PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0012 May 2019

Guidance for Integrating Unmanned Aircraft Systems (UAS) into Airport Security

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Faith Group, LLC
St. Louis, MO

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about airport security technologies and procedures.

Through the Airport Security Systems Integrated Support Testing (ASSIST) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying perimeter and access control security technologies and procedures.

Through the Performance and Operational System Testing (POST) Program, Safe Skies assesses the continued operational effectiveness of airport-owned security technologies.

Through the Program for Applied Research in Airport Security (PARAS), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

AUTHOR ACKNOWLEDGMENTS

Faith Group would like to acknowledge the following for their contributions in the development of this guidebook:

- Safe Skies' PARAS, which provided funding, and the Program Manager, Jessica Grizzle
- Members of the Safe Skies Perimeter Test Facility team located at the McGhee Tyson Airport in Knoxville, Tennessee
- PARAS 0012 Project Panel Members, who also provided significant review and contributions
- The following airports, who provided invaluable input during Use Case Study testing and interviews; the direction of this guidebook was shaped, in part, thanks to their input
  - Farmville Municipal Airport, OH
  - Springfield-Beckley Municipal Airport, OH
  - Savannah/Hilton Head International Airport, GA
  - McGhee Tyson Airport, TN
  - Safe Skies Perimeter Test Facility, TN
- A team of authors from the following firms who contributed to this document:
  - Faith Group, LLC, Principal Investigator
  - Woolpert
  - Futron Aviation Corporation

CONTENTS

LIST OF TABLES & FIGURES

EXECUTIVE SUMMARY

This guidebook is intended to be used by airport management and staff, as well as unmanned aircraft system (UAS) operators for the purpose of understanding the benefits of, and the processes for, the integration of UAS into airport security programs. UAS enables airport management to project resource capabilities beyond what a typical human workforce can achieve. It provides a force multiplier in many ways and can become an integral part of an airport's security system. UAS can provide a faster response to security alarms, keep visual contact on a situation from a safe distance, track threats, and inspect or patrol facilities as necessary. Within current regulations, applications for UAS in airport security are limited, but offer several benefits.

This guidebook provides the reader with an overview of UAS, and their different characteristics, capabilities, limitations, and possible uses. A section is devoted to the regulations associated with operating a UAS within the National Airspace System, and the approval processes and tools used to gain approval from the FAA. Other sections in this guidebook include information and processes necessary to integrate current UAS with existing security systems, such as Perimeter Intrusion Detection Systems (PIDS), Physical Security Information Management (PSIM) systems, and CCTV. There is also a section that provides information concerning several "drone" detection systems available today. Detection and deterrence of drone use around airports by non-authorized personnel is also a big part of airport security and is addressed as such.

The reader will be able to follow the guidebook section by section or utilize independent sections depending on the airport's objectives. The guidebook is intended to offer different approaches and tools for airports of all sizes and complexity. It should be noted that regulations and UAS capabilities are both changing at a rapid rate. Therefore, the contents of this guidebook should be considered as a baseline at the time of publication. Airport management should always investigate the most current regulations and technologies when considering the implementation of UAS into airport security.

Lastly, as summarized in the Conclusion section, airports should approach the following list as a minimum for developing UAS integration with security programs:

- Consider implementing UAS in the airport security program for the application of:
    - PIDS monitoring and response
    - Patrols for the perimeter and highly sensitive areas of the airport
    - Tracking of potential and identified threats
    - Visual inspections of hard-to-reach areas
    - Threat deterrents during major events
    - Additional and flexible video monitoring of specific areas with a determined need (e.g., special event parking)
- Consider the potential data impacts and requirements. Write a specific policy and concept of operations (CONOPS) for the management and protection of the data generated from UAS operations.
- Start small and take a phased approach to becoming UAS competent and savvy.
- Talk with the FAA Airport District Office and FAA Air Traffic Control Tower (ATCT) personnel (if ATCT-equipped airport).
    - Openly communicate and listen to stakeholder concerns; use this information to help guide the approval processes.

- Explore Certificate of Authorization application and familiarize the staff with the Low Altitude Authorization and Notification Capability program.
- Develop and implement a public awareness campaign so that interested and potential UAS operators know how and when to communicate with the airport.
- Lastly, look broadly at the long term potential use of UAS. Look at instances where humans are put in danger or are asked to see and report findings; those are the times that a UAS can replace or augment people.

PARAS ACRONYMS & ABBREVIATIONS

The following acronyms and abbreviations are used without definitions in PARAS publications:

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue and Fire Fighting
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

GLOSSARY OF KEY TERMS

The following is a list of key definitions applicable to UAS operations, airport operations, and general aircraft operations:

Above Ground Level (AGL)
The altitude at which an aircraft, including a UAS, is flying. Under current Part 107 limits, an sUAS may operate no higher than 400 feet (121.9 meters) above the ground, but may operate within 400 feet of a structure (including above that structure), even if the structure is higher than 400 feet.

Airman
In the context of FAA pilot certification, an airman is any person who has met the requirements and is certified to perform the role of pilot. In the context of sUAS operating under Part 107 regulations, a person must meet the remote pilot certification requirements to operate, or to supervise the operation of, an sUAS being operated for commercial purposes.

Airspace
A portion of the atmosphere sustaining aircraft flight that has defined boundaries and specified dimensions. Airspace may be classified according to the specific types of flight allowed, rules of operation and restrictions in accordance with International Civil Aviation Organization standards, or State regulation.

Airspace: Class A
Generally, airspace from 18,000 feet mean sea level (MSL) up to approximately 60,000 feet, including the airspace overlying the waters within 12 nautical miles (nm) of the coast of the 48 contiguous states and Alaska. Unless otherwise authorized, all persons must operate their aircraft under Instrument Flight Rules (IFR).

Airspace: Class B
Generally, airspace from the surface to 10,000 feet MSL surrounding the nation's busiest airports in terms of airport operations or passenger enplanements.

Airspace: Class C
Generally, airspace from the surface to 4,000 feet above the airport elevation (charted in MSL) surrounding those airports with an operational control tower, that are serviced by a radar approach control, and that have a certain number of IFR operations or passenger enplanements. Although the configuration of each Class C area is individually tailored, the airspace usually consists of a surface area with a 5 nm radius, and an outer circle with a 10 nm radius that extends from no lower than 1,200 feet up to 4,000 feet above the airport elevation.

Airspace: Class D
Generally, airspace from the surface to 2,500 feet above the airport elevation (charted in MSL) surrounding those airports with an operational control tower. The configuration of each Class D airspace area is individually tailored, and when instrument procedures are published, the airspace will normally be designed to contain the procedures.

Airspace: Class E
Generally, if the airspace is not Class A, Class B, Class C or Class D, and is controlled airspace, it is Class E airspace. Class E airspace extends from 1,200 feet (370 m) above ground level (AGL) up to but not including 18,000 feet (5,500 m) MSL, the lower limit of Class A airspace. Most airspace in the United States is Class E.

Airspace: Class G
Class G airspace (uncontrolled) is airspace not designated as Class A, B, C, D, or E airspace.

Air Traffic Control (ATC)
A service operated by appropriate authority (such as the FAA) to promote the safe, orderly, and expeditious flow of air traffic. This term is often used to designate the Air Traffic Controllers (sometimes called ATCOs) that ensure this service locally.

Automatic Dependent Surveillance-Broadcast (ADS-B)
Surveillance technology in which an aircraft determines its position via satellite navigation and periodically broadcasts it, enabling it to be tracked.

Autonomous Flight
Flying guided by GPS waypoints.

Axis
Every UAV has a longitudinal axis, which runs from the tail to the nose of the unit, and a lateral axis, which runs from one side to the other side.

Certificate of Waiver or Authorization (COW/COA)
An FAA grant of approval for a specific flight operation. The authorization to operate a UAS in the National Airspace System as a public aircraft outside of Restricted, Warning, or Prohibited areas approved for aviation activities.

Concept of Operations (CONOPS)
A document describing the operational processes and procedures required for a consistent and efficient operation. In the application of UAS in airport security, it refers to the obligations of the UAS operator, the airport owner and operator, and other agencies or organizations involved in the UAS deployment. In essence, CONOPS documents who and how things are accomplished.

Detect and Avoid
The capability to see, sense, or detect conflicting traffic or other hazards and take the appropriate action to comply with the applicable rules of flight.

Geofencing
A software feature that uses GPS or some other navigational system to define a virtual geographical barrier. In a UAS that includes a navigational or positioning system, a geofencing feature may be used to prevent the UAV from taking off while in a restricted area, or may prevent it from flying into a restricted area.

Global Positioning System (GPS)
A space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. The system provides critical capabilities to military, civil, and commercial users around the world. It is maintained by the US government and is freely accessible to anyone with a GPS receiver.

Ground Control Station
A system of software and hardware receiving telemetry data from a UAV to monitor its status and transmit in-flight commands.

Gyroscope
A device for measuring or maintaining orientation, based on the principles of angular momentum.

Hexacopter
A rotorcraft with six rotors.

LIDAR (also LiDar or Lidar)
Light Detection and Ranging is a distance-measuring technique using pulsed laser light. When used as a sensor for UAS, LIDAR can be applied for a variety of purposes, including airborne mapping and security surveillance. LIDAR can accurately measure objects that may be partially hidden by obstructions such as leaves.

Lithium Polymer Battery (LiPo)
A rechargeable lithium-ion battery in a pouch format. LiPos come in a soft package or pouch, which makes them lighter but also lack rigidity.

Line of Sight (LOS)
Flying while watching the UAV and always keeping it within sight.

Notice to Airmen (NOTAM)
Published by the FAA, provides details of any changes or conditions at an airport or in any part of the airspace system that may affect flight operations. For sUAS operators, a NOTAM may include a temporary flight restriction (TFR) due to events such as major sports events or security events.

Octocopter
A rotorcraft with eight rotors.

Part 107
Shorthand for the portion of the US Code of Federal Regulations (14 USC Part 107) that regulates commercial use of UAS that weigh less than 55 lbs (25 kg); i.e., an sUAS.

Payload
The carrying capacity of an aircraft, usually measured in terms of weight.

Pilot in Command
A UAS operator (pilot) of an unmanned aircraft that is flying in a state of direct control (i.e., not in autonomous flight).

Quadcopter
A rotorcraft with four rotors

Section 333 Exemption
An exemption from a US requirement for an operator of an sUAS to have an airworthiness certificate to operate in US national airspace. This refers to a specific section of the FAA Modernization and Reform Act of 2012 that allowed operation of drones within US airspace prior to the implementation of Part 107. While most operators who have followed the requirements of Part 107 no longer have a need to apply for a Section 333 exemption, those operators who have an active Section 333 exemption may choose to continue to fly under that exemption until it expires. Additionally, there may be some situations when operators of UAS that weigh more than 55 lbs (25 kg) cannot operate under Part 107 and therefore may need to acquire or maintain a Section 333 exemption.

Small Unmanned Aircraft System (sUAS)
A small UAV, typically less than 55 lbs.

Telemetry
A highly automated communications process by which measurements are made and other data is collected at remote or inaccessible points and are transmitted to receiving equipment for monitoring.

Unmanned Aircraft System (UAS)
The unmanned aircraft together with its ground-based controller, and the system of communications connecting the two. This term was adopted by the Department of Defense (DoD) and FAA in 2005.

Unmanned Aerial Vehicle (UAV)
An aircraft with no pilot onboard. Also known as a drone.

Visual Observer
A UAS flight crewmember who assists the UAS pilot in the duties associated with collision avoidance. This includes, but is not limited to, avoidance of other traffic, airborne objects, clouds, obstructions, and terrain.

Waypoint
A reference point in physical space used for purposes of navigation.

Wing Span
The maximum distance from wingtip to wingtip.

ABBREVIATIONS, ACRONYMS, & INITIALISMS

ACS	Access Control System
ADS-B	Automatic Dependent Surveillance-Broadcast
AI	Artificial Intelligence
AGL	Above Ground Level
AOA	Air Operations Area
AOC	Airport Operations Center
API	Application Program Interface
ASP	Airport Security Program
ATC	Air Traffic Control
ATCT	Air Traffic Control Tower
BVLOS	Beyond Visual Line of Sight
C3	Command, Control, and Communication
CAD	Computer Aided Dispatch
CMS	Cloud Management Software
COA	Certificate of Authorization
CONOPS	Concept of Operations
COTS	Commercial Off-The-Shelf
COW	Certificate of Waiver
CTAF	Common Traffic Advisor Frequency
C-UAS	Counter-UAS
EO	Electro-Optical
IDS	Intrusion Detection System
IoT	Internet of Things
iPAMS	Integrated PIDS Alarm Management System
IR	Infrared
JSON	JavaScript Object Notation
LAANC	Low Altitude Authorization and Notification Capability

LiPo	Lithium Ion Polymer
LOS	Line of Sight
MSL	Mean Sea Level
NAS	National Airspace System
NOTAM	Notice to Airmen
NTSB	National Transportation Safety Board
PIDS	Perimeter Intrusion Detection System
PSIM	Physical Security Information Management
PTF	Perimeter Test Facility
RPIC	Remote Pilot in Command
SDK	Software Development Kit
SMS	Safety Management System
SOC	Security Operations Center
SRM	Safety Risk Management
sUAS	Small Unmanned Aircraft System
TFR	Temporary Flight Restriction
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UTM	Unmanned Aircraft System Traffic Management
VLOS	Visual Line of Sight
VMS	Video Management System
VTOL	Vertical Take-Off and Landing

SECTION 1. GUIDEBOOK OVERVIEW

1.1 Introduction

The UAS industry is changing rapidly, and the application of UAS in our daily lives is becoming almost commonplace. The amount of information available about using UAS for numerous applications is growing daily. While many airports have been proactive in engaging the public regarding notification requirements associated with UAS operations near airports, and the FAA has produced several informational notices regarding new and pending regulations, UAS use by airports is very limited. Few airports are utilizing UAS within their security programs. However, the use of UAS in such industries as film making and advertising provides great examples of success. Success in these industries primarily results from UAS operations that allow filming from points of view that could not otherwise have been accomplished without extreme expense. This type of cost-effective application is where UAS can be useful in airport security as well. Further, UAS use may reduce the need for human intervention in certain situations.

For airport owners and operators to have a better understanding of the possibilities, processes, and procedures involved in utilizing UAS, a consolidated source of information was identified as an industry need. To that end, this guidebook is intended to provide airport officials with the knowledge and tools necessary to determine if the use of UAS in their security program would be beneficial. This guidebook also provides information on the limits and best practices associated with UAS.

Given the need for efficient video-based perimeter monitoring and alarm response, airport security managers and planners are likely to utilize small UAS (sUAS; UAS that weigh less than 55 lbs) as a potential force multiplier in support of existing security systems. sUAS have a relatively low cost of entry, limited support requirements, and are versatile. This guidebook focuses primarily on sUAS applications and information, and all the Use Case Studies documented in this guidebook utilized sUAS. However, unless necessary for technical accuracy, the guidebook will herein refer only to UAS.

The interesting challenge with the use of UAS in airport security is how they may or may not be integrated, or what level of integration may be undertaken, with existing systems. Airports have significant investments in their security programs' systems such as CCTV, Video Management Systems (VMS), Access Control Systems (ACS), and PIDS. All of these systems require significant infrastructure and detailed operational protocols. To maximize UAS for airport security, integration with these systems is critical.

This guidebook explores these challenges and utilizes Use Case Studies in four different airport environments and under several different scenarios to determine the feasibility of integration into airport security systems. Of the four Use Case Studies conducted, the last one utilized a fence-mounted PIDS, which was installed and had undergone testing at the Safe Skies Perimeter Test Facility (PTF) adjacent to the McGhee Tyson Airport (TYS). This study utilized two types of unmanned aircraft systems (one autonomous and one tethered) from commercial vendors. The details of and findings from all of the Use Case Studies are provided herein along with lessons learned and ways to overcome challenges (see Appendices A and C).

1.1.1 Elements of the Guidebook

This guidebook is presented in five separate sections, all intended to allow the reader to utilize the content effectively and at their own pace. The following is a brief description of each section.

Section 2: provides an overview of UAS, including information regarding the wide range of UAS, their capabilities, limitations, and applications. Further, this section includes the required FAA approval processes and tools in order to operate UAS in an airport security environment.

Section 3: provides information regarding the integration of UAS with existing and emerging security systems already deployed at airports. The integration of UAS into existing systems is necessary in order to maximize their application and efficiency.

Section 4: provides information regarding the most current counter-UAS / UAS-detection technologies and how those might be applied in the airport environment.

Section 5: provides the results of the four Use Case Studies that demonstrated how UAS operating in the airport environment was not only viable but very valuable at the same time. This section also includes a summary of the lessons learned from the studies. Further, the last Use Case Study demonstrated that integration of UAS into existing systems was achievable and could be accomplished with limited resources.

Appendix A: Integration Use Case Study
Appendix B: Certificate of Authorization Application Example
Appendix C: Additional Use Case Documentation
Appendix D: sUAS SOP Template
Appendix E: UAS Operations Approval Tools

This guidebook is not all-inclusive. The UAS industry and regulations are continually evolving. Therefore, the contents of this document should be used only as guidance. The information contained herein is designed to assist in the planning and ultimately execution of integrating UAS into airport security. Many of the resources contained in this guidebook can be used immediately, while other documents are examples to be used to gain approval to operate UAS. Throughout this guidebook, points that are particularly valuable and information that can be directly used in the decision-making around UAS use are presented in a gray box. The reader should note, however, that these callouts should be taken as suggestions and not as specific directions.

SECTION 2. UNMANNED AIRCRAFT SYSTEM S OVERVIEW

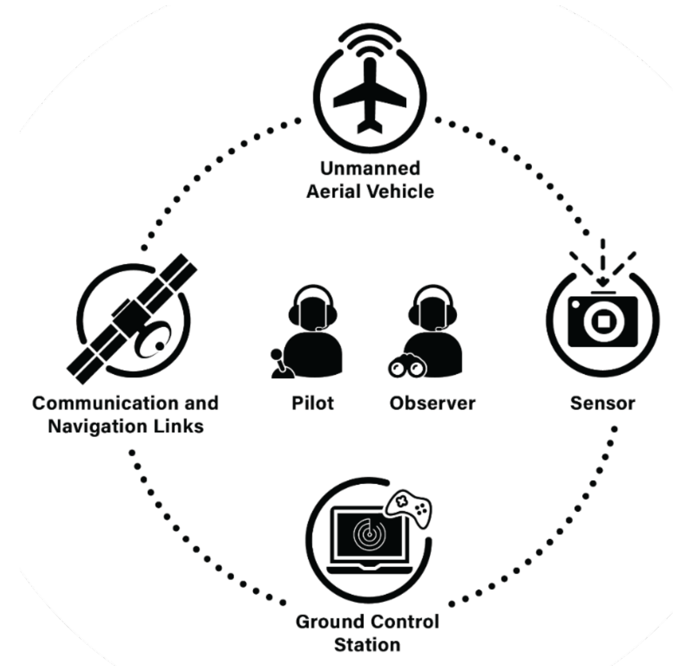
UAS contain all the necessary equipment to operate an unmanned aircraft. The most notable component of a UAS is the UAV. The difference between a UAS and a UAV is that UAS is inclusive of the entire system that enables the UAV itself to operate effectively. Given the potential confusion these acronyms may cause, for the purposes of this guidebook the use of the acronym UAV is minimized and may be referred to as vehicle or aircraft. A ground control station and communication system are typically the additional UAS components. Understanding each component of a UAS, along with the regulatory environment and supporting systems, is fundamental to successfully integrating UAS into an airport security environment.

In recent years, there has been a technology explosion of UAS/UAVs, resulting in an evolving and rapidly changing market. Thorough internal reviews should take place before purchasing a UAS to understand the scope of a complete UAS and data management program. The following sections outline the components of a UAS along with best practices and challenges when implementing a UAS program for airport security

UAS is a broad category that covers anything from large DoD systems like the MQ-4 Broad Area Maritime Surveillance (BAMS), which that has a wingspan of 114 feet and can stay airborne for 30 hours or longer, to the consumer-level micro UAS that fit in the palm of a hand. While this guidebook will briefly touch on some of the larger UAS that are rail-launched or that may use runways for launch and recovery, the primary focus is on sUAS.

The FAA defines a UAS as the unmanned aircraft and all the components required to safely and efficiently operate in the National Airspace System (NAS), and an sUAS as any UAS that weighs less than 55 lbs. Figure 2-1 depicts all the components needed to operate a UAS in the NAS. The only excepted requirement is the observer. While an observer is not actually required when not flying beyond the pilot's visual LOS, one is always recommended to be present to aid in the see-and-avoid requirement.

Figure 2-1. Diagram of Typical sUAS Components



2.1 Types of UAS (Existing and Emerging Technology)

There are generally three types of UAS available: fixed-wing, rotary-wing and multi-rotor (quad, hex or octocopter). Fixed-wing systems tend to have a longer overall endurance and therefore are capable of longer range and longer time airborne in its designated operating area, but they lack the ability to hover directly over a selected target area. Single rotary-wing systems (like a conventional helicopter) provide an increased endurance provided forward flight is maintained, but will rapidly lose any advantage if required to hover over a target. Multi-rotor systems are by far the most widely produced and operated aircraft. The major production lines for most sUAS manufacturers consist of multi-rotor UAS, which also generally cost less than their fixed-wing or single-rotor counterparts. Typically, multi-rotor UAS have shorter flight endurance times than either fixed-wing or single-rotor systems. Each type has advantages over the others depending upon the tasks needed. No single system can provide a solution for every task. It is recommended to match the right UAS to the specific task(s) as closely as possible.

2.1.1 Classes of UAS

UAS can be considered to fit into four general classes or categories: consumer, professional, commercial, and industrial/enterprise. These classes are presented here to assist the reader in determining the relative cost and level of effort required to implement and train personnel to basic proficiency, durability of the product, and level of manufacturer's support, as well as help categorize the various systems based on their ability to carry different sensors and perform tasks. While each system generally falls under a single class, grade, or category; a category may share characteristics with others.

Consumer-grade UAS typically have an integrated sensor, require little or no training to operate effectively, and generally are very affordable. Consumer-grade UAS can be purchased online or through a variety of retail outlets. Training for these systems can easily be accomplished using manufacturer-provided training material or through a peer-to-peer training system that leverages experience of those with UAS flying experience. This class would typically not be used by airport security or integrated into airport security systems.

> Consumer-grade UAS may have issues relative to the control and security of the data they collect.

Professional-grade platforms typically require some level of formal training and experience to gain a maximum level of pilot proficiency. These systems are more durable than the consumer grade. An in-house, standardized training program can provide the necessary level of competence needed to employ these systems effectively. This type of training can either be provided by the UAS manufacturer or by an organization that already uses the platform in question and is willing and able to provide the training. These platforms often have removable or interchangeable sensors, and their flight control systems provide greater levels of stability, allowing the user to produce higher quality images. This class of UAS offers an airport some entry-level capability for inspections but, as with the consumer class, may have issues relative to the control and security of data collected.

Commercial-grade platforms may require a higher level of training (as explained in the definition of Professional grade) and more experience than can be gained from just day-to-day flight operations to effectively employ them. These systems are more durable and have better manufacturer support than the Professional-grade UAS. Training for commercial platforms may be provided by the manufacturer, contracted to third-party companies, or can be accomplished through an in-house standardized training syllabus. The commercial class of UAS offers airports a hardened platform that can be routinely used by smaller airports in support of their airport security program.

Industrial/Enterprise-grade systems may have a more complex footprint that could potentially require a higher level of logistical and maintenance support. Compared to lower grade systems, Enterprise systems have better sensor integration, more feature sets, and the greatest level of overall system durability. Because of their complexity, these systems may require specialized training programs that involve in-depth classroom sessions, supervised practical flight operations, and specialized maintenance instruction. Practical training exercises are also recommended to hone the skills and gain the confidence necessary to operate and maintain these aircraft safely and efficiently, and also improve the performance of the operators. Enterprise-class UAS are typically available with docking base stations, and have sophisticated command-and-control software applications to support autonomous takeoff, landing, and flight. In some cases, the software can be used to configure multiple UAVs and their associated docking base stations to operate as a coordinated fleet. These UAS provide the highest level of secure systems integration between the UAS and existing airport security systems.

2.1.2 UAV Type Selection

There are numerous benefits and challenges associated with each type of UAV (see Table 2-1). Selecting the correct type of UAV is critical to UAS mission success and efficiency, as needs may vary depending on weather, terrain, and mission goals. Complete UAS programs may operate multiple types of UAVs.

Table 2-1. UAV Benefits and Challenges

UAV Type	Benefits	Challenges
Fixed-Wing	• Long range • High speeds	• Large landing area • High learning curve • Increased crash potential • Increased space required for turns
Multi-Rotor	• Vertical take-off/landing (VTOL) • Extensive camera control • Hover flight	• Short battery life/flight time • Small payload capacity

Multi-rotor UAVs can be tethered to the ground via a cable. Utilizing a tethered UAV mitigates risks associated with losing communication between the UAV and ground control station during night flying and challenging wind/weather conditions. Tethered UAVs also provide a fixed location, which Air Traffic Control (ATC) can monitor with confidence. Powered cables can also allow the multi-rotor UAV to stay airborne for long periods of time. Utilizing a tethered UAV decreases the area and speed a UAS can travel, limiting its uses and autonomous features. Tethered options should be explored for high-risk missions or missions in controlled airspace. Tethered UAVs are subject to the same restrictions as untethered UAVs.

Maintaining the UAV’s airworthiness is crucial to the safe operation of a UAS and includes scheduled and unscheduled maintenance, and updating hardware and software. Each UAV’s maintenance schedule and practice should be published in the CONOPS document (discussed further in Section 2.2). A CONOPS will serve as an airport’s specific operational guide tailored to UAS programs. These guidelines should be gathered from the manufacturer or, if not available, developed by the owner of the UAV.

2.1.3 Additional Components of a UAS

GROUND CONTROL STATIONS

Ground control stations are used to control a UAS and connect the flight-planning software to the UAV for autonomous flight. A ground control station is portable—typically a laptop or tablet (such as an Apple iPad) that has internet capabilities—allowing for it to be used in the field while a UAS is in the air.

During UAS missions, the pilot in command should have control of the ground control station. Visual observers may use data derived from ground control stations, such as battery life or altitude, to inform the pilot in command about any hazards or risks during flight. Before each flight, the ground control station connection to the UAV should be checked to help mitigate lost-link risks.

BASE STATIONS

Fixed UAS base stations provide a weatherproof shelter and charging station for the UAV, as well as communication links to the command-and-control infrastructure of the UAV. This allows the UAV to function autonomously, without the need for human involvement or intervention, making it ideal for continuous operation. Most UAS that incorporate a base station in their design have automated lid and precision landing mechanisms that allow the UAV to be deployed at strategic locations around the airport facility.

2.2 Flight Planning

Prior to flying any UAS mission, a flight plan must be developed. Flight-planning software is used to create automated flights for the UAV to collect data with predefined parameters, for both video and still imagery (see Table 2-2). Once a thorough field investigation of the proposed flight area has been completed, most of the UAS flight planning can be completed prior to traveling into the field for each flight. Before the start of each flight, the flight-planning software is to be reviewed and verified with current field conditions, weather, airspace advisories, and locations where non-participants may be.

Table 2-2. Flight Planning Information

Parameter	Definition/Effect
Altitude	• Determines how high the UAV will fly during data collection; FAA regulations govern altitude ceiling to be 400 feet above the tallest object • Directly affects resolution; higher altitude will result in lower resolution
Resolution	• The fidelity of video or the pixel resolution of a photograph • Overlap affects the amount of common area between two photos; higher overlaps result in denser models
Geofences	• Established areas where the UAV will not operate under any circumstance • Geofences are important to mitigate risk, particularly in controlled airspace

IN-FLIGHT

UAS software's inflight features are crucial to safe operation of a UAS. Inflight software gives the pilot in command critical information such as remaining battery capacity, real-time altitude and current GPS position, and live onboard camera feed. Inflight software or manual control can be used to make adjustments while the UAV is in the air or terminate a mission. Most UAVs will have automatic procedures if the connection between the ground control station/flight software is lost during flight. Generally, the UAV will return to home, autonomously returning to its take-off location, but this can be reconfigured.

LAUNCH/RECOVERY AREAS

Established UAS implementations have designated areas for launch and recovery operations. These areas are clearly defined and must always be clear. UAVs may sometimes not be able return to the launch area for a variety of reasons (mechanical/electrical, inclement weather, etc.) Also, in an implementation with multiple UAVs, the launch area cannot be collocated with the recovery area when moving the UAVs to maximize efficiency.

PAYLOAD

UAVs either have standard or interchangeable payload configurations, allowing for the UAV to be customized to each mission. UAV payloads can include color cameras, LIDAR, or thermal sensors.

Payloads affect not only the data acquired from the UAS but also the performance of the UAV, as the weight of a payload can affect the UAV's speed and endurance of the UAV. For higher endurance, a lighter payload is desired.

BATTERIES

UAV batteries can come in many forms but are most typically lithium ion polymer (LiPo) batteries. LiPo batteries are highly flammable and can be dangerous to the flight crew and/or the UAV. Fires can be caused by extreme temperatures, short circuits, damage, or a defect. Per the FAA's rules for sUAS (Part 107), the pilot in command should follow the manufacturer recommendations to ensure safe battery storage and handling.

Traveling or shipping UAV batteries can be challenging and costly. For example, the US Postal Service has placed several restrictions on mailing LiPo batteries, and currently will only mail "small consumer-type primary lithium cells or batteries" with a watt-hour (Wh) rating below 100 Wh per battery. Check with the airline or shipping carrier before planning to ship/travel with any LiPo batteries.

CONOPS

The CONOPS is a critical document that must be developed prior to the implementation of a UAS program. This document should outline all UAS mission activities and procedures and be made available organization-wide. The CONOPS should contain sections including, but not limited to:

- UAV operational procedures and checklists
- Airspace regulations
- Risk assessment matrix and mitigation tools
- Hardware and software system updates
- Maintenance schedules
- Training procedures
- Data processing and management guidelines

Due to the many safety hazards present while operating on an airfield, the CONOPS must be followed to standardize operations and maintain high safety standards. The CONOPS is a living document, and when updates are made each person working with UAS should be made aware of the changes. Many CONOPS documents will require signature upon receipt by an employee/UAS team member for accountability and to ensure that it has been read and its practices are accepted by crew members. Individual security-related missions should be documented separately as they are likely SSI.

UAS OPERATIONS

Having standard operating and safety procedures will aid in conducting successful UAS missions. A CONOPS should be developed and reviewed regularly to serve as the documented SOP. Safety is the number one priority of all UAS operations, and necessary precautions and measures must be taken for each flight. Each person working with the UAS mission should have adequate training and inclusion during mission development and operation.

2.3 FAA Regulations

The FAA has created numerous regulations to ensure the safe integration of UAS into the NAS. The Small Aircraft Rule, Part 107, covers commercial uses for UAV under 55 lbs. Also, individual states may have regulations/restrictions relating to the operation of UAS. All federal, state, and local regulations should be examined regularly to ensure compliance and safe operation of UAS.

UAS are always restricted within controlled Class B, C, and D airspace. Airports looking to utilize UAS in these airspace areas will need to go through a waiver/authorization process. There are multiple avenues for an airport to obtain a waiver/authorization; a review of how often UAS will be used should determine which form is best. See “Waivers/Authorizations” below.

According to the FAA, there are two options for government entities to fly sUAS (see Table 2-3). Also, refer to Appendix D for an sUAS SOP template.

Organizations can either opt to follow all rules of Part 107 or obtain a blanket public Certificate of Waiver or Authorization (COA). A COA is a form of authorization/waiver that follows a government organization rather than a specific mission. Obtaining a COA can be a lengthy process, though the option allows for greater flexibility for using UAS, as defined in each individual COA.

Table 2-3. Summary of FAA Regulatory Rules

Regulation	Rules
Part 107	• Permits flights in Class G airspace at or under 400 feet • Pilots must hold a Remote Pilot Certification • Cannot fly directly over people, over 100 mph, at night, or beyond visual line-of-sight
COA	• Permits flights in Class G airspace at or under 400 feet • Self-certification of the UAS pilot • Option to obtain emergency COAs under special circumstances

The largest difference between the two is that under Part 107 each pilot must hold a Remote Pilot Certification. COAs tend to be more flexible for public entities that wish to use UAS on an everyday or near-everyday basis. To obtain a COA, an in-depth safety and program review must take place, and an application must be submitted to the FAA for approval. The benefits and tradeoffs for each regulatory avenue should be reviewed extensively before selection as the two cannot be used simultaneously. Organizations looking to begin a UAS program may consider contracting with an organization that is well versed in the authorization/waiver processes to help standardize, expedite, and ensure the compliance of all regulatory requirements.

PART 107

The small unmanned aircraft rule governs all commercial UAS operations of a UAS under 55 lbs. Every pilot in command must hold a current Remote Pilot Certification from the FAA. To receive a Remote

Pilot Certification, one must be 16 years old, fluent in English, and pass the aeronautical knowledge exam. Below is the list of requirements, or "performance-based standards," that must be met under Part 107, as listed on the FAA website: https://www.faa.gov/uas/media/Part_107_Summary.pdf

- UAVs weighing more than 0.55 lbs and under 55 lbs must be registered via the FAADroneZone online application
- The UAV must always be within visual line-of-sight of the pilot in command
- No operation may take place over persons not directly participating in the flight
- Operations can take place in daylight and civil twilight (30 minutes before sunrise to 30 minutes after sunset) with appropriate anti-collision lighting.
- Operations must remain under 400 feet above ground and within 400 feet above a structure
- A pilot in command may only operate one UAV at a time
- The UAV groundspeed cannot exceed 100 mph
- No operations can take place from moving aircraft or moving vehicles, unless operation is over a sparsely populated area

Part 107 pilots in command can request a waiver for most operational restrictions and/or an airspace authorization to conduct UAS missions in controlled Class B, C, or D airspace. See the Waivers/Authorizations section below for more information.

WAIVERS/AUTHORIZATIONS

A mission that goes beyond certain listed requirements of Part 107 can be flown with the necessary permissions. Part 107 restrictions that can be waived are[1]:

- Operating from a moving vehicle or aircraft
- Daylight operation
- Following all visual observer requirements
- Operation of multiple UAS
- Yielding the right of way
- Operation over people
- Operation in certain airspace
- Operating limitations for small unmanned aircraft

Waivers and authorizations can be submitted online through the FAA Drone Zone portal[2] (Appendix E). The FAA strives to make a decision on submissions within 90 days. Organizations responding to emergency situations can get expedited approval through the Special Governmental Interest process.

Submitting a waiver/authorization is a lengthy process and requires an extensive look into an airport's internal safety and risk mitigation plans. Each submission should be detailed and shared with all stakeholders to ensure its compliance and scope. The waiver safety explanation field asks for a description of the proposed operation(s) and for the applicant to describe risks and mitigation methods.

[1] See https://www.faa.gov/uas/commercial_operators/part_107_waivers/
[2] See https://faadronezone.faa.gov

Risks will be different for each type of UAS, making it critical to know what specific system(s) the applicant will be using for the proposed mission.

The first step is to identify all risks associated with the airport's operation and specific UAV. Risks can include, but are not limited to, weather, obstacle strikes, non-participant interaction, lost-link with the GCS, and battery failure. All stakeholders should have input in formulating a list of risks to ensure no hazard is overlooked. Once all the risks are identified, steps should be taken to document and mitigate risk with avenues such as technology, communication protocols, and changes in flight parameters or UAS capabilities.

Operation will often have similar risks associated with it. For example, battery failure can happen anytime a UAV is flying, regardless of location or mission type. These types of risks and associated mitigation procedures can be standardized. Many risk-mitigation strategies should be outlined in the CONOPS to have consistent procedures and accelerate the waiver/authorization process.

Creating an operation-specific risk matrix helps to make informed decisions in the field. Risk matrices are used by the pilot in command before a flight to determine how safe an operation is to proceed. Given the value of all potential consequences, a set risk level should be used to determine whether the conditions are safe enough for flight. Table 2-4 and Figure 2-2 depict the FAA's standard risk matrix. Standard matrices should be placed in the CONOPS for UAS crew members to use.

LOW ALTITUDE AUTHORIZATION AND NOTIFICATION CAPABILITY (LAANC)

LAANC provides the first level of immediate airspace authorization. Remote pilot certification holders can submit airspace authorization requests and receive authorization close to real time in controlled airspace for flights below a designated altitude ceiling. Fourteen companies currently provide LAANC services. Some companies are integrating their LAANC program into the flight-planning software of their sUAS.

Typically, LAANC does not offer immediate authorization for UAS operations on a controlled airfield.

LAANC is set up with different zones laid out into "tiles"—predetermined area blocks around a controlled airport that have altitude ceilings for UAS operations that correspond to the level of risk and distance from an airport and its approach. When a request is submitted in an LAANC tile with a zero-altitude ceiling, which is typically found directly on and near an airfield, the submission gets automatically denied. LAANC does allow for an override process, initiated by the local ATC manager.

Overriding a denial from the LAANC program can only be done on a per-day basis. Receiving an LAANC-denial override can be time consuming and requires defined risk mitigations and extensive coordination with ATC.

To receive an LAANC-denial override, the tiles and coordination should take place more than one week before the desired operation date and time.

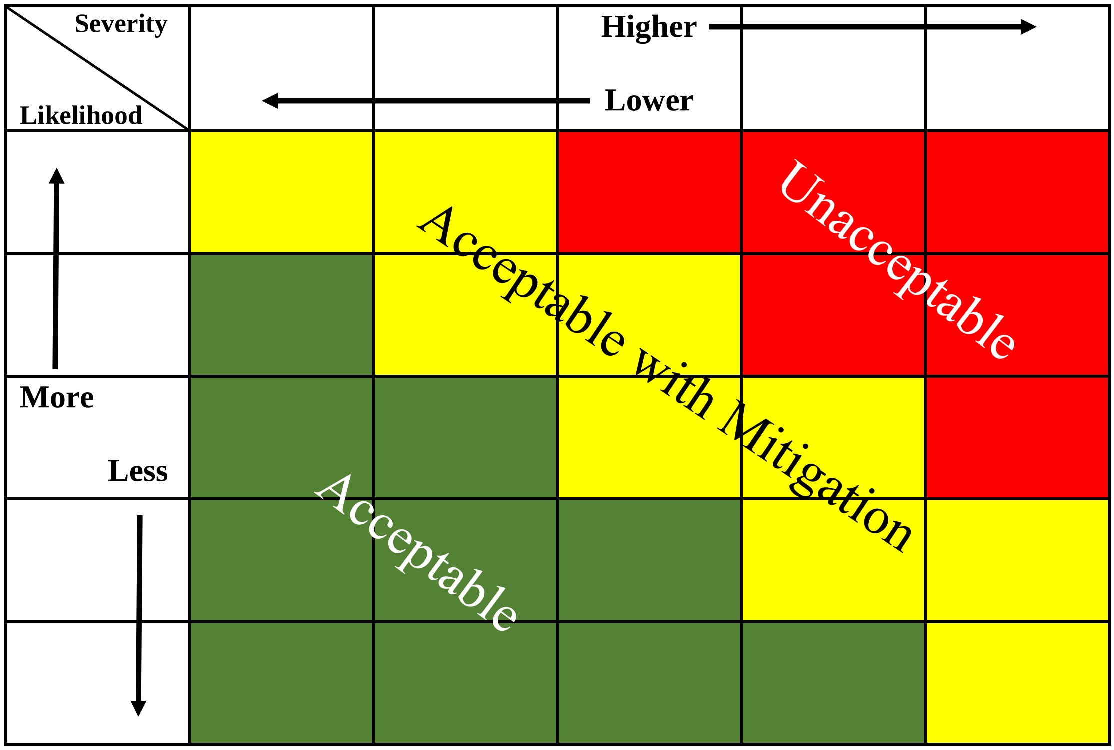
> While this program is useful for one-time or infrequent UAS users, airport looking implement security monitoring or emergency rapid response should not depend on LAANC-denial overrides as their form of authorization.

Table 2-4. Risk Definitions

Severity of Consequences			Likelihood of Occurrence		
Severity Level	**Definition**	**Value**	**Likelihood Level**	**Definition**	**Value**
Catastrophic	Equipment destroyed, multiple deaths.	5	**Frequent**	Likely to occur many times	5
Hazardous	Large reduction in safety margins, physical distress, or a workload such that crewmembers cannot be relied upon to perform their tasks accurately or completely. Serious injury or death. Major equipment damage.	4	**Occasional**	Likely to occur sometimes	4
Major	Significant reduction in safety margins, reduction in the ability of crewmembers to cope and adverse operating conditions as a result of an increase in workload, or as result of conditions impairing their efficiency. Serious incident. Injury to persons.	3	**Remote**	Unlikely, but possible to occur	3
Minor	Nuisance. Operating limitations. Use of emergency procedures. Minor incident.	2	**Improbable**	Very unlikely to occur	2
Negligible	Little consequence.	1	**Extremely Improbable**	Almost inconceivable that the event will occur	1

Source: FAA AC 107

Figure 2-2. Risk Matrix



Source: FAA AC 107

2.4 Common sUAS Manufacturers

The manufacturing base for sUAS is large and varied. A growing number of companies build capable aircraft in a variety of sizes, shapes, and configurations. As noted above, they are made available as commercial off-the-shelf (COTS) technologies, ranging from consumer grade systems to industrial level configurations with specialized custom aircraft or high-end systems with multiple capabilities. This list is not intended to be all inclusive, and while the list of sUAS manufacturers is large and growing, there are a few companies worth mentioning, for background and introduction, as they hold a large share of the market.

Shenzhen Dajiang Baiwang Technology Co., Ltd. (DJI) is one of the most prolific COTS UAS manufacturers today. They provide consumer-grade to commercial-grade systems that are used for anything from taking selfies, to inspecting infrastructure, to agricultural management. DJI systems have a high degree of interoperability with a wide array of mission planning and post-mission data processing software suites, such as UGCS and Pix4D respectively, making them useful for many applications.

A challenge to operating DJI systems in the airport environment is the aircraft have factory installed geofencing technology that prevents the UAS from being operated in an area that is classified as restricted by the FAA. On the surface, it appears that DJI is being forward-leaning and safety-minded, but the only way to fly in one of these areas is to petition DJI in China to grant what is called a Token. The Token will unlock the geofencing and allow operation in one of these restricted areas. DJI will provide the Token once they receive proof of the approved FAA waiver. Therefore, it is critical to ensure this step is part of the planning when operating a DJI UAS. However, even after following the unlock process, the Token often fails to work properly, and the pilot will have to spend time on the job site talking to the DJI service desk to correct the issue.

Yuneec International Co. Ltd. is another company that produces COTS sUAS for the consumer- and commercial-grade markets. Higher end Yuneec systems provide increased interoperability with proprietary software applications for mission planning and post-mission data processing as compared to the consumer end of their product line. These systems support a large range of sensors. Yuneec also has a factory-installed geofence; however, the process to remove the flight restrictions is simplified. To complete the Yuneec No-Fly unlock process, the user simply submits a form with the user and system information; the new software is then available to download and install. There is no need to submit approved FAA waivers to the manufacturer.

Parrot Drones SAS, the parent company of SenseFly, manufactures several sUAS for consumer and professional applications. Parrot systems are compatible with Pix4D software[3], and do not require any application or modification to operate in restricted areas. SenseFly manufactures UAS for commercial applications for the Parrot Group. Current UAS models available from SenseFly are compatible with Pix4D in addition to open source software; and the systems are used for numerous and varied imaging applications, from construction to infrastructure inspections.

SPECIALIZED INDUSTRIAL UAS

In addition to the sUAS that have a very small footprint and require little space from which to operate, there are systems with much larger footprints that could fill mission needs at some airports. Some of these systems, including some fixed-wing systems, need a larger area to operate, and may require large crews to fly and maintain all the associated equipment. Integrator and ScanEagle®, both produced by Insitu, a Boeing subsidiary, fit this sUAS description. These systems are currently in production and are deployed by private industry and government organizations.

ScanEagle falls within the FAA definition of an sUAS, but its performance characteristics exceed most other sUAS. They are well suited to missions that need persistent observation, but they require a significant amount of space to launch, recover, and maneuver when compared to commercially available multi-rotor systems.

[3] Pix4D is a Swiss company that develops a suite of software products that use photogrammetry and computer vision algorithms to transform RGB, thermal, and multispectral images into 3D maps and models.

AIRCRAFT CHARACTERISTICS

Table 2-5 provides a comparison of typical UAV characteristics. The table has been color-coded to aid the reader in identifying general physical sizes of UAV.

Table 2-5. Aircraft Characteristics

Model	Size	Weight	Payload	Endurance	Max Speed[4]	Launch	Recovery	Manufacturer
Beebop 2	N/A	1.2 lbs	EO[5]	25 min	35 mph	VTOL	VTOL	Parrot
Phantom 4	Diagonal 13.7 in	3.03 lbs	EO	30 min	45 mph	VTOL	VTOL	DJI
Typhoon H Plus	Diagonal 20.4 in	3.62 lbs[6]	EO	28 min	30 mph	VTOL	VTOL	Yuneec
Inspire 2	Diagonal 23.8 in	7.58 lbs	EO, IR[7]	27 min	58 mph	VTOL	VTOL	DJI
Typhoon H590	20.4 x 17.9 x 12.2 in	3.62 lbs[8]	EO, IR	28 min	38 mph	VTOL	VTOL	Yuneec
Albris	22 x 32 x 7 in	3.96 lbs	EO, IR	22 min	26 mph	VTOL	VTOL	SenseFly
eBee	37.8 in	1.52 lbs	EO, IR, Multispectral	50 min	56 mph	Hand	Belly Skid	SenseFly
Matrice 210	35.9 x 34.6 x 14.9 in	13.53 lbs	EO, IR	24 min	51 mph	VTOL	VTOL	DJI
Tornado H920 Plus	Diagonal 36.2 in	N/A	EO, IR	24 min	24 mph	VTOL	VTOL	Yuneec
FireFLY6 PRO	32.6 x 60 in	8.4–9.9 lbs	EO, IR, Multispectral	59 min	40 mph	VTOL	VTOL	BirdsEyeView Aerobotics
Integrator™	8.2 x 16 ft	40 lbs	EO, IR	24+ hrs	103 mph	Launcher	SKyHook®	Insitu
Prion	12.4 x 9.8 ft	59.5 lbs[9]	LIDAR, EO, Hyperspectral, Aeromagnetometry	N/A	49 mph	Launcher	Runway	UAVE
ScanEagle®	5.3 x 10.2 ft	35.3 lbs	EO, IR	24+ hr	69 mph	Launcher	SkyHook®	Insitu

[4] All speeds have been converted to standard measurements and rounded to the nearest whole number
[5] **EO:** Electro-Optical
[6] Weight without sensor
[7] **IR:** Infrared
[8] Weight with battery
[9] Weight is based on the aircraft in a survey configuration

2.5 Functional Components of UAS

UAS SOFTWARE

UAS software is necessary to successfully plan and fly missions, and mitigate risk. Many UAV manufacturers will create hardware specific to a flight planning/data acquisition software. There are also numerous third-party software platforms that are compatible with multiple UAS. When selecting a software, it is important to determine whether the airport wants to plan, collect, and process data within a single software or differentiate each process.

FLIGHT CONTROL

COTS systems come with integrated hardware and software designed to support flight control and sensor control on the aircraft. These software applications are often designed to be downloaded to a handheld device or tablet, and are usually supported by both iOS and Android operating systems. The software internal to the UAS provides command and control of the aircraft as well as its associated sub-systems (payload/sensor, autopilot, navigation, etc.), and is often subject to proprietary restrictions. Some autopilot systems, like Pixhawk®, allow for end-user software editing and development via open source code; this requires knowledge of computer programming techniques.

MISSION PLANNING SOFTWARE

Some COTS manufacturers produce UAS that are compatible with mission planning software suites developed by third parties such as Pix4DCapture. These mission planning applications allow the operator to create and execute detailed mission routes to optimize the performance and efficiency of each flight.

Many enterprise-class UAS manufacturers provide purpose-built command-and-control software that supports not only the mission planning functions, but also provides for specific interfaces to the unique characteristics of the UAS, its payload, and base station(s) to allow for autonomous takeoff, landing, and complex alarm response and/or patrol missions. Typically, these software packages provide for Application Program Interfaces (API) to enable integration with the airport's VMS and alarm management platforms, such as PSIM systems.

UAS mission planning support software can enhance system use in the airport environment. Whether the software is produced by the manufacturer or by a third party, such suites employed prior to mission planning are essential to providing efficient and safe flight routes. Some mission planning software allows the user to preset and save specific mission profiles, saving the user time during a reactive response scenario by having preset and designated profiles available based on the location of the required response. This capability allows first responders and airport personnel to coordinate a general response situation with preplanned UAS actions, which other stakeholders can anticipate, thus reducing confusion and enhancing response performance. Ultimately, the software used for mission planning will need to meet the requirements of the operating organization that is documented in the CONOPS.

POST-MISSION PROCESSING

A large selection of software suites for post-mission data and imagery processing is readily available to any UAS operator. A cursory search on the internet will reveal a vast array of software suites available, from open source applications with no associated fees to subscription services that can cost more than $5,000 per subscription. Processing suites can represent significant upfront or recurring costs; thus, it is important to understand what capabilities are required to ensure the most appropriate software suite is acquired. For airport security applications, software that can create 3D images, point clouds, and elevation and terrain maps and models are likely not required; basic still-image and video processing should suffice.

DATA AND DATA STORAGE (LOCAL/TRANSMITTED/ENCRYPTION)

The most common and usable form of data acquired by airport UAS assets will be visual data in the form of still images and video. Such imagery is typically captured by either an electro-optical or infrared sensor. Current sensors carried onboard UAS can collect large volumes of information in very short periods of time, making data storage and transmission challenging.

An important consideration when researching UAS acquisition or operational use is the amount of local data storage available. The storage capacity of the aircraft can vary depending on the manufacturer. Some systems can accept a microSD card while others have a fixed storage capacity integrated into the system hardware.

Developing a data acquisition plan can streamline and enhance collection and storage. Such a plan does not need to be complicated nor in-depth, but should highlight the specific information to be collected during the mission. The plan can be as simple as setting parameters that should be met prior to recording video, such as “video should only be collected when a suspect target is in view, being pursued, or when within 500 meters of a target observation area.” For still-image collection, target areas should be identified in the sequence in which they will be approached during the mission, and the specific types of images that are required for mission success. The data acquisition plan should be documented in the CONOPS.

Another factor impacting data storage requirements is the resolution of images and video captured. High resolution video and still images will require more memory and therefore may reduce the number of images or amount of video that can be collected. It may be necessary to establish a cap on the resolution to be used during any given mission by prioritizing the need for quality of resolution versus the volume of imagery anticipated.

> Developing a data acquisition plan may appear unnecessary and simplistic, but such a strategy may prevent collecting too much data, which would then require excessive amounts of time during the post-mission phase sorting through video and images to identify the footage needed. Plan development also can minimize the risk of spending too much time over a single target area and exhausting the UAS power supply prematurely.

Some systems allow for video to be recorded directly to the UAS controller or mobile device. While this capability may work perfectly well for certain mission requirements, the transmission of imagery may result in lower quality video or still images due to loss of fidelity during transmission from the aircraft to the receiving station.

UAS-TO-UAS COMMUNICATION

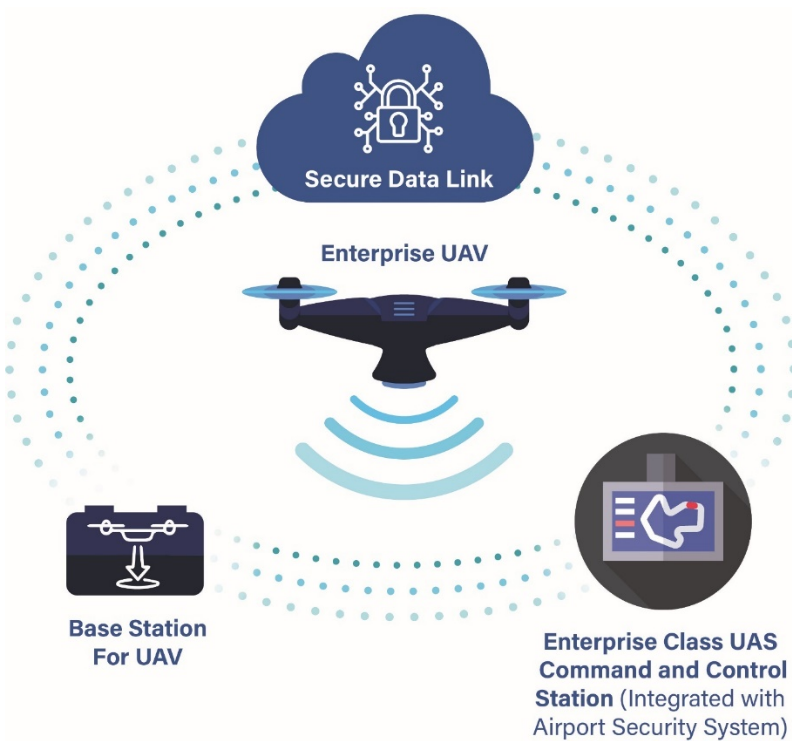
UAS-to-UAS communication and datalinks are in the early stages of development at the time of this guidebook publication. This type of capability is typically seen in UAS Traffic Management (UTM) visions, which use intercommunications to maintain aircraft proximities from other UAS and manned aircraft in the low-altitude airspace, and allow individual UAS to execute specific tasks while minimizing the risk of aircraft collisions. Some enterprise-level UAS also have the ability to intercommunicate to enable mission handoffs (ex., when multiple UAS have been deployed at a site to form a UAS fleet). This evolving technology also minimizes inputs from a human controller, thus allowing pilots and observers to concentrate on the information the UAS is providing.

2.6 Integration with Airport Security Systems

The value of UAS in the airport security environment will be maximized when a video and/or sensor downlink from the aircraft is fed into the VMS so it can be used by airport security personnel as well as other key stakeholders, such as the Security Command Center, and potentially the Airport Operations Center (AOC) and/or Emergency Operations Center (EOC) through a secure airport Wi-Fi or cellular network.

One approach to achieve this capability is to use software apps produced by the UAS manufacturer for wireless mobile devices that allow the user to connect remotely to the UAS video downlink. A review of enterprise-level UAS reveals that these manufacturers have purposefully built secure communications links to allow airports to integrate their UAS command-and-control applications with security alarm monitoring, VMSs, and PSIMs and/or situational awareness platforms (see Figure 2-3). This allows real-time viewing of UAS imagery by airport security personnel. It also allows users to switch between the UAS video feed and the surveillance camera video feed, thus having the UAS serve as an additional, mobile security camera in the airport system.

Figure 2-3. Secure UAS Sensor and Data Downlink



2.6.1 UAS Base Station Systems and Configurations

A base station system is a fully self-contained UAS system that can be used to perform virtually any mission that a conventional UAS can perform. Base station systems can be operated autonomously or manually, pre-positioned temporarily to reduce response time, and installed permanently around the airport perimeter. Users of these systems currently must meet or receive waivers to regulatory requirements for commercial UAS operations. (See Appendix A for the integrated Use Case Study discussion for autonomous base station-based deployment). It should be that noted many of these systems can be configured to support multiple base stations that can be configured to communicate together to form a network of UAVs to support the perimeter.

When these systems are deployed to remote areas of an airport, waivers to the requirement to maintain visual line of sight between the pilot and the aircraft, or the observer and the aircraft, may be necessary to fully realize system advantages.

UAS STORAGE

Base station systems are self-contained and therefore stored in weatherproof, water-resistant boxes that open when directed by a human controller, or upon a pre-programmed schedule, allowing the aircraft to take off from and land on a level surface that is protected from the elements.

POWER AND CHARGING SYSTEMS

The power requirements for base station systems vary by manufacturer, but most are designed to be connected to the existing power grid and are equipped with a backup power supply. Some systems are designed to be operated off-grid using a solar power supply.

DATA SYSTEMS

Base station UAS can provide direct, real-time surveillance, or the data can be uploaded to a network after the mission has been completed. Some systems have an autonomous cueing and notification capability, providing another means of alerting security personnel to an intrusion.

2.6.2 UAS Data, Data Storage, IoT, and Cybersecurity

The Internet of Things (IoT) refers to the network of physical objects with embedded sensors, controllers, and electronics that enables those objects to exchange data with each other, vendors, operators, and other connected devices.

The UAV has an onboard network of sensors, controllers, and network devices that share data related to operations and the mission. A UAS is, in systems engineering terms, a “system of systems” consisting of the aircraft, the ground station, the GPS satellite(s), the communication infrastructure, and the personnel.

Security issues include Data Security, Interception Prevention, and Hostile Takeover. Data Privacy is also a concern. A common theme between UAS and other IoT-enabled services is that they leverage and rely on wireless solutions for either command-and-control or real-time sensor-data management and transfer. When considering implementation of a UAS, it is assumed that the data service model includes virtualization and cloud infrastructures that will be leveraged to provide flexibility, scalability, and the ability to deliver richer services quickly with high reliability. All aspects of these systems must be secured and maintain information assurance, as data is constantly transmitted in the form of information and commands. Data security should be documented in the CONOPS.

> UAS cybersecurity should be included in any data acquisition and storage plan. Airport security departments should consider the UAS and its associate sensors as any other connected device, and should partner with their IT departments to help develop connectivity, data acquisition, and data storage plans. UAS security measures should include restricted access to data through encryption, user-authentication methodologies, and anti-spoofing technologies.

2.6.3 Airport Security Operations – Autonomous and Manual Deployment

UAS are well suited for several airport security and support operations. Their ability to collect real time visual data from long distances means they can provide enhanced situational awareness of potential threats or hazardous situations while providing a safe standoff.

The ability to deploy systems in an autonomous mode means that UAS could be used to conduct surveillance missions, such as perimeter patrols, without the direct intervention of a human, thereby freeing personnel to respond to incidents in other locations. A current barrier to operating autonomously is the regulatory environment. Under current regulations, a UAS must have a certified remote pilot in command (RPIC) who can take positive control of the UAS; if the UAS is flown beyond the VLOS of the RPIC, there must be an observer able to maintain visual contact with the aircraft and positive communication with the RPIC. With these regulations in place and without a waiver from the FAA, autonomous operations are currently not practical. While this requires additional staff to serve as observers if the flight area is beyond what a single individual can reasonably see, which increases the cost of UAS operations over a large area, it is anticipated that changes to the regulatory environment are possible. To that end, many enterprise UAS manufacturers have developed the command-and-control software capability for autonomous operations, allowing real time analytics and fully autonomous cycles, including conducting takeoff, navigation, and landing. Please see Appendix A for examples of this from the case studies.

It is also possible to get authorization to obtain a BVLOS FAA Part 107 waiver. The general steps are as follows (Antonelli 2017):

1. Develop a CONOPS and risk assessment
2. Gather test data either overseas or at an FAA test site. Alternatively, participate in the FAA Pathfinder Program.
3. Draft the actual BVLOS waiver request under Part 107, specifically Parts 107.31, 107.200, and 107.205.

Currently, the most practical means of control is VLOS, where the RPIC provides input to the UAS flight controls while maintaining VLOS. VLOS flight does not preclude the use of autonomous or semi-autonomous operations, such as preprogrammed flight routes; it simply means that while the UAS is in these modes, the RPIC and observer, if used, must be able to maintain visual contact and take positive control of the aircraft if required. In most scenarios, equipping the security force with UAS in the patrol vehicles would greatly enhance their ability to put a UAV over a target area to reduce response times.

PERIMETER PATROLS

Perimeter patrols are an active, preventative security measure requiring at least one person to walk or drive along a secure fence line or designated landmarks surrounding a location to dissuade an adversary or intruder from entering the area, and to identify breaches in secure perimeters. Perimeter patrols are typically conducted on a random basis and usually cover the entire perimeter during a given period. At large airports, a patrol may take several hours to complete using a typical vehicle. By using a UAS, the security force can cover large areas of the perimeter from a single location, reducing the time needed to complete an inspection, especially in situations when a foot patrol would typically be required. UAS also provide a platform for target acquisition and tracking in much the same way a guard or sentry would.

RESPONSE TO PERIMETER INTRUSION ALARMS – TARGET ACQUISITION AND TRACKING

During a response to an alarm, UAS can provide real time verification of a perimeter breach, target acquisition, and tracking of the target, and recognition as to whether it is animal or human. The UAS in these situations may allow for a more rapid response, providing the ability to travel in a direct line to the area where the intrusion is detected, reducing response time, and providing much-needed situational awareness to the security force.

RESPONSE TO VEHICLE GATE ACCESS CONTROL ALARMS – TARGET ACQUISITION AND TRACKING

UAS can provide real time target acquisition and tracking in response to a Vehicle Gate Access Control alarm. The UAV in these situations may allow for a more rapid response by being able to fly in a direct line to the area where the intrusion was detected, reducing response time and enhancing situational awareness for the security force.

EMERGENCY INCIDENT RESPONSE – REAL TIME SITUATIONAL AWARENESS

UAS are also coming to the forefront of emergency response. UAS are uniquely suited to deploy to dangerous situations in advance of emergency personnel to provide situational awareness. The systems can aid in identifying hazards at the incident site, or providing the response team with the safest approach guidance without compromising the safety of responders.

REMOTE AREA SURVEILLANCE – TARGET ACQUISITION AND TRACKING

Remote areas on airports are vulnerable to intrusion even if they are difficult for security personnel to access. Surveillance of these areas will likely be preventative in nature, but UAS will allow security personnel to develop a well-defined plan for dealing with intrusions into these areas, and a defined picture of any intrusion incident to enhance situational awareness.

> Appendix A provides and in-depth review of UAS integrated with airport security systems

2.6.4 Unmanned Aircraft System Traffic Management

Integration of UAS discussions with the FAA may lead to a conversation on the Integration of Civil UAS in the NAS. A link to the FAA roadmap available at the time of publication of this guidance is provided below for informational purposes.

Additionally, no discussion on integration of UAS can be complete without a brief discussion on UAS Traffic Management (UTM). UTM is how airspace will be managed to enable multiple UAS operations conducted BVLOS, where air traffic services are not provided.

UTM is essentially a traffic management system for uncontrolled operations that is separate from, but complementary to, the FAA's Air Traffic Management system. UTM development will ultimately identify services, roles and responsibilities, information architecture, data exchange protocols, software functions, infrastructure, and performance requirements for enabling the management of low-altitude uncontrolled UAV operations (see Figure 2-4).

Additional information on UTM can be found at the following link: https://www.faa.gov/uas/research_development/traffic_management/

Additional information on integration of civil UAS in the NAS roadmap can be found at: https://www.faa.gov/uas/resources/policy_library/media/Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf

Figure 2-4. A Vision of UTM

Source: NASA (https://utm.arc.nasa.gov/index.shtml)

SECTION 3. UAS INTEGRATION CONSIDERATIONS

3.1 Emerging Technology

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial Intelligence (AI) is the emerging computer technology field that develops computing techniques to simulate the workings of the human brain. This field of study is developing technologies that allow machines to learn from experience (i.e., machine learning), and thus complete increasingly complicated tasks. AI is used in object recognition, facial recognition, and in voice recognition software for things like talk-to-text applications. These technologies are used today in airport security systems and will enhance the capabilities that UAS bring to the field.

Computer vision is theory and technology for retrieving information from images or dimensional space, which can enable robotic systems to navigate through a real environment without human input. Such technologies would enhance the UAS ability to navigate more effectively and efficiently without pilot input.

OBJECT RECOGNITION AND TRACKING

Object recognition is a subset of computer vision, which itself is a subset of machine learning. With this technology, a computer is trained over time to recognize variations in pixels. The more times the computer analyzes images of a specific object, the higher its accuracy in identifying the object, and the greater its reliability of tracking the object. By incorporating such technologies with UAS, images provided from a UAS can be analyzed in real time, thus producing significant time savings as well as a means for automated tracking of threats.

3.2 Safety

SAFETY ANALYSIS AND CONSIDERATIONS

Perhaps the most complicated issue in the integration of UAS into the NAS is how to ensure separation between UAS and manned aircraft. This issue is relevant to the use of UAS in support of airport security in that this mission puts UAS operations within the boundaries of airport property. The initial approach to managing UAS and manned aircraft operations was to separate, segregate, and, if needed, eliminate UAS operations in and around manned aircraft. This model was effective in reducing the likelihood of a collision between the two types of aircraft, but it neglected the inevitability of the emerging mass arrival of UAS in the commercial market place in August 2016.

August 2016 changed the way in which UAS could be viewed when the FAA created a path for commercial sUAS operators to become certificated Remote Pilots under 14 CFR Part 107. Since then, the technology has proliferated significantly, demanding that these aircraft be considered when discussing aviation and airport safety.

At the time of this guidebook’s publication, the FAA had yet to finalize the rule requiring airports to develop and implement a Safety Management System (SMS). That said, the processes involved in proactively managing safety can greatly enhance the success of introducing UAS as a supporting technology for the airport security program.

The most important operational component of the SMS is Safety Risk Management (SRM). SRM is the disciplined application of a defined process to identify, analyze, and control the risk posed by safety hazards. The FAA requires that certain airports formally apply the SRM process in what is known as a Risk Assessment whenever a change to the airport system of procedures is considered. Introducing UAS into the airport environment will present new safety hazards to operations, and would be a change to the airport system; thus, conducting one or more Risk Assessments to devise appropriate risk mitigations is appropriate.

A Risk Assessment is a formal application of the SRM process by which the system is described, hazards are identified, risks are analyzed and assessed, and mitigations are developed, making SRM critical in addressing UAS operational risks. The Risk Assessment will provide the opportunity to effectively identify and develop mitigation strategies for not only the additional risks that UAS bring to an airport, but will provide the means to identify the hazards and risks that the complex infrastructure and operations of an airport present to UAS operations.

A Risk Assessment could explore the overall impacts of UAS introduction into the airport's operations, including identifying the hazards created from the ramp areas to the runway environment, or it could focus on proposed limited uses of UAS, such as identifying the impacts if UAS use is limited to one side of the primary runway. Either way, before the UAS are deployed, airport stakeholders should be convened to consider the associated hazards and proactively plan ways to control the risks to normal airport operations.

3.2.1 Risk Management

FAA RISK MANAGEMENT TOOLS: (COMMON IDENTIFIED HAZARDS ASSOCIATED WITH UAS OPERATING ON OR NEAR AIRPORTS)

Every airport is different (airport layouts, the daily flow of air traffic, the proximity to populated areas, etc.), so there may be hazards unique to an individual airport. However, some hazards associated with UAS will be common to all airports and should be addressed prior to each operation, and further reviewed if any significant changes occur to the airport's layout or infrastructure. Some of these common hazards are:

- Manned Aircraft – The presence of other aircraft in the local pattern below the 400-foot maximum altitude restriction for UAS flight creates the potential for collisions at the approach and departure ends of the runway.
- Airport Personnel – The number of people working at the airport increases the likelihood that the UAS will inadvertently overfly personnel, presenting a higher risk of UAS-to-person contact.
- RF Spectrum Interference – The extensive frequency usage and the large Wi-Fi networks at some airports increases the chances for RF spectrum interference that will impact the ability to communicate with the UAS or other Wi-Fi-enabled devices.
- Vertical Obstructions – While obstructions in the airport environment are controlled to minimize the risk to manned aircraft, the fact that UAS fly at very low altitudes make any vertical obstruction a hazard to UAS flight. Obstructions such as the ATCT, and radio and microwave antennas can present significant risks, especially if they are supported by guy wires.
- Jet Blast and Prop Wash – High velocity exhaust from jet engines and wind created by propellers can cause unstable flight conditions, resulting in the loss of control of the UAS.
- Wildlife – Wildlife, particularly birds, are ever present hazards to UAS flight.
- Environmental Conditions – High temperatures, high humidity, high winds, and precipitation adversely impact the performance of the UAS, making safe operations more challenging.

The list of common hazards is a double-sided coin. While this list is presented in a way that addresses the risk to UAS operations, the UAS is a hazard in some of these categories as well. As examples, manned aircraft are a hazard to the UAS and vice versa; or a UAS colliding with an antenna could destroy the drone, but the drone could also damage the antenna, thus disrupting airport communications. Hazards and their associated risks need to be assessed from the perspectives of both the UAS operator and the airport operations. A section on SRM should be included in the CONOPS.

3.3 UAS Research

This section is a synopsis from the literature review and guidance regarding where and how further information can be obtained.

The UAS is a highly diversified technology, spanning from smaller consumer-based civilian applications to the 32,250-lb RQ-4 Global Hawk. Among the many platforms and applicable uses, the introduction of the UAS to the airport environment has sparked industry research to better develop safe integration strategies. Organizations like the ACRP, FAA, Airports Council International-North America, and National Safe Skies Alliance are currently engaged in initiatives to define NAS regulations and integrations for commercial UAS purposes, public purposes, and recreational use. The purpose of this guidebook is to identify practical avenues for UAS applications in airport operations and security environments. The following content should be used to assist airports in gaining understanding of UAS and its potential uses, and safely integrating UAS into the NAS.

According to the ACRP's document, "Unmanned Aircraft Systems at Airports: A Primer," there are a few key considerations that airport stakeholders will need to address for UAS integration (Table 3-1). In addition to those listed, further operational considerations may include the number of operations projected, types of UAS systems expected, and number/type of facilities needed to meet UAS operational requirements are among the topical areas that need to be considered. Should an airport operator want to attract UAS operations as an additional source of business and revenue, an inventory of facilities should be collected and used to market to UAS operators.

Table 3-1. Airport UAS Preparation Checklist

Airport Action	Benefits to the Airport
Engage with a UAS National Test Site	Test sites have available segregated airspace; COAs in place; potential research requirements for airports.
Engage with Area Universities	Multiple universities offer UAS related courses; multiple universities conduct UAS research; universities are partnered with national UAS test sites and Center of Excellence proposal teams.
Contact State Government	Departments of Aviation; Commerce, Agriculture and Forestry; Mines, Minerals, and Energy; state police may be potential advocates for UAS business at airports.
Attend UAS Conferences and Seminars	Conferences and seminars on aspects of the UAS industry are conducted regularly to network and become informed on upcoming technologies.
Investigate Complementary UAS Businesses	Research UAS businesses that could be supported by the airport or by the local economy.
Determine UAS Facility/Infrastructure Requirements	Inventory airport facilities and infrastructure that could be used by UAS operators for marketing purposes.
Contact the FAA	FAA Office of Airports (ARP) and FAA UAS Integration Office (AFS-80) can inform and offer direction to interested airports.

Source: ACRP "Unmanned Aircraft Systems (UAS) at Airports: A Primer"

These considerations will vary depending on the airport's needs and strategic vision. Some smaller UAS require less infrastructure and can take off via a handheld operator or by truck. Like a manned aircraft, the larger UAS may require runway clearance and hangar space, thus making it very important for planning and operations to understand the types of systems being introduced into the airport environment.

Within the airport vicinity, it is crucial that the system operations of a given UAS are communicated to the FAA and ATC. An operational plan for UAS is used to address several issues, including the process for initiating, developing, and maintaining the unmanned aircraft system; required resources (human, infrastructure, and regulatory); potential threats posed by UAS flight; and emergency plans. To ensure the most significant factors are considered, the airport should evaluate the operational environment, stakeholder coordination, flight planning, and execution within regulatory guidance at it relates to UAS operation.

According to the FAA Small UAS Rule (Part 107), unmanned aircraft weighing less than 55 lbs must remain within VLOS and are limited to daylight operations, with exception to civil twilight clearance if the aircraft is equipped with appropriate anti-collision lighting. The UAS must yield right of way to other aircraft and shall not exceed a maximum groundspeed of 100 mph.

ADDITIONAL RESEARCH AND TEST SITE SUMMARIES

The aviation-related research conducted for this guidebook concludes that a wide sampling of resources address UAS and guidance for use around airports. The review showed that there is a growing body of literature relating to the various applications of UAS, and the regulations in place and those planned for the future will ensure the safety of UAS operations in the NAS. However, no current reference material exists on the application of UAS to support airport security initiatives.

The information documented from the review introduces the aviation industry to the advancements in the UAS industry. These aircraft are being integrated into the NAS in a slow and methodical way. This is a disruptive technology that is expanding at a very rapid rate; thus, the literature is being updated constantly, and users of this technology should make efforts to improve their own understanding as the information becomes available.

The research can be divided into two categories: introductory information for the industry and regulatory references from the FAA. The introductory information discussed how larger UAS can be operated from airport facilities, the considerations regarding sUAS that operate on or near airports, and articles and reports about the future of UAS in the industry.

The FAA has issued several references relating to UAS, particularly sUAS, such as the recently published rule for sUAS operations (14 CFR Part 107), a study guide for small remote pilots, and articles on airspace restrictions for UAS. The FAA is exploring the use of UAS on airports for various purposes through numerous projects, such as one performed at Atlanta Hartsfield International Airport to survey runway pavement conditions.

In addition to the published resources on UAS, the research team contacted the seven FAA-designated UAS National Test Sites and the FAA-designated ASSURE UAS Center of Excellence to determine whether any of the sites were conducting or planning to conduct research of UAS applications for airport security. Though none of the sites are conducting or planning to conduct such research, the ASSURE Alliance and specifically Mississippi State University are exploring methods and techniques for detecting and identifying UAS that are approaching an airport—research that in many ways crosses over with the tasks of this project. The following is a summary of each site's focus at the time of the survey.

ASSURE UAS Center of Excellence

Most of the ASSURE efforts are related to exploring US integration into the NAS for different applications that put UAS in the same airspace as other manned aircraft. ASSURE is also supporting the work discussed under the New Mexico State University test site.

New Mexico State University – Unmanned Aircraft Systems Flight Test Center (UAS FTC)

The New Mexico UAS FTC is engaged with the ASSURE UAS Center of Excellence in researching technologies and techniques to detect UAS. This research crosses over with the scope of this guidebook, as UAS could intrude in the airspace or property controlled by an airport.

New York Griffiss UAS Test Site – Northeast UAS Airspace Integration Research (NUAIR) Alliance

The NUAIR Alliance is the only airport-based test site, and airport security is an area that they might consider for a potential future test. They did recently complete a test where they conducted airport surveys using UAS.

North Dakota Department of Commerce – Northern Plains UAS Test Site

The Northern Plains UAS Test Site has experience integrating UAS into public-use airports. A specific example is that they operate an Elbit Hermes 450 (about a 1,000-lb UAS) from a public use airport in North Dakota.

Pan-Pacific UAS Test Range Complex – University of Alaska Fairbanks

The primary research being conducted at the Pan-Pacific Test Site is associated with infrastructure inspections and environmental monitoring.

State of Nevada UAS Test Site – Nevada Institute for Autonomous Systems (NIAS)

NIAS recommends unmanned aviation lessons learned to the FAA and NASA.

Texas A&M University Corpus Christi – Lone Star UAS Center (LSUASC) of Excellence and Innovation

The LSUASC provides the FAA with information regarding overall UAS safety, airworthiness, command and control link issues, control station layout and certification (human factors), ground and airborne detect-and-avoid technologies, and environmental impacts of UAS operations.

Virginia Tech University – Mid-Atlantic Aviation Partnership

Mid-Atlantic has research projects in progress with industry partners exploring beyond-line-of-sight operations in the inspection and monitoring of infrastructure such as electric power line inspection.

SECTION 4. COUNTER-UAS TECHNOLOGY FOR AIRPORT SECURITY

COUNTER-DRONE TECHNOLOGY

Counter-drone technology (C-UAS) can detect, localize, track and/or interact with rogue UAS in many ways that range from alerting and initializing security and safety measures to activating some form of defense to the threat. However, it also presents a window into the potential harm these same C-UAS could cause. Consumer drones are inexpensive and modifications are easy to make. Therefore, UAS operations around airports, with ill intentions or not, can occur very easily.

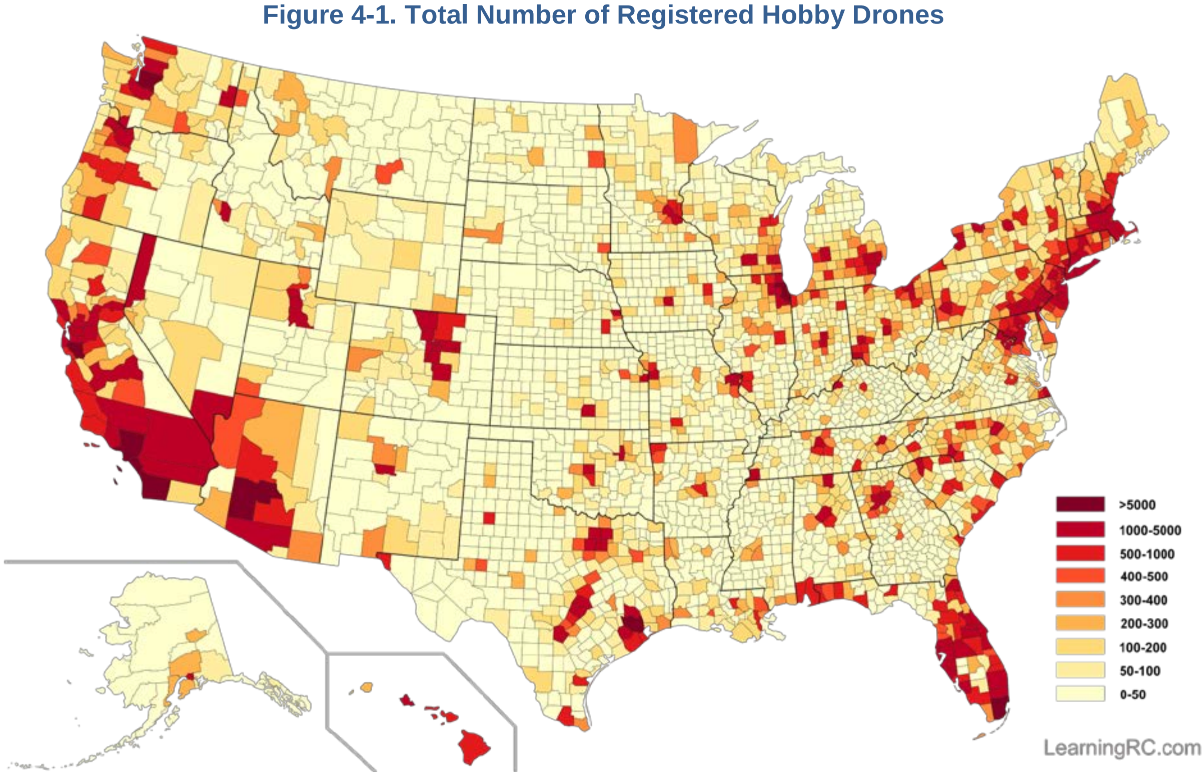
No discussion on the integration and use of UAS for security purposes at airports can ignore the need to also include a high-level discussion on the use and implementation of counter-drone technology.

THE THREAT

As every airport operator is keenly aware, the number of UAS in use continues to grow in the United States and around the world, as does the possibility of a UAS-related airport security violation, whether from an innocent flight error, or a planned terrorist attack. The FAA has already reported numerous cases of drones flying dangerously close to airports and aircraft. The concern being raised is that as more UAS take to the skies, hazardous mid-air encounters will become more likely. While more and more airports have installed PIDS to support monitoring of their AOA boundaries, an unknown (and potentially dangerous) UAS presents an additional vulnerability in the form of an aerial threat.

In January 2018, the FAA reported that their Drone Registry topped one million. That figure includes 878,000 hobbyists, who receive one identification number for all the drones they own (see Figure 4-1), and 122,000 commercial, public, and other drones, which are individually registered. Various sources indicate that there are there are 10 times more drones registered in the United States than manned aircraft.

Figure 4-1. Total Number of Registered Hobby Drones



Source: LearningRC.com

Additionally, on October 10, 2018, FBI Director Christopher Wray, in written testimony, warned the Senate Homeland Security and Governmental Affairs Committee that "The threat from unmanned aircraft systems in the U.S. is steadily escalating" and "The FBI assesses with high confidence that terrorists overseas will continue to use sUAS to advance nefarious activities and exploit physical protective measures." Wray went on to indicate that "Terrorist groups could easily export their battlefield experiences to use weaponized UAS outside the conflict zone." (Wray 2018)

REAUTHORIZATION ACT OF 2018

The FBI testimony came shortly after the Reauthorization Act of 2018 was signed into law, while the FAA stated that they were evaluating the impacts of the change. As of the writing of this guidance document, the new law does provide for:

- UAS punishments: Sections outline stiff punishments for illegal UAS operation over wildfires, near airports, and in other restricted airspace.
- UAS threat elimination: There are a few sections of note:
  - (363) Prohibits operating a UAS equipped or armed with a weapon
  - (364) Review of any additional authorities needed by the FAA to oversee C-UAS
  - (365) Instructs the FAA to leverage the DoD as it relates to use of certain C-UAS
  - (366) Directs the FAA to develop a strategy and guidance to LEOs on how to ID and respond to public safety threats posed by UAS

4.1 Counter-UAS Technology in Airport Security Systems

An example use case for an idealized, fully integrated airport perimeter security system would include the implementation of C-UAS technology in support of the airport's own "Security Support UAS," along with other components such as the airport's PIDS and VMS to provide the airport with full situational awareness.

The airport's Security Support UAS would be programmed to patrol the airport's perimeter fence line autonomously from a fixed base location, following a predetermined path using GPS coordinates. The UAS would provide real-time video of the patrol back to the VMS or the PSIM. (See Appendix A for a Use Case Study example.)

For example, if an alarm is generated at a fence zone or secure gate, a UAS on patrol could respond to the alarm event to transmit real-time video back to the SOC. This would allow the security operator to evaluate the threat and, if necessary, support other response resources by continuing to track the cause of the breach.

When C-UAS detection technology is also installed, the airport's own Security Support UAS could be configured to respond not only to PIDS zone alarms but also to C-UAS alarm notifications from one or more fixed-base locations. (Depending on the size and complexity of the airport's perimeter, there could be several Security Support UAS fixed-base station locations). The UAS responds to the notification autonomously, via the integration, and proceeds to the alarm location using GPS coordinates provided by the C-UAS technology. Once the potential threat is detected, the UAS would then provide a real-time video feed back to the SOC, allowing the security operator to assess the threat.

In the example airport security system, a geofenced perimeter associated with the C-UAS system would be configured to encompass an isolation zone, well outside of the airport's AOA boundary fence. An unknown UAS entering this geofenced perimeter will be detected and reported to the SOC.

Typical C-UAS alerts would include the type, location, and direction of the unknown UAS. Armed with this information, the SOC can take specific action. As indicated above, one such action could be to dispatch the airport's own Security Support UAS inside the AOA boundary fence to track (and potentially follow) the threat without compromising personnel safety. The airport's UAS onboard systems can be used by SOC personnel to evaluate the threat potential of the unknown UAS, enabling real-time decisions to be made regarding deployment of additional security and LEO resources to help mitigate the threat, including potential preventative intervention.

4.2 Counter-UAS Technology

While it is not the intent of this guidance document to provide a detailed analysis of C-UAS technology, or weigh the pros and cons of any one product or technology, this section offers some background information for airports to use when evaluating C-UAS strategies. C-UAS technology is not new and has already been in use successfully for some time on the battlefield for base protection. It has also been used and tested for airspace protection at airports, and for security during large sporting events.

DETECTION

According to a report entitled "Counter-Drone Systems"(Michel 2018), there were (as of February 2018) at least 235 counter-drone products on the market or under active development, with the most popular detection techniques being the following types of sensors:

- Radar
- RF detection
- Electro-Optical (EO)
- Infrared (IR)
- Acoustic
- Thermal

Each of the above listed detection systems has some limitations, with radar potentially being the most cost effective.

Day/night and thermal camera systems are common at airport perimeters, and often are part of C-UAS detection systems. However, just as with PIDS, it is important to understand the distinction between detection and verification. Often the best application of a camera systems is a pan-tilt-zoom camera in a slew-to-cue configuration, with detection being provided by a primary sensor (potentially radar and/or RF). Additionally, the use of video analytics can be implemented to aid the SOC in UAS identification.

As with PIDS, a multi-sensor detection solution may be the most effective for any airport. It is also important to understand that, as with any technology, there is no future-proof C-UAS system, as manufacturers work to keep up with the evolving UAS technology itself.

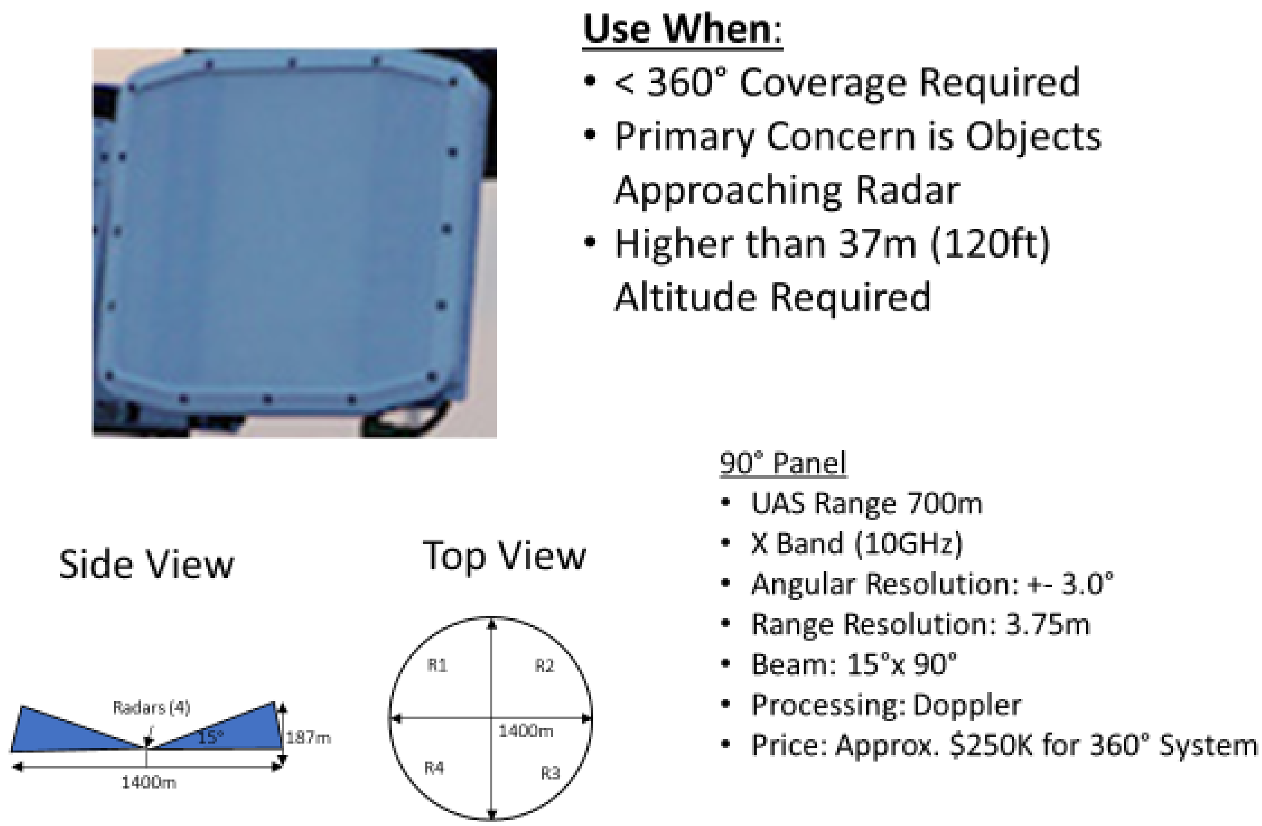
RADAR

When researching radar systems for C-UAS use, airports should first look at system resolution. It is critical for the radar system to have sufficiently fine resolution to detect sUAS, whereas UAV over 55 lbs are more easily detected by radar. Horizontal coverage angles typically range from 90 degrees to 360 degrees. If necessary, multiple radars can be used to deliver a wider angle, when using radar unit with less than 360-degree coverage.

Two sets of example radar options are provided below for UAS detection comparison and discussion purposes, in order to give airport security and operations personnel a perspective on potential system coverage.

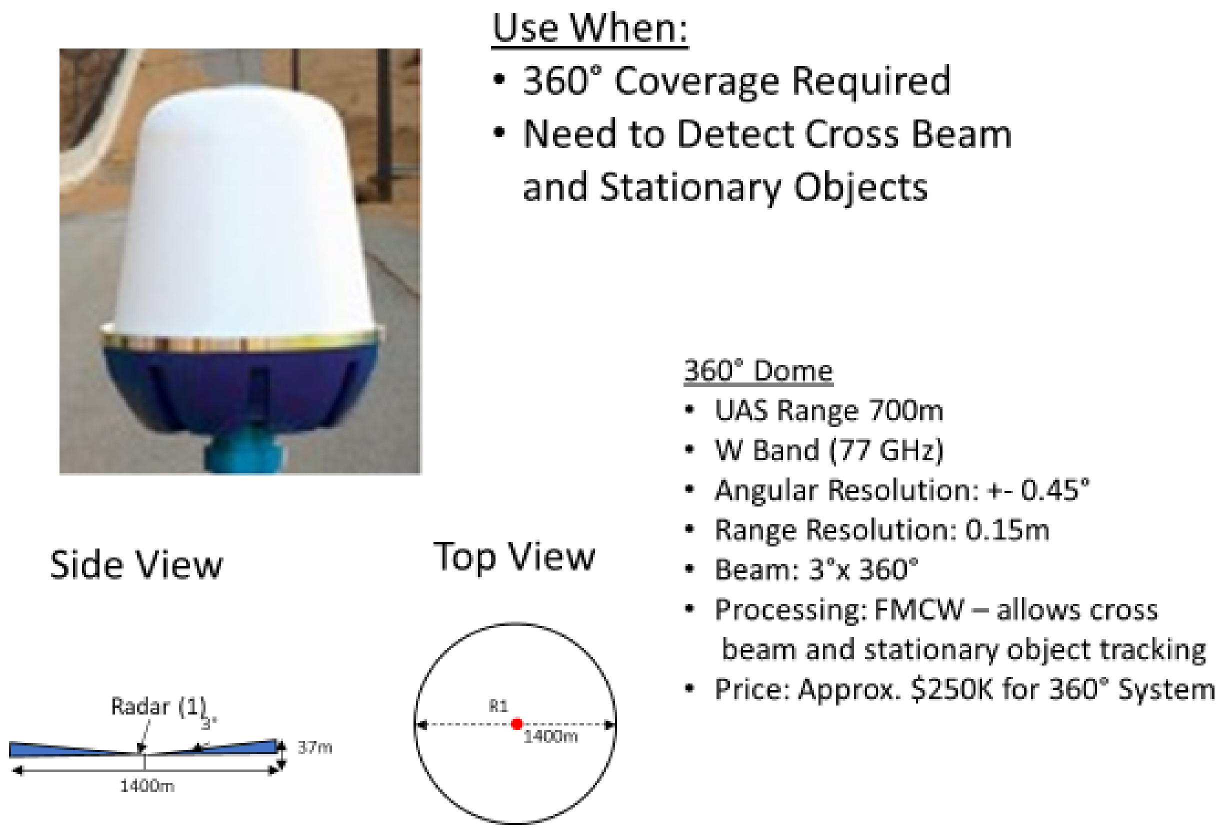
- The 90-degree panel radar (Figure 4-2) has a range of 700 meters and an elevation of 15 degrees, which gets the beam up high. It should be noted that another model is available with an 860-meter range, but the beam is only 45 degrees wide so one would need twice as many.
- The 360-degree dome radar (Figure 4-3) has been UAS-detection tested to 700 meters. The beam elevation is 3 degrees, which gets the user 36 meters or 120 feet altitude at 700 meters away. Since that is a linear measurement, at 350 meters the FOV would be 60 meters high. These altitudes may be suitable for airports, and then the user would get the added benefit of security and airfield safety.

Figure 4-2. Example Radar Option for UAS Detection – 90-Degree Panel Type



Source: SpotterRF

Figure 4-3. Example Radar Option for UAS Detection – 360-Degree Dome Type



Source: NavTech Radar

INTERDICTION

This guidance document does not constitute or offer any legal advice. Airports must seek their own advice for the use of C-UAS interdiction technology. Currently in the United States, interdiction type systems may be considered illegal. The FAA has advised airports against the use of jammers since they can interrupt air traffic management operations.

- Signal jamming devices, including the more advanced directed jamming systems, are either illegal or restricted.
- Jamming systems may violate the Wiretap Act, which forbids the interception of electronic communications. Jamming systems can also interfere with legitimate communications links near a C-UAS system.

On a high level, there are two types of interdiction systems: Kinetic and Non-Kinetic.

- Kinetic interdiction systems are those that use physical means to interrupt the flight of a UAS. (Note that this may also violate the US Aircraft Sabotage Act, which imposes heavy fines and even prison sentences for anybody who willfully “sets fire to, damages, destroys, disables, or wrecks any aircraft” in US airspace).
- Non-Kinetic interdiction systems are those that disrupt the UAV’s communications

Both types of systems have drawbacks. Kinetic systems could be dangerous in that UAV flight is interrupted, causing it to fall to the ground. Some systems have been equipped with nets and/or parachutes, but their safety has not been fully tested. Additionally, if a hostile UAV is carrying explosives, a controlled, safe, and isolated descent becomes critical.

Non-Kinetic systems may also be ineffective and prove problematic, as these systems work by disrupting the UAV’s communications link with the operator. However, many UAV can be programmed to operate autonomously without an active RF link. “Dark drones” do not emit RF signals and have scripted flight paths. Furthermore, jamming systems can also interfere with legitimate communications links.

SECTION 5. USE CASE STUDIES AND LESSONS LEARNED

5.1 Use Case Study Results

A Use Case Study was conducted for the implementation of autonomous UAS integrated with airport security systems. Due to the current regulatory environment, this was possible by having a pilot in command standing by with an observer in place. This Integration Use Case provided data for an automated threat response and measure situational awareness in support of airport security. The study was conducted at the Safe Skies Perimeter Test Facility (PTF) from October 29 to November 2, 2018. Due to the complexity of the Use Case Study and the resultant findings, along with its supporting information and data, a more complete report can be found in Appendix A.

5.2 General Lessons Learned

In the course of preparing this guidance document, the research team had an opportunity to review several documents and photos, and visit and discuss the topic with multiple airports. This section provides some general lessons learned.

On a high level, airports looking to incorporate UAS into their security program may find the following helpful:

- Establish an Airport Working Group for communications, stakeholder meetings, and consortium-building; there are various stigmas and potential fears with the use of UAS at an airport. Through these meetings, an understanding can be established to assuage any fears and ambiguity over goals, and address any potential stigma that may be associated with the use of UAS at the airport. One airport indicated that they held quarterly meetings with Police, Fire, Security, Operations, local FAA (ATC), legal department, and key airlines.
- Create internal and interdepartmental UAS operations policies (consider including Security, LEO, Fire, Operations, Maintenance, AOC, EOC, and ATC) that cover the planned use of UAS
- Consider a UAS SOP for security
- Consider a Letter of Agreement or MOU between the airport and the FAA/ATC
- Work with the stakeholders to finalize the application for a COA
- Create a UAS Deployment Procedures/FAA Coordination Quick Guide

Potential roadblocks that some airports face:

- FAA DroneZone Portal: As discussed later in this Guidebook, the FAA DroneZone Portal provides only one method for UAS operational approvals, which may or may not result in a successful approval. Further, the portal should be viewed as a piece of the overall process for UAS utilization, and not a representation for all of the considerations that an airport operator should take.
- LAANC System: The system is inadequate for event-driven airport security and public safety use (see Section 2.3).
- The ability of an airport to obtain a Public COA allowing for jurisdictional flight as well as flying at night, BVLOS, or over people. (For additional information on waivers, see Section 2.3, FAA Regulations.)
- Evolving technology and challenges in regulating a rapidly changing industry.

Depending on the specific airport applying for a Part 91 (Public Agency) COA, the FAA's Legal Department may not recognize that airport as a government agency.

5.2.1 Use of Tethered UAS

The Use Case Study provided the research team with the following understanding relative to the use of a tethered UAS for airport security:

- The tethered UAS can provide situational awareness of the airport perimeter, offering a relatively high vantage point for a high-resolution color or thermal camera to observe an area, such as a roadway, fence segment, or a vehicle gate for long periods of time.
- The tethered UAS can be quickly located and set up in an area to provide an almost instant camera tower in support of airport security and/or operations events and activities providing secure video streaming via the tether.
- The tethered UAV was observed having issues in windy conditions and may not be able to operate in rain.
- There are fewer safety considerations due to the fact that the UAV is tethered.
- Although not tested, the ability of the Hoverfly Tethered UAS to be configured in a "follow me" mode may allow perimeter patrols to take place from the ground and from an elevated position. The patrols can be recorded and/or be observed live by the SOC, and the patrol vehicle can act as a force multiplier.

Figure 5-1. Golf Cart Outfitted with Hoverfly Tethered UAS

Source: Hoverfly

5.2.2 Use of Autonomous UAS

The Use Case Study provided the research team with the following understanding relative to the use of an autonomous UAS for airport security[10]:

- The autonomous UAV was able to fly programmed, autonomous missions up and down the PTF perimeter, providing situational awareness of personnel, vehicles, and items along the PTF fence line.

[10] Again, this was only possible because an RPIC and an observer were present.

- The autonomous UAS was able to fly programmed, autonomous missions in response to PIDS alarms, providing support for threat response.
- The autonomous UAS allowed for object tracking and manual control, and supported the ability to take snapshots of the observed scene.
- An autonomous UAS was configured with geofence mapping to ensure the UAV stayed within designated areas as it responded to alarms or conducted perimeter patrols.
- As the UAS autonomously responds to alarm events, an SOC operator can use the situational-awareness data provided to direct LEO and/or security guard response, thereby keeping responders safe.
- The autonomous UAS is configured with real-time analytics that support fully autonomous navigation and landing, anomaly notification, and object tracking.

5.3 Recommendations for Airports Based on the Use Case Study Results

GENERAL

The Integration for the Use Case Study was successfully accomplished with both the autonomous and tethered UAS. Both autonomous and tethered UAS performed well overall, and in accordance with their published specifications.

Most security system manufacturers have some form of Software Development Kit (SDK)[11], In some cases, a software framework exists that allows for data sharing and data transfer. In other cases, it will be necessary to purchase a software driver, which provides a software interface to hardware devices, enabling operating systems and other computer programs to access hardware functions without needing to know precise details about the hardware being used. Drivers are hardware-dependent and operating-system-specific. For example, an airport wishing to have real-time video from their UAS integrated with their existing VMS may need to obtain the proper driver to allow this functionality.

Airports will need to create and document an internal set of needs and requirements in order to establish the level of integration needed at their specific location. Overall, it is recommended that a complete CONOPS be established for the use and operation of the UAS in order to best inform the integration and implementation process.

For example, if an airport has an Intrusion Detection System and it wishes to have an autonomous UAS respond to an alarm, the airport will need to determine if a security operator should review the alarm information and make a determination to dispatch a UAS (which is how the Use Case Study implemented the integration), or if the alarm should go directly to the UAS for dispatch.

In either case, the UAS flight management software will need to integrate with the Intrusion Detection System management software, PSIM, or Computer Aided Dispatch (CAD) software that the airport uses to review alarms and dispatch resources. One potential methodology would be to have the integration with the PIDS, for example, require that the security operator receive the alarm from the PIDS, and then manually, based on the pre-established CONOPS, decide to initiate a preprogrammed (within the UAS software) sequence associated with either fence inspection or direct alarm response.

[11] **Software Development Kit (SDK):** Typically, a set of software development tools that allows the creation of application interfaces to allow intercommunication between software packages.

SELECTION OF UAS

Whether an airport chooses to deploy a tethered UAS, contracted UAS (UAS contractor to provide operational and logistical services), UAS as a Service (Robotic Aerial Security using UAV service, which is based on a subscription model), or an autonomous UAS, consideration should be given to enterprise-level systems that are purposefully built to support security operations. This recommendation is made as a result from the research and the Use Case Studies conducted. While these systems may have a higher initial cost, manufacturers of these types of systems provide a greater level of support, understand the need to have secure communications, and have a better understanding of the potential airport security mission.

COTS UAS can have significant benefits as well. Their low cost of entry and current capabilities do make them valuable for an airport that is interested in learning more, experimenting with different deployment models, or just wants staff to become more aware of the nuances of operating UAS.

The key takeaway from the Use Case Studies is that airports can regularly use UAS for routine security inspections as well as for alarm response. Automation can improve performance for a security department and provide additional levels of situational awareness.

DATA SECURITY

Prior to purchase and implementation, airports like other enterprise users must ask the right questions about their data. As these devices may be capturing and recording SSI, all data that a UAS captures must be secure and encrypted. Audit logs must be available. Data security is critical.

5.4 Other Considerations

Two significant program initiatives have been rolled out by the FAA to further develop an understanding of how UAS technology can integrate into commercial and public spaces. In 2014, the FAA selected six UAS test sites (as previously presented) for research in a variety of disciplines:

- University of Alaska's defining of safety standards for UAS categories, as well as monitoring and navigation
- Nevada's research into ATC procedures as they pertain to the introduction of UAS in the NAS and the Next Generation Air Transportation
- Griffiss Airport (New York) testing of sense-and-avoid technologies in a congested airspace
- North Dakota Department of Commerce measurement of UAS suitability for safe flight
- Texas A&M University (Corpus Christi) tested system safety requirements for UAS
- Virginia Tech researched the UAS failure mode and identified operational and technical risk of UAS integration

Recently, the FAA announced awardees for the Integration Pilot Program, which can be defined as an opportunity for state and local governments to partner with the private sector to speed up integration. Announced in August 2018, these awardees and UAS research areas include:

- Choctaw Nation of Oklahoma (Durant) investment in mobile ground-based detect and avoid radars, testing Extended Visual Line of Sight technology
- City of San Diego border protection, employing communication technologies, 5G test networks, and AT&T's national first responder network authority (FirstNet)

- Herndon, Virginia’s Innovation and Entrepreneurship Investment Authority, researching package delivery and will utilize detect-and-avoid technologies and radar systems
- Kansas Department of Transportation (Topeka) BVLOS operations testing, utilizing technologies like detect-and-avoid, automatic dependent surveillance-broadcast (ADS-B), and geofencing to improve agricultural operations
- Memphis-Shelby County Airport Authority aircraft inspection research and testing, and perimeter security surveillance
- Reno, Nevada medical equipment delivery service as a first responder effort, in which UAS uses radar technology to deploy drones and address medical emergencies
- University of Alaska (Fairbanks) pipeline inspection and surveying with technologies in collision avoidance, detect-and-avoid, ADS-B, GPS, satellite services, and infrared imaging

Further information on these recently awarded pilot programs can be found on the FAA UAS webpage (www.faa.gov/uas).

Individual airports have already started to deploy UAS technology for operational use. Following are some examples of those deployments.

London Southend Airport – Drone Surveillance System:

- Rapid identification of UAS and operator location, to address “rogue drone operations”

Hartsfield-Jackson Atlanta International Airport – Runway Maintenance:

- 3D mapping of runway to identify cracks and be able to better plan for runway repairs and full resurfacing projects. This type of field work is typically conducted by personnel on foot; however, UAS operations cut the completion time in half, which allows the airfield to be open longer, increasing revenue and efficiency as a result.
  - More consistent data capture in imagery applications
  - More repeatable and accurate to compare changes between inspections
  - Higher resolution of data coverage
  - Reduced safety risk to the workforce, more specifically for building inspections
  - Time savings
  - Airport Surface Surveillance Capability – improvement of situational awareness via UAS technology

Dallas-Fort Worth International Airport – Department of Public Safety use:

- Police and Fire on the airport in support of first responders and LEOs
- For interior (terminal) and exterior use

GRANT ASSURANCES

A primary UAS grant made available by the FAA is titled 030E-07-SUAS “System, Small Unmanned Aircraft,” for funding aviation equipment to enforce Homeland Security objectives and permissible program activities. The FAA has also allocated $73 million toward developing standards for safe UAS operations in the FY2019 budget.

The Radio Technical Commission for Aeronautics released a report in March 2018 that recommends focus areas for funding in the near and long term. Policies and procedures for UAS integration were suggested to concentrate on flight standards, operators, air traffic control, and airports. The standards that were said to be of high importance for research and development included pilot certification and qualification, command and control, air worthiness certification, detect-and-avoid, and geofencing.

PUBLIC RELATIONS

The public perception and acceptance of UAS in the NAS has bolstered a tremendous amount of concern because of the risk associated with aircraft operations. However, more recently, airports have made tremendous strides in the public awareness and understanding of UAS use by engaging in social media campaigns and providing links on websites for UAS airport advisory requirements. Further, many airports have embarked on a specific public education campaign by speaking at universities and conferences aimed at helping the public understand the dangers and benefits of UAS use. The primary focus is on education of the risks associated with UAS having contact with an aircraft and causing an accident.

ECONOMIC DEVELOPMENT

The emergence of airport tenant-based UAS test facilities have a direct impact on local economic development. As an example, in August 2018, the US Department of Commerce announced an investment of $3 million to build a “UAS innovation and training center” at the Cape County Airport in New Jersey, an initiative that is expected to create 130 new jobs in the region, and is projected to generate $1.9 million in private investment.

Airports who have become part of the FAA test sites have seen economic growth as UAS operations and their employees have become part of the local economy. An airport that is seen as friendly to UAS can also be a place the UAS industry can invest. Therefore, airports that can partner with UAS operators and/or even show the benefits of UAS in their daily operations can see the economic benefits of another aviation-related industry investing in that airport.

ENVIRONMENTAL IMPACTS

The research and Use Case Study work clearly demonstrated that UAS are far less impactful on the environment than traditional security operations and manned aircraft. The following are some simple examples:

- sUAS are almost exclusively battery powered. Therefore, they are zero-emission vehicles and can patrol a perimeter and respond to threats with little to no carbon footprint, as compared to a gasoline- or diesel-powered vehicle.
- The amount of power required to charge sUAS batteries is almost negligible. Therefore they are extremely cost effective from a fuel perspective, and require minimal fossil or alternative fuel to generate the needed electrical power.
- sUAS are extremely quiet in their operation and can go almost undetected; therefore, they do not contribute to noise pollution.

Environmental assessments, Environmental Impact Studies, and Categorical Exclusions have not yet been proven necessary for UAS operations on or near airports, as they do not require land or facility construction or demolition. UAS are already considered aviation use and do not impact land-use compatibility around airports.

5.5 Conclusion

Specific conclusions for airport management and security professionals include the following:

- Consider the implementation of UAS in the airport security program for the application of:
  - PIDS monitoring and response
  - Patrols for the perimeter and highly sensitive areas of the airport
  - Tracking of potential and identified threats
  - Visual inspections of hard-to-reach areas
  - Threat deterrents during major events
  - Additional and flexible video monitoring of specific areas with a determined need (e.g., special event parking)
- Consider the potential data impacts and requirements. Write a specific policy and CONOPS for the management and protection of the data generated from UAS operations.
- Start small and take a phased approach to becoming UAS competent and savvy.
  - Determine the most easily impactful application of UAS and pursue it first either using consultants or engineering firms, or through staff education and application.
  - When the staff are comfortable, and the benefits start to become self-evident, then pursue a wider application of UAS in the operation.
- Talk with the FAA ADO and, if applicable, FAA ATCT personnel.
  - Openly communicate and listen to stakeholder concerns; use this information to help guide the approval processes.
- Explore COA application and familiarize the staff with the LAANC program.
- Develop and implement a public awareness campaign so that interested and potential UAS operators know how and when to communicate with the airport.
- Lastly, look broadly at the long term potential use of UAS. Look at instances where humans are put in danger or are asked to see and report findings; those are the times a UAS can replace or augment people.

The following is a checklist for airport operators to determine if the use of UAS is appropriate and, if so, how to start the process of determining the best path to deployment.

Table 5-1. UAS Deployment Checklist

X	Task	Agency Involvement	Timeframe	Milestone
☐	Make an assessment of the airport's readiness • Infrastructure (IT) (Gaps to support) • Financial impacts of gap findings • Airspace restrictions • Research current industry products • Regulatory restrictions and updates • Staff skills and expertise in the area • Determine organizational impacts	• FAA UAS • Internal Staff	~6 months (shorter period for smaller airports and up to a year for larger ones)	UAS Assessment Report (findings completed)
☐	Consider legal implications	Governing Body's Council	1 month	Findings Report
☐	Determine applications (uses) may require a phased approach and vendor trials or demonstrations	• Airport security personnel • TSA	2 months	• Recommendation(s) Report • Implementation Plan
☐	Assign internal staff to to be responsible for the UAS program. Identify if there are Part 107 pilots within the organization	Internal Staff	TBD on Organizational Impact	• Education and or Recruiting plan • Updated Implementation Plan
☐	Budget for needed infrastructure gaps	Internal Capital Program Staff	TBD based on CIP	Projects identified and Included in CIP
☐	Develop all required processes and procedures (CONOPS)	• Internal staff • FAA ATC • TSA (update ASP)	6 months	SOP Manual for UAS Operations
☐	Execute infrastructure improvements and training	• Internal staff • FAA ADO	During CONOPS development	• Completion of projects • Receipt of certifications
☐	Acquire equipment (UAS) if not already acquired during infrastructure improvements	UAS vendors	As soon as practical	• Receipt of UAS • Staff acceptance
☐	Complete COA Application Process (see Appendix B)	• FAA (DroneZone) • FAA ATC	30–90 days on average	FAA COA approval
☐	Implement plan (inclusive of measurements for success)	• FAA ATC • TSA (as applicable)	TBD based on phases	Results monitoring starts
☐	Review results and adjust as needed	• FAA ATC • TSA	Minimum of 1 year's data	Progress report

REFERENCES

AIROBOTICS. n.d. *Automated Industrial Drones - Airobotics.* Accessed August 31, 2018. https://www.airoboticsdrones.com/.

Antonelli, Jeffrey. 2017. "How to Get a Beyond Line of Sight (BLOS) FAA Part 107 Waiver." http://dronelawsblog.com/get-beyond/line-sight-blos-faa-part-107-waiver/

BMVA. n.d. *What is Computer Vision.* Accessed August 31, 2018. http://www.bmva.org/visionoverview.

Boucher, Tim. 2015. *What is an orthomosaic photo?* January 13. Accessed August 30, 2018. https://medium.com/new-farmer/what-is-an-orthomosaic-photo-11140c0601df.

Cebul, Daniel. 2018. *Unmanned.* March 26. Accessed August 27, 2018. https://www.c4isrnet.com/unmanned/2018/03/26/raytheon-darpa-developing-technology-to-control-drone-swarms/.

Dronematrix. n.d. *YACOB.* Accessed August 31, 2018. https://www.dronematrix.eu/en_US/page/yacob.

Esri. n.d. *Esri Support GIS Dictionary.* Accessed August 30, 2018. https://support.esri.com/en/other-resources/gis-dictionary.

FAA. 2019. "14 CFR PART 107—SMALL UNMANNED AIRCRAFT SYSTEMS." *Code of Federal Regulations.* Washington D.C.: Government Publishing Office, March 26.

—. 2016. Advisory Circular 107-2, "Small Unmanned Aircraft Systems (sUAS)." https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf.

—. 2009. *Risk Managment Handbook.* Washington D.C.: United States Government Printing Office.

GIS Geography. 2018. *DEM, DSM & DTM Differences – A Look at Elevation Models in GIS.* February 20. Accessed August 30, 2018. https://gisgeography.com/dem-dsm-dtm-differences/.

H3 Dynamics. n.d. *H3 Dynamics.* Accessed August 31, 2018. https://www.h3dynamics.com/products/drone-box/.

Insitu Inc. 2017. "SCANEAGLE." Bingen: Insitu Inc.

Kenneth Neubauer, Dave Fleet, Filippo Grosoli and Harry Verstynen. 2015. *Unmanned Aircraft Systems (UAS) at Airports: A Primer.* Guidebook, Washington D.C.: Airport Cooperative Research Program.

Michel, Arthur Holland. "Counter-Drone Systems." Center for the Study of the Drone at Bard College, February 20, 2018, http://dronecenter.bard.edu/counter-drone-systems/.

Miriam Webster. n.d. *Artificial Intelligence Miriam Webster.com.* Accessed August 31, 2018. Merriam-Webster, www.merriam-webster.com/dictionary/artificial intelligence.

Nightengale Security. n.d. *Specs & FAQ - Nightengale Security - Robitic Aerial Security.* Accessed August 31, 2018. https://www.nightingalesecurity.com/specs-faqs/.

NTIA. 2016. *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability.*

Raytheon. 2018. *Raytheon: Mind of the swarm- Amazing new technology allows drones to flock together as they fly*. July 23. Accessed August 23, 2018. https://www.raytheon.com/news/feature/mind-swarm.

Wray, Christopher. 2018. "FBI." *News/Testimony.* October 10. https://www.fbi.gov/news/testimony/threats-to-the-homeland-101018.

This section also lists documents, reports, and website links that the reader may find useful in the deployment of UAS for airport security.

DOCUMENTS AND REPORTS

"Airport and UAS: Integrating UAS into Airport Infrastructure and Planning." Airport Cooperative Research Program. Mar. 2016. PDF. http://onlinepubs.trb.org/onlinepubs/acrp/fy2017ps/17-03-09Hasper.pdf

"Airspace Restrictions." Federal Aviation Administration, U.S. Dept. of Transportation, Washington, D.C., May. 2017. Web. https://www.faa.gov/uas/where_to_fly/airspace_restrictions/#ssar

"ATL Uses UAS on Runway Inspection Tour." Aviation Daily, Aviation Week Network, Apr. 27, 2017. Web. http://aviationweek.com/awincommercial/atl-uses-uas-runway-inspection-tour

"Budget Highlights Fiscal Year 2019." U.S. Department of Transportation. https://www.transportation.gov/sites/dot.gov/files/docs/mission/budget/304476/508-dot-bh2019.pdf

"Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program." National Institute of Justice, U.S. Dept. of Justice, Dec. 2016. PDF. https://www.ncjrs.gov/pdffiles1/nij/250283.pdf

"Drone Integration Funding." Radio Technical Commission for Aeronautics. https://www.rtca.org/sites/default/files/dac_tg3_funding_report_long_term_final.pdf

"FAA UAS Data Exchange." Federal Aviation Administration. https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/

"First UK Airport Trial of a Drone Surveillance System." UAS Vision. https://www.uasvision.com/2018/05/14/first-uk-airport-trial-of-a-drone-surveillance-system/

"How an Atlanta airport is using drones to help with runway maintenance." Market Place. https://www.marketplace.org/2017/05/31/business/how-atlanta-airport-using-drones-help-with-runway-maintenance

"Integrating of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap." Federal Aviation Administration, U.S. Dept. of Transportation, First Edition, 2013. PDF. https://www.faa.gov/uas/media/uas_roadmap_2013.pdf

"Managing Unmanned Aircraft Systems in the Vicinity of Airports." Airport Cooperative Research Program. http://onlinepubs.trb.org/onlinepubs/acrp/docs/ACRP03-42_TopicAreaA_GuidanceDocument.pdf

"Remote Pilot – Small Unmanned Aircraft Systems Study Guide." Federal Aviation Administration, U.S. Dept. of Transportation, Aug. 2016. PDF. https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/media/remote_pilot_study_guide.pdf

"Safely Integrating UAS Operations at Airports." Federal Aviation Administration, U.S. Dept. of Transportation, Oct. 2016. PDF. http://aci-na.org/sites/default/files/odonnell_airports_council_international_10-18-2016_for_publicaiton_.pdf

"The use of drones for airport asset management." International Airport Review. https://www.internationalairportreview.com/article/38728/38728/

"UAS Infrastructure Considérations." Airport Cooperative Research Program. https://www.nap.edu/read/21907/chapter/7

"UAS Technology Offers Soaring Potential." Burns McDonnell, Sept. 2016, PDF. file:///C:/Users/Jon.Watson/Downloads/UASTechnologyOffersSoaringPotentialWhitePaper092216.pdf

"Understanding Unmanned Aircraft Systems (UAS) for Airport Operators." North Carolina Airport Technical Assistance Program. https://itre.ncsu.edu/wp-content/uploads/2016/05/NCAirTAP_UAS_NCAA_RegMtgs_Sep2016-1.pdf

"Unmanned Aerial Vehicles (UAVs): An Emerging Technology for Logistics." International Journal of Business and Management Invention, 2319-8028, Vol. 5 Iss. 5, p. 86-92, May 2016. PDF. http://www.ijbmi.org/papers/Vol(5)5/version-2/L050502086092%20.pdf

"Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace." National Center for Policy Analysis, Mar. 2013. PDF. http://www.ncpa.org/pdfs/sp-Drones-long-paper.pdf

"Updated Guidance on Guidance on Unmanned Aircraft Systems (UAS) Detection and Countermeasures Technology (Counter-UAS) at Airports, 19 July 2018." Federal Aviation Administration, Office of Airport Safety and Standards. https://www.faa.gov/airports/airport_safety/media/Counter-UAS-Airport-Sponsor-Letter-July-2018.pdf

WEB LINKS

Advisory Circular Subject: Small Unmanned Aircraft Systems (sUAS) Date: 6/21/16 AC No: 107-2
https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf
The PDF this links connects to contains detailed information on the 14 CFR Part 107.

FAA homepage for UAS: https://www.faa.gov/uas/
The FAA homepage provides links to pages with pertinent information for sUAS operations and training.

FAA B4UFly Mobile App: https://www.faa.gov/uas/where_to_fly/b4ufly/

FAA Certificate of Waiver or Authorization (COA):
https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/

FAA Drone Zone homepage: https://faadronezone.faa.gov/#/
This site is where aircraft registration, mishap reporting and Part 107 waivers are completed.

FAA UAS Data Exchange: https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/
This link explains the FAA UAS Data Exchange, including Low Altitude Authorization and Notification Capability (LAANC)

FAA Frequently Asked Questions: https://www.faa.gov/uas/faqs/

FAA Reauthorization Act 0f 2018: https://www.congress.gov/115/bills/hr302/BILLS-115hr302enr.pdf

FAA's Sample Preflight Inspection Checklist:
https://www.faasafety.gov/files/gslac/courses/content/451/1458/Preflight%20Inspection%20Checklist.pdf

Know Before You Fly: http://knowbeforeyoufly.org/

Part 107 Testing Guide: https://www.faa.gov/uas/getting_started/part_107/remote_pilot_cert/
The testing guide provides the basic information that is required to the take and pass the 14 CFR Part 107 certificate test for commercial operators as well as the certification requirements.

Part 107 Waiver Guide: https://www.faa.gov/uas/request_waiver/
The waiver guide provides detailed instructions on how to properly request a waiver*.
*All waivers are not processed through the FAA Drone Zone site.

U.S. DHS Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in UAS Programs:
https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf

Waiver Safety Explanation Guidelines:
https://www.faa.gov/uas/request_waiver/waiver_safety_explanation_guidelines/
The waiver safety explanation guidelines walk the user step-by-step through identifying the safety measures that the FAA is looking for when they review waiver requests.

APPENDIX A: INTEGRATED USE CASE STUDY

A Use Case Study for the implementation of autonomous UAS integrated with a security system was conducted. Autonomous UAS was only possible with a pilot in command standing by and an observer; however, the UAS operated in fully autonomous mode. The intent was to provide data for an automated threat response and measure situational awareness in support of airport security.

1. Background

The research team developed a Use Case Study in support of the integration aspects of a UAS in the context of airport security systems, threat response, and situational awareness.

For this study, the team utilized a fence mounted perimeter intrusion detection system, which was installed and had previously undergone technology testing under the Airport Security System Integrated Support Testing (ASSIST) program, at the Safe Skies Perimeter Test Facility (PTF), which is adjacent to the McGhee Tyson Airport (TYS). This study utilized two types of unmanned aircraft systems, one autonomous and one tethered, from commercial vendors.

For more information on the TYS COA see Appendix B: Certificate of Authorization Application Example

The onsite testing efforts for this Use Case Study took place between October 29 and November 2, 2018. Formal testing was conducted November 1, 2018. The weather on November 1 was blustery and overcast, with temperatures in the mid to high 60’s, and with periods of rain during the day.

In preparation for the onsite demonstration testing for this Use Case Study, the PARAS 0012 research team applied for and received a COA to operate in Class C airspace at TYS.

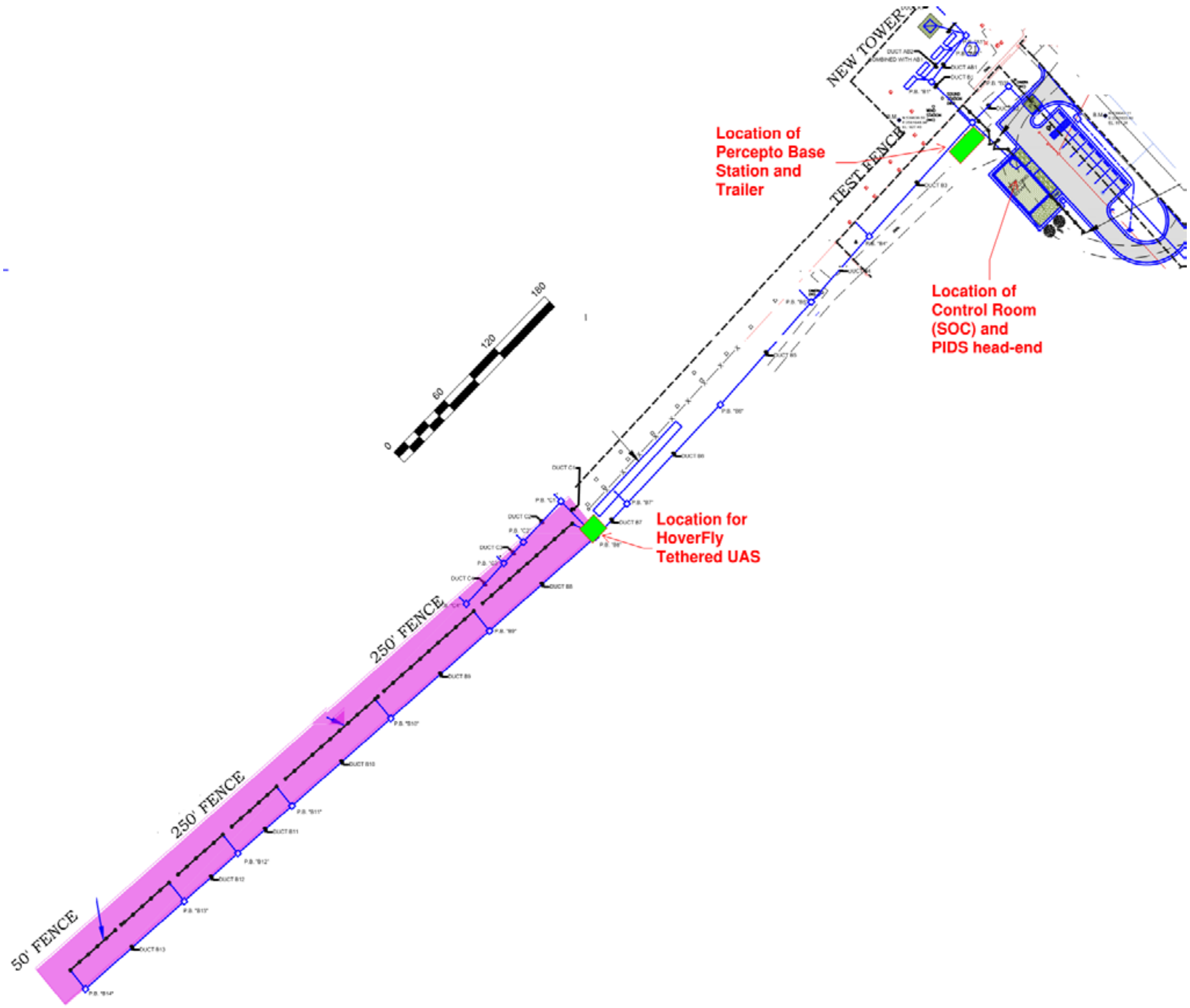
2. Primary Objectives

1. To demonstrate the ability to integrate the UAV’s command, control, and communication system software with an airport’s alarm monitoring and management software systems.
2. Demonstrate the ability to use UAS to safely and securely support a typical ASP. This included the use of UAV-mounted payloads such as day/night camera systems and associated video analytics to perform perimeter patrols and threat response, and provide overall situational awareness to a SOC.
3. Utilize the results of the Use Case Study to support the development of a guidebook to assist airports of various types and sizes in the use of UAS for airport security applications.

3. Site Plan and Equipment Location

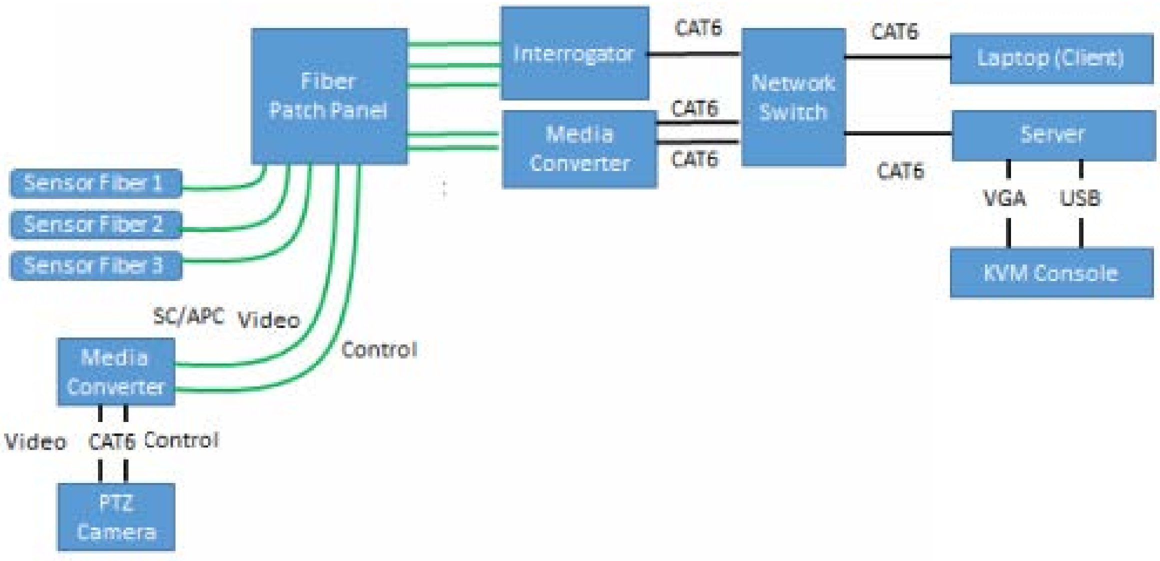
The two UAS were deployed along the existing PTF fence line. The control room, which acted as the SOC, and the headend for the AgilFence PIDS were located within the Safe Skies PTF command center. A copy of the site layout is shown in Figure A-1.

Figure A-1. UAS Equipment Placement and Layout at the Safe Skies PTF



The PIDS communication network used at the PTF, depicted in Figure A-2, is representative of a typical intrusion detection system in that the sensor fibers terminate in the vendor's system interrogator and are then connected via the network to system servers (Figure A-3) and workstations. In this example, an IP-based PTZ camera programmed to view PIDS alarms is connected via fiber-based media converters to the network.

Figure A-2. PIDS Communication Network at PTF



4. Certificate of Authorization and Use Case Study Flight Procedures

In order to ensure that all UAS activity performed as part of this Use Case Study was performed safely and in compliance with FAA rules and regulations, the PARAS 0012 research team submitted an Application for COA in Class C airspace. A Notice to Airmen was generated for the test flight dates and LAANC tiles were submitted in order to request digital (automated) airspace authorization for controlled airspace.

The COA document details the pilot in command, planned location, area of operation, points of contact/chain of command listing, field communication equipment for the flights, Risk Matrix, UAS Risk Mitigation in Class C Airspace, flight procedures, and Quality Assurance Checklists. The COA for this Use Case Study can be found in Appendix B.

4.1 Launch/Recovery Site Determination

Prior to the overall start of the Use Case Study, specific launch/recovery site locations were confirmed. Radio communication with ATC and cell phone network coverage was verified.

4.2 Safety Briefing and Flight Area Access

A safety briefing took place between Safe Skies PTF support personnel, the research team, and the UAS flight crews prior to deployment at the PTF. Flight plans, site access, safety concerns, and potential hazards were discussed.

4.3 Establishing Boundary Zones (Geofences)

While the tethered UAV is captive to the physical boundary established by the automated coiling tether, the boundary zones (geofences) for the Percepto Autonomous UAV for its predetermined flight/mission area was created in the Percepto cloud management flight software. If the geofences had not been uploaded to the UAS directly, the internal checks within the Percepto system would prohibit the UAV takeoff. Field verification of the boundaries was conducted to eliminate any imagery errors during initial planning.

4.4 Integrated Demonstration Security Missions (test flights)

Prior to all the Use Case Study test flights, designated team members were responsible for primary communication with TYS ATC. An agreement with the ATCT required that a designated team member place a call to ATC prior to the start of each day's mobilization and when all operations were completed for that day. Use Case Study operations did not commence without approval by ATC.

Additionally, to ensure safe operations, designated team members were provided with radios and stationed at various key locations along the test flight routes. A radio on the same frequency was located within the simulated control room, which acted as the security command center. Announcements were made each time a UAS mission was launched.

5. Integrated System Descriptions

The following sections describe the systems that were integrated for this evaluation: the AgilFence PIDS, the Percepto Sparrow UAS, and the Hoverfly LiveSky SENTRY UAS.[12]

5.1 AgilFence

AgilFence is a fence mounted PIDS, manufactured by ST Electronics (Satcom and Sensor Systems) Pte. Ltd., that uses Fiber Bragg Grating (FBG) technology. The FBG-embedded optical fiber cable sensor detects changed in mechanical strain caused by fence disturbances. A signal processing algorithm analyses the sensor data to eliminate false and nuisance alarms. It provides an alarm indication with GPS location +/-10 feet along the fence line. At the PTF, the system was installed on approximately 1,000 feet of chain-link fence.

Alarm notifications from AgilFence were reported to an Integrated PIDS Alarm Management System (iPAMS) and displayed on an operator workstation. iPAMS utilizes JSON (JavaScript Object Notation), a lightweight data-interchange format, to send and interchange alarms with other systems.

5.2 Percepto Sparrow UAS

The Percepto Sparrow, manufactured by Percepto - Autonomous Drones, is a weatherproof, autonomous, enterprise-level drone system capable of flying up to 35 minutes on a charge. It is equipped with a FLIR Blackfly USB 3.0 vision industrial camera for daytime recording and a FLIR TAU 2 640 for night operations. The UAV is stored in a weatherproof Base Station, which was connected to the PTF network and 240-V AC power source. The Base Station provides a dedicated landing zone, automatically charges the Sparrow UAV, and transfers data to the Sparrow and the cloud (as part of its cloud management software), to enable the Sparrow UAV to operate fully autonomously. Figure A-3 shows the Base Station in both open and closed positions, and the Sparrow in flight. The system is equipped with the PerceptoCore™, which allows real-time analytics and fully autonomous cycles including conducting takeoff, navigation, and landing. See Attachment A to this appendix for the Percepto Sparrow system datasheet.

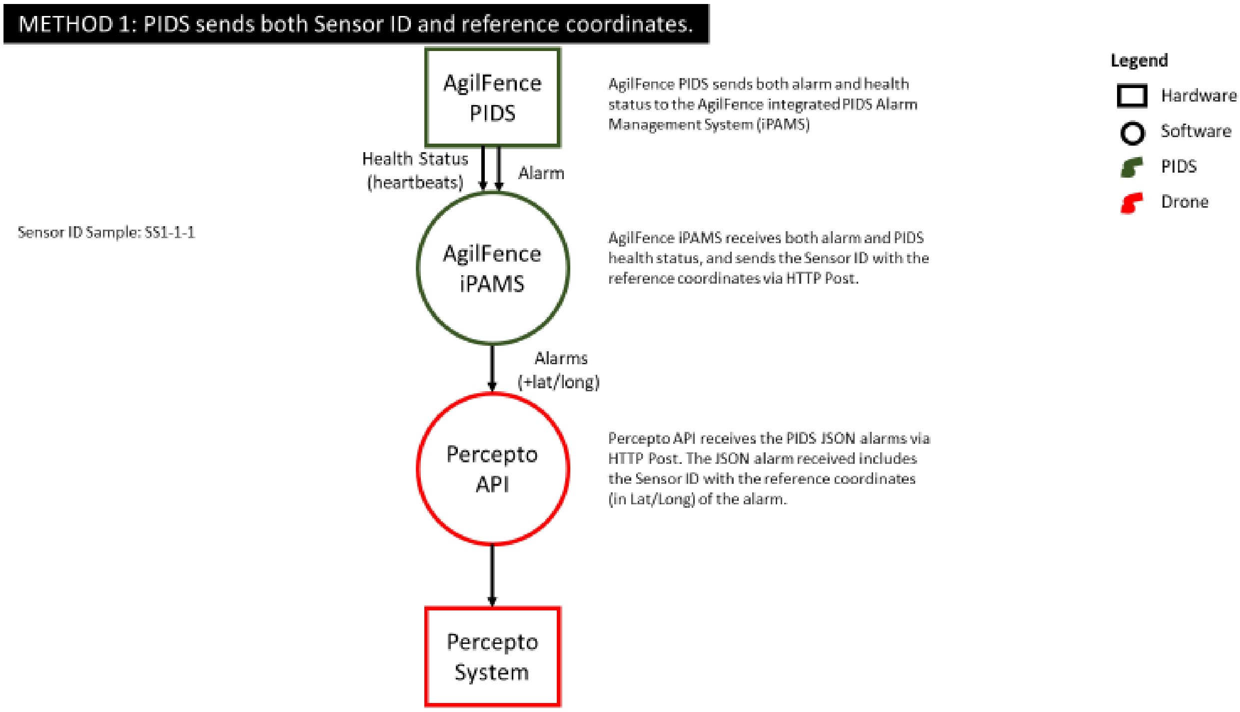
[12] Use of these products shall not be construed as a formal endorsement by the research team or Safe Skies.

Figure A-3. Percepto System Components (clockwise from top left): Base Station (Closed), Base Station (Open), Sparrow in Flight

Integration of the Percepto UAS with the AgilFence PIDS was accomplished with the Percepto Cloud Management Software (CMS), which is a web-based management system enabling the monitoring and management of the UAV (or a fleet of UAVs) by a remote pilot, and provides for mission setup and live activation. The CMS defines the operational landscape, and flight limitations and restrictions, including the graphic mapping of free-flight zones, no-flight zones, and alarm points for the UAV response. The CMS also provides a map-based common operating picture to the operator. Pre-scheduled missions and reactive triggers are set within the CMS.

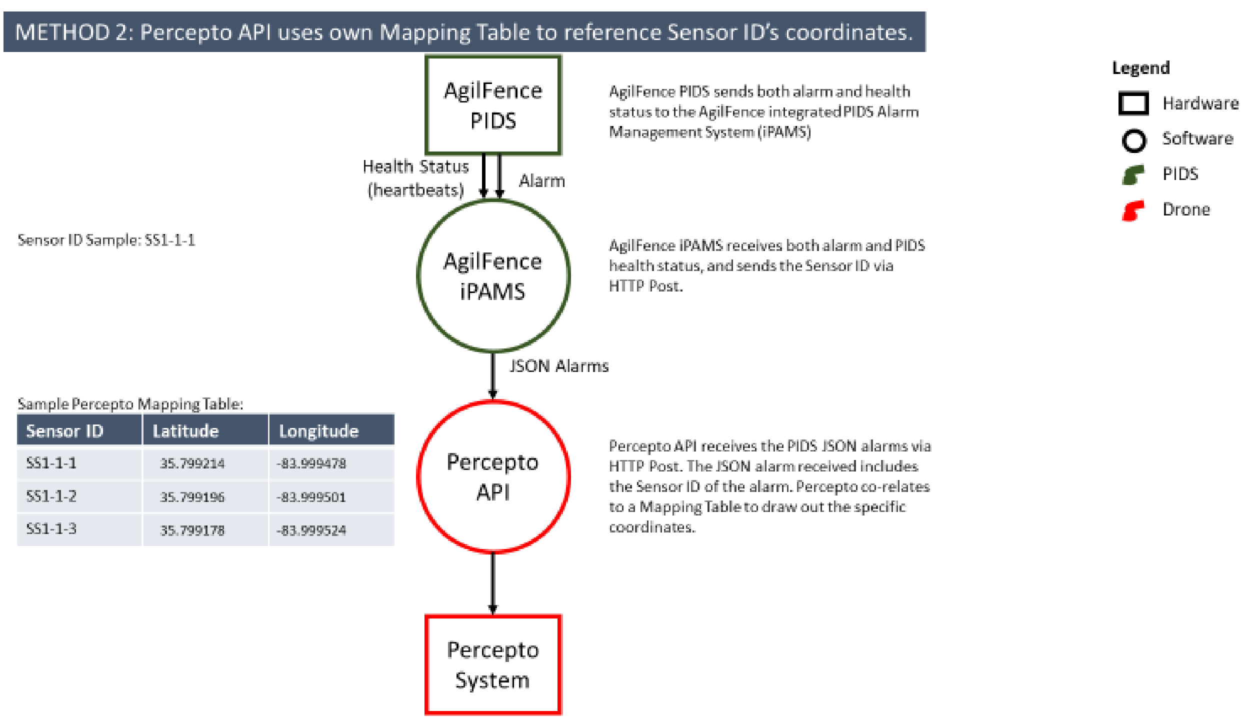
Percepto's CMS has an API that can be used to interface and integrate with a PSIM, CAD, or, as in this case, the PIDS, such that the Percepto CMS API receives the PIDS JSON alarms via an HTTP post. The JSON alarm received includes the sensor ID with the reference coordinates of the alarm (in latitude/longitude). Figure A-4 depicts the integration performed for this specific Use Case Study.

Figure A-4. PIDS to Percepto CMS – Method 1



Airports can also consider an alternative integration method in which the UAS API receives the PIDS alarm, which includes the sensor ID of the alarm, and the UAS software internally correlates a Mapping Table to draw out the specific coordinates. Figure A-5 depicts Method 2, which may be more efficient depending on the PIDS and/or PSIM deployed at an airport.

Figure A-5. PIDS to Percepto CMS – Method 2



Sensor ID	Latitude	Longitude
SS1-1-1	35.799214	-83.999478
SS1-1-2	35.799196	-83.999501
SS1-1-3	35.799178	-83.999524

5.3 Hoverfly LiveSky SENTRY UAS

LiveSky SENTRY, manufactured by HoverFly Technology Inc., is an autonomous tether-powered enterprise-level UAV. The LiveSky tethered UAV obtained its power for operation from a local 120-V AC power connection adjacent to the fence line where it was deployed, which allowed it to fly for extended periods of time. The UAV was equipped with two cameras, one for day and one for night operations. Figure A-6 shows the LiveSky UAV and its field launch kit. See Attachment B to this Appendix for the Hoverfly and Hexagon datasheets.

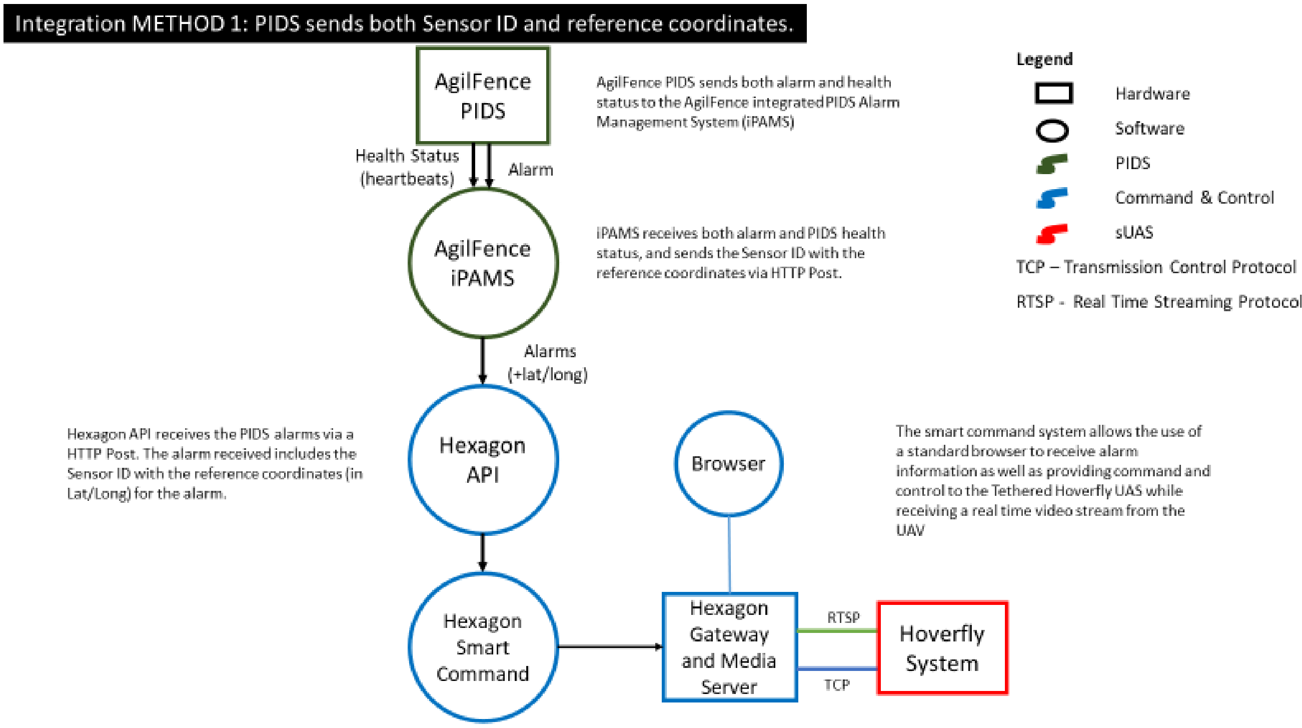
Figure A-6. HoverFly System Components (clockwise from top left): LiveSky on Its Base, Field Launch Kit, LiveSky in Flight

Integration of the LiveSky UAV with the AgilFence PIDs was accomplished using Hexagon Safety and Infrastructure's HxGN Smart Command Center. HxGN Smart Command is a cloud-based security and monitoring software, which interfaces with the Hoverfly UAS platform. The Hexagon/Hoverfly integrated system provided situational awareness by displaying the information from the UAV within a map-based common operating picture.

The team was interested in integrating with Hexagon, as Hexagon's core product is a CAD Public Safety and Security PSIM software system that is currently in use at many airports. Smart Command is built based on this system. It is our understanding that Hexagon intends to integrate its Smart Command software with its Public Safety and Security CAD system to allow for a seamless dispatch of a UAS.

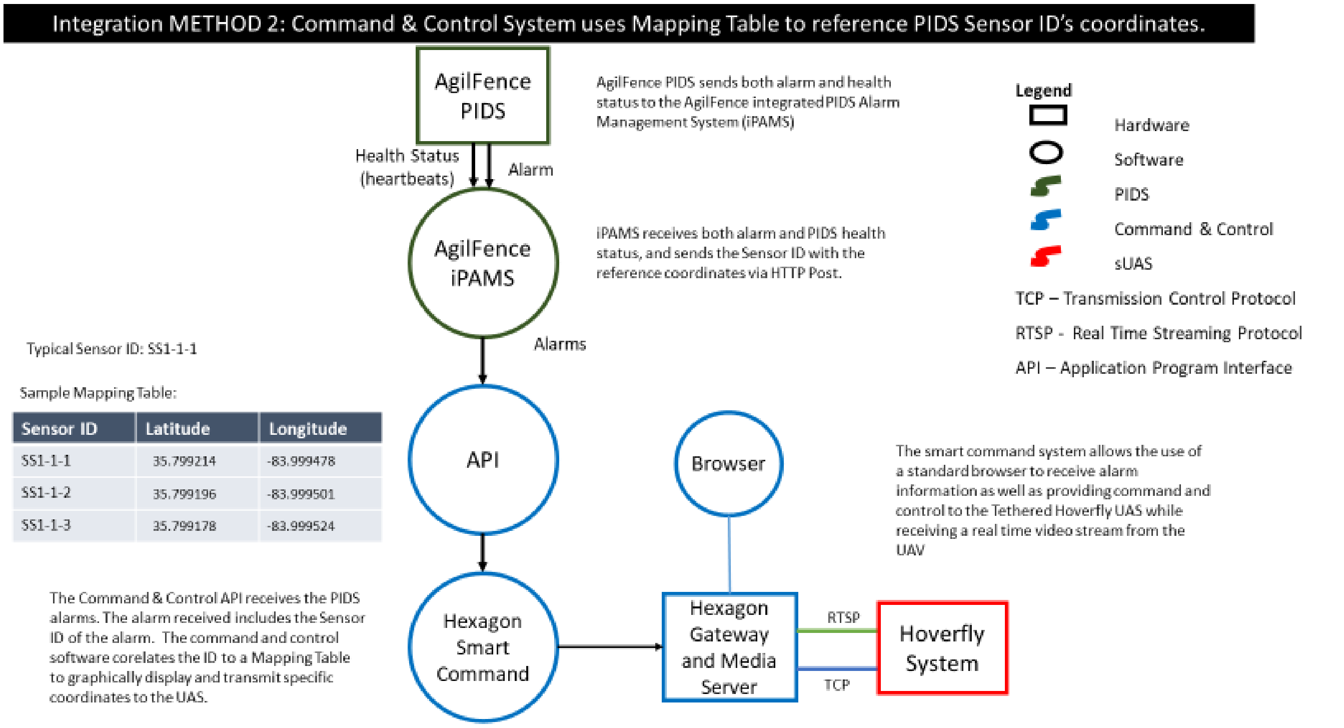
Hexagon has an API, which was used to interface and integrate with the PIDS such that the API received the PIDS JSON alarms via an HTTP post. The JSON alarm received included the sensor ID with the reference coordinates (latitude/longitude) of the alarm. Figure A-7 depicts the integration that we chose to perform for this specific Use Case Study.

Figure A-7. PIDS to the HxGN Smart Command Center – Method 1



As with the Percepto example, airports can also consider an alternative method in which the Hexagon software receives the PIDS alarms, which include the sensor ID of the alarm, and the Smart Command Center internally correlates a Mapping Table to draw out the specific coordinates. Figure A-8 depicts this as Method 2, which may be more efficient depending on the PIDS or Hexagon CAD system deployed at an airport.

Figure A-8. PIDS to the HxGN Smart Command Center – Method 2



5.4 Test Methodology

The Use Case Study demonstration and testing effort consisted of the following set of scenarios:

1. Scheduled Percepto Autonomous UAS patrol(s)
2. Scheduled Hoverfly Tethered UAS observation/inspection flight(s)
3. Percepto Autonomous UAS threat response flight(s)
4. Hoverfly Tethered UAS threat response flight(s)
5. Control room operator manually dispatching the Percepto Autonomous UAS for threat response and observation flight(s)
6. Control room operator manually dispatching the Hoverfly Tethered UAS for threat response and observation flight(s)

For "threat response" scenarios (3–6), Safe Skies personnel were sent to specific locations to create a disturbance on the fence in order to generate an alarm on the AgilFence system. For the purposes of the Use Case Study, alarms were generated by shaking and/or kicking the fence fabric.

Each PIDS alarm generated during testing was logged in iPAMS, and the workstation display provided a graphical depiction of the location of the alarm along with an associated video surveillance clip of that location. Table A-1 documents each alarm created and received by the iPAMS during the Use Case Study demonstration testing. The SOC operator used the alarm screen to determine if and what type of a response was required. For our testing, the alarm response entailed dispatching both the autonomous and tethered onsite UAVs.

Table A-1. PIDS Alarm Log

AgilFence PIDS Alarm Log 20181101										
CATEGORY	**TIME OCCURED**	**CAMERA**	**SENSOR ID**	**DESCRIPTION**	**TYPE**	**ACK BY**	**ACK TIME**	**RESOLUTION TYPE**	**STATUS**	**RSV TIME**
Intrusion	11/1/2018 8:57	CAM01	SS1-1-6	Intrusion @ SS1-1-6	Activities	ops	11/1/2018 8:58	A2 - System testing	resolved	11/1/2018 8:58
Intrusion	11/1/2018 9:00	CAM01	SS1-3-21	Intrusion @ SS1-3-21	Activities	ops	11/1/2018 9:03	A2 - System testing	resolved	11/1/2018 9:03
Intrusion	11/1/2018 9:00	CAM01	SS1-3-22	Intrusion @ SS1-3-22	Activities	ops	11/1/2018 9:03	A2 - System testing	resolved	11/1/2018 9:03
Intrusion	11/1/2018 9:01	CAM01	SS1-3-20	Intrusion @ SS1-3-20	Activities	ops	11/1/2018 9:03	A2 - System testing	resolved	11/1/2018 9:03
Intrusion	11/1/2018 9:02	CAM01	SS1-3-24	Intrusion @ SS1-3-24	TRUE	ops	11/1/2018 9:05	T5 - Send drone	resolved	11/1/2018 9:05
Intrusion	11/1/2018 9:12	CAM01	SS1-2-7	Intrusion @ SS1-2-7	TRUE	ops	11/1/2018 9:12	T5 - Send drone	resolved	11/1/2018 9:13
Intrusion	11/1/2018 9:49	CAM01	SS1-3-23	Intrusion @ SS1-3-23	TRUE	ops	11/1/2018 9:49	T5 - Send drone	resolved	11/1/2018 9:49
Intrusion	11/1/2018 10:13	CAM01	SS1-1-11	Intrusion @ SS1-1-11	TRUE	ops	11/1/2018 10:13	T5 - Send drone	resolved	11/1/2018 10:14
Intrusion	11/1/2018 11:03	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 11:05	A2 - System testing	resolved	11/1/2018 11:05
Intrusion	11/1/2018 11:03	CAM01	SS1-3-21	Intrusion @ SS1-3-21	Activities	ops	11/1/2018 11:04	A2 - System testing	resolved	11/1/2018 11:04
Intrusion	11/1/2018 11:06	CAM01	SS1-3-18	Intrusion @ SS1-3-18	Activities	ops	11/1/2018 11:07	A2 - System testing	resolved	11/1/2018 11:08
Intrusion	11/1/2018 11:06	CAM01	SS1-3-14	Intrusion @ SS1-3-14	TRUE	ops	11/1/2018 11:06	T5 - Send drone	resolved	11/1/2018 11:07
Intrusion	11/1/2018 11:06	CAM01	SS1-3-17	Intrusion @ SS1-3-17	Activities	ops	11/1/2018 11:07	A2 - System testing	resolved	11/1/2018 11:07
Intrusion	11/1/2018 11:25	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 11:26	A2 - System testing	resolved	11/1/2018 11:26
Intrusion	11/1/2018 11:25	CAM01	SS1-3-3	Intrusion @ SS1-3-3	Activities	ops	11/1/2018 11:25	A2 - System testing	resolved	11/1/2018 11:25
Intrusion	11/1/2018 11:32	CAM01	SS1-3-24	Intrusion @ SS1-3-24	Activities	ops	11/1/2018 11:34	A2 - System testing	resolved	11/1/2018 11:35
Intrusion	11/1/2018 11:32	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 11:34	A2 - System testing	resolved	11/1/2018 11:34
Intrusion	11/1/2018 12:21	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 12:25	A2 - System testing	resolved	11/1/2018 12:25
Intrusion	11/1/2018 13:26	CAM01	SS1-3-24	Intrusion @ SS1-3-24	Activities	ops	11/1/2018 13:27	A2 - System testing	resolved	11/1/2018 13:27
Intrusion	11/1/2018 13:27	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 13:27	A2 - System testing	resolved	11/1/2018 13:27
Intrusion	11/1/2018 13:39	CAM01	SS1-3-19	Intrusion @ SS1-3-19	TRUE	ops	11/1/2018 13:39	T5 - Send drone	resolved	11/1/2018 13:39
Intrusion	11/1/2018 13:39	CAM01	SS1-3-18	Intrusion @ SS1-3-18	Activities	ops	11/1/2018 13:39	A2 - System testing	resolved	11/1/2018 13:40
Intrusion	11/1/2018 13:42	CAM01	SS1-3-19	Intrusion @ SS1-3-19	TRUE	ops	11/1/2018 13:42	T5 - Send drone	resolved	11/1/2018 13:42
Intrusion	11/1/2018 13:49	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 13:49	A2 - System testing	resolved	11/1/2018 13:49
Intrusion	11/1/2018 13:50	CAM01	SS1-3-18	Intrusion @ SS1-3-18	Activities	ops	11/1/2018 13:51	A2 - System testing	resolved	11/1/2018 13:51
Intrusion	11/1/2018 13:50	CAM01	SS1-3-17	Intrusion @ SS1-3-17	TRUE	ops	11/1/2018 13:50	T5 - Send drone	resolved	11/1/2018 13:51
Intrusion	11/1/2018 13:52	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 13:55	A2 - System testing	resolved	11/1/2018 13:55
Intrusion	11/1/2018 14:07	CAM01	SS1-3-22	Intrusion @ SS1-3-22	TRUE	ops	11/1/2018 14:07	T5 - Send drone	resolved	11/1/2018 14:07
Intrusion	11/1/2018 14:07	CAM01	SS1-3-21	Intrusion @ SS1-3-21	Activities	ops	11/1/2018 14:07	A2 - System testing	resolved	11/1/2018 14:07
Intrusion	11/1/2018 14:20	CAM01	SS1-3-14	Intrusion @ SS1-3-14	Activities	ops	11/1/2018 14:23	A2 - System testing	resolved	11/1/2018 14:23
Intrusion	11/1/2018 14:26	CAM01	SS1-1-1	Intrusion @ SS1-1-1	Activities	ops	11/1/2018 14:27	A2 - System testing	resolved	11/1/2018 14:28
Intrusion	11/1/2018 16:16	CAM01	SS1-1-5	Intrusion @ SS1-1-5	Activities	ops	11/1/2018 16:17	A2 - System testing	resolved	11/1/2018 16:19

Figure A-9 shows that an alarm was received and the associated camera displays a potential intruder to the operator, who can then decide to dispatch resources or not.

Figure A-9. IPAMS Screen – Valid Alarm Received

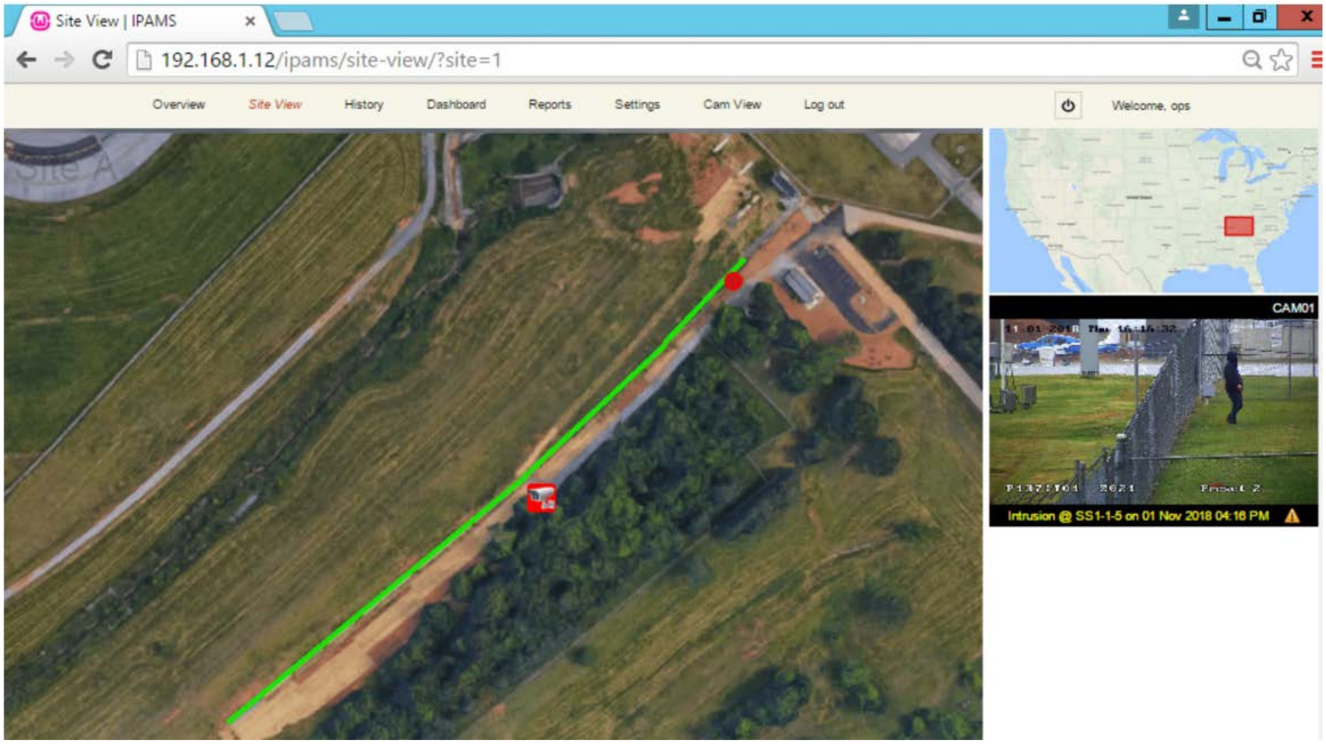
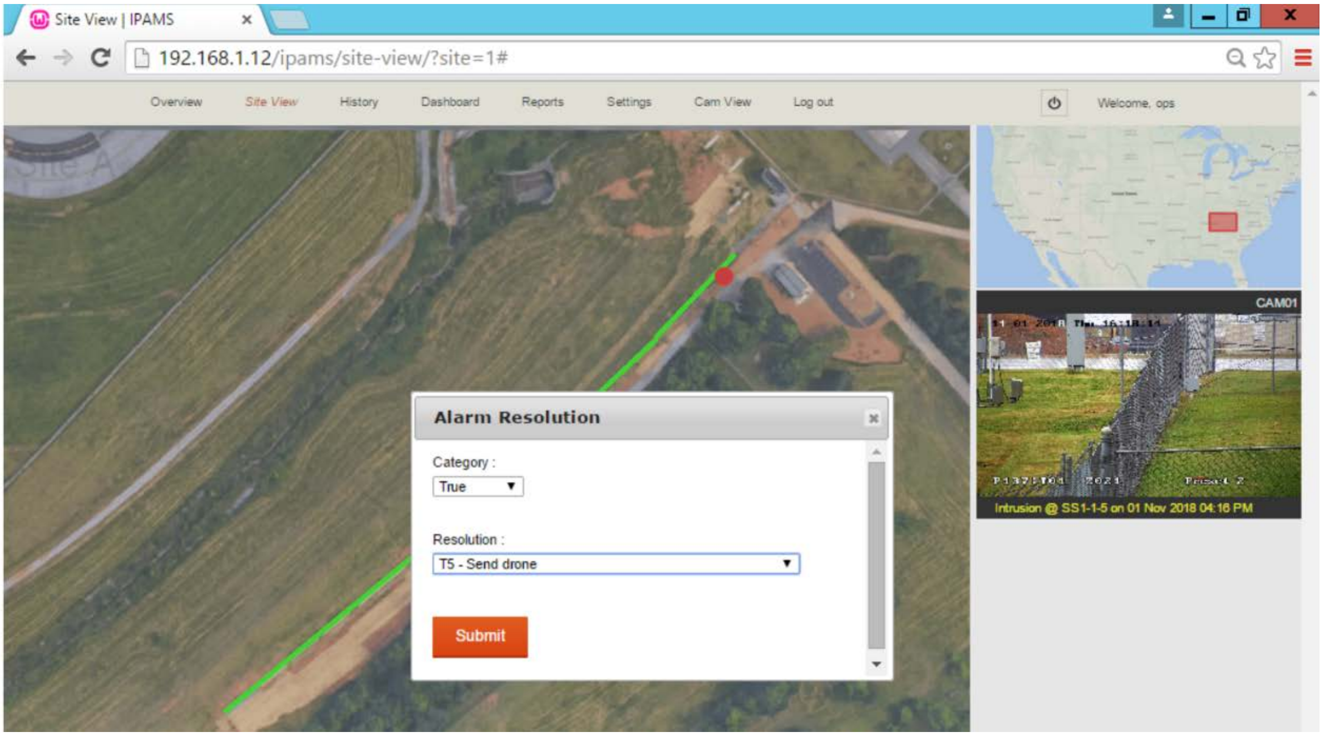


Figure A-10 depicts the SOC operator's response after evaluation of the alarm event, which was to "Send drone." Additionally, as shown in Table A-1's Resolution Type column, the operator made the determination that no response was required for some of the PIDS alarms that were received (i.e., "System testing").

Figure A-10. IPAMS Screen – UAS Alarm Response



6. Percepto Autonomous UAS Results

As part of the site setup prior to the start of testing, the Percepto UAS was programmed and geofenced to the PTF fence configuration, which included the configurations of an ‘exclusion zone’ so that the Percepto UAV would avoid the area designated for the Hoverfly Tethered UAS.

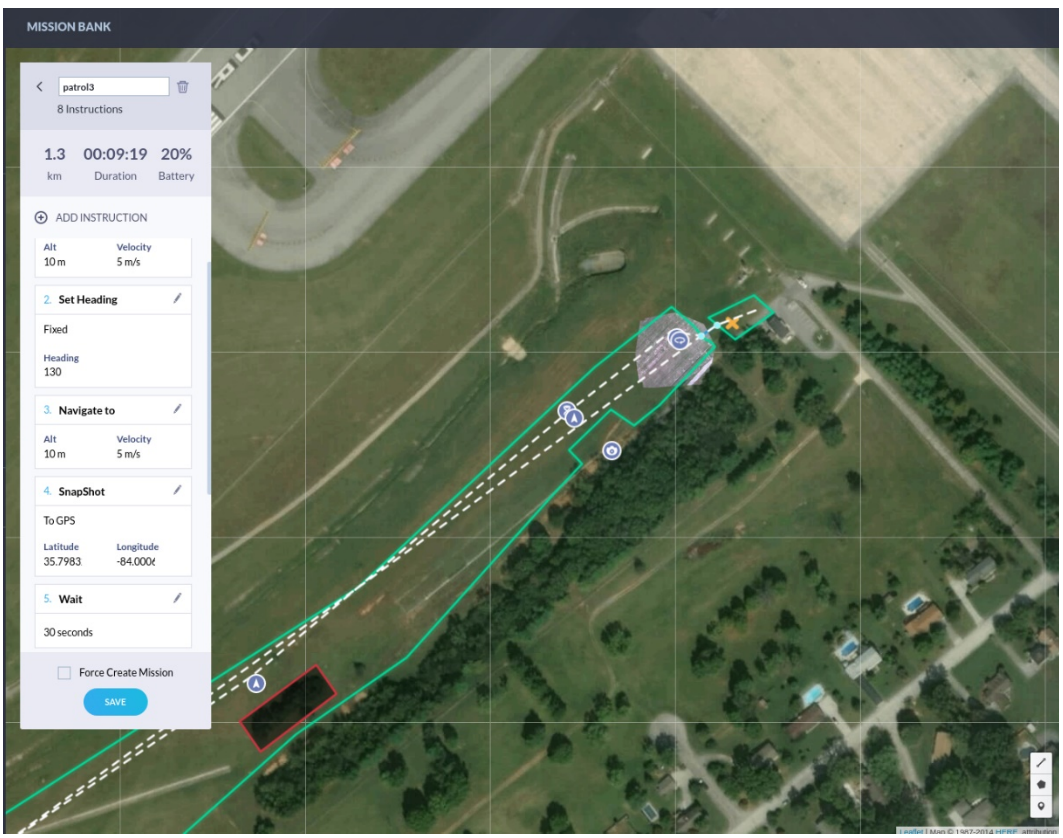
Two pre-programmed perimeter fence patrols were configured within the Percepto CMS: Patrol Mission 2 (Figure A-11) and Patrol Mission 3 (Figure A-12). The green lines represent the geofenced mission flight bounding box, which within their system becomes a free zone for the UAV to fly.

The system is intuitive. The white dotted line is the UAV path; the exclusion zone is bounded in red. The chart on the left-hand side of the screenshot represents the mission planning. It is noted that for Patrol 2, 12 instructions were to be carried out by the UAV. One instruction caused the UAV to switch from day to night camera mode. While not shown under in the visible portion of the ‘instructions’ window, the mission screen detailed the requirement for the UAV to use its camera to pan a wide area for observational purposes prior to reaching the end of the mission and heading back to Percepto Base Station, which is depicted with an X at the top right-hand side of the screen. The CMS also gives the operator an overall indication of the flight mission duration and the amount of UAV battery power need to accomplish the mission.

The Percepto UAS was also programmed to respond to PIDS sensor alarms and the associated pre-programmed GPS information associated with that PIDS sensor from its fixed base station location.

Figure A-11. Percepto Patrol Mission 2: Percepto CMS Screenshot

Figure A-12. Percepto Patrol Mission 3: CMS Screenshot



6.1 Autonomous UAS Scenario Review

This section provides detailed information with the pertinent information for the Percepto Autonomous UAS carrying out the various generic scenarios set up as part of the Use Case Study effort. Table A-2 documents all the test missions that were carried out at the PTF. It should be noted that the table only includes unique documentation to avoid redundancy, as multiple mission flights were undertaken.

Setup and demonstration testing took place on October 31, 2018, and the formal testing effort was conducted on November 1. Note that Table A-2 has been corrected for the PTF local time zone. The screenshots shown in the sections below were taken from the Percepto UAS laptop, which was set to Israel time (GMT+2).

Table A-2. Percepto UAS Test Log

Mission ID	Date	Time	Mission Name	Duration (in seconds)	Comments	Reference Information
10201	10/31/18	8:50	Jump To Alert-30	647	Setup Testing	
10202	10/31/18	9:16	Jump To Alert-31	464	Setup Testing	
10206	10/31/18	10:02	Auto Jump To Alert-35	282	Testing	
10215	10/31/18	11:11	patrol2	259	Setup Testing	
10216	10/31/18	12:47	patrol2	416	Fence patrol	mission plan, snapshots from drone, playback screenshot, thermal snapshot, video
10217	10/31/18	13:31	patrol2	762	Testing	
2439	10/31/18	15:00	Jump_to_alert-32	715	Tracking	video
10218	10/31/18	15:39	mapping	646	Demonstration Testing	
2443	11/1/18	9:02	Jump To Alert-43	574	PIDS Alarm Received Suspect Tracking	video
10219	11/1/18	9:12	Auto Jump To Alert-44	323	PIDS Alarm Received	
10221	11/1/18	9:17	patrol2	402	Fence patrol	operation screenshot, snapshots from drone
10222	11/1/18	9:49	Auto Jump To Alert-46	289	PIDS Alarm Received	Video
10223	11/1/18	9:09	patrol2	375	Fence patrol	
10224	11/1/18	10:15	Jump To Alert-47	348	Manually Launch Mission based on PIDS Alarm Received	
10225	11/1/18	10:55	patrol3	404	Fence patrol	
10226	11/1/18	11:06	Auto Jump To Alert-48	327	PIDS Alarm Received	
10227	11/1/18	11:52	patrol3	605	Fence patrol	mission plan, video, thermal image
10228	11/1/18	13:43	Jump To Alert-51	327	PIDS Alarm Received	playback screenshot, snapshot, thermal image, video
10229	11/1/18	14:07	Auto Jump To Alert-53	298	PIDS Alarm Received	
10231	11/1/18	16:38	mapping	644	Demonstration	

6.2 Missions 10216 and 10221: Autonomous UAS

The test script for this patrol scenario calls for the UAS to perform an autonomous perimeter patrol. The UAV shall provide real-time data and video back to the command-and-control workstation, allowing the security operator to evaluate the perimeter.

The Percepto UAS was launched and told to follow Patrol 2 for this mission (Figures A-13 and A-14). For these test flights, the mission was to patrol the PTF perimeter autonomously within the pre-programmed geofenced bounding box. (See Figure A-15 for a screenshot of the CMS live view of Mission 10221). The UAV was to leave its base station and autonomously follow a predetermined path using GPS coordinates, stop to inspect the Hoverfly launch site, provide a panorama and take color and thermal image snapshots of the area, perform a general flyover of the perimeter, turn to return home and provide a full view the PTF, complete the fence patrol, and return to base. This mission was carried out successfully.

Figure A-13. Percepto Mission 10221, Patrol 2: CMS Live View

Figure A-14. Percepto Mission 10221, Patrol 2: Snapshot of HoverFly Area

Figure A-15. Percepto Mission 10221: Live View Screenshot – Thermal Snapshot of Hoverfly Area

The Percepto UAS provided real-time data and video back to the command-and-control workstation, allowing the security operator to evaluate the perimeter patrol in real time. The CMS also allowed for video to be stored for future playback.

This mission can be viewed at:
https://youtu.be/8r1FcuncSeM

6.3 Mission 10227: Autonomous UAS

The test script for this patrol scenario calls for the UAS to perform an autonomous fence patrol. Should a human and/or vehicle be detected during the fence line patrol, the UAV shall support human/vehicle detection and tracking, along with notification to the operator. The UAV shall provide real time data and video back to the command-and-control workstation, allowing the security operator to evaluate the threat along the fence line.

The Percepto UAS was launched and told to follow Patrol 3 for this mission (Figure A-16). For this test flight, the mission was to patrol the PTF perimeter fence line autonomously. The UAV would leave from its base station and follow a predetermined path using GPS coordinates, stop to inspect the Hoverfly launch site, provide a panorama of the area, take a thermal image snapshot of the area adjacent to the Hoverfly launch location, and alert the operator when objects appeared in the scene to allow for object tracking. The system allowed for the operator to take command and then return the system to autonomously complete the fence patrol and return to base. This mission was carried out successfully.

Figure A-16. Percepto Mission 10227, Patrol 3: Thermal Image

The Percepto UAS provided real-time data and video back to the command-and-control workstation, allowing the security operator to evaluate the fence line and the potential threat in real time. The CMS also allowed for video to be stored for future playback.

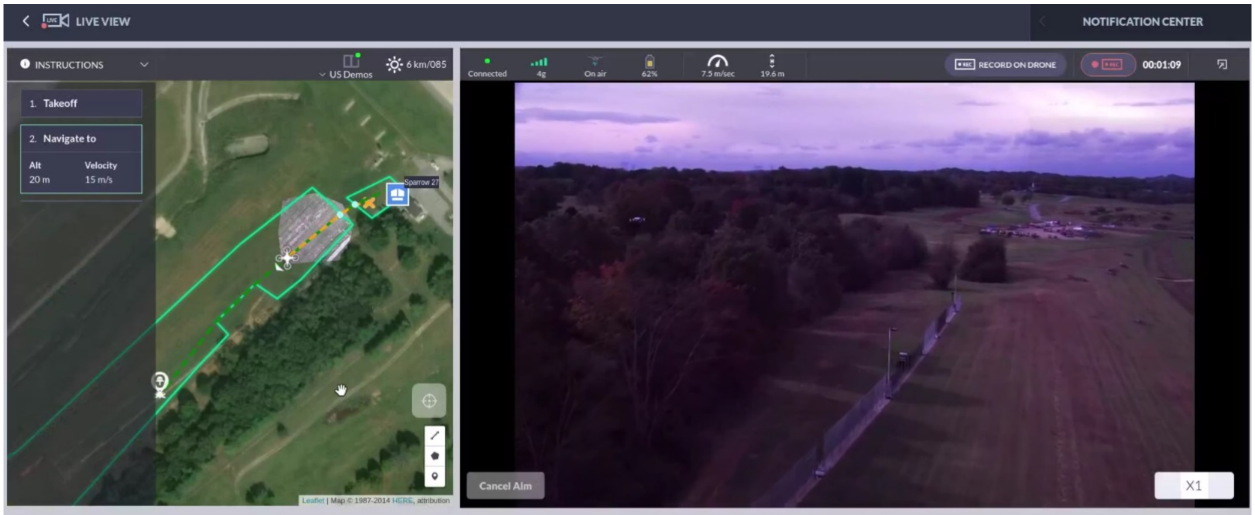
This mission can be viewed at:
https://youtu.be/Bri5dwvrSnI

6.4 Mission 10219: Autonomous UAS Alarm Response

The test script for this scenario calls for the UAS to respond to a PIDS alarm and the associated pre-programmed GPS information associated with the PIDS sensor, from the fixed-base location. Once the potential threat is detected, the UAS shall provide real time video feed back to the command-and-control workstation, allowing the security operator to evaluate the threat.

The Percepto UAS received a PIDS alarm and responded autonomously to the pre-programmed GPS information associated with the PIDS sensor from the fixed-base location. The UAS would respond to the notification autonomously via the UAS CMS integration, and proceed to the alarm location using the predefined sensor/zone information. The screenshot of the CMS in Figure A-17 shows the PIDS alarm location on the left-hand side map view, while the image on the right shows the UAV heading toward the alarm. The mission was carried out successfully.

Figure A-17. Percepto Mission 10219: Autonomous Alarm Response with Image



6.5 Mission 2443: Autonomous UAS Alarm Response and Tracking

The test script for this scenario calls for the UAS to respond to a PIDS alarm and the associated preprogrammed GPS information associated with the PIDS sensor from the fixed base station. Once the potential threat is detected, the UAV shall use machine learning and video analytics to track the potential threat and provide real time video feed back to the command-and-control workstation, allowing the security operator to evaluate the needed threat response.

The Percepto UAS received a PIDS alarm and responded autonomously to the preprogrammed GPS information associated with the PIDS sensor from the fixed base station. Once the potential threat was detected, the UAV alerted the operator and began to track the threat. Real-time video was continuously transmitted back, allowing the security operator to evaluate the threat. The operator then disengaged the tracking and sent the UAV back to its base station.

The screenshot of the CMS in Figure A-18 shows the PIDS alarm location on the left-hand side map view, while the image on the right shows the UAV heading toward the alarm. The mission was carried out successfully.

The Percepto UAS sent data and video back to the command-and-control workstation, allowing the security operator to evaluate the PIDS alarm and the tracking of the potential threat in real time. The CMS also allowed for video to be stored for future playback.

This mission can be viewed at:
https://youtu.be/qo58SQdDAkU

6.6 Mission 10228: Autonomous UAS Fence Patrol with Alarm Response

The test script for this scenario called for the UAS to perform an autonomous fence patrol. During the patrol flight, the test team shall generate a PIDS alarm at a fence segment (sensor location), requiring the UAV to abandon the programmed patrol route along the fence line and respond to this alarm event. The UAV shall provide alarm response support and inspection by transmitting real-time data and video feed back to the command-and-control workstation, allowing the security operator to evaluate the threat.

The Percepto UAS was launched and told to follow Patrol 3 for this mission (Figure A-18). For this test flight, the mission was to patrol the PTF fence line autonomously, leaving from its base station and following a predetermined path using GPS coordinates. A PIDS alarm was received after launch, causing the UAV to redirect to the alarm location (Figure A-18). The operator was able to take snapshots of the potential threat using both the day (Figure A-19) and thermal (Figure A-20) cameras. After the threat evaluation was complete, the operator sent the UAV back to the base station. This mission was carried out successfully.

Figure A-18. Percepto Mission 10228: Autonomous Alarm Response

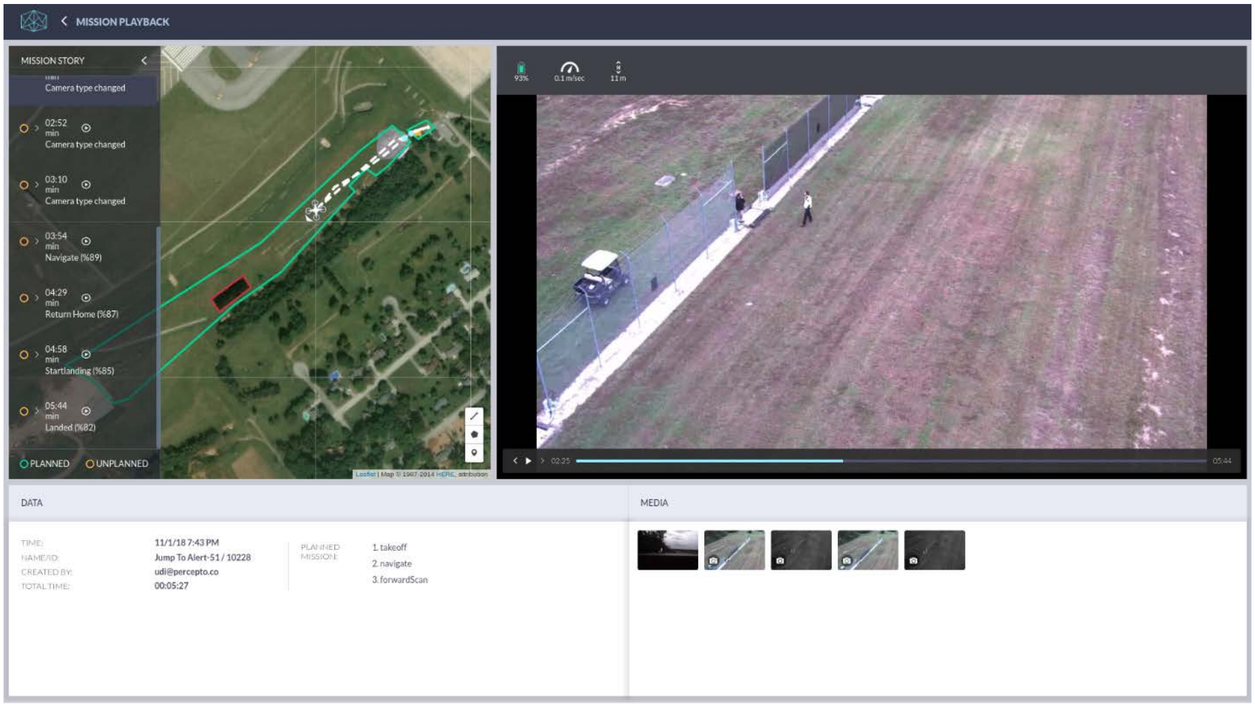


Figure A-19. Percepto Mission 10228: Color Camera Snapshot at Alarm Location

Figure A-20. Percepto Mission 10228: Thermal Camera Snapshot at Alarm Location

The Percepto UAS provided data and video to the command-and-control workstation, allowing the security operator to evaluate the PIDS alarm associated with the potential threat along with the fence line in real time. The CMS also allowed for video to be stored for future playback.

This mission can be viewed at:
https://youtu.be/oFdfvgkg0Rg

6.7 Mission 10231: Autonomous UAS Anomaly Mapping

The UAV shall use computer vision and machine learning capabilities to perform anomaly detection.

Note: The Percepto representatives indicated that the software installed on the demonstration system required the use of post processing algorithms to detect anomalies, and that the newer software performs this function in real time.

The screenshot in Figure A-21 shows the area that the UAS was told to observe for anomaly detection. Figure A-22 provides the screenshot from the system's anomaly comparison analytic, and Figure A-23 is an example screenshot from when the system detected the anomaly.

While this functionality was deemed important, the research team found it difficult to assess this demonstration as a complete success, since only the older software was available. That said, the system was able to properly detect when an object was left behind, albeit not in real time.

Figure A-21. Percepto Mapping Compare Screen

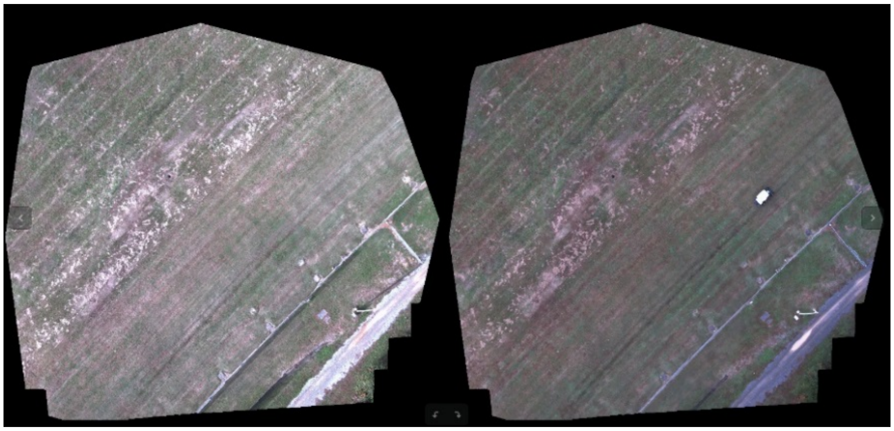
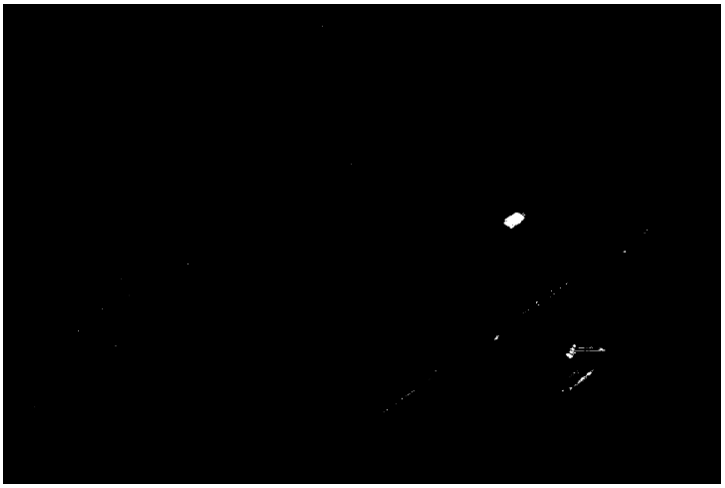


Figure A-22. Percepto Mapping Mission 10231

Figure A-23. Percepto Mapping Differential Screenshot



7. HoverFly Tethered UAS Results

As a tethered UAS, the Hoverfly LiveSky UAS did not need to be geofenced. The Hoverfly UAS has the option of operating from a local command-and-control hardened launch kit, or connected to a network via the HxGN Smart Command Center. For this Use Case Study, command and control for the Hoverfly

UAS was accomplished using the network connected HxGN Smart Command Center. As part of the site setup, prior to the start of testing, the HxGN Smart Command Center was programmed to support the PTF fence configuration.

The HxGN Smart Command Center is part of Hexagon Safety and Infrastructure's HxGN Smart Command application. HxGN Smart Command is a cloud-based security and monitoring software application, which interfaces with the Hoverfly UAS platform. The system is browser-based.

The Smart Command Center setup at the PTF can be viewed at: https://youtu.be/VxyBgYrm8DE

One preprogrammed perimeter fence patrol was configured within the HxGN Smart Command Center. The system uses a map of the site, which uses GPS coordinates for the location of the Hoverfly LiveSky as well as the PIDS alarm points. The software allows the operator to launch the LiveSky, adjust the flight elevation, rotate, and zoom and switch between the color and thermal cameras

7.1 Tethered UAS Scenario Overview

This section provides detailed information along with pertinent information and photos for the Hoverfly Tethered UAS carrying out the various generic scenarios set up as part of the Use Case Study effort.

Hoverfly and their support team were only able to commit to being at the PTF October 31 and the morning of November 1, 2018. Setup and demonstration testing took place on October 31, and formal test flights were performed the morning of November 1. Table A-3 documents all the test flights that were carried out at the PTF. Note that the table has been corrected for the PTF local time zone. The videos and screenshots shown in the below were taken from the HxGN Smart Command workstation, which was set to central time zone.

In order for airports to get a better sense of the amount of space required for the tethered UAS, a video has been provided showing one of UAS landings at the PTF.

The Hoverfly Tethered UAS landing can be viewed at: https://youtu.be/1QYnO8gX80k

Table A-3. Hoverfly Tethered UAS Test Log

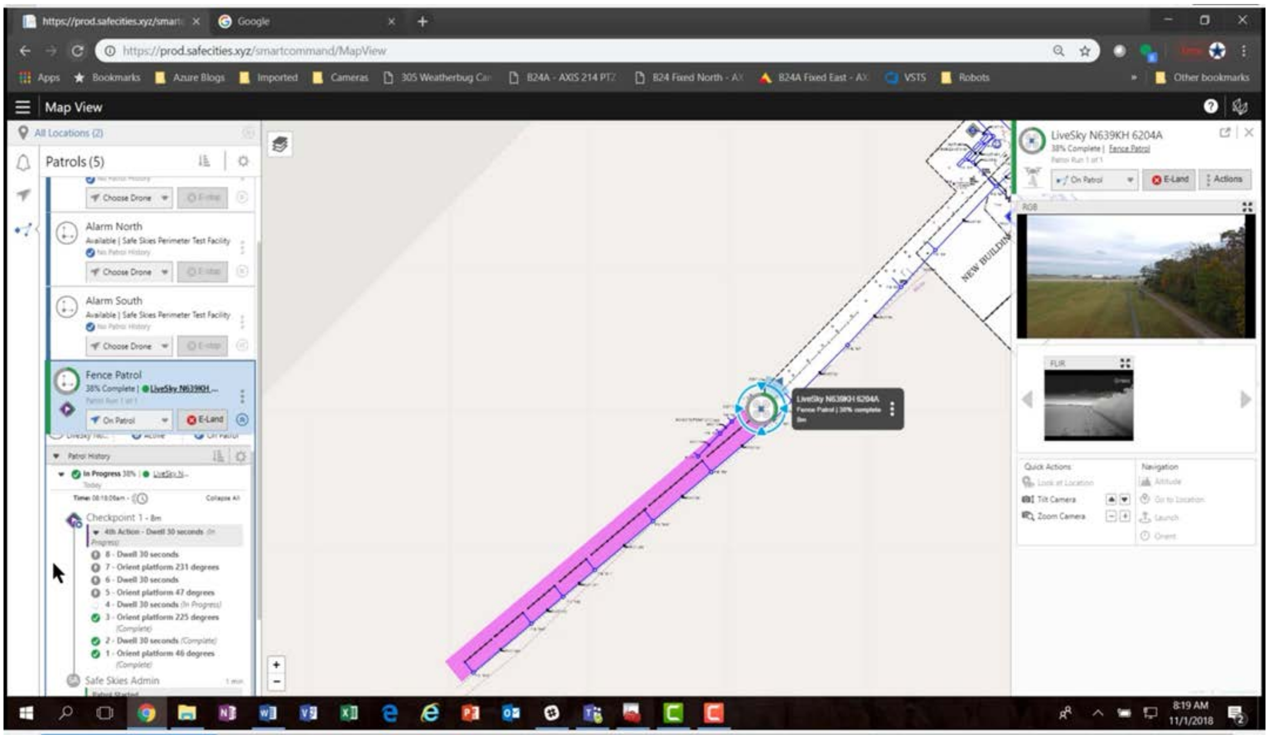
Flight No	Date	Time	Flight Type	Comments	Reference Information
1	11/1/18	9:17	Fence Patrol	Manually Launched	HoverFly at PTF Flight 1 (Fence Patrol)
2	11/1/18	9:49	PIDS Alarm	PIDS Alarm Received	Video
3	11/1/18	10:09	Fence Patrol / PIDS Alarm	Launch Fence Patrol and then respond to PIDS Alarm	Video of manual start of Fence Patrol, then response to PIDS alarm, manual landing.
4	11/1/18	10:25	Perimeter Patrol	Manually Launch and control a Fence and Perimeter review	Video of patrol and manual tracking of potential intruder
5	11/1/18	10:56	Fence Patrol	Manaul Fence patrol	Video of the Patrol and landing of Percepto
6	11/1/18	11:07	PIDS Alarm	PIDS Alarm Received	Video of Day and Thermal Camera Images
7	11/1/18	11:52	Fence Patrol	Manually Launch and track suspect along fenceline	Video of patrol and manual tracking of potential intruder

7.2 Flights 1 and 5: Tethered UAS Fence Patrols

The test script for this patrol scenario calls for the UAS to perform a fence patrol. The UAV shall provide real time data and video back to the command-and-control workstation, allowing the security operator to evaluate the perimeter.

Using the Smart Command Center, the security operator manually launched the Hoverfly UAS to start a programmed fence patrol to view locations along the fence line for inspection and/or evaluation. Video was transmitted in real time to the Smart Command Center, allowing a security operator to evaluate and perform a remote inspection of the fence line. The flight was carried out successfully. Figure A-24 shows a screenshot of the location, identifying the test area.

Figure A-24. Hoverfly Fence Patrol Flight 1



In order to preserve the flight information and all the operator actions, as well as the real-time data and video coming into the HxGN Smart Command Center, the operator screens were recorded.

These flights can be viewed at:
Flight 1 https://youtu.be/-1LYpAoWoRI;
Flight 5: https://youtu.be/gSdaVeymdvc

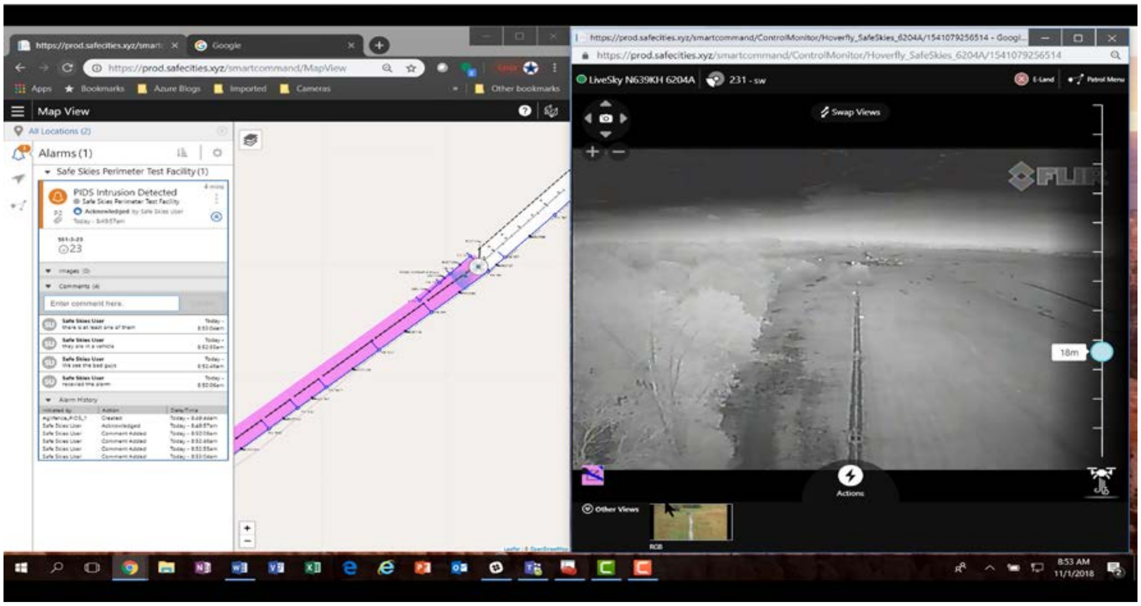
7.3 Flights 2 and 6: Tethered UAS Alarm Response

The test script for this scenario calls for the UAS to respond to a PIDS alarm and the associated preprogrammed GPS information associated with the PIDS sensor, from the fixed-base location. Once the potential threat is detected, the UAS shall provide real time video feed back to the command-and-control workstation, allowing the security operator to evaluate the threat.

The LiveSky Tethered UAS was configured to respond to a PIDS alarm from its fixed launch location. The Hexagon software obtained the alarm via the integration. The operator launched the UAS in response to the notification, which then proceeded to aim its camera toward the alarm location using predefined sensor GPS coordinates.

Real-time video was transmitted back to the HxGN Smart Command Center, allowing the security operator to evaluate the threat. For Flight 6, the operator switched from the day to the thermal camera to observe the potential threat at the PIDS alarm location. Figure A-25 shows screenshots that indicate the location compared to the test area and the video from that location.

Figure A-25. Hoverfly Fence Patrol Flight 2



In order to preserve the flight information and all the operator actions, as well as the real-time data and video coming into the HxGN Smart Command Center, the operator screens were recorded.

These flights can be viewed at:
Flight 2: https://youtu.be/-1LYpAoWoRI
Flight 6: https://youtu.be/Syoq2EjKrXo

It should be noted that Hoverfly has the capability to be configured in a "follow me" mode for perimeter fence patrols. This test was not performed at the PTF as the UAV provided was not configured to support this test. However, it is our understanding that the Hoverfly On the Move vehicle capability is a standard feature of the tether-powered system and receives its power either through a 110-V generator or a DC-to-AC vehicle inverter. Hoverfly informed the research team that their UAS can be configured to lead, flank, or follow a vehicle traveling at speeds up to 25 mph when equipped with Hoverfly's mobile integration solution where there are safe overhead clearances. Video is transmitted back to the Smart Command Center via cellular or wireless connectivity.

7.4 Flight 3: Tethered UAS Perimeter Patrol with Alarm Response

The test script for this scenario calls for the UAS to perform a perimeter patrol. During the patrol flight, the test team shall generate a PIDS alarm at a fence segment (sensor location) requiring the UAV to *redirect its camera from the patrol route along the fence line and respond to this alarm event. The UAV shall provide alarm response support and inspection by transmitting real time data and video feed back to the command-and-control workstation, allowing the security operator to evaluate the threat.*

With the Hoverfly UAS at its fixed location, and while the LiveSky UAV is observing a fence segment while performing a perimeter patrol, (Figure A-26) the research team generated a PIDS alarm at a fence segment. Upon receipt of the alarm, the UAS operator redirected the UAV camera from the patrol route along the fence line to respond to the alarm event to provide inspection by transmitting real-time video feed back to the Smart Command Center (Figure A-27), allowing the security operator to evaluate the threat and provide as-needed breach tracking. This flight was completed successfully.

Figure A-26. Hoverfly Perimeter Patrol Flight 3

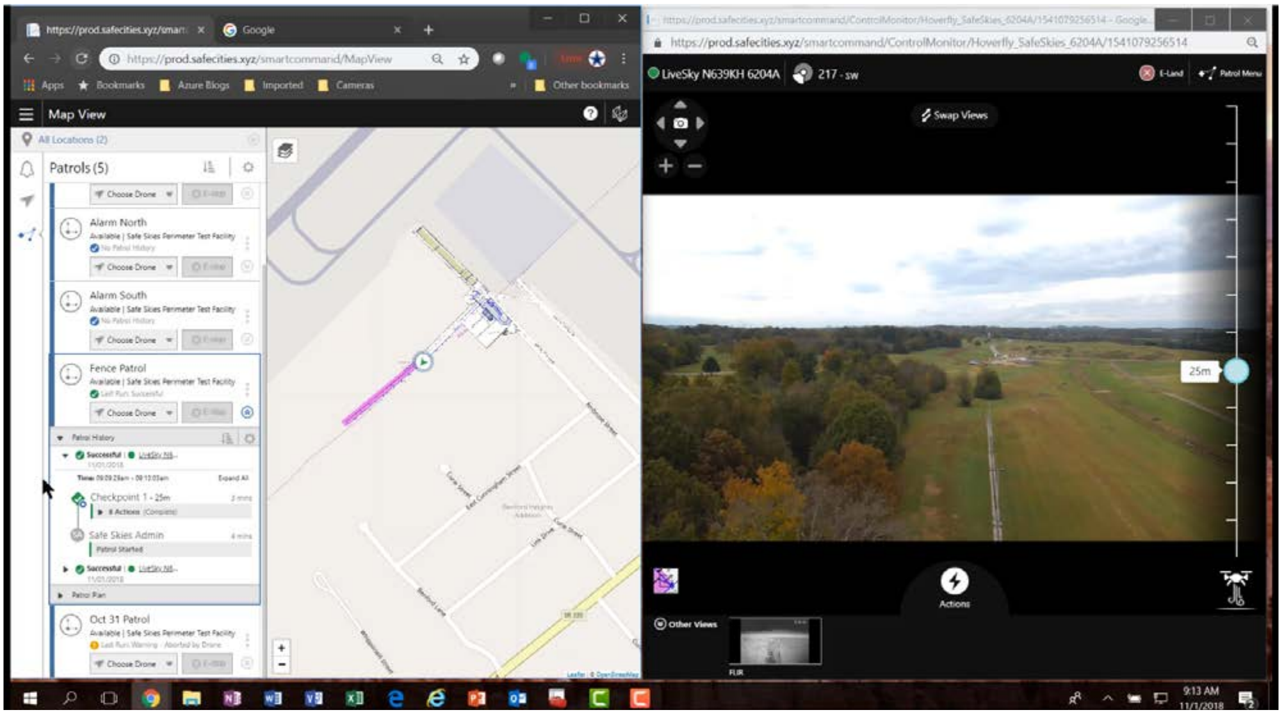
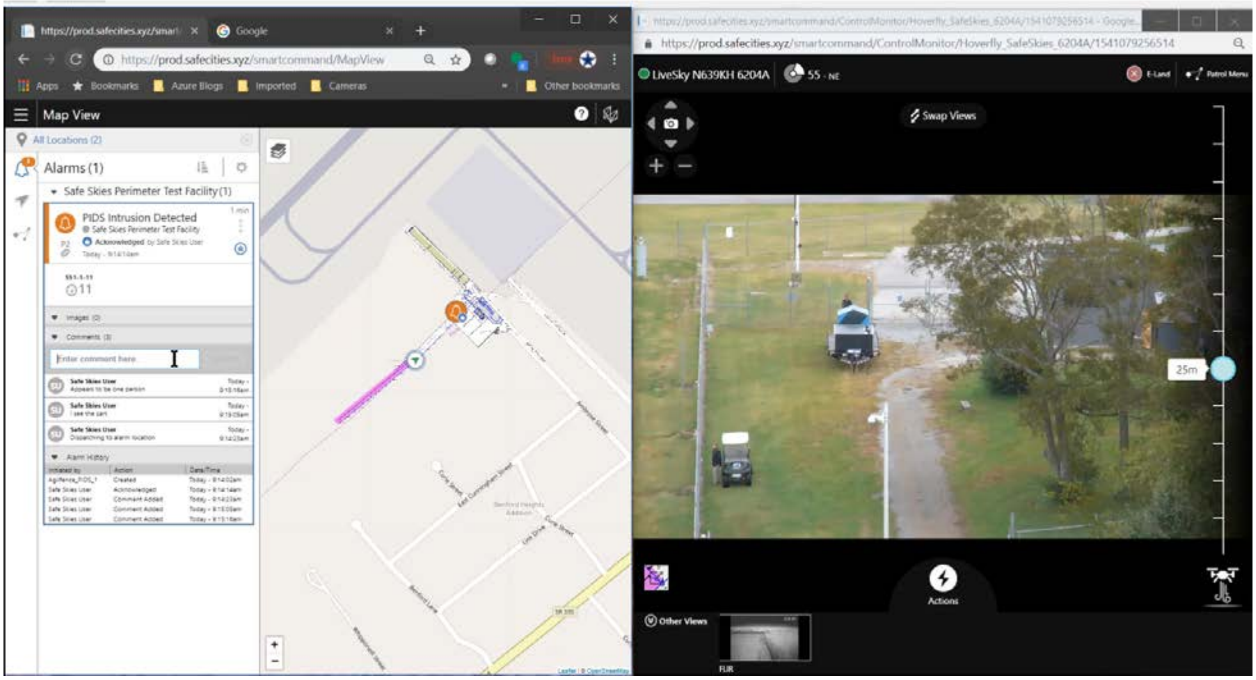


Figure A-27. Hoverfly Perimeter Patrol with PIDS Alarm Response Flight 3



In order to preserve the flight information and all the operator actions, as well as the real time data and video coming into the HxGN Smart Command Center, the operator screens were recorded.

This flight can be viewed at:
https://youtu.be/S0HXKp7P3Ac

7.5 Flights 4 and 7: Tethered UAS Manual Tracking

The test script for this patrol scenario calls for the tethered UAS to perform a fence patrol. Should a human and/or vehicle be detected during the fence-line patrol, the UAS operator shall track the human and/or vehicle, while providing real-time data and video back to the command-and-control workstation, allowing the security operator to evaluate the threat along the fence line.

For Flight 4, the security operator manually launched the Hoverfly UAS to a view a specific location along the fence line for inspection and/or evaluation. A potential threat was observed, and the operator zoomed into the area to investigate.

For Flight 7, the security operator was directed to view the fence line and track an observed potential threat. Real-time video was transmitted back to the Smart Command Center, allowing a security operator to evaluate these potential threats while performing remote inspections of the fence line. These flights were completed successfully.

In order to preserve the flight information and all the operator actions, as well as the real-time data and video coming into the HxGN Smart Command Center, the operator screens were recorded.

These flights can be viewed at:
Flight 4: https://youtu.be/0GKwMaJ0-IQ
Flight 7: https://youtu.be/pvvFQUsblQc

8. Summary of Results and Findings

- The integration was successfully accomplished with both the autonomous and the tethered UAS.
    - Prior to arrival, Hoverfly disclosed that the HxGN Smart Command Center internal integration with Hoverfly was still under development, such that the integration with the PIDS required that the HxGN operator receive the PIDS alarm and manually start a preprogrammed sequence for either Fence Inspection or Alarm Response.
- Both UAS performed well overall, and in accordance with their published specifications.
- Testing of the tethered UAS provided the following information:
    - The tethered UAS can provide situational awareness of the airport perimeter by providing a relatively high vantage point for a high-resolution color or thermal camera to observe an area, such as a roadway, fence segment, or a vehicle gate for long periods of time.
    - The tethered UAS can be quickly set up in an area to provide an almost instant camera tower in support of airport security and/or operations events and activities, providing secure video streaming via the tether.
    - The tethered UAV was observed having issues in windy conditions and may not be able to operate in rain.
    - There are fewer safety considerations, due to the fact that the UAV is tethered.
    - Although not tested, the Hoverfly Tethered UAS "follow me" mode would allow perimeter patrols to take place from the ground and from an elevated position. The patrols can be recorded or be observed live by the SOC to act as a force multiplier.
- Testing of the autonomous UAS provided the following information:
    - The Percepto Autonomous UAS was able to fly programmed, autonomous missions along the PTF perimeter, providing situational awareness along the fence line.
    - The Percepto Autonomous UAS was able to fly programmed, autonomous missions in response to PIDS alarms, providing support for threat response. The UAS allowed for object tracking and manual control, and supported the ability to take snapshots of the observed scene.
    - An autonomous UAS is configured with geofence mapping to ensure the UAV stays within designated areas as it responds to alarms or provides perimeter patrols.
    - As the UAS autonomously responds to alarm events, an SOC operator can use the situational awareness data provided to direct LEO and/or security guard response, thereby keeping responders safe.
    - The Percepto Autonomous UAS is configured with real-time analytics that support fully autonomous navigation and landing, anomaly notification, and object tracking.
        - It should be noted that at the end of one PIDS alarm response mission, while attempting an autonomous landing, it got windy and started to rain. The Percepto UAV autonomously landed in 19 mph wind, while gusts up to 22 mph were recorded. The UAV made multiple landing attempts, automatically adjusting for the wind and using AI and machine learning to continuously adjust to find the center of its landing pad, in order to safely land on the Percepto Base Station.

This landing can be viewed at:
https://youtu.be/qY7PShtphEU

ATTACHMENT A: PERCEPTO SPARROW AUTOMATED DRONE SYSTEM DATASHEET

SPARROW 2.0
AUTOMATED DRONE SYSTEM

ON-SITE 24/7 MULTI-TASK DRONE

The Sparrow 2.0 Automated Drone System enables high-quality fully-automated security, safety and inspection missions to be executed on-site with powerful technologies such as dynamic flight applications, automatic safety features and PerceptoCore 2.0 processing unit. The system eliminates human risk and provides a safer, more efficient and cost-effective method compared to traditional security, safety and inspection methods. Together with the Base Station and the Cloud Management Software (CMS), the Sparrow 2.0 carries out once hazardous and imprecise missions with ease and incredible accuracy.

PERFORMANCE SPECIFICATIONS

- Up to 35 minutes of continuous flight
- Charging time under 1 hour
- Max. Range: 5km (3 mi)
- Max. Altitude 130m (400ft.)
- Max Speed: 30 Knots
- Max. Take-off Weight (MTOF): 10kg (22lbs)

INTUITIVE INTERFACE

The Cloud Management Software is a single software tool whose intuitive interface optimizes mission planning, monitoring and analysis. The remote pilot schedules pre-defined missions in the CMS, delivering heightened site safety and operation. Security, safety and inspection missions are pre-defined with numerous mission operations and customized site maps.

PRECISION LANDING

The Base Station supports accurate landing for a drone equipped with the Percepto precise landing feature. The base station, in its open position, provides a flat landing pad. The landing pad is the highest part in its proximity, providing a landing surroundings with no obstructions. The clear landing area is compatible with a landing pattern cover, which complements the computer vision algorithm and enables the accurate landing feature. The base station accounts for error margins of up to 30cm in landing final positioning, and up to 20° in landing final heading. Landing pad is also able to perform night landings with day camera.

LIVE FEATURES

The Sparrow 2.0 Automated Drone System can be controlled by the remote pilot at any time via live operation features. The remote pilot can command the drone to perform specific tasks to manage any unforeseen situation—such as detect and track a target, toggle the night camera, and navigate to a specific location and land.

EMERGENCY PROCEDURES

The Sparrow 2.0 Automated Drone System automatically carries out a number of emergency procedures, responding to extreme weather conditions, security breaches, and potential system failures. When emergency triggers are detected, the Sparrow 2.0 automatically returns to the base station for landing, or lands in a 'safe zone' on site. In order to effectively carry out emergency procedures, the Sparrow 2.0 System automatically keeps track of the latest known battery state, GPS coordinate, and the closest 'safe zone' GPS coordinate.

APPLICATIONS

Safety » Detect and track people and moving objects in FOV 24/7 delivering live data stream to remote pilot
Security » Scan site for fires and gas leaks and automatically alert authorities and on-site personnel
Inspection » Capture and analyze high definition snapshots and continuous video streams

QUICK SPECS

DRONE

Dimensions (propeller tip; diagonal)..............................1062 (mm)
Weight:..9.5kg
Material:...Carbon fiber composite IP55
Propulsion:.........................KDE Electric Motor; 360 RPM/V; 230g
Battery:.. 6S Li-ion Battery
Day Camera:...................................4096x3000 resolution at 30FPS
Thermal Camera:................ 640x512 resolution, frame rate 30 Hz

Base Station

Dimensions:..153x153x157 (cm, closed)
Weight:...162kg
Material:...IP55
Communications:...Ethernet

SPARROW 2.0 SPECIFICATIONS

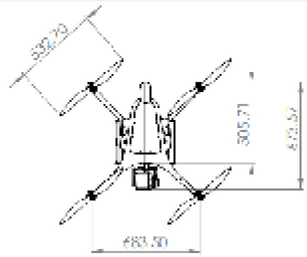
Overview

The Sparrow 2.0 delivers an industrial grade, highly automated drone solution equipped with cutting edge technology providing high-quality live feedback from every mission. Weighing just 9.5kg (21 lbs.), the Sparrow 2.0 dexterously performs security, safety and inspection missions. Its fully redundant design featuring 2 GPS and 2 IMU provides for impressively precise results. Based on technology unique to Percepto, the Sparrow 2.0 combines robust design with powerful sensors allowing for 24/7 data capture and surveillance to optimize site production, safety and security.

Fuselage

The Sparrow chassis is a Composite material, mainly carbon fiber quad copter classic monocoque frame.

Rotor Diameter: 239mm
Height (ground to rotor): 245mm
Arm Length: 370mm
Skids Distance: 237mm



Flight Controls

Pixhawk 2.1 Flight Controller is a triple redundant open sourced PX-4 based autopilot module designed by 3D Robotics that runs an efficient, real-time operating system. With a total of 29 sensors the Pixhawk 2.1 delivers reliable, high-quality performance and reliability.

- 168 MHz Cortex M4F CPU
- Sensors:
  - 3 x GPS Capability
  - 2 x Compass
  - 2 x Barometer
  - 3 x Triple Axis Gyroscope
  - 3 x Triple Axis Magnetometer
  - 3 x Triple Axis Accelerometer
- Integrated backup, override and failsafe processor

Propulsion System

The Sparrow 2.0 is powered by the impressive KDE Direct brushless electric motor, delivering high-efficiency performance to the Sparrow and its components. Together with the carbon fiber Mejzlik propeller blades, the propulsion system delivers unprecedented smoothness and efficient flight performance.

Percepto Power Distribution Board

The **Percepto PDB module** provides onboard power delivery and power management capabilities to consumer and commercial drones. The Percepto PDB provides a hot swap controller and allows a board to be safely inserted and removed from a live power supply. The high precision measurement along with adjustable two steps down switching regulator, 10 Amps each, present a power management solution for high current applications. Non-volatile configuration allows for flexibility in the automatic generation of alerts and responding to faults. The Electro Magnetic Compatibility (EMC) oriented design helps establish Electro Magnetic Interference (EMI) proof environment and a better power distribution flow. EMI can hinder circuit performance and even halt performance all together. Therefore, by reducing EMI, data can securely and efficiently be transmitted.

Automatic Charging

Automatic charging inside the base station ensures for fully autonomous missions without any human interference required. Charging at 36 Amps minimizes charging time allowing the Sparrow 2.0 to quickly embark on its next mission.

PAYLOAD SPECIFICATIONS

Overview

The Sparrow 2.0 Payload packs powerful technologies into the Sparrow 2.0 while maintaining fast operation and a slim design. The Payload and onboard sensors are customized to fit the mission needs with cutting-edge sensors such as day and thermal cameras, *PIXHAWK 2.1 Autopilot* and *Mobilicom* IP communication unit. When combined, the Sparrow 2.0 Payload delivers powerful navigation, communication and data acquisition features enhancing the performance of the system.

Day Camera

The *FLIR Blackfly S USB 3.0 Vision* industrial camera, with Sony's 12.3 MP sensor IMX 253 provides low-noise performance with excellent image quality.

Specifications

Dimensions........57.5x50x44mm
Resolution........4096x3000
Weight........90g
Power Connector........USB 3
Frame Rate........30FPS

Electrical Specifications

Input Voltage........5V
Power Consumption........4.5W

Thermal Camera

Flir Tau 2 640 is a small form factor long wave IR camera with digital video.

Specifications

Dimension........43x43x43 (mm, without lens mount)
Resolution........640x512
Weight........72g
Power Connect........50-pin Hirose
Frame Rate........30Hz

Electrical Specifications

Input Voltage........4-6V DC
Power Dissipation (avg.)........1.3W

Communication

Mobilicom MCU30 Ruggedized Unit is an IP communication unit that provides ad-hoc direct wireless mobile communication.

Specifications

Dimensions........120x90x60 (mm)
Weight........550g
Frequency Range........75 MHz to 5.9GHz
Radio Band........2.4GHz

Electrical Specifications

Input Voltage........7-14.5V DC
Power Consumption........8-12W

LTE communication is established using the *Sierra EM-7455* LTE modem mounted on the drone

Sierra EM-7455

Dimensions........51X30X2.7(mm)
Frequency Bands........B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B2, B29, B30, B41

Sierra MP-70

Dimensions........190x45x105(mm)
Weight........0.76kg
Frequency Bands......B2, B4, B5, B13, B17, B25
Input Voltage........7-36V DC

Secondary Communication Channel
Low Frequency Radio Communication
5-8V and ECB

The low frequency emergency channel will retain the ability of the remote pilot to intervene and take any action necessary to. This allows the remote pilot to perform several emergency responses, preventing a potential dangerous situation.

Gimbal

The forward mounted, 2-axis brushless gimbal delivers impressive range of motion to achieve proper camera balance. *BaseCam Simple BGC 32-bit Extended* Controller with built-in frame IMU measures battery power consumption while controlling high quality 3-axix camera stabilizing systems.

Dimensions........50x50 (mm)
Power Consumption........8-26 V (3s-6s LiPo)

Flight Controller

PIXHAWK 2.1 Autopilot is an all-in-one 3 times redundant unit, combining FMU and IO into a single package with hardware floating point unit and SIMD.

Specifications

Dimensions........81.5x50.15.5 (mm)
Weight........38g
Processor........32-bit STM32F427 Cortex M4 core with FPU

Electrical Specifications

Input Voltage........5V DC (min 9V, max 57V)
Power Dissipation (avg.)........3.1W

PERCEPTO CORE 2.0 SPECIFICATIONS

Overview

The PerceptoCore 2.0 Module delivers real-time, onboard computer vision capabilities to consumer and commercial drones combined with high current power distribution board and pixhwak 2.1 carrier board. The low-cost, high-performance, and exceptionally powerful Linux module seamlessly connects to the drone's flight controller. Packing an NVIDIA® Jetson® TX2 power efficient high-end module, the module weighs less than 430 grams and is compatible with most commercial and consumer drones.

Features

- NVIDIA® Jetson® TX2 SoC
  - NVIDIA Pascal GPU with 256 CUDA Cores
  - ARM® Cortex® -A57 MPCore (Quad-Core) ProcessorA15 CPU
- On board Pixhawk 2.1 compatibility
- 120A Power Distribution Board
- DRAM – LPDDR4 – 1866, 8GB
- Flash – eMMC 32GB
- WIFI
- Bluetooth
- Up to 1 Tera SSD slot
- 3x Gigabit Ethernet
- USB
  - 1x USB 2.0 Micro B
  - 3x USB 3.0 Type C
- 8 x Temperature Sensor
- Optional Debug Port
- General Expansion
  - PPN/S.BUS
  - I2C
  - UART
  - CANBUS

System Architecture

The PerceptoCore 2.0 Platform is based on the NVIDIA® Jetson® TX2 application processor – a powerful computing chip responsible for all autonomous capabilities, due to its ability to process complex image algorithms. Pascal GPU architecture coupled with ARM® Cortex® -A57 CPU complex provide a near real-time solution for high-performance image processing.
The Lattice low power consumption MACH-XO2 FPGA allows the PerceptoCore 2.0 to control the drone by generating a PPM/SBUS signal. It also enables simultaneous control of the remote pilot and the computer control by manipulating the input R/C signal in real time. A safety mechanism allows for immediate transfer of control to the remote pilot at any time. The MACH-XO2 devices are based on a 65 nm non-volatile low-power process, providing low static power to all system components.

Connections

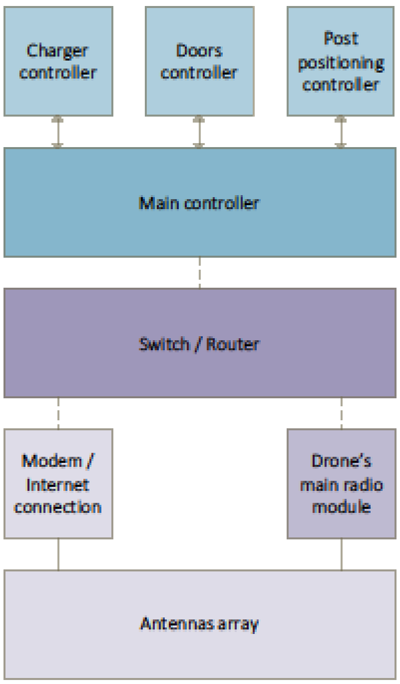
PerceptoCore 2.0 provides mechanisms to communicate with a PC and/or *USB 2.0 peripherals* and *USB 3.0 peripherals*, such as a camera or storage device. A *12C-bus* specification-compliant 12C master controller is implemented, supporting serial device communications to multiple devices. The *UART* provides serial data synchronization and data conversion for both receiver and transmitter sections. It also implements cutoff switch and an onboard *FPGA* generating a PPM/SBUS signal, enabling connection to the Flight Controller. The PerceptoCore 2.0 can be connected to a ground computer using the SDK via various channels including WIFI and LTE.

PERCEPTO

BASE STATION 3.0

SPECIFICATIONS

The Base Station rapidly charges the Sparrow 2.0, simultaneously transferring data to the Sparrow and the Cloud and protecting the Sparrow from harm. Automatic rapid charging enables the Sparrow 2.0 to operate autonomously with minimal human intervention. IP65 enclosure protects the Sparrow 2.0 from hazardous weather conditions, wildlife and malicious human interference. Automated lid and precision landing mechanisms with sub-millimeter positioning ensure accurate and safe takeoff and landing. The PCB 36 Amp charger rapidly charges the drone, while data is transferred and saved in the cloud.



Specifications

Electrical Specifications
Supply Voltage.........110V or 220V, single phase
Typical Power Consumption.........................2KW
Maximum Power Consumption 3KW
Operating Temperature..........................0-55°C
Charger..PowerLab 8 (v2)
Charger Input Voltage.........................10-32V DC
Charger Output Current.................................36A
Mechanical Specifications
Motor........Siemens 3.0Nm Synchronous Motor
Material..IP65

Controller

High level *Simatic HMI TP7000 Comfort* delivers an intuitive interface in its compact 7-in touch screen to effortlessly manage and control the Base Station. *Siemens S7-1200* CPU industrial grade controller provides exceptional real-time performance and powerful communication options. The integrated *PROFINET IO Controller* interface provides for communication to the HMU and other automation components.

Specifications

Simatic HMI TP7000 Comfort
Dimensions.................152.4x91.4 (mm)
Resolution..................................800x480
Input Voltage...............................24V DC
Memory.......................................12 MB

Siemens S7-1200 CPU
Dimensions.................152.4x91.4 (mm)
CPU..1214C
Input Voltage...............................24V DC
Memory...100KB

Power

TRIO POWER
Dimensions............139x130x190 (mm)
Weight..2.9 kg
Operation Temperature.........-25...70°C
Output Voltage...........................24V DC
Output Power................................960W

SINAMICS V90
Dimensions............80x180x200 (mm)
Weight...1.85kg
Operation Temperature...........0...45°C
Input Voltage.........................380-480V
Output Power....................................1kW

CLOUD MANAGEMENT SYSTEM 2.0 SPECIFICATIONS

Overview

Percepto Cloud Management Software enables 24/7 monitoring and management of the Sparrow 2.0 System by a remote pilot from any location. The software provides an interface for site setup, mission setup, mission scheduling, and live activation and monitoring of the Sparrow 2.0 system. It communicates with the drone and the base station either using a public LTE channel or with the site's own local internet connection. The remote pilot programs and schedules flight routes and manages the drones' activity via the management software. It connects the remote pilot to the system full control of the mission. The system includes a web based management system which allows the remote pilot to customize flight missions, watch real-time footage, and analyze data collected by the Sparrow.

Mission Management

In **mission setup**, the remote pilot can deploy a drone on a pre-defined mission or can customize a new mission choosing from the various mission applications.

Mission Applications:

- Navigate
- Track Detection
- Toggle Camera Type (day/night)
- Enable/Disable Detector
- Bird's View
- Move Camera Up/Down
- Spin Drone x Degrees
- Manually Set Target to Track
- Record Raw Video
- Ascend
- Wait
- Snapshot
- Drone Heading
- Forward Scan
- Return Home
- Go To Alert

Drone & Base Station Management

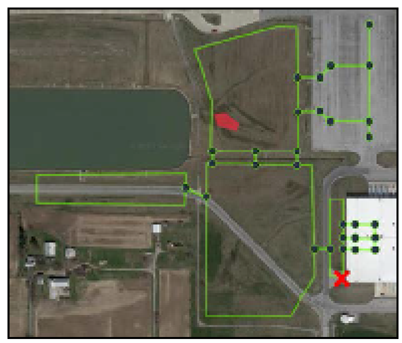
This crucial feature provides the remote pilot with key information regarding drone and base station status and health, contributing to the ability to safely manage the system.

Key features:

- Deployed drones and base stations are listed with status, health, and location
- Maintenance log including parts serial numbers and history
- Drone mission and data history
- Fleet control and drone selection for deployment
- Live camera feed and mission controls

Site Management

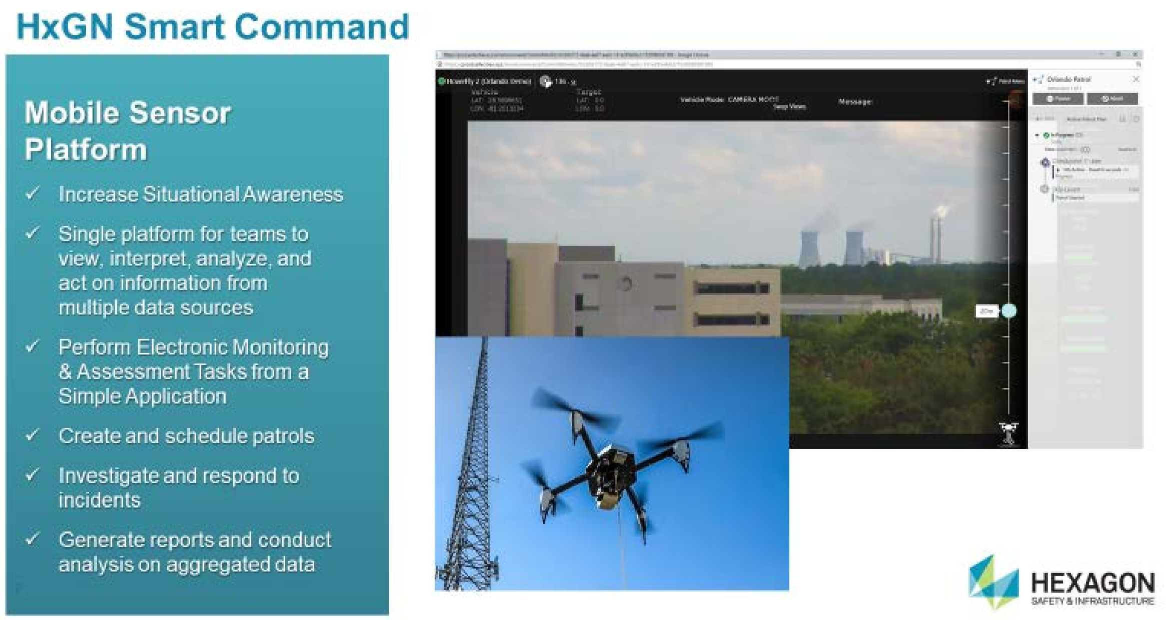
Site management features facilitate safe and optimal operation of the site by programming physical parameters in 3D space such as 'free fly zones', 'no-fly zones' and 'flight routes.' The 'live map' provides the remote pilot with key information such as system component locations, site notifications, and system component activity. The 'site schedule' manages completed, ongoing, and future missions scheduled for each drone. All relevant site parameters are displayed in the site management in real time, with crucial updates and alerts provided to the remote pilot as notifications.



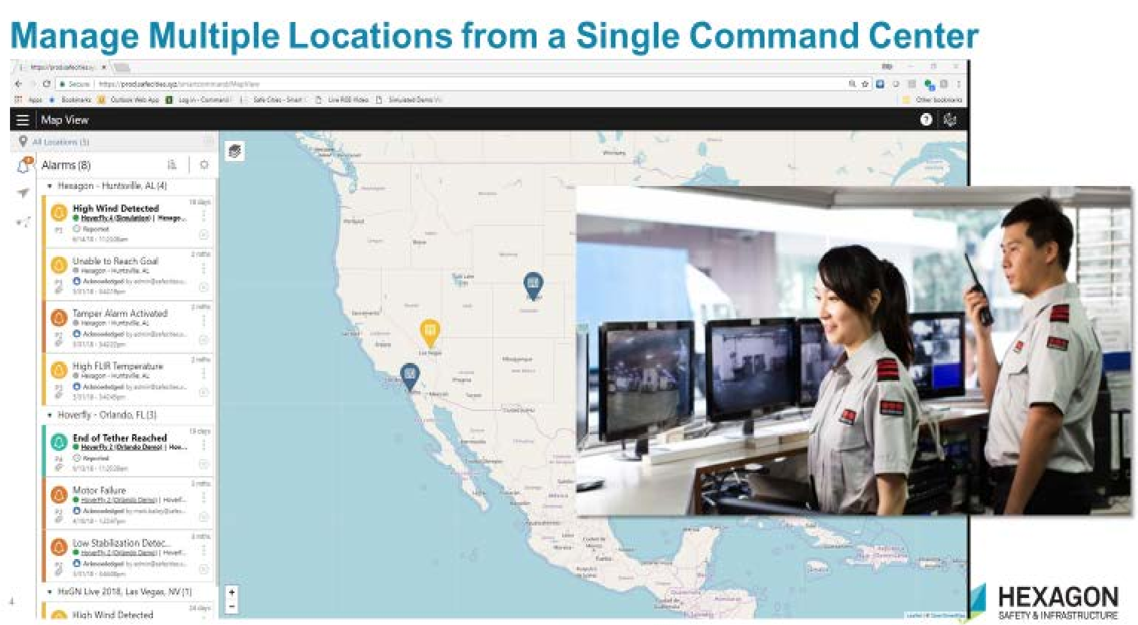
Data Management & Analytics

After each mission, the drone is capable of uploading collected data to the cloud database. This data can be sorted and/or undergo further processing and analytics, providing the remote pilot with crucial information and insights from the drone's mission.

ATTACHMENT B: HOVERFLY TECHNOLOGIES, INC. & HEXAGON SMART COMMAND



Hexagon's core product is a CAD Public Safety and Security PSIM software system. SMART Command is built based on this system, which is currently being used in major cities and airports all over the United States. Hexagon intends to integrate its Smart Command software with its Public Safety and Security CAD system for seamless dispatch and response as emergencies are detected from monitoring Hoverfly UAS activity.



HoverFly LiveSky SENTRY

Model LSP-6205 Features and Functional Capabilities:

- COTS/NDI developed at private expense
- Fifth generation tether-powered sUAS built on long history of innovation with growing capability and mission set
- LiveSky Series 6205 Systems are designed for MIL-STD-810 harsh environmental compatibility
- New SkyBox deployment container options for LiveSky
- Local or remote (network) control with enterprise compatibility from any TOC/SOC
- Multi-payload capability
    - EO/IR (ITAR) sensor payload with simultaneous h.264 streams
    - MPU MANET payloads
- Persistent Intelligence, Surveillance, and Reconnaissance (ISR) from 200 feet with swappable MPU-5 MANET payload (1kg)
- Autonomous operation (no pilot required; operator optional) from vehicle or remote location
- Secure RF-less C2 and simultaneous dual stream (EO/IR) video over tether
- Open architecture payload hot shoe, with access to vehicle power and tether network
- HD video and thermal sensors
    - EO 1080p, high def, 30 fps
    - 30x digital zoom, 10x optical zoom
    - Low LUX imager
    - FLIR BOSON thermal imager
    - 8x digital zoom
    - Accepts 3 FOV lenses
    - Color palette selection
- Secure video and command-and-control transport over tether with no RF radio transmission
- Advanced tether sensor for precision take-off/landing
- Non-GPS operation capability below 30 feet
- Advanced tether kit with proprietary automatic tether spooler and flight management computer, with Ethernet and external software control
- Open SDK, open payload interface
- Dual video (EO and IR simultaneous) streaming output
- 50Mb/s tether network
- Simplified field-supportable mechanical design with single circuit board assembly (CBA)
- 12+4 hex fasteners to R/R CBA
- Replaceable props, booms, and skids
- Plug-in flight controller and motor boom connectors improve predictability, reliability, and supportability

- Improved self-diagnostics, monitoring, and condition-reporting features
  - Real-time health and safety monitoring
  - Reports system status and health data
  - Mode interlocks for flight safety controls
  - Automatic self-protect features
- Advanced feature controls
  - Follow-Me enable/disable
  - Vehicle cone translate and camera mode
  - Dual EO/IR display control – Picture-in-picture mode toggle
- Five-button flight control
  - Arm, Launch, Land, Up, and Down
- Intuitive and informative multi-mode GUI

Additional Features – LiveSky SENTRY model # LSP-6205 with Covered SkyBox

1. All-weather IP54-rated aircraft and tether management system for use in rain, snow, and other hazardous weather conditions.
   a. The covered SkyBox is a self-contained, weatherproof nesting pod for remotely controlled autonomous operation.
2. Three different configurations for maximum flexibility for airports
   i. Remotely operated, covered, autonomous SkyBox system
   ii. Dismounted expeditionary mobile system for emergency and disaster operations
   iii. Vehicle-mounted "On the Move" mobile operations for mobility of tethered UAS

Notes and Product Disclosures to Use Case Testing Conditions:

The Hoverfly LiveSky system that was tested was an older version of the UAS. It was also Hoverfly's portable or dismounted version. The new LiveSky SENTRY (Model LSP 6205) was in development and scheduled for release in the first quarter of 2019.

Prior to accepting the invitation to test at the Safe Skies PTF, Hoverfly and Hexagon both disclosed that current capabilities and integration of Hexagon's Smart Command cloud-based software and Hoverfly Technologies were still under development. It was noted that certain planned autonomous features would still need to be managed manually.

APPENDIX B: CERTIFICATE OF AUTHORIZATION APPLICATION EXAMPLE

The following section is provided to assist airports in understanding the basic requirements needed to apply for a COA. An example application is also provided.

As discussed in the FAA Regulations section (Section 2.3), it is imperative to conduct a review of which regulatory avenue is best for each specific airport. The most common is to operate under Part 107, which will require an authorization to utilize UAS if the airport is in controlled airspace. Each airport will present independent risks and challenges that will need to be mitigated.

Below is a generalized list of risks and steps to take when submitting an application for certificate of authorization. ATC coordination and communications are a must for tower-controlled airports.

1. Risks to mitigate:
   a. Rotor failure
   b. Lost link with base controller
   c. Weather impediment
   d. Obstacle strike
   e. Non-participant interference/perception
   f. Interference with manned aircraft flight area
   g. Loss of radio contact
   h. Battery failure
2. Determine launch and recovery site(s)
3. Establish boundary zones (geofences)
4. Plan and conduct daily safety briefings/debriefings for all stakeholders
5. Check for Temporary Flight Restrictions and changes in weather
6. Develop and conduct a pre- and post-flight checklist
7. Document an emergency contingency plan

The FAA has numerous resources that can assist in submitting a waiver or authorization. The link below explains the safety aspects needed in Part 107 waivers:
https://www.faa.gov/uas/commercial_operators/part_107_waivers/waiver_safety_explanation_guidelines/.

The following checklist has been developed for use by airport staff when applying for a COA.

1. Focus should be on the risks and risk mitigations of the anticipated operation.
2. After the risks are identified and considered, then as part of the mitigation plan, launch, recovery, and lost-link locations should be identified.
3. The entire operation must be defined so as to mark the boundaries and/or zones needed for the operation.
4. A communication and/or safety briefing plan must be developed.
5. Coordination with the FAA must take place to identify any TFRs
6. Potential weather impacts should be identified and, given the duration of the operation, updates to anticipated weather should be built into the procedures.
7. Both pre- and post-flight checklists need to be developed. Again, these should be targeted toward the risk mitigation plans.

Application for Certificate of Authorization in Class C Airspace

Supplementary Attachment – McGhee Tyson Airport (TYS)

Table of Contents

Project Overview

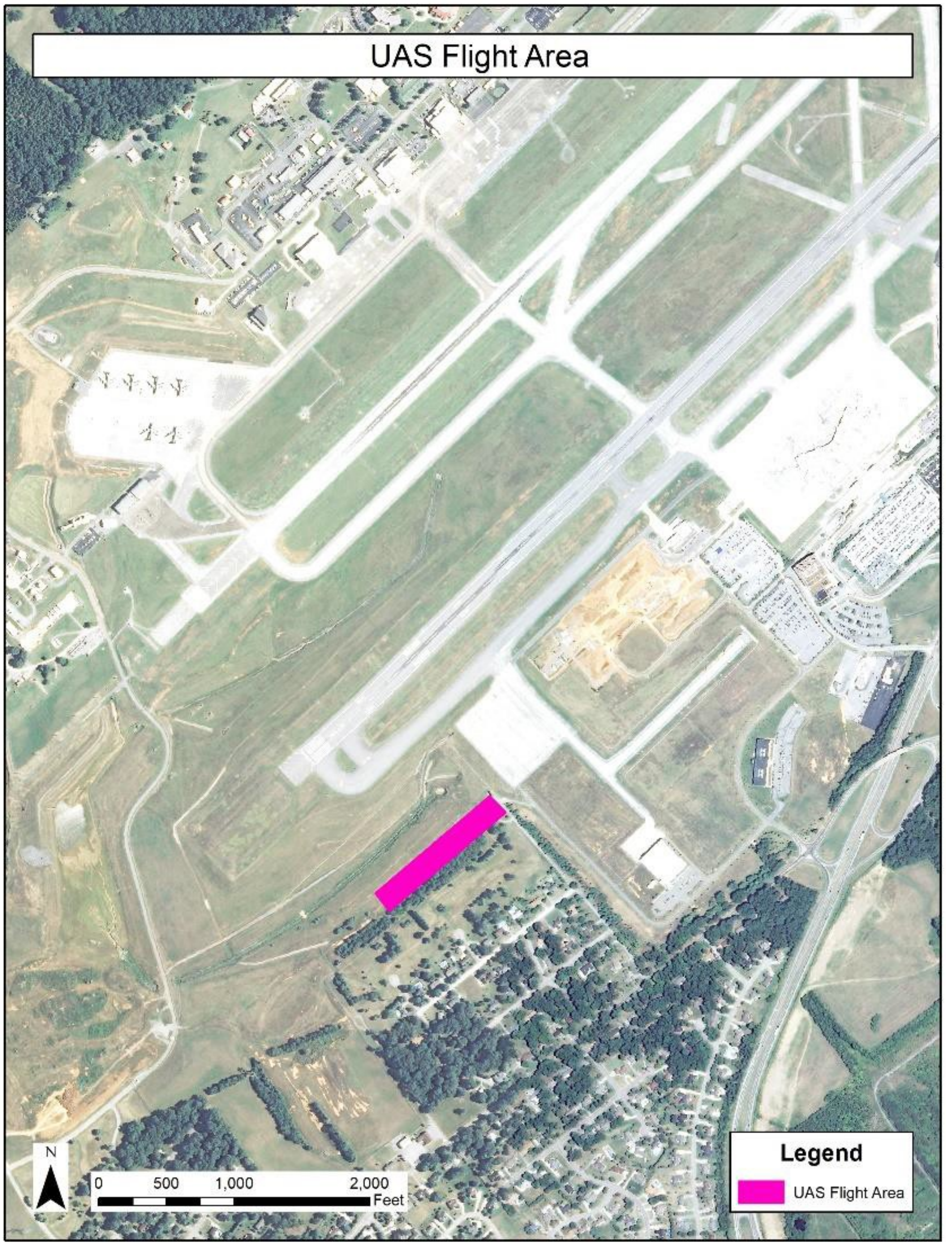
UAS Operation in Class C Airspace – McGhee Tyson Airport (TYS)	
Local Start Date	9/24/2018
Local End Date	3/1/2019
Time Span of UAS Operation (Daily)	As needed to complete the study. In coordination with ATC
Local Time Zone	Eastern Time (EST) [UTC-5]
Airport Location (City, State)	12 Miles SSW of Knoxville, TN
Proposed Area of Operation (General)	The National Safe Skies Test Facility, located beyond any AOA.
Proposed Maximum Flight Altitude (Above Ground Level)	150 Feet AGL (1131 Feet MSL based on Airport Elevation)
Airport Reference Point Latitude (DD°MM'SS")	N 35°48'40"
Airport Reference Point Longitude (DD°MM'SS")	W 083°59'38"
Max Radius from Airport Reference Point	.83 Mile
Total Flight Area	<.50 Sq. Mile

National Safe Skies Alliance seeks to evaluate Unmanned Aerial Systems (UAS) as a tool for future airport security monitoring and response through a series of intermittent test flights within the requested start/end dates of application. The Research Team intends to oversee and collect aerial imagery on McGhee Tyson Airport's airfield to demonstrate UAS capabilities for future operational implementation. All UAS activity performed by the Research Team will be directly overseen by the National Safe Skies Alliance on their test facility. A designated crew member will be responsible for primary communication with Air Traffic Control (ATC).

UAS Risk Mitigation in Class C Airspace

UAS Operation Contacts at McGhee Tyson Airport (TYS)	
Director, Airport Operations	Name: Work: Mobile: Email:
ATC Manager	Name: Email:

ATC has been provided the following diagram and has granted permission for The Research Team to conduct UAS operations in the designated area (magenta).



Risk Matrix for UAS Application in Class C Airspace

Severity of Consequence	Catastrophic	E	1E	2E	3E	4E	5E
	Hazardous	D	1D	2D	3D	4D	5D
	Major	C	1C	2C	3C	4C	5C
	Minor	B	1B	2B	3B	4B	5B
	Negligible	A	1A	2A	3A	4A	5A
Unacceptable			1	2	3	4	5
Acceptable with Mitigation			Extremely Improbable	Improbable	Remote	Occasional	Frequent
Acceptable			**Likelihood of Occurrence**				

Risk Matrix Definitions from AC 107-2, Table A-1

Extremely Improbably (1): Almost inconceivable that the event will occur.

Improbably (2): Very unlikely to occur.

Remote (3): Unlikely, but possible to occur.

Occasional (4): Likely to occur sometimes.

Frequent (5): Likely to occur many times.

Negligible (A): Little consequence.

Minor (B): Nuisance. Operating limitations. Use of emergency procedures. Minor incident.

Major (C): Significant reduction in safety margins, reduction in the ability of crewmembers to cope with adverse operating conditions as a result of an increase in workload, or as result of conditions impairing their efficiency. Serious incident. Injury to persons.

Hazardous (D): Large reduction in safety margins, physical distress, or a workload such that crewmembers cannot be relied upon to perform their tasks accurately or completely. Serious injury or death. Major Equipment Damage.

Catastrophic (E): Equipment destroyed, multiple deaths.

Risk Register

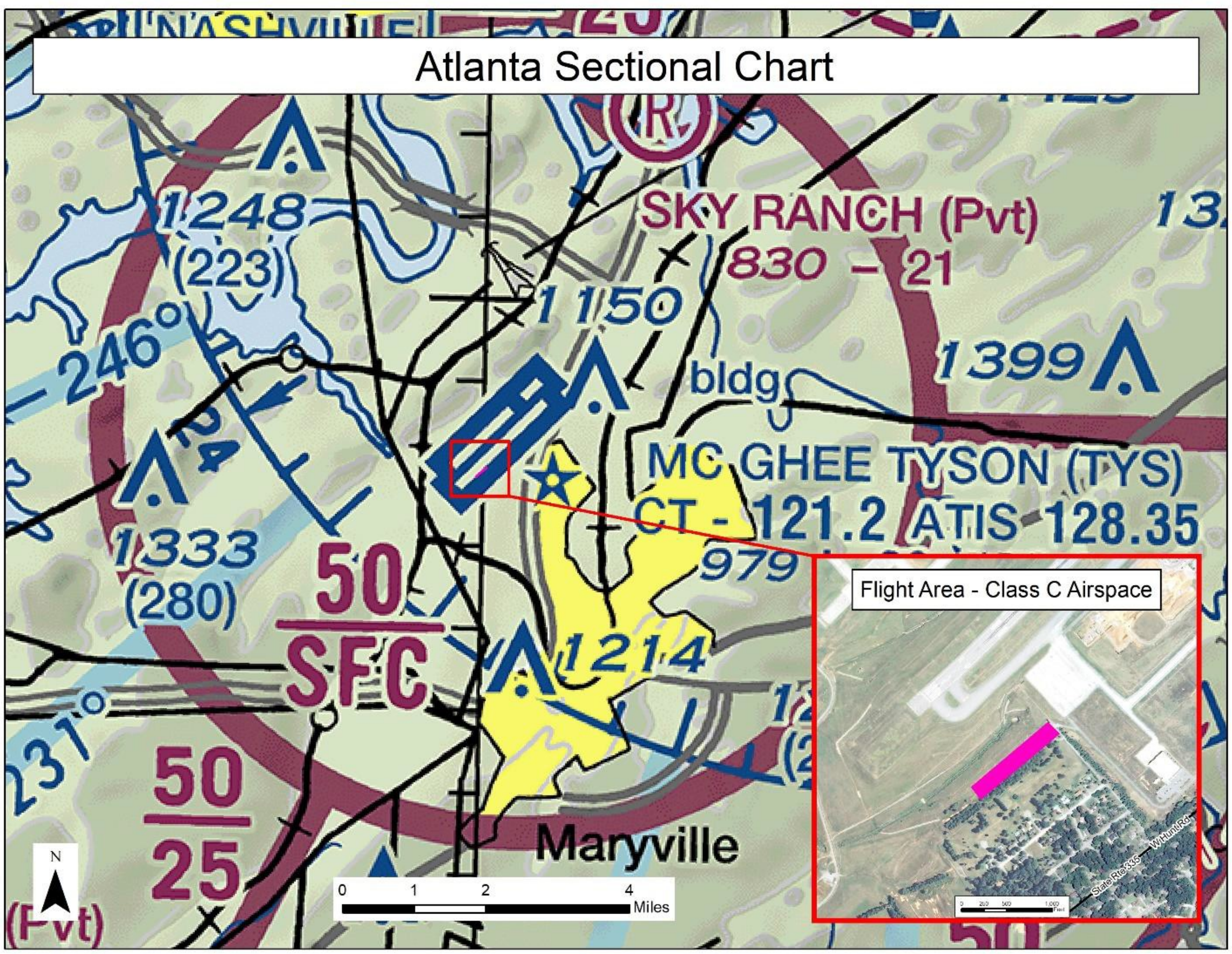
Risk Event	**Mitigation through Risk Cause Analysis**
Rotor failure during flight (Disabled UAS)	Each airport will present independent risks and challenges needing to be mitigated. On the left is a **generalized** list of risks for when submitting an application for certificate of authorization. System and airport specific mitigations will go in this column.
Lost link with base controller	
Weather Impediment	
Obstacle Strike	
Non-participant interference	

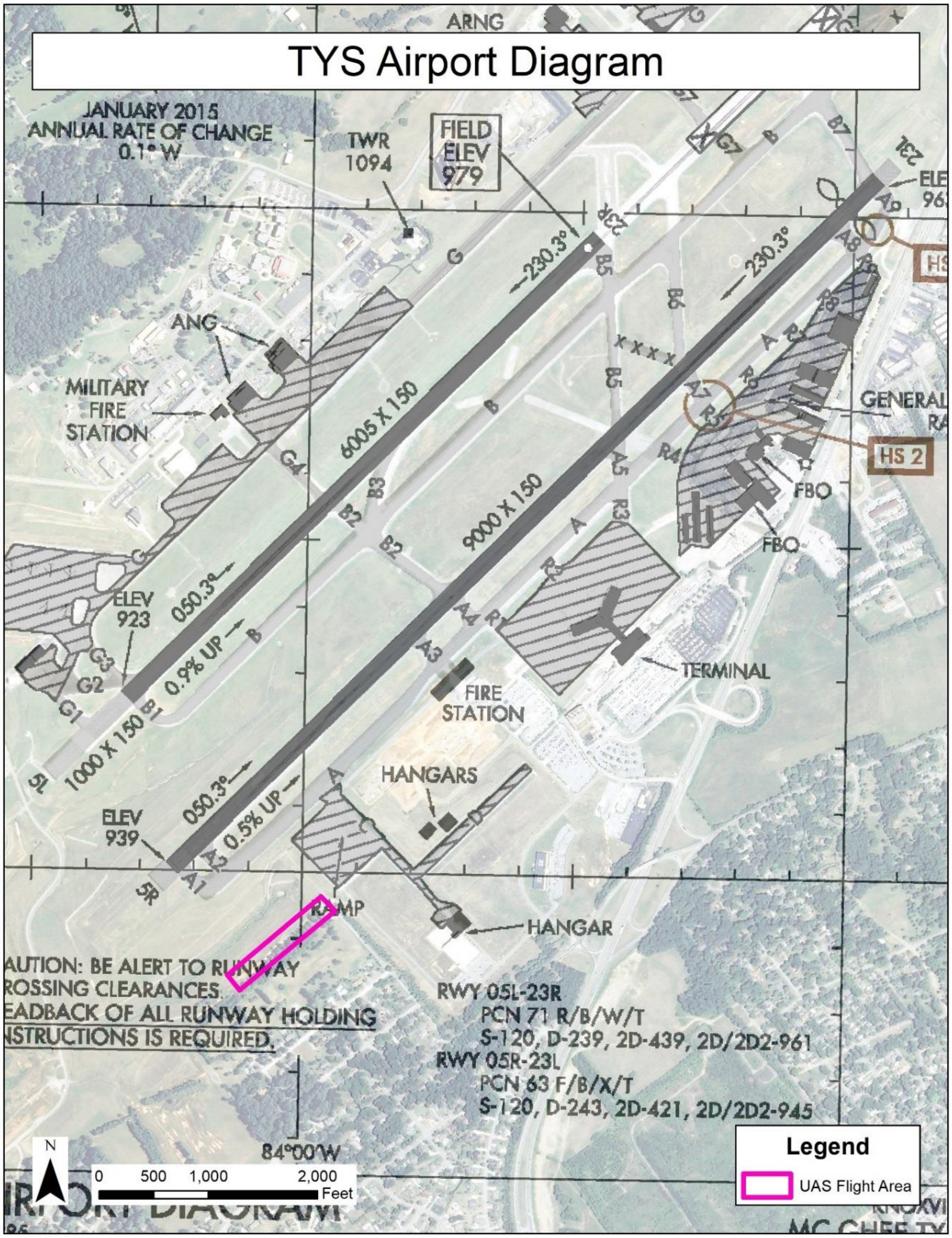
Manned aircraft deviating from existing flight procedures			
Loss of radio contact			
UAS Battery Drain/Failure			
Loss of electronic UAS audio queues (hand-held controller)			

Field Equipment Communications

Radio Frequency & Cell Phone Coverage Information	
Equipment	**Intended Frequency/Network**
Communication between UAS and Transmitter	Radio (5.725~5.825 GHz, 2.400~2.483 GHz) and Encrypted Wi-Fi
Cell Phone Coverage	Verizon Wireless Network
Air Band Handheld Radio - The Research Team(ICOM IC-A6) Range: 118.000-136.975 MHz	121.200 MHz (CTAF)
Hand Held Radio Communication between secondary ground personnel and PIC – XXXX (Motorola XPR 3500E)	Predetermined frequency by manufacturer (Selection of channels between 1-16)
Air Traffic Control Frequency	121.200 MHz (CTAF)

Area of Operation




TYS Airport Diagram
JANUARY 2015
ANNUAL RATE OF CHANGE
0.1° W
TWR
1094
FIELD
ELEV
979
ARNG
ANG
MILITARY
FIRE
STATION
230.3°
6005 X 150
9000 X 150
050.3°
0.9% UP
ELEV
923
1000 X 150
ELEV
939
0.5% UP
FIRE
STATION
TERMINAL
GENERAL
HS 2
FBO
FBO
HANGARS
RAMP
HANGAR
AUTION: BE ALERT TO RUNWAY
ROSSING CLEARANCES.
EADBACK OF ALL RUNWAY HOLDING
NSTRUCTIONS IS REQUIRED.
RWY 05L-23R
PCN 71 R/B/W/T
S-120, D-239, 2D-439, 2D/2D2-961
RWY 05R-23L
PCN 63 F/B/X/T
S-120, D-243, 2D-421, 2D/2D2-945
84°00'W
N
0 500 1,000 2,000
Feet
Legend
UAS Flight Area

The PARAS 0012 Research Team UAS Flight Areas

The flight areas will be on the National Safe Skies Alliance test facility. More detailed descriptions of the flight area are discussed in the following pages. The proposed launch/recovery site within the area is depicted in the detailed description. It was selected based on desired areas of flight and available space for launch and recovery of the UAS. The proposed location provides the PIC direct line of sight with the UAS at all times during each flight mission but is subject to change after site visit is completed if an unknown obstacle exists impairing direct line of sight.

Figure B-1. TYS UAS Flight Area #1

Flight Area #1

UAS Flight Area #1 (TYS)	
Central Position Latitude (DD°MM'SS")	N 35°47'53.52"
Central Position Longitude (DD°MM'SS")	W 084°00'02.27"
Maximum Radius from Central Position	.11 Miles
Total Flight Area	.01 Sq. Miles
Proposed Maximum Flight Altitude (Above Ground Level)	150 Feet
Boundaries	East- Airfield West- Ambrose St. South- .13 Mile NW of E Cunningham St North- .08 Miles SE of airfield fence

The proposed flight area is .01 square miles and includes a test fence line, paved lot, and trees. The launch/recovery site will be the parking lot located on the north-east end of the flight area. This lot will be dedicated space by the National Safe Skies Alliance for the UAS missions.

FLIGHT PROCEDURES

Each airport should create system- and mission-specific flight procedures to standardize operations and ensure safety. This section should also include sample checklists to be used while utilizing UAS in the field. Topics that should be addressed are:

- Daily safety briefings
- Launch/recovery site determinations
- GeoFences
- Active flight procedures
- Emergency guidelines
- Checklists (components, mission set-up, hardware inspections, image quality control)

See Flight Planning and CONOPS sections in the above guidebook.

Pilot in Command Roster under Part 107

Pilot in Command (Primary)	
Remote Pilot in Command License Number Status	
Contact Information	
Driver's License Number State of Issue Expiration Date Status	
Approximate Total Air-Time Under Part 107	

Pilot in Command (Secondary/Observer)	
Remote Pilot in Command License Number Status	
Contact Information	
Driver's License Number State of Issue Expiration Date Status	
Approximate Total Air-Time Under Part 107	

APPENDIX C: ADDITIONAL USE CASE DOCUMENTATION

Use Case Study #1 – Farmville Regional Airport (FVX)

OVERVIEW

- Conducted March 8–9, 2018.
- Participants: Futron Aviation and Woolpert
- Meeting with the Farmville Police Chief
    - The team met with the Police Chief prior to proceeding to the airport.
    - FVX is owned by the city of Farmville, and thus the Farmville police are charged with patrolling and security responses at the airport.
    - Parts of Farmville are located within the boundaries of both Prince Edward and Cumberland counties, while the airport lies within Cumberland County. As a result, the City of Farmville has an agreement with the County Sheriff of Cumberland County for response that spells out their responsibilities.
    - The Chief stated the following:
        - No experience with UAS
        - Officers patrol the airport multiple times a day
        - Have existing traffic camera infrastructure to be able to stream data from sUAS or other camera systems
        - Felt that a means to monitor on a regular basis with video to another location would be beneficial

FVX ACTIVITY

- Weather was cold: 42.6–46.4 °F
- Winds: 6–10 Knots, gusting to 15 out of the west.
- Both days had air traffic operating in the local pattern and on the airfield; however, no interruptions to airport operations occurred as a result flying sUAS on the airfield.
- All sUAS activity ceased while there were manned aircraft operating in the local pattern or on the airfield.

OPERATOR QUALIFICATION

The RPIC is currently Part 107 certified. The operator was qualified on the systems that he operated (Table C-1)[13]. Training was either on-the-job training (OJT) or provided by the manufacturer of the UAS.

Table C-1. UAS Used at FVX

Model	Max Range	Max Air Speed	Max Endurance
DJI Inspire 1	3.1 miles	49 mph	18 minutes
DJI Inspire 2	4.3 miles	58 mph	28 minutes
Parrot Bebop 2	0.2 miles	35 mph (16 m/s)	25 minutes

[13] All aircraft specifications are from the manufacturer

SENSORS

- DJI Zenmuse X7 (daytime camera)
- DJI Zenmuse XT (thermal camera)
- Beebop onboard camera (daytime camera)

TESTING SETUP

- Provided a copy of the FVX airport layout plan, which was used to plan where to deploy and what to view with the sensors.
- Coordination with the airport was done several weeks prior by speaking with the FBO that manages the airport.
- The team was given permission to drive on the airfield and given a portable radio to monitor the UNICOM.
- The DJI UAS was unlocked to fly on the airport prior to arrival, but there were still some issues that needed to be resolved onsite so that the aircraft would work at the airport.
- Woolpert provided the checklist for operating (safety gear, certificates, systems, etc.)
- A handheld range finder was used to check the range to obstacles and the height of trees

GENERAL FLIGHT INFORMATION

- 6 flights were conducted utilizing autonomous and manual flight modes
- All flights remained below 400 feet above ground level (AGL)
- DJI altitudes are based on the elevation of the Home Point location.
- In general, all flights were limited to 20 mph fixed airspeed
- The maximum groundspeed achieved was 65 mph, with a set airspeed of 58 mph.
- All flights remained within VLOS, with a maximum distance from the Home Point of approximately 3,600 feet.
- There was no issue with Electronic Line of Sight or loss of uplink or downlink with the UAV.
- On the first day, all flights were flown from the tie-down area adjacent to the airport operations building.
- Flights on the second day were flown from the south end of the runway.

Table C-2 summarizes the flights that are detailed in the sections below.

Table C-2. FVX Use Case Study: Flight Summaries

Flight #	Aircraft	Sensor	Alt Feet AGL	Range	Duration
1	Inspire 2	Zenmuse X7	175	2,088 feet	08:38
2	Inspire 1	Zenmuse XT	50	2500 feet	08:00
3	Inspire 2	Zenmuse X7	50	600 feet	04:00
4	Inspire 2	Zenmuse X7	50	3,150 feet	09:00
5	Inspire 2	Zenmuse X7	50	600 x 200 sq. feet	03:30
6	Bebop	Integral	<50	——	06:00

FLIGHT 1

- Flight 1 was used to test the sensors. Camera focus was an issue at first. This was corrected, and the UAS were prepared to fly around the airfield.
- Other test flight information is found in the mission tables developed for the project
    - A second flight to a point 2,866 feet from the pilot took about 1 min 15 sec in transit time into the 10-knot wind at 20 mph fixed airspeed.
    - It took 1 min 10 sec to transition and land from 75 feet AGL.
    - Total flight duration was 8 minutes and 38 seconds.

FLIGHT 2

- Flight 2 was conducted utilizing manual control with the Inspire 1.
- Flew out to 2,500 feet and returned via same routing
- Airspeed was 20 mph
- Altitude 50 feet AGL
- Total flight duration was 8 min
- This was to test the clarity of the thermal camera (Zenmuse XT)

FLIGHT 3

- Flight 3 was an Autonomous to Manual control with the Inspire 2
- Flew out approximately 2,000 feet and returned using a route parallel to the outbound leg
- Airspeed 22 mph
- Altitude 50 feet AGL
- Total flight duration was 4 min
- Aircraft was flown out utilizing a point-to-point function, which enables a pre-programmed course to be utilized.
- Once on station at the second point, the operator took control and returned to the home point
- A demonstration of the aircraft’s tracking ability was conducted at the end of this flight
- The sensor was able to hold track on the RPIC, even while the observer was walking directly between the RPIC and the sensor line of sight.

FLIGHT 4

- Flight 4 was flown in Manual control with the Inspire 2
- Flew out 3,150 feet and returned using reverse routing
- Airspeed 22 mph
- Altitude 50 feet AGL
- Total flight duration 9 min
- Once on station, the operator collected still images of a sign from an altitude of 50 feet to demonstrate the resolution of the sensor.

FLIGHT 5

- Flight 5 was flown in waypoint mode with the Inspire 2.
- Route was a 600- x 200-foot box
- Airspeed 7.8 mph
- Altitude 50 feet AGL
- Total flight duration 3 min 30 sec
- Operator allowed the aircraft to execute the waypoint until it was approximately halfway through the programmed mission and took control to take still images of the airport and runway; the operator then placed the aircraft back in waypoint mode to complete the flight

FLIGHT 6

- Flight 6 was a demonstration of a consumer-grade sUAS.
- Altitude <50 feet AGL
- Total flight duration 6 min
- The aircraft was kept in its transit case until the flight was going to be executed.
- The total time from unpack to airborne was 2 min 20 sec
- The aircraft has intelligent flight mode capabilities that allow the sensor to lock onto a target while the sUAS follows the target.

ISSUES AND SUGGESTIONS

- Airports will need to consider the life of the technology they purchase.
    - Manufacturers update sensors and flight systems (avionics) on a regular basis
- Technology can become obsolete in as few as 3 years.
    - Some manufacturers discontinue technical and parts support when they deploy new or updated systems.
    - Airports will need to decide whether to purchase inexpensive versus expensive systems given the life expectancy and supportability of the systems.
- Flying from a single location
    - The testing on the first day was done as if operating from a small airport with a small staff, with the UAS located near the operations building.
    - The operations were limited to line of sight only (as all current Part 107 operations are).
        - With nearly ideal visual conditions (10 nm visibility, mid-high overcast increasing contrast) the UAS operator was comfortable controlling the aircraft out to a range of approximately 0.667 statute miles or 3,680 feet.
        - This range allowed the operator to cover the property at FVX from a single position, but this is a small airport with a single 5,000-foot runway.
        - A daisy chain of observers might be a way to support longer ranges for a system like the one used at FVX.
- Batteries
    - Battery life was an issue due to temperature and winds.
        - The air was cold during the day, with a high temp of only about 43 °F.
        - The air temperature degraded the length of time the aircraft could be on station.

        - Winds caused the aircraft to make a significant number of corrections to remain in station, thus depleting the battery life.
- UAS Calibration
    - Calibrating the aircraft systems was an issue and took time.
        - Metal and steel around the location made calibration difficult.
        - EM interference in the airport environment also impacted the ease of calibration.
    - All three of the systems experienced initial setup issues.
- Flight planning versus manual flying
    - At first glance, it appears that response times for getting a UAS onsite might be maximized by flying in autonomous mode to pre-planned waypoints and then switching over to manual flying once on station.
    - UAS software can make loading waypoints very easy (tapping the screen).
    - Woolpert uses Drone Deploy and Pix4D software packages to plan mission.
- Technology advances
    - Sensor/camera technologies are outpacing flight planning software. Therefore, it is not uncommon for UAS operators to work within the limited flight planning capabilities to the extent necessary to maximize the camera technology.
    - Flight management software may not be able to trigger the camera to take preplanned images due to camera software. Integration of UAS operational software and cameras is an important consideration.
- Autonomous flying
    - The team tried to deploy the Kespry autonomous system on day one, but light aircraft traffic along with battery-life limitations due to the cold postponed the auto-perimeter flight.

DATA STORAGE

- Data archiving and storage will require a significant amount of storage space.
- Videos range from a few MB to several GB of data. Total video collected was 14.5 GB.
- Local storage on a laptop was sufficient for the Use Case Study.
- Data was transferred to Google Drive for long-term storage and recall.
- A local file naming convention would be beneficial for the recall of information and video data.

DATA DISSEMINATION

- At FVX, data dissemination would have to go from the aircraft to local data storage, and be transmitted through e-mail or hand-delivered to the agency responsible for security.
- DJI Inspire can stream live video through several different live streaming services.
- A test of live streaming video through YouTube was conducted using a mobile Wi-Fi hotspot and the airport's local Wi-Fi:
    - The team streamed live video to a teammate in Williamsburg, Virginia.
    - The livestream experienced a latency of around 30 seconds from capture to receipt by the Williamsburg-based teammate using the mobile Wi-Fi hotspot; streaming through the airport's Wi-Fi did not work.

- DJI is developing a 4G LTE system for the Inspire 2 that will allow transmission of video data across long distance to a network server or long-range control of the aircraft. The advertised latency is 500 milliseconds.

RISKS

- Wind
- Temperature (battery life)
- Local air traffic

Use Case Study #2 Springfield Beckley Municipal Airport (SGH)

OVERVIEW

- Conducted April 11–12, 2018
- Participants: Futron Aviation and Woolpert
- A diagram of the operating area at the airport is provided as Figure C-1 at the end of this Use Case Study description.
- Meeting with the SGH Airport Manager
    - Airport Operations
        - The airport is actively seeking UAS operators to fly at SGH. Operators are required to submit risk mitigation plans and are charged a small fee, which goes back into the airport operating accounts.
        - Number one concern with operating UAS in an unconstrained environment is a midair collision.
        - All UAS operations within VLOS are conducted inside a specific operational area that is limited to a ceiling of 400 feet AGL. For operations that are BVLOS, the operating area can be extended 18 miles to the south with a ceiling of 2,000 feet AGL
        - All UAS operations are required to submit a Notice to Airmen (NOTAM) no less than 24 hours prior.
        - Transient pilots flying through the airspace around the airport present a challenge as they are not always comfortable with UAS operations while they are in the area. Conversely, the pilots that operate out of SGH are comfortable with and accepting of UAS operations.
    - Security
        - Airport manager is responsible for the security of the airfield.
        - The airport is owned by the city of Springfield, and the local Police Department conducts drive-by security checks of the airfield after hours.
        - Local Police and the County Sheriff are the principal responders for emergency calls.
        - The Ohio Air National Guard (OANG) operates a facility that supports overseas contingency operations with Multirole ISR services.

SGH ACTIVITY

- Temperature: 40–60 °F
- Winds: 12–25 knots, gusting to 38 knots
- No precipitation
- Both days had air traffic operating in the local pattern and on the airfield.
- The only interruption to operations was shutting down Runway 33, for which a NOTAM was issued.
- All sUAS activity continued while there was aircraft in the pattern.

OPERATOR QUALIFICATION

The RPIC is currently Part 107 certified. The RPIC was qualified on the systems that he operated (see Table C-3). Training was either OJT or provided by the manufacturer of the sUAS system.

Table C-3. UAS Used at SGH

Model	Max Range	Max Airspeed	Max Endurance
DJI Inspire 1	3.1 miles	49 mph	18 minutes
DJI Inspire 2	4.3 miles	58 mph	28 minutes
Kespry 2S	Dependent on configuration	Determined by the system	30 minutes

SENSORS

- DJI Zenmuse X5 (daytime camera)
- DJI Zenmuse X7 (daytime camera)
- DJI Zenmuse XTR (thermal camera)
- Kespry onboard camera (daytime camera)

TESTING SETUP

- Representative from Woolpert was qualified and authorized to drive on the airfield.
- The DJI UAS was unlocked to fly on the airport prior to arrival, but there were still some issues that needed to be resolved onsite so that the aircraft would work at the airport. This was the second event where attempting to operate a DJI UAS within an airport's boundaries was problematic.
- Due to the cold weather, the batteries in the DJI Inspire UAV experienced shortened maximum operating durations. Colder temperatures shorten battery life of UAS as with any other battery. The amount of impact will vary based on mission, the UAS itself, and the battery's age. Operators should consult with their UAS vendor about optimum temperature ranges for best battery-life performance.
- The team experienced system-related issues that prevented the uploading of waypoint data from the controller to the aircraft.

GENERAL FLIGHT INFORMATION

- Six flights were conducted utilizing autonomous and manual modes of flight and 4 different sensors.
- The flights were flown as close to the written direction as possible; however, there were issues with battery performance; the perimeter area where the aircraft was operated was based on avoiding private land and roadways adjacent to the airfield; and electronic line of sight in the case of the Kespry.
- All flights remained below 400 feet AGL.
- Speed for the flights varied depending on what was required to capture the data needed.
    - There is a trade-off for clarity of the image versus altitude flown and the speed at which the aircraft is flown. This will likely be an issue with any system.
- All flights remained within VLOS.

Table C-4 summarizes the flights that are detailed in the sections below.

Table C-4. SGH Use Case Study: Flight Summaries

Flight #	Aircraft	Sensor	Alt Feet AGL	Route Length	Duration
1 & 2	Kespry	Integrated	200	23,000 feet	28:00
3	Inspire 1	X5	20	6,782 feet	11:21
4	Inspire 2	X7	36	5,265 feet	14:20
5	Inspire 2	X7	Varied	800 feet	Untimed
6	Inspire 1	XTR	Varied	650 feet	Untimed

FLIGHTS 1 & 2

- The first two flights executed Use Case Scenario 1 (Autonomous Surveillance).
- For Autonomous Surveillance, the UAV flew along a preprogrammed route that allowed for coverage of an area that was approximately 56 acres at an altitude of 200 feet AGL at a safe ground speed until completion of the surveillance mission.
- The flight was broken into two segments because the aircraft entered its return mode and landed due to lost link caused by vehicle interference. A subsequent flight to complete surveillance of the given area was required.
- The approximate length of the route was 23,000 feet at an altitude of 200 feet AGL.
- Area covered was approximately 56 acres.
- Total mission duration was 28 minutes: the first segment was 12 minutes and the second segment was 16 minutes.
- The mission was conducted with the Kespry.

FLIGHT 3

- Flight 3 tested Use Case Scenario 3 (RPIC Response). This flight also provided a means of obtaining waypoint data for the execution of Use Case Scenario 2.
- For the RPIC Response, the RPIC flew along the perimeter fence in a clockwise direction, following the contour of the airport perimeter while maintaining an approximate 66 to 164-foot stand-off from the fence line at 20 feet AGL and at a safe ground speed until it ran down the battery and had to return to the home point.
- The aircraft was flown along a section of fence line on the southern end of the airfield next to a public road and a private residence and farm.
- To clearly see the fence, the aircraft was flown at a speed that only allowed for the coverage of a little more than a mile of fence.
- Max Speed was approximately 10 mph
- Altitude 36 feet AGL
- Route length was 6,782 feet
- Duration was 11 min 21 sec
- The mission was conducted using the DJI Inspire 1 Zenmuse X5.

FLIGHT 4

- Flight 4 tested Use Case Scenario 2 (Autonomous Response).
- The UAV flew along the perimeter fence in a counter-clockwise direction, following the contour of the airport perimeter while maintaining a 66 to 164-foot stand-off to the inside of the fence line at an altitude of approximately 36 feet AGL and at a safe ground speed until it reached the point of the reported breach. The UAV then retraced its route during recovery.
- The route length was 5,265 feet.
- Max speed was 5.1 mph. This speed was a trade-off for speed over quality of image.
- Total duration 14 min 20 sec
- The mission was conducted using the DJI Inspire 2 Zenmuse X7.

FLIGHT 5

- Flight 5 demonstrated the ability of the camera to provide a usable image of a human-sized object both along a fence line and tree line.
- Images were taken from different altitudes and ranges.
- The ability to discern the individual from the background became difficult at a range of approximately 800 feet from the target area.
- The mission was conducted using the DJI Inspire 2 with the Zenmuse X7.

FLIGHT 6

- Flight 6 was flown to demonstrate the ability of the thermal camera to provide a usable image of a human-sized object.
- Images were taken from different altitudes and ranges.
- The ability to discern the individual from the background became difficult at a range of approximately 650 feet from the target area.
- The mission was conducted using the DJI Inspire 1 with the Zenmuse XTR.

ISSUES & SUGGESTIONS

- There was no issue with electronic line of sight or loss of uplink and downlink with the DJI air vehicles.
- The Kespry experienced a loss of uplink and executed its planned return home failsafe. It was discovered that the ground station line of sight to the air vehicle was obstructed by a truck at the site.
- The DJI Inspire 1 would not execute the waypoint due to a system fault.
- The DJI Inspire 2 had difficulty with the unlock feature for airports and required additional coordination with manufacturer support so it could be flown at the airport.
- None of the UAS were able to fly the entire perimeter due to the length.
- To provide a usable image, the aircraft speed had to be slowed to less than 5 mph.
- All flights were flown near the south end of Runway 33.
- Batteries
    - Battery life was an issue due to temperature and winds
    - The air temperature degraded the length of time the aircraft could be on station.

  - Winds caused the aircraft to make a significant number of corrections to remain in station, thus depleting the battery life.
- Flight Planning versus Manual flying
  - The flight planning software was problematic and caused significant delays in the conduct of autonomous/semi-autonomous missions.
  - The possibility of preplanned routes should be considered to reduce delays and time on the ground setting up waypoint missions.

RISKS

- Temperature (battery life)
- Local air traffic
- Local air traffic was often below what appeared to be 1,000 feet, reducing the altitude buffer.
  - Local air traffic often did not make traffic calls when taking off from or approaching the airport.

Figure C-1. Flight Area

Use Case Study #3 – Savannah/Hilton Head International Airport (SAV)

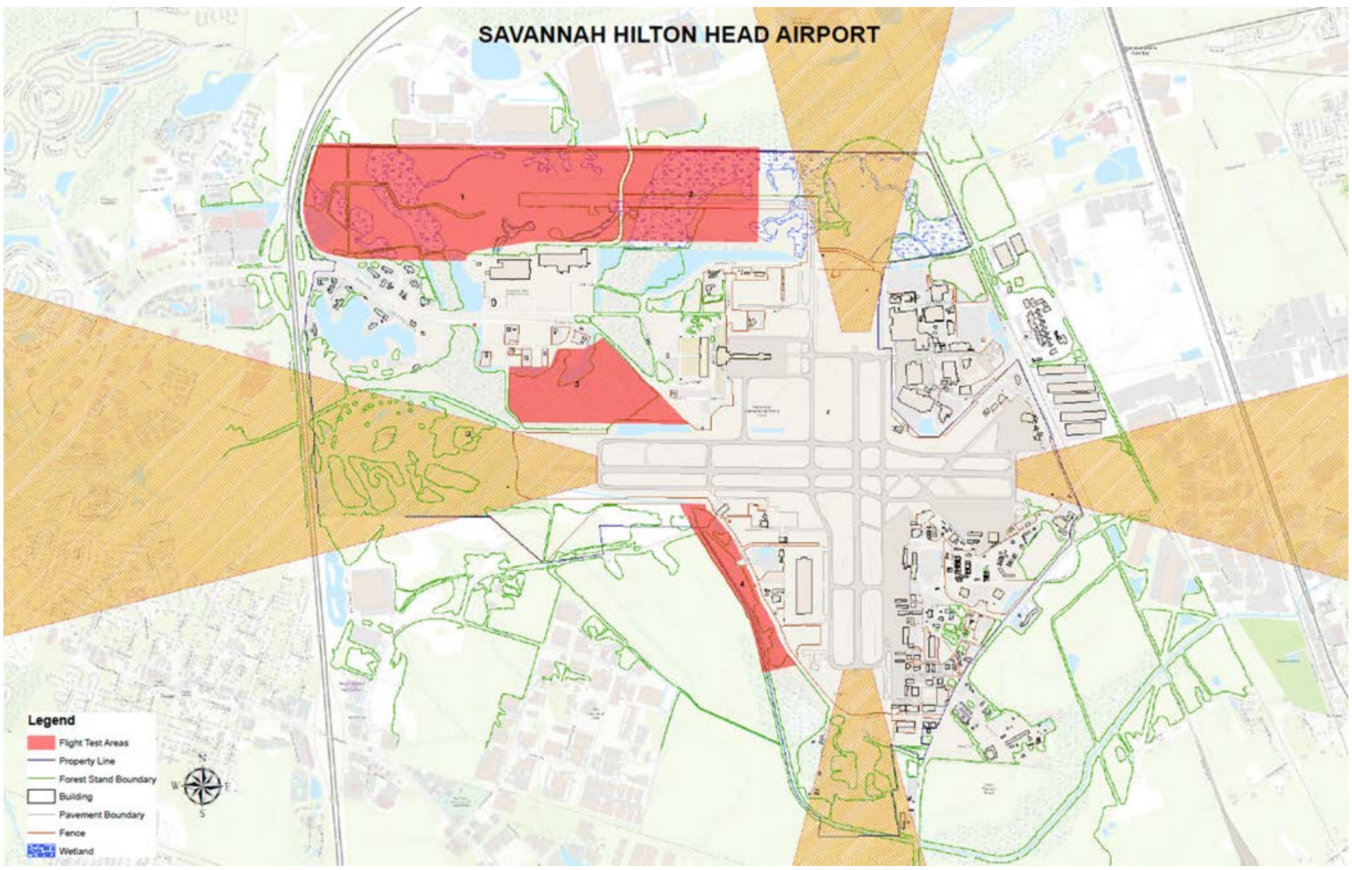
OVERVIEW

The purpose of the SAV Airport Use Case Study was to identify procedures, techniques, and best practices for airports to safely and effectively integrate UAS into security operations with minimal disturbance to airport operations. The Use Case executed four flight scenarios, which focused on routine perimeter surveillance and responding to perimeter breaches utilizing UAS operating in autonomous and manual modes of control. All scenarios were conducted at Savannah/Hilton Head International (SAV) in Savannah, Georgia in coordination with airport authorities and the FAA ATCT Manager. This Use Case Study was conducted June 19–20, 2018.

SCENARIOS – GENERAL

A description of each of the Use Case Study scenarios was prepared. The UAS basic flight profiles and some additional planning considerations were developed in detail. Each scenario was conducted under SAV's Memorandum of Agreement with the FAA ATC and occurred within the permitted operational areas, identified as red tinted zones depicted in Figure C-2 below.

Figure C-2. SAV UAS Operational Zones



SCENARIO 1 (TIME RESPONSE BENEFIT)

In close coordination with the local ATC jurisdictional manager, Scenario 1 was executed to provide dawn and dusk routine security patrol along a predetermined perimeter route. The timed test was to determine if a UAS can monitor a perimeter area as quickly as or more efficiently than manned patrols. The test included a timed human response to different areas of the perimeter and a UAS response to those same locations. The difference in time and the ability to effectively put "eyes on" a certain location was documented.

This scenario also demonstrated that a UAS, while in an autonomous mode being monitored by a qualified, competent, and certified (Part 107 or Section 333 exemption) pilot in command, can safely operate and communicate with ATCT inside of the airport's controlled airspace, and routinely collect detailed security information in a timely manner and relay it to the AOC/security authority for dissemination or follow-on action.

SCENARIO 2 (INTERFERENCE WITH COMMUNICATIONS OF UAS)

In close coordination with the ATCT, Scenario 2 was executed to provide a well-documented example of how fixed ground-based objects may interfere with UAS communications. In previous UAS operations at SAV, this was discovered and determined to be a nuisance. The causal factors are believed to be hangars and other large metal structures. This test was to specifically determine the degree to which interference needs to be proactively determined prior to engaging UAS at an airport.

The intended outcome of this scenario was to provide much needed information for airport operators in order to determine the areas of highest and most likely impact on UAS communications.

SCENARIO 3 (FAA REGULATION DIFFICULTIES IN FLIGHT OPERATIONS)

The team identified that, given certain operating restrictions placed on UAS operators, airport operators who are deploying UAS may encounter challenges. Scenarios 1–3 were conducted in such a way as to require the sUAS to divert and or stop and wait because of specific regulations. The UAS pausing to cross a public roadway was an example of how regulations might hamper or even eliminate a UAS response to a particular area of an airport.

SCENARIO 4 (SWAMP CANOPY COVERAGE)

A large portion of the SAV's perimeter is inclusive of swamp land, and the forest canopy there makes it difficult for UAS cameras to accurately track and monitor a target. The team tested the capabilities of both standard cameras and thermal technology in this area.

ADDITIONAL PLANNING CONSIDERATIONS

- Location/Operational Environment
- Time of day
- Duration of the flight
- Profile
- RPIC
- Aircraft Type
- Sensor type
- Flight Mode
- Information Collection Requirement
- Information Dissemination Plan
- Risk Information

AIRPORT INFORMATION

- SAV
  - Location: Savannah, GA
  - Traffic: 252 General, Commercial, Air Taxi, and Military Operations Daily
  - Runways: 10/28 and 1/19
  - Facilities:
    - Fuel: 100LL JET-A++, A++100(MIL)
    - Parking: Hangars and tiedowns
    - Airframe service: MAJOR
    - Powerplant service: MAJOR
    - Bottled oxygen: HIGH/LOW
    - Bulk oxygen: HIGH/LOW
  - Perimeter length: ~10 miles
  - Preflight Approvals: Class C airspace, FAA Airspace Authorization to Part 107.41 required prior to flight

Table C-5. SAV Use Case Study: Available Aircraft

Model	Type	Manufacturer	Width	Speed	Weight	Endurance	Frequencies
Inspire 1	Rotary	DJI	28”	49 mph	7.71 lbs	18 Min	5.725–5.825 GHz 2.400–2.483 GHz
Inspire 2	Rotary	DJI	23.8”	58 mph	7.58 lbs	27 Min	5.725–5.825 GHz 2.400–2.483 GHz
Kespry 2	Rotary	Kespry	29”	20 mph	5.8 lbs	30 Min	900 MHz

Table C-6. SAV Use Case Study Available Aircraft and Sensors

UAS Platform	Sensor	Type	Resolution
Kespry	Sony	RGB	24 Megapixel
DJI	Zenmuse X7	RGB	24Megapixel
DJI	FLIR XTR	Thermal	8 Megapixel

EXECUTION PLANNING

- ATCT Communications
  - SAV
    - CTAF: 119.1
    - UNICOM: 122.95
    - ATIS:123.75
- NOTAMS
- List of Waivers
  - Flying near airports / in controlled airspace (Part 107.41)
    - Shall be conducted by Woolpert pilots for SAV study per current waiver

- Airspace
  - SAV FAA Waiver and AOC
  - ATCT coordination prior to flight
- Data collection storage and analysis
  - Privacy Policy

SAFETY & RISK ASSESSMENT

A safety risk assessment was conducted, and the results documented during the detailed mission planning to identify the hazards and associated risks, and ensure proper risk controls were in place. The participating airfields required additional operational safety plans and mitigation tactics. Additional plans were developed as required.

Mishap Plan

While no mishap occurred, the plan to respond to a mishap was as follows:

The team conducting the operations will follow local, FAA, and National Transportation Safety Board (NTSB) guidance regarding mishap reporting and investigation. The team conducting the operation will refer to the emergency response plans they have in place to secure the mishap scene and notify authorities. In addition to any investigation, RPIC will report the following information if the mishap results in serious injury or property damage exceeding $500 to repair or replace the damaged property.

All mishaps meeting the defined threshold will report the following information in compliance with AC 107-2, 4.5–4.5.2:

1. sUAS RPIC's name and contact information
2. sUAS RPIC's FAA airman certificate number
3. sUAS registration number issued to the aircraft, if required (FAA registration number)
4. Location of the accident
5. Date of the accident
6. Time of the accident
7. Person(s) injured and extent of injury, if any or known
8. Property damaged and extent of damage, if any or known
9. Description of what happened

Reports can be submitted by phone or web

FAA Regional Operations Center
South Carolina: 404-305-5156
Texas: 817-222-5006
www.faa.gov/uas

NTSB shall be notified if the mishap results in death or serious injury

Planning included:

- Flight control system malfunction or failure: For an unmanned aircraft, a true "fly-away" would qualify. A lost link that behaves as expected does not qualify.
- Inability of any required flight crewmember to perform normal flight duties as a result of injury or illness. Examples of required flight crewmembers include the pilot, remote pilot, and visual observer if required by regulation. This does not include an optional payload operator.

- Inflight fire, which is expected to be generally associated with batteries
- Aircraft collision in flight
- More than $25,000 in damage to objects other than the aircraft
- Release of all or a portion of a propeller blade from an aircraft, excluding release caused solely by ground contact
- Damage to helicopter tail or main rotor blades, including ground damage, which requires major repair or replacement of the blade(s)
- An aircraft is overdue and is believed to have been involved in an accident

General Safety Considerations

The airport operator, UAS RPIC, and the rest of the team were briefed on and discussed all safety considerations prior to conducting flight operations.

- All autonomous operations were conducted in accordance with AC 107-2 5.2.3 or COA/Waiver
- Considerations for ATC Requirements
    a. Current COA
    b. Detailed procedures, routes, and objectives of the UAS
    c. Preflight ATCT coordination
        i. Start time and expected end time of operations.
        ii. Area to be flown
        iii. Two-way communications checks (phone)
        iv. Areas to avoid
    d. Airport management was briefed on procedures, including emergency response and other airport stakeholders as necessary
    e. Instant method of communication with UAS to cease/adjust UAS operations
        i. It may be necessary for UAS operator to have an operational VHF radio for instant communications, depending on complexity of airport and traffic density. Cellphone may not be acceptable.
        ii. UAS operation must be capable of abandoning its flight profile immediately if ATC requires it.
    f. Identifiable areas within the AOA for ATC situational awareness of UAS
    g. Schedule of operations, if routine
    h. Procedures for off-nominal, unscheduled UAS response to incidents/hazards, etc.
- Possible interference from domestic Wi-Fi
- Environmental conditions

POST FLIGHT MEETING

The following notes represent a high-level summary of the follow up meeting to the SAV Use Case Study flights.

The purpose of the meeting was to discuss the UAS Use Case Study that took place at SAV on June 19, 2018. The goal was also to obtain comments from the airport with regards to security and operational issues.

Discussion on implementation of UAS for security:

- SAV indicated that they see UAS as another tool in a security and operations toolbox to respond to zone-based alarms and routine surveillance.
- Integration should not only be with airport security systems, but also with the FAA and Airport Operations.
- It was noted that each UAS should be equipped with a transponder that would send (potentially) a location to the ATC and ground towers to indicate that the UAS has been dispatched and is responding to an alarm.
- Systems must be configured with a feature that will send it to a home location after loss of signal or low-power situations.
- A security-related UAS should have its programming geofenced and be configured to not cross movement areas, but to travel along the AOA perimeter fence line.
- System should be equipped with a grid map and configured to not fly above 200 feet. In most cases, the intent would/should be to fly safely above and along the AOA fence and report back data from fence/perimeter inspections and intrusion attempts.
- Security departments acknowledge the ability to use an UAS in support of an airport's Vulnerability Assessment.

Discussion on use and implementation of UAS for airport-wide support:

- Other uses and tasks outside of security were discussed, such as:
    - Wildlife inspection and mitigation
    - Roof inspections
    - FOD inspections
    - Support for maintenance, engineering, and operations units
- Overall, it was noted that a set of guidance tools for airports will help them move forward with decisions regarding the use and implementation of UAS.

APPENDIX D: SUAS STANDARD OPERATING PROCEDURE TEMPLATE

STANDARD OPERATING PROCEDURE (SOP) TEMPLATE

Title: SMALL UNMANNED AIRCRAFT SYSTEMS		Code Number: DRAFT
Functional Category: SECURITY SERVICES	Issuing Department: *(SECURITY)*	Effective Date: mm/dd/yyyy

DRAFT – FOR GUIDANCE DISCUSSION PURPOSES ONLY

1.0 PURPOSE

1.1 This policy is intended to provide personnel who are assigned responsibilities associated with the deployment and use of small unmanned aircraft systems (sUAS) with instructions on when and how this technology and the information it provides may be used for (security / law enforcement/ public safety) purposes in accordance with law.

2.0 DEPARTMENTS / PERSONS AFFECTED

2.1 *(to be determined by each specific airport)*

3.0 POLICY

3.1 It is the policy of this department that duly trained and authorized (*department)* personnel may deploy sUAS when such use is appropriate in the performance of their official duties.

4.0 PROCEDURE

4.1 Procedures for UAS operations

4.1.1 Operations will be conducted in accordance with (IAW) all Federal Aviation Administration (FAA) regulations and IAW any applicable operating agreements and waivers.

4.1.2 The sUAS will be operated only by personnel who have been trained and certified in the operation of the system.

4.1.2.1 Outdoor operations require one (1) FAA Part 107 licensed pilot on scene at all times the drone is in flight.

4.1.2.2 Indoor operations require at least one (1) operator certified by (*department*).

4.1.3 Remote Pilot in Command (PIC):

4.1.3.1 One PIC will be designated for each flight.

4.1.3.2 Must be on scene during all flight operations.

4.1.3.3 PIC has the final authority in relation to flight operations and is responsible for the safety of flight operations.

4.1.3.4 Ensure on-duty Police supervisor, Communications, and the Airport Duty Manager ((XXX) xxx-xxxx) are notified of outdoor launch.

4.1.3.5 Designates personnel as crew members as required.

4.1.4 The sUAS equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the Security Department (and may be considered SSI)

Page 1 of 2 SMALL UNMANNED AIRCRAFT SYSTEMS

STANDARD OPERATING PROCEDURE (SOP) TEMPLATE

4.2 **Digital Multimedia Evidence (DME) Retention and Management**

4.2.1 All DME shall be handled in accordance with existing policy on data and record retention, where applicable.

5.0 DEFINITIONS

5.1 **Beyond visual line-of-sight (BVLOS):** when a pilot/operator of an unmanned aircraft can no longer see the aircraft with unaided vision.

5.2 **Certificate of Waiver or Authorization (COA):** Issued by the FAA for operation in certain airspaces; waiver

5.3 **Digital Multimedia Evidence (DME):** Digital recording of images, sounds, and associated data.

5.4 **Indoor Operations:** Flight within a permanent or temporary structure which prohibits vertical access to airspace.

5.5 **Unmanned Aircraft System (UAS):** A system that includes the necessary equipment, network, and personnel to control an unmanned aircraft.

5.6 **Small Unmanned Aircraft Systems (sUAS):** UAS systems that utilize UAVs weighing less than 55 pounds and are consistent with Federal Aviation Administration (FAA) regulations. Referred to as a drone.

5.7 **UAS Aircraft Pilot:** A person exercising control over a UA/UAV/UAS during flight.

5.8 **UAS Remote Pilot in Command:** Designated pilot with authority over on scene flight operations. Must be FAA Part 107 licensed pilot for outdoor operations or DFW DPS certified for indoor operations.

6.0 REVISION HISTORY

6.1 02/21/2017 Original document.

APPROVED:

____

UAS Flight Log

UAS Flight Log			Mission #
Mission/Flight Plan			
Pilot Name:		RP Cert. #:	
Address:		Phone:	
Visual Observer(s):			
Location:			
Date:		Aircraft Type/Name:	
Planned Time:		Aircraft Certificate #:	
Estimated Mission Duration:		Mission Type (VFR, IFR):	
Airports within 5 miles:			
Waivers Applied for:			
Mission Description/Route:			

Mission/Flight Record			
Flight 1	Takeoff Loc:	Launch Time:	Flight Notes:
	Landing Loc:	Landing Time:	
	Battery Voltage:	Elapsed Time:	
Flight 2	Takeoff Loc:	Launch Time:	Flight Notes:
	Landing Loc:	Landing Time:	
	Battery Voltage:	Elapsed Time:	
Flight 3	Takeoff Loc:	Launch Time:	Flight Notes:
	Landing Loc:	Landing Time:	
	Battery Voltage:	Elapsed Time:	
Flight 4	Takeoff Loc:	Launch Time:	Flight Notes:
	Landing Loc:	Landing Time:	
	Battery Voltage:	Elapsed Time:	
Mission Notes:			

APPENDIX E: UAS OPERATIONS APPROVAL TOOLS

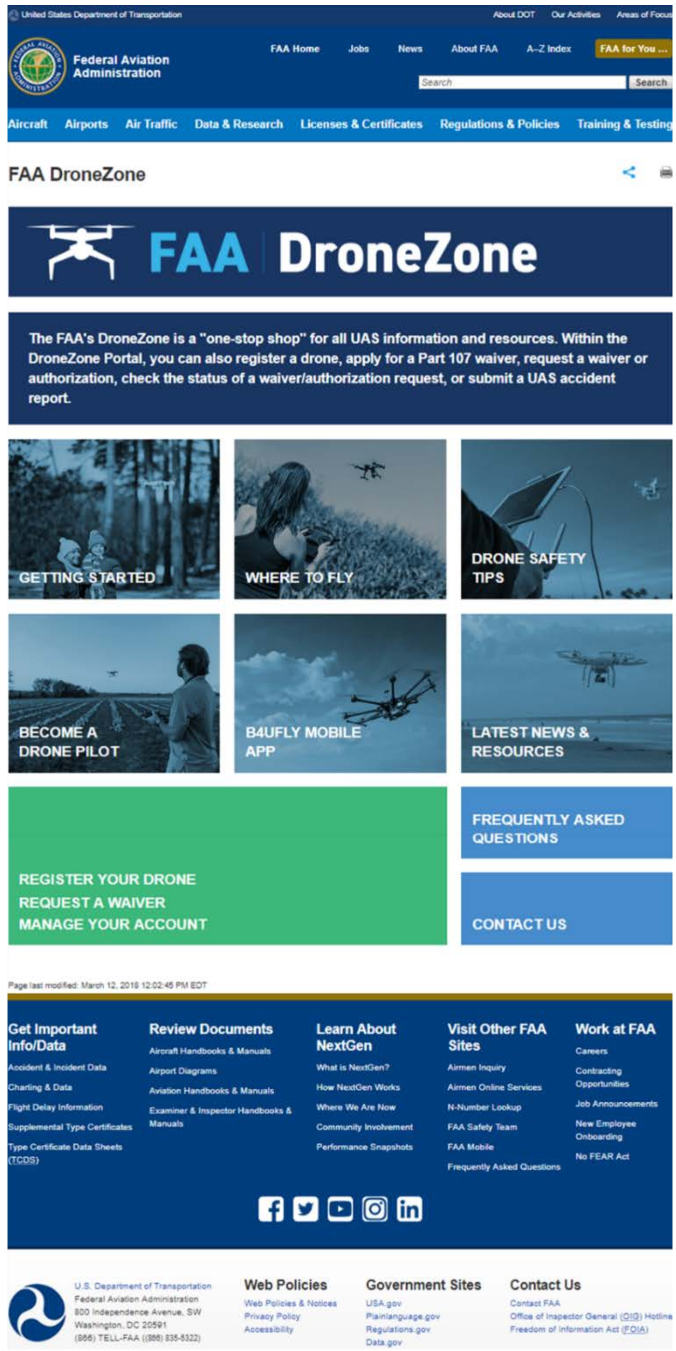
Tables and templates for submitting UAS requests for approval (FAA and others, as appropriate) are included in this appendix.

As of August 2018, three primary user tools have been established to reduce risk involved in sUAS operations, and to ensure regulatory compliance with 14 CFR Part 107: the FAA DroneZone app, the Low Altitude Authorization and Notification Capability (LAANC) access app, and the B4UFLY mobile app.

The FAA DroneZone home page (Figure E-1) contains links for retrieving critical information for safe operation, becoming a certified Remote Pilot, and connecting to the Part 107 Dashboard.

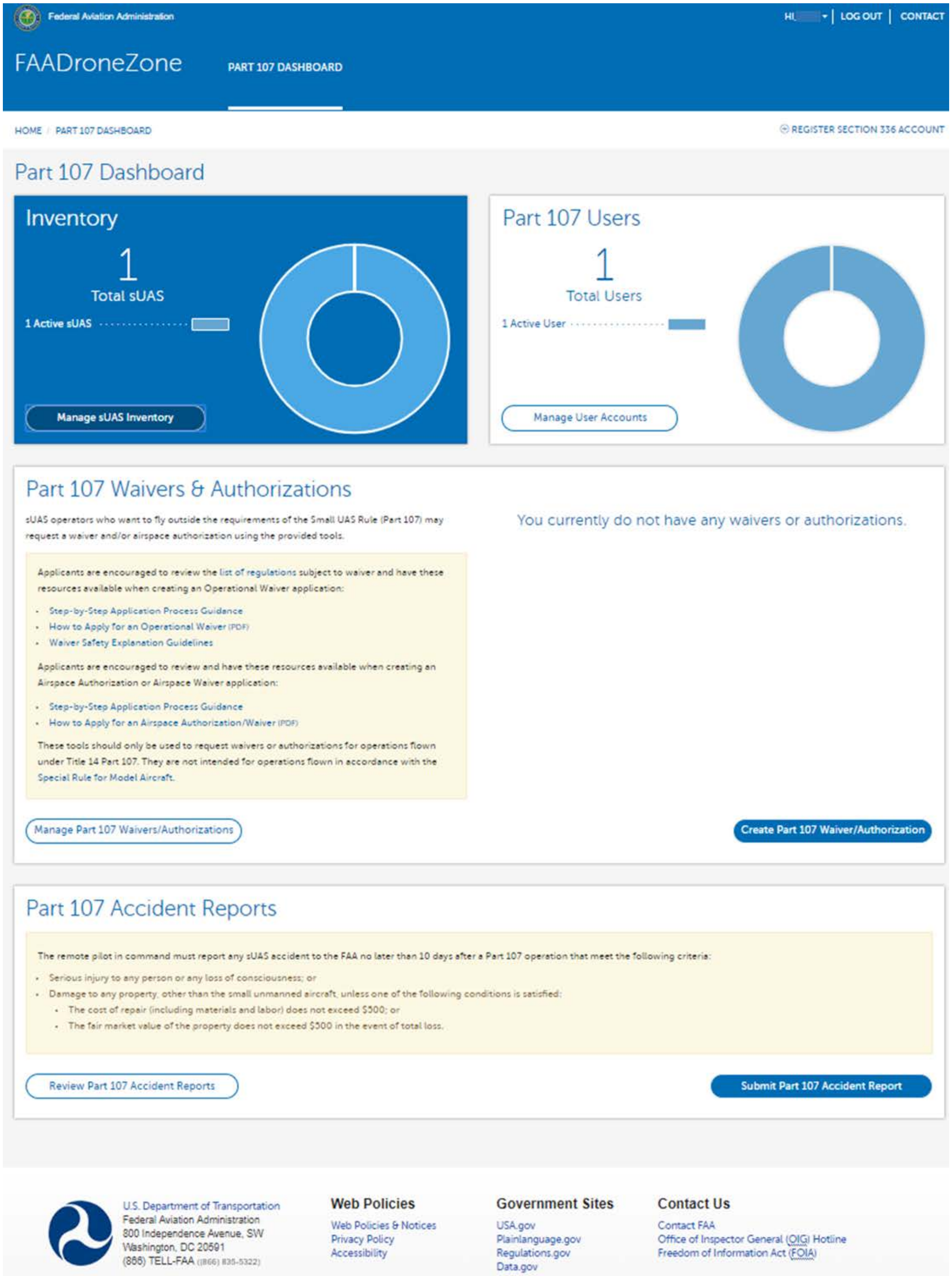
The FAA DroneZone Part 107 Dashboard (Figure E-2) provides a means for both recreational and commercial sUAS pilots to request waivers, register sUAS, and file accident reports in accordance with Part 107 regulations.

Figure E-1. FAA DroneZone Home Page



Source: FAA

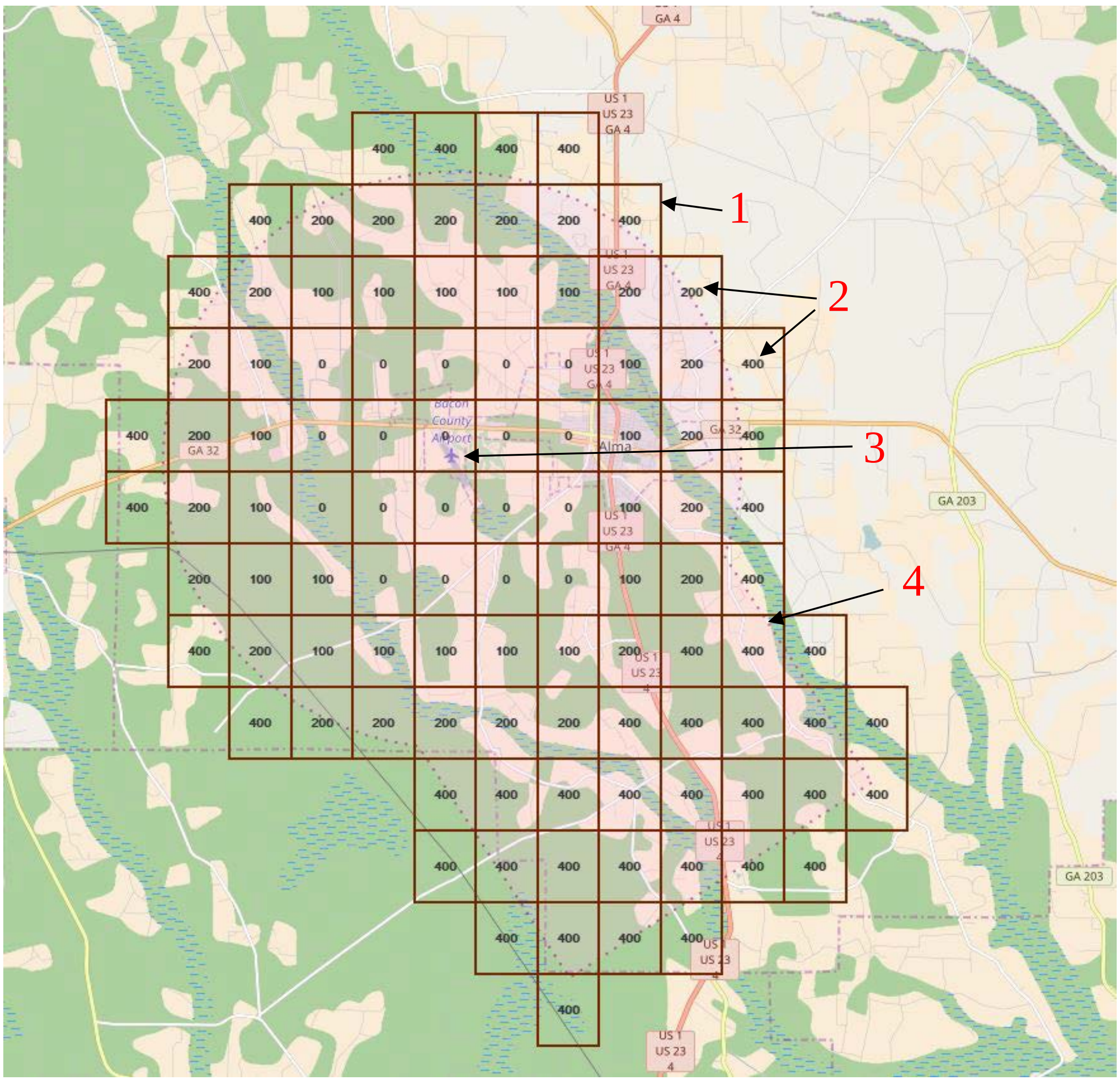
Figure E-2. FAA DroneZone Part 107 Dashboard



Source: FAA

As of August 2018, AIRMAP and Skyward are two apps that allow the user to request airspace approvals in near real-time, facilitating the LAANC. The process is simple and only requires access to a cellular network or the web. The user locates the airspace they want to operate in, designates the operating area dimensions they will be working in, inputs the user and aircraft information, and submits the request, which will be approved or denied at the time that is submitted. AIRMAP provides the ability to request airspace up to 90 days prior to the operation. Figure E-3 is an example of a facility map that a user would see on AIRMAP.

Figure E-3. Class E Surface UASFM: Bacon County Airport (AMG)



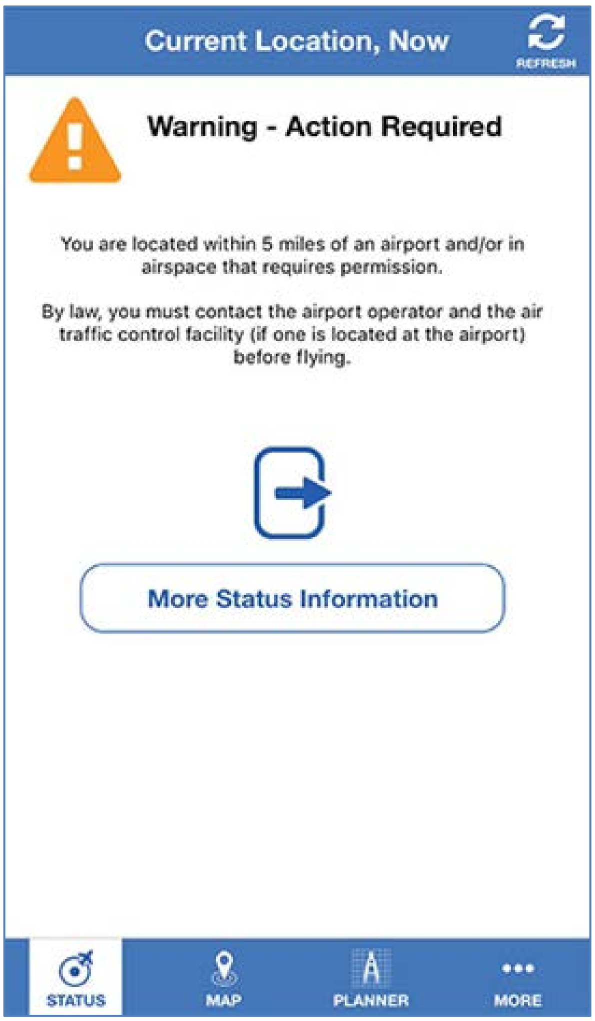
Source: FAA

1. Designated airspace section
2. Authorize operating altitude in feet AGL
3. Airport location
4. Class E airspace border

B4UFLY is an FAA mobile app that can be downloaded to a mobile device for free and provides the following:

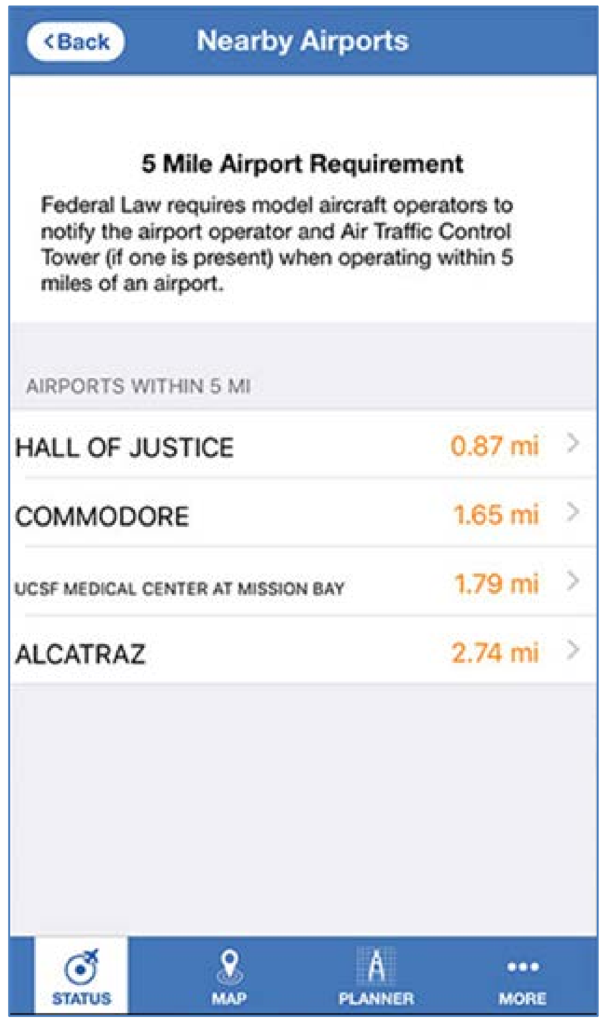
- A clear status indicator that immediately informs the operator about the current or planned location. For example, it shows that flying in the Special Flight Rules Area around Washington, DC is prohibited (Figure E-4).
- Information on the parameters that drive the status indicator (Figure E-5)
- A Planner Mode for future flights in different locations (Figure E-6)
- Informative, interactive maps with filtering options (Figure E-7)
- Links to other FAA UAS resources and regulatory information

Figure E-4. Status Indicator



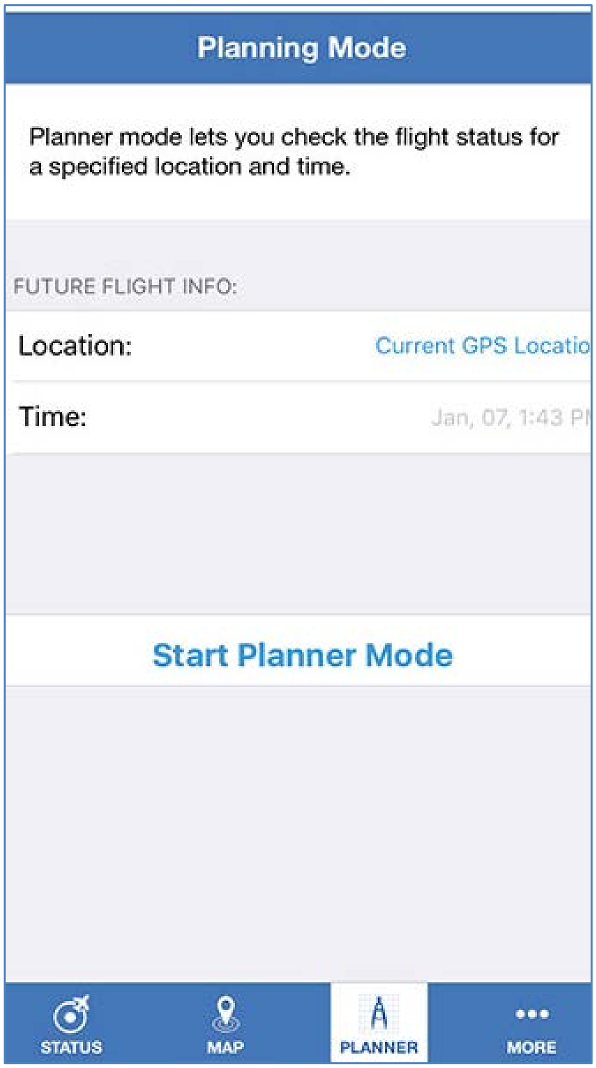
Source: FAA

Figure E-5. Status Indicator Parameters



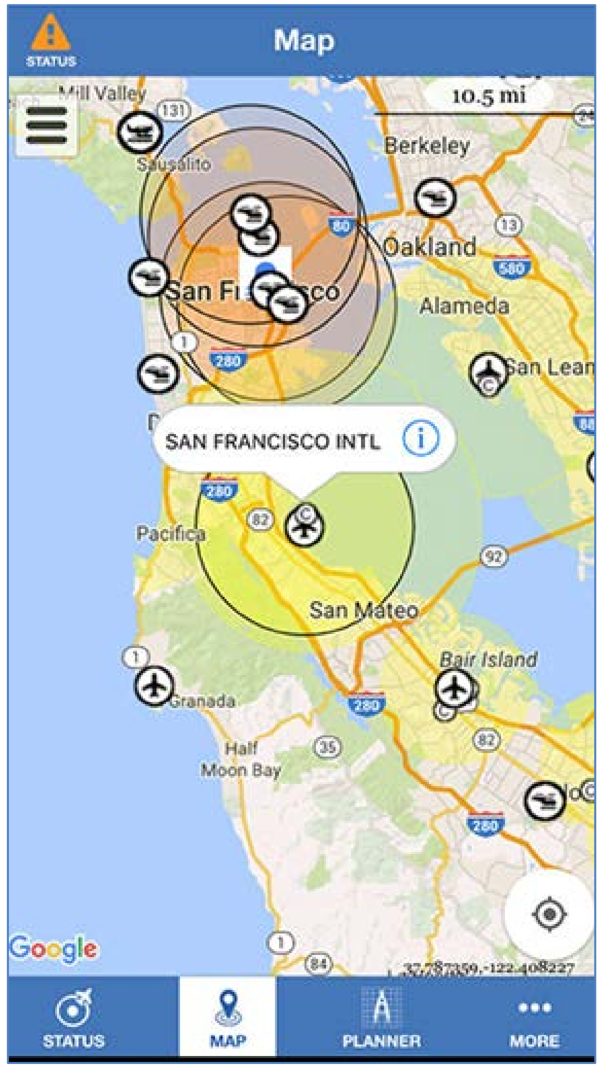
Source: FAA

Figure E-6. Flight Planning



Source: FAA

Figure E-7. Airspace Interactive Maps



Source: FAA