political entities enacting Digital legislation} I will find a place for it as a reference but will not reissue 12A or Table RA-0. Thank you for the heads-up. Best Randy. Professor Randall K Nichols" (Tue 07-Sep-21 20:52)

[v] "It seems the FAA views the primary risk of GPS denial as pertinent to system reliability and not much more. For most sUAS, particularly multi rotors, this perspective may be appropriate. But keep in mind that there are some sUAS (fixed wing) that can have hours' worth of endurance. As we see the industry, the FAA, and other Civil Aviation Authorities (CAAs) evolving into BVLOS and transitioning into larger systems (think urban air mobility and advanced air mobility/cargo delivery), nefarious threats will become an increased concern. Many agencies are not necessarily thinking this far ahead…but need to. In those cases, it is helpful to factor in vulnerabilities seen in other transportation modalities. Is that beyond the scope of this project? If so, we can capture it in the lit review and pin it for future work. **If not, it is important to consider, even if we are ahead of the CAAs on the subject (actually, that means we're adding significant value with our work**). Kurt, Kurt J. Carraway, UAS Department Head
UAS Executive Director, Applied Aviation Research Center, Kansas State University, Aerospace and Technology Campus" (Wed 08-Sep-21 09:15)

[vi] "I agree with you, and I believe our risk analysis should indicate that this situation does result a higher risk level when we are operating in BVLOS mode. **I hope our findings do help guide efforts in the more sever risk cases, as is intended.** William H. Semke, PhD, Associate Dean for Academic Affairs, Professor of Mechanical Engineering
College of Engineering and Mines, University of North Dakota" (Wed 08-Sep-21 12:44)

[vii] The author translated part of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) reference from the original German.

[viii] The author has nicknamed Dr. Manuel Eichelberger's brilliant doctorial research, ECD. ECD is Dr. Manuel Eichelberger's advanced implementation of CD to detect and mitigate spoofing attacks on GPS or ADS-B signals

[ix] This is a key point. CD reduces this timestamping process significantly.

[x] Data is sent on a carrier frequency of 1575.42 MHz. (IS-GPS-200G, 2013)

[xi] This is a key point. CD reduces this timestamping process significantly.

[xii] This is a key point. CD reduces this timestamping process significantly.

[xiii] GPS satellites operate on atomic frequency standard, the receivers are not synchronized to GPS time.

[xiv] This is a key point. CD reduces this timestamping process significantly.

[xv] Because the receiver must decode all that data, it has to continuously track and process the satellite signals, which translates to high energy consumption. Furthermore, the TTFF on startup cost the user both latency and power.

[xvi] This is a key point. CD reduces this timestamping process significantly.

[xvii] The deviation is defined as the time offset multiplied by the speed of light plus the location distance.

[xviii] For those who insist on SI / metric, 1 km = ~ 0.62 mi (miles)

[xix] Data bit flips can happen. The normal practice is 2 milliseconds of sample time.

[xx] The vector / tensor mathematics for localization are reasonably complex and can be found in Chapter 5.3 of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

[xxi] Cloud offloading also makes ECD suitable for energy- constrained sensors.

[xxii] (Nichols & al., Unmanned Vehicle Systems and Operations on Air, Sea, and Land, 2020) have argued the case for cryptographic authentication on civilian UAS /UUV and expanded the INFOSEC requirements.

[xxiii] To evaluate the performance of the (Jovanovic & Botteron, 2014) CM, an attack was performed on a GNSS receiver through a GSS8000 full constellation simulator attached to a rooftop antenna.
[xxiv] This cross-correlation portion of this CM method syncs well as a forerunner of ECD.
[xxv] Author opinion.
[xxvi] This is a key section to understanding the beauty of ECD. The entire SIC algorithm and ECD implications is found in detail in (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) p81-ff.
[xxvii] This is what makes jamming a lesser attack. The jamming is detectable by observing the noise floor, in-band power levels and loss of signal -lock takeover.
[xxviii] See (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) Sections 6.5 – 6.7 pages 84-94.
[xxix] See (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) Sections 5.34 – 5.5 for extended discussions on space discretization, satellite visible set **V**, time discretization, averaging over likely hypotheses, hypothesis **h**, coding, efficient implementation of the B&B, local oscillator bias, criteria and test evaluations of ECD, computational considerations, and conclusions. (Closas & al., 2007) (J.Liu & et.al., 2012) (Diggelen 2009)
[xxx] This is accomplished in the acquisition stage of a GPS receiver. The received signals is correlated with the C/A codes.
[xxxi] (Nichols R. K., 2020) presents a model of Risk as a function of Threats, Vulnerabilities, Impact and Countermeasures known as the Ryan- Nichols equations, that models the qualitative effects of information flow through the communications and navigation systems in UAS.
[xxxii] These INFOSEC goals are admirable but considering that most GPS and UAS COTS do not have sufficient GPS spoofing countermeasures or cybersecurity protections (most are legacy), the list is more of a wish list. [Author opinion]
[xxxiii] Please note the word "should." Hackers just love this word.
[xxxiv] Wireless networks present few obstacles to access and can easily be attacked by open-source software. (R.K. Nichols, 2020)
[xxxv] This is still true in legacy systems. Newer implementations have additional protections. UAS systems are notoriously weak in terms of security.
[xxxvi] Ali, et al. identified that jamming of GPS transmissions from the satellite affected the ADS-B system. (Ali, 2014)This is a rather obvious statement of research considering that we have also established that the vulnerabilities of GNSS/GPS pass down to ADS-B systems because they are subset of the larger problem.
[xxxvii] Dave Adamy is the leading global expert in EW. He teaches it is more difficult to jam a PSR due to its rotating antenna and higher transmission power. (Adamy 2001)
[xxxviii] This might have been true in 2011, however a decade of change, growth, cost-effective COTS, and state sponsored hackers says that this observation is severely dated. (Author comment)
[xxxix] Author comment based on experience. Jamming devices are as small as your cell phone and more powerful than computers available in 2011. (Nichols R. K., 2020)
[xl] This is a headache to say the least. Consider a SWARM of 100 + UAS bursting onto the controller's screen at a busy airport.
[xli] This is about the consumption of a GSM base station.
[xlii] A Boeing 747 has an average power consumption of 140 MW, leaving power to spare for GPS communications.

[xliii] Uncompensated latency of up to 0.6 s. (Cornell-LII 2021)
[xliv] 1 m = 3.280 ft
[xlv] TDOA is also called multilateration.
[xlvi] DIY – Do it yourself
[xlvii] INS- an inertial navigation system is composed of motion sensors (accelerometer, gyrometer, and magnetometer) allowing determination of the absolute movement of a platform. Using this information and knowledge of the last position, it is possible using dead reckoning to provide an estimation of position, velocity, and time of the platform after spoofing or jamming detection.
[xlviii] All Acronyms taken from (Nichols R. K., 2020) unless otherwise noted.
[xlix] All Definitions taken from (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019) unless otherwise noted.
[l] $\acute{O}$ = Order of magnitude; dot = dot product for vectors
[li] All these systems are discussed in Chapter 2 of (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)
[lii] Each satellite has a unique 1023-bit PRN sequence, plus some current navigation data, D. Each bit is repeated 20 times for better robustness. Navigation data rate is limited to 50 bit / s. This also limits sending timestamps every 6 seconds, satellite orbit parameters (function of the satellite location over time) only every 30 seconds. As a result, the latency of the first location estimates after turning on a classic receiver, called the time to first fix (TTFF), can be high.