Analysis of the FAA's Small UAS Regulations for Airports Security Support UAS Operations

by

Akbota Ashirbek

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved April 2022 by the
Graduate Supervisory Committee:

Michael Cirillo, Chair
Katherine Wallmueller
Nancy Cooke

ARIZONA STATE UNIVERSITY

May 2022

ABSTRACT

Unmanned Aircraft Systems (UAS) are finding new applications in various industries, including airport operations. One of the most recent examples of this type of application is the Security Support UAS, which serves as a supporting technology for airport security. Their ability to conduct surveillance autonomously at a higher rate of speed in regions inaccessible to vehicles makes them a perfect instrument for supporting numerous airport security activities such as perimeter patrol, security alert response, and threat tracking. Despite the benefits, present regulations restrict the usage of this technology in airports. This study aims to determine how well equipped the regulatory framework is to support safe UAS flights at US airports. The Federal Aviation Administration's (FAA) Small Unmanned Aerial System Rule, generally referred to as Part 107, was analyzed qualitatively to examine the current regulatory environment. Although Part 107 is intended to regulate low-risk small UAS flights, findings indicate that requests for waivers to Part 107 that include appropriate risk mitigation can enable more complex UAS operations. The FAA has made tremendous strides in adapting current regulations to meet the operational requirements of numerous emergent UAS applications through its waiver procedure. On the other hand, more permanent solutions are required to enable scalable operations.

ACKNOWLEDGMENTS

I would like to acknowledge and thank my thesis advisor Michael Cirillo for his significant assistance and supervision. Additionally, I would like to express my gratitude to Andrew Mihaley, my summer internship supervisor, for sparking my interest in the drone sector. Finally, I want to express my gratitude to my family and friends for their encouragement and support throughout this challenging academic path.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

INTRODUCTION

Many different public and private sector industries have benefited from the use of Unmanned Aerial Systems (UAS), also known as drones. For example, the healthcare industry transports human organs and medications from hospital to hospital. Law enforcement agencies employs drones for locating missing persons or public surveillance; and the military sector uses numerous drone applications to set up internet hotspots in remote locations (Chao & Chen, 2012). Aside from being an entertainment tool for model airplane enthusiasts, the commonplace adoption of UAS by various industries shows that this technology may also be an effective tool to serve public needs. Commercial airports are no exception to this ubiquitous usage of drones. There are multiple opportunities to use drones in airport operations, such as airport assessment; wildlife and environmental control; aircraft, and airport infrastructure inspection; etc. Although there are numerous opportunities to incorporate drones within airport security programs, this thesis paper concentrates on employing this newly developing technology for commercial airport perimeter patrols.

Airport perimeter security presents a wide array of challenges. In addition to the larger areas that must be safeguarded, there are numerous minor entrance points, fuel depots, and other vulnerable locations. Any unwelcome airport entry carries a great danger of harm, even reaching the level of national security (Griffiths & Boehm, 2018). Considering the increasing threat level and the complexity of airport security, airports must install security solutions that are adaptable, flexible, and reliable. For airport security, drones represent a fresh approach and have already proved to be an efficient

tool. Airports like Savannah Hilton and Dallas/Fort Worth International have begun using drones as part of their routine operations programs for inspection, maintenance, and law enforcement.

The technology's capabilities and applications are increasing at a rapid pace. To give just a few examples, UAS in airport security programs could be used for perimeter patrols, perimeter intrusion detection systems (PIDS) monitoring and reaction to alarm systems, threat tracking, visual inspection of the airport's remote areas, and many other tasks. The most recent use case of similar UAS application was demonstrated by the Safe Skies Alliance. Namely, the case presented the novel application of Security Support UAS - autonomous drones which can be operated from fixed base stations permanently installed around the airport perimeter. In addition to providing a shelter from precipitation and other weather conditions, the UAS base stations will serve as a charging unit and communication links to the vehicle command-and-control location, making it an appropriate instrument for performing uninterrupted functions for airport security controls. It is anticipated that a network of several autonomous UAS will be used to support the perimeter security activities, such as responding to intrusion alarms and detecting threats and relaying real-time surveillance video back to the operators in command (National Safe Skies Alliance, 2019). This will allow security officers to assess the danger at a distance and decide what resources are needed to counteract it. Even small hub airports may have to conduct perimeter patrols multiple times a day, and the capacity to dispatch drones autonomously might have a considerable impact on airport efficiency.

Drone activities in airport surroundings are currently limited, and no US airports have implemented such technology within their security programs. The review of case studies revealed that the primary constraint for the realization of the full advantages of this novel method in airport security is obtaining approval through the current aviation regulatory process. Furthermore, this thesis will explore how Security Support UAS operations can be made possible under present regulatory conditions.

Purpose and Scope

The purpose of this thesis is to examine how well the current regulatory environment is structured to enable safe UAS operations at airports, as well as the legal pathway for operators seeking to use UAS in the vicinity of airports.

Although there are broad categories of drones, starting from palm size UAS to large UAS with a wingspan equal to the B737; from rotary-wing to fixed-wing, and hybrid UASs (rotary-wing and fixed-wing in one platform), the small quadcopter UASs weighing less than 59 lbs. have proven to be especially productive in an airport environment. They are small, can be launched quickly, are able to hover in one place to collect the necessary data, and do not require much space for launch unlike fixed-wing counterparts which may require a full-length runway for take-off and recovery. Moreover, small UAS platforms are versatile. Their interchangeable camera configurations allow the operator to customize the UAS platform for different missions. Thus, this thesis focuses primarily on small UAS, and all the application examples stated in this paper refer only to small UAS.

LITERATURE REVIEW

Airport Perimeter Security

Historically, aircraft and airports have been linked to terrorist activity, such as hijackings or attacks on airport facilities. The tragic events of September 11, 2001 are a prime example. Those events triggered activities by airports and the federal government aimed at strengthening the physical security of airport property. Today, airports monitor the perimeters more closely using state of the art technologies to detect and interdict possible intrusion attempts.

Airport perimeter defines the boundaries of an airport property (Bartholomew, 2010). Airport perimeter security consists of various physical measures which may vary from airport to airport. The most common protection measures of commercial airport perimeters include fences equipped with access control, surveillance technologies, and patrols.

The perimeter security of any commercial aviation airport begins with the fencing of the property line of the airport; it is the simplest and cheapest measure to secure the perimeter but provides minimal protection. Therefore, fences do not provide complete security. However, fencing is a crucial component of commercial airport security as it is "the first line of defense against intrusion" (the National Crime Prevention Institute, 1986, as cited in Sweet, 2008) at any airport. According to Sweet's book (2008), the following are requirements for airport fencing: chain link fences are commonly used with a minimum height of eight feet and a mesh size minimum of two inches to prevent wild animals from getting through; the fence must be topped with barbed wire; the fence has

to be recessed into the ground so that people or animals cannot tunnel into the airport territory. Some other more controversial methods include electrifying the fences and extending barbed wire at an outward angle. While these methods can be effective in deterring intruders, they are not commonly permitted due to liability issues (p.330).

Although it is a requirement that large commercial passenger airports install fences along the entire perimeter of airports (Bartholomew, 2010), some airports cannot follow this policy due to their specific topographic features. Such features may be a natural barrier such as lakes, rivers, cliffs. For example, a significant portion of airports such as Boston Logan International Airport and San Francisco International Airport are surrounded by water making them impractical for fencing. Such natural boundaries present a vulnerability to intrusion due to lack of protection; they should not be disregarded and perimeter defenses other than fences should be implemented.

After fencing, the next common measure in airport perimeter security is surveillance technologies. Close Circuit Television (CCTV) is probably the most ubiquitous and indispensable means of perimeter security at many airports. The main requirement for the cameras is that they must be capable to monitoring beyond the fence line, thus providing a deterrent and early warning of unauthorized access. Today's CCTV cameras have the capability to monitor activity near a fence and record the intruder if so needed. The components of the monitoring system, such as 24/7 color vision cameras and the infrared cameras, allow surveillance in poor visibility. Some cameras are equipped with motion detectors to alert a guard that a camera has spotted an individual near the fence (Sweet, 2008). The latter is especially helpful considering human factors

limitations that are ever present in the aviation environment - the potential threat may not be detected due to human inattention, fatigue, or lack of adequate staffing.

To ensure the efficiency of perimeter monitoring cameras at nighttime, sufficient lighting measures should be considered. Airport security lighting should be directed towards the fencing area, ideally from inside the fence, lighting the area for at least 20 feet from the fence (Sweet, 2008). Additionally, it is essential that surveillance cameras and security lighting are checked regularly for signs of damage or inoperability.

A primary method of detection for intrusions at airport perimeters has always been security patrols. They remain so today, even in an era of advanced technology and surveillance. Law enforcement agencies with jurisdiction are also widely relied upon to offer support for a variety of security responsibilities, such as conducting airport facility patrols (Bartholomew, 2010). Nevertheless, the local police department's role in airport perimeter security is small, and it is mainly predicated on responding to calls, rather than early detection and prevention (TSA Hearing, 2011). In addition to traditional intelligence and law enforcement measures, some airports have instituted new and unique methods for keeping an eye out for unusual activity around their perimeters and on the airfield itself. Price & Forrest, (2016) demonstrated two examples of such unique applications in their book:

- At Boston Logan International Airport, the airport management had sought the support of local fishermen who work close to the airport's shoreline. The participants in this program received security awareness training, as well as phone

numbers to inform the airport security representatives in the event they notice any attempts of break-in to the airport territory (p.259).

- At the Houston George HW Bush International Airport, the management relies on the "airport rangers" who volunteer and monitor the airport's 3000 acres of highly wooded area on horseback (p.260).

Last but not least, each person working at the airport plays a key role in maintaining airport security. As a condition of keeping their badge, the employees are obligated to report anybody who is within the perimeter fence in an unauthorized capacity. As noted by the Charlotte Airport manager, “the fence is a deterrent, it says, keep out, however, the final line of security is the eyes and ears of the people who work inside the fence”(TSA Hearing, 2011).

With this abundance of security measures in place, we keep hearing about instances of airport security breaches. For example, after leaping over a barrier at San Jose International Airport in April 2014, an unaccompanied 15-year-old immigrant made it into an airplane's wheel well and managed to reach Hawaii alive. Investigations into breaches of perimeter fences at US airports were triggered by this high-profile case. In 2016, the Associated Press (the AP), an American non-profit media outlet, reviewed the frequency and nature of such invasions. The investigation revealed that in the period between January 1, 2004, and January 31, 2015, at least 268 persons were caught breaking into the perimeter of the country's major commercial airports by jumping fences, sneaking past access points, or driving their cars through fences (The Associated Press, 2015). The Nation’s airports’ perimeters are often breached, allowing unlawful

passage to the highly protected planes and airport terminal. Massachusetts Congressman William Keating described an airport security breach as, "It's like shutting the doors of your house but leaving the windows ajar" (GAO, 2016).

The main challenge in airport perimeter security is that airports typically have large territories that need to be monitored. The average mid-size airport in the US has approximately 15-20 miles of perimeter length; this requires a lot of personnel and monetary investment to acquire necessary equipment (Sweet, 2008). At the world's most fortified airport, Ben Gurion Airport in Israel, with no known perimeter intrusion history, they spend more than $200 million annually on perimeter security. The airport's director reported to the AP that their measures include two fences with a radar system between them, cameras, and hundreds of armed agents. In the US, as commented by the reporters, it may not be financially or physically feasible to implement such drastic measures in all the nation's commercial airports (Mendoza & Pritchard, 2015).

Although, since the events of September 11, US airports have made huge strides to improve airport security and invested hundreds of millions of dollars to upgrade their fencing, security cameras, and other detection technology, the airport perimeter continues to be a weak link. The instances of perimeter breaches revealed by the AP is proof that there are clearly still gaps in the multi million worth of surveillance cameras and motion detecting systems which remain to be subject to breaches by intruders. Airport security experts interviewed by the AP remarked: "show me a 10-foot fence, and I will show you an 11-foot ladder" (Mendoza & Pritchard, 2015). No solution can guarantee a fool-proof airport security system. It should be noted that even though these barriers cannot provide

full protection, they provide airport security personnel the benefit of time and distance to reach the intruder if detected soon enough (Sweet, 2008). For example, in the same interview with the AP, airports representatives revealed the intruder suspects were detected within 10 minutes after breach with several people being undetected or never being caught. Sweet, (2008) argues that the combination of several layers of protection adds to the protection level and increases the probability that an intruder will be detected. Early threat identification and response will enable rapid measures to reduce risk to the airfield operations. The goal should be to put in place many layers of security as part of an integrated security program for the maximum effect in deterring and detecting criminal activity and terrorism at the airport (Benny, 2013).

Integration of Unmanned Aircraft Systems into Airfield Operations

Integration of Unmanned Aircraft Systems (UAS) in airport security operations is a brand-new approach. The Federal Aviation Administration (FAA) defines a UAS as a system that consists of an unmanned aircraft, including all of the components required to to efficiently and safely function in the National Airspace System (NAS). For airport security, understanding the components of a UAS, as well as regulatory and supportive systems, is essential. The aerial vehicle, base station, payloads, and communication systems are the main components included in an unmanned aircraft system. To control a UAS and connect flight systems to the unmanned aircraft, ground stations are used. These devices are often laptops or tablets that have internet capabilities (National Safe Skies Alliance, 2019). UAS payloads can be replaceable or standard, allowing the UAS

platform to be tailored to each mission's specific requirements. These payloads can include cameras in various colors or thermal sensors.

In 2019, the National Safe Skies Alliance conducted a study that was funded by the FAA to evaluate UAS applications in airport security. As a result, a *Guidance for Integrating UAS in Airport Security* was produced. The report revealed that the ability of a UAS to launch quickly, monitor a situation hovering from a safe distance, and track an object makes them a “force multiplier” in many ways to support existing airport security systems (National Safe Skies Alliance, 2019). Drones enable airports to minimize the number of personnel required to complete certain tasks and maximize the efficiency of existing systems they are supporting. For example, drones can conduct runway pavement inspection at airports in half an hour. Doing the same tasks using conventional methods would require up to eight hours, during which time the runway must be closed to all traffic; whereas, if planned smartly, use of UAS would require no runway closure. The inspection can be accomplished in between landings and take-offs (Hubbart et al, 2017). The main benefit in this approach is that human presence in safety critical areas is not necessary. The drone can be controlled from a safe distance, which is extremely helpful in airport environments where persons or the presence of physical obstructions in critical areas may interfere with navigational systems and cause errors.

In addition to saving considerable time, drones also have a minimal start-up cost. National Counter Terrorism Policing Headquarters in England indicated that UAS can do tasks seven times faster and at one-tenth the cost compared to ground-based task management, lowering the number of personnel required for patrolling at a savings of

£1.2m ($1.5m USD) over three years (Beake, 2015). Also, the Office of Inspector General of the Department of Justice announced in a September 2013 report that small UAS ranging up to 55 pounds can have significantly cheaper operational and maintenance expenses than manned aircraft. Estimates of $25 per hour for unmanned aircraft compared to $650 per hour for manned aircraft operations are cited in the report. A growing number of law enforcement agencies will be able to use UAS as a low-cost alternative to manned aircraft as the technology advances. The report also revealed that UAS can be a helpful tool in situations with high risk. Examples include hazardous material assessments and crime scene evaluations. This provides the working group with the optimum approach to dealing with threats without compromising responders' safety (National Institute of Justice, 2016).

UAS can serve an airport as an "eye in the sky" due to their capability of gathering real-time visual information from a safe distance of up to 25 feet above the ground. Improved situational awareness, i.e. an improved vantage point and wider range of view for human operators reduces the time required to conduct an inspection (Korecki et al, 2021). As was mentioned above, due to topographical conditions in some airports, not all of the periphery is regularly patrolled or always under surveillance. UAS could help to solve the surveillance issues of airport territories covered largely by water or wood where human access or security measure implementation is complicated, and where security alarms are likely to be more frequent due to the increased frequency of wildlife activity attracted to the habitat.

The use of UAS in perimeter patrol results in reduced risk of intrusion and fewer instances in which humans must respond to false alarms. False alarms are a common occurrence and must be addressed on a daily basis by airport security. The security manager at Philadelphia International Airport, in her interview with the AP, reported that "most airports that have invested in new technologies spend a lot of time responding to false alarms" (Mendoza & Pritchard, 2015). Even if the alarm is triggered by a plastic bag or a wild animal, a human patrol must be dispatched to check the perimeter. Use of a UAS by airport security to verify perimeter breaches can provide advantages such as a faster response time, the freedom to navigate directly to the location where the incursion is detected, and much-needed situational awareness to security forces. Dispatching UAS to respond to false alarms, allowing security officers to only conduct inspections when they are necessary, may help alleviate the shortage of personnel. Additional security measures include regular inspections of the cameras, lighting, and fences to ensure that they are working properly and that they haven't been damaged or breached. It takes a long time to dispatch humans to do these kinds of tasks. Using drones to carry out these tasks can be far more efficient. As an example, a UAS can perform inspections on a regular basis, supervised by humans, thereby eliminating or reducing the number of physical inspections by airport staff.

The current integration of UAS into airfield operations has been largely done airport-by-airport, with no uniform rules or specific standards in place for this technology. Some airports have moved ahead on their own to test and deploy UAS technologies in their security programs without waiting for formal technical assistance from the FAA.

Deployments such as these are outlined in the Guidance for Integrating UAS in Airport Security that was mentioned above. Several examples of these deployments are presented in the following paragraphs.

In order to successfully plan for runway repairs and full resurfacing projects, Atlanta International Airport has used drones for 3D mapping of runway surfaces to detect cracks. Typically, this type of work would require the inspected runway to be closed for several hours for the airport staff using specialized equipment to complete runway inspections. Whereas, using UAS for the same tasks allowed the runways to stay open longer, raising revenue and effectiveness because of the shorter completion time (National Safe Skies Alliance, 2019).

Savannah/Hilton Head International Airport's use case is noteworthy as well due to the fact that it was one of the first airports to officially integrate UAS to support their regular operations, including airport inspection, maintenance, monitoring, facility management, etc. The detailed description of this use case is provided in a paper by Mackie and Lawrence (2019). The authors point out that with the employment of the UAS, instead of driving up and down the runway to identify pavement, lighting, and marking issues, the airport deployed their UAS to collect data remotely. As a result, the airport team was able to analyze the conditions of the pavement and create work orders with accurate coordinates and imagery, which were immediately uploaded and documented in the relevant airport system for future reference. This minimizes the frequency of visits and the duration that workers spend on airport safety-critical areas. The use case demonstrated that drones could be used efficiently for routine airport

operational needs and validated the productivity and safety benefits for the airport staff (Mackie & Lawrence, 2019).

One more prominent example is the integration of UAS by Dallas-Fort Worth International Airport. The use case is well described in Sichko's (2019) paper. According to this study, Dallas airport was one of the first airports to receive the FAA's approval to fly UAS in highly regulated airspace. In 2016, recognizing the potential of this emerging technology and the benefits it can bring to improve airport operations, the DFW Airport management created a UAS working group. The procedures developed by this group enabled UAS flights on airport property in support of law enforcement activities, airport construction, facility inspection, runway inspection, wildlife control activities along the airport perimeter fence, etc. The use of UAS by the police department (unattended vehicle, package investigation); Airport Fire Department (FAA emergency response exercise); airline companies (for aircraft inspection); and construction departments (to track progress, to conduct inspection) are anticipated as well. An important finding that was highlighted in the study was that the inspection of the runway by UAS will reduce the runway closure time – which in turn results in reducing aircraft delays (Sichko, 2019).

Use cases of drones in the airport security domain are currently very limited. In the Guidance for Integrating UAS in Airport Security (National Safe Skies Alliance, 2019), the Safe Skies Alliance (SSA) provided the results of a unique case study involving autonomous security support UAS integration. To conduct this study, the research team installed a fence-mounted perimeter detection system at one of the SSA's test facilities near the McGhee Tyson Airport in Tennessee. During the trials, several missions were

carried out. For example, in one of the test flights, an autonomous drone left its base station to follow a predetermined route using GPS coordinates in order to investigate the test site of another UAS (which served as a target object to track), and provide a panoramic view of the area adjacent to the target UAS's launch site. The autonomous UAS notified the operator when the target object appeared on the scene and began tracking the threat. The security guard was able to assess the danger by monitoring the continuous transmission of real-time video. The mission was successfully completed.

As part of the validation of potential uses of autonomous vehicles for airport security purposes, the results of the latter case study provided the research group with the following information: autonomous UAS's capability to fly pre-programmed routes and switch to manual control when necessary enables the airport staff to deploy this technology for tasks such as routine perimeter patrol, PIDS alarm response, threat detection, and tracking. Moreover, these systems can be configured to support the function of multiple unmanned vehicles and base stations that can interact together to create a network of UASs to support the perimeter security. According to the study, increased efficiency, enhanced situational awareness, and the safety of security personnel are examples of the benefits this technology could bring to the airport environment (National Safe Skies Alliance, 2019).

Based upon the information discussed above, one can draw a conclusion that airports should pursue a strategy of integrating drones into all facets of airfield operations. The reality is that, currently, very few airports are utilizing UAS to support their routine operations. This slow progress can be explained by the fact that the airport environment

is highly regulated, and any technology introduced in this environment is closely scrutinized. Unmanned aircraft have always been prohibited from flying in controlled airspace above airports because of safety concerns. Despite the proven benefits of this technology, the current regulatory framework makes it difficult to obtain authorization for complex UAS operations in an airport environment.

METHODOLOGY

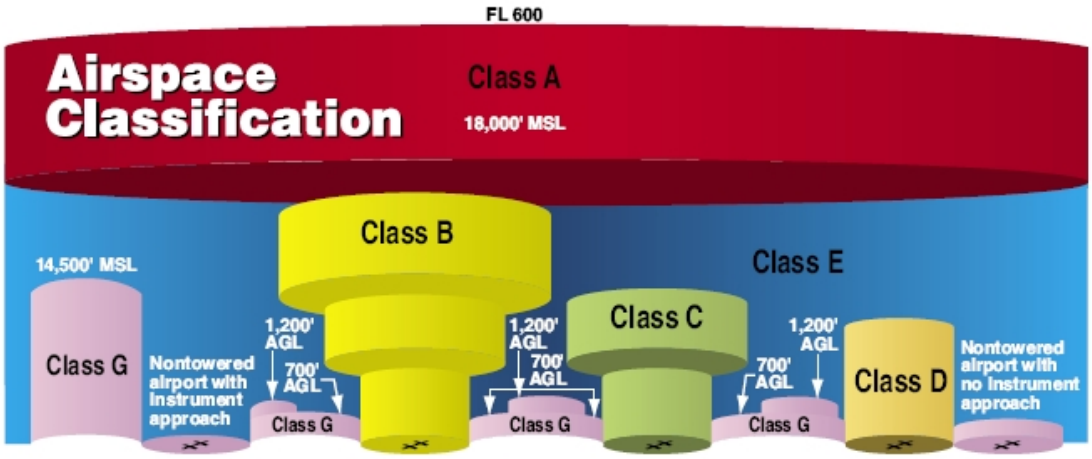
The framework used to inform this thesis is a qualitative analysis of existing literature. As part of the qualitative analysis research, the author found merit in consulting with regulatory agency representatives. Through these interviews, the list of available documentary data was identified. As a result, the study examined Part 107 of Title 14 of the Code of Federal Regulations, advisory circulars, and other guidance and report materials from the FAA.

Current Regulations for small UAS Operations

There are two types of airspace over airports: controlled and uncontrolled. According to the Federal Aviation Administration's airspace classification standards (FAA, 2021b), controlled airspace encompasses the five classes of airspace with set dimensions and includes airspace classes A, B, C, D, and E. Uncontrolled airspace consists of class G airspace. It includes the stretch of airspace that extends from surface up to the floor of class A airspace; air traffic control (ATC) has no jurisdiction or responsibility to maintain traffic separation in this class of airspace. Figure 1 demonstrates the proportions of each airspace type.

Figure 1

Airspace Profile



Note. From Pilot's Handbook of Aeronautical Knowledge, by the FAA, 2021 (https://www.faa.gov/sites/faa.gov/files/regulations_policies/handbooks_manuals/aviation/phak/17_phak_ch15.pdf)

Class B airspace surrounding busy airports and Class C or Class D airspace surrounding medium-sized or smaller airports are expected to be used for Security

Support UAS missions. Class A and Class E are out of scope for UAS airport security integration concepts since these drones are not intended to operate at such high altitudes, such as in Class A airspace (i.e., the layer of airspace between 18,000 feet and 60,000 feet Mean Sea Level); and they are not intended to cross the Class E boundary but remain inside the airspace surrounding airports (Classes B, C, or D). Operating rules for UAS users are different in each type of airspace. In Class G airspace, operators have unrestricted access to the airspace under present regulations, while activities in other airspace classes require authorization.

From the ground up, the FAA oversees US airspace. UASs are subject to FAA regulations for the safety of flight and protection for ground-based residents. Part 107 of Title 14 of the Code of Federal Regulations consisting of the rules for "Operation and Certification of Small Unmanned Aircraft Systems" was issued by the FAA in June 2016 (hence referred to as "Part 107"). Routine UAS operations became possible in the National Airspace System (NAS) under this rule. According to Part 107, a remote pilot certificate must be obtained by completing a pilot training knowledge test before commercial operators can fly their drones, indicating that they understand the impact of weather, airspace rules and safety considerations. The following is the summary of the Part 107 rules imposed by the FAA, (2016):

- the weight of an unmanned aircraft shall not exceed 55 pounds;
- the UAS should always stay within the remote pilot's line of sight;
- only operate during daylight hours (official sunrise to official sunset, local time);

- operations during civil twilight (30 minutes before and after official daylight hours) are allowed if UAS is outfitted with anti-collision lights;
- UAS must yield the right-of-way to other airborne traffic;
- UAS may not operate above any persons who are not directly participating in the operation;
- a pilot in command may only run one UAS at a time;
- UAS's ground speed must not exceed 100 miles per hour;
- UAS must remain under the altitude of 400 feet unless flying in the vicinity of a structure where the maximum flying altitude is not more than 400 feet over the structure's immediate topmost limit;
- Class B, C, D, and E aerial operations are not permitted without the appropriate ATC approval;
- Class G airspace users does not require a prior ATC authorization;

A significant step forward in the FAA's gradual approach to integrating unmanned aircraft into the NAS was taken on January 15, 2021, when the FAA published its final rule amending Part 107 to permit the routine operations of small UAS over people or moving vehicles, and at night without a waiver if they fulfil the criteria defined in the rule (14 C.F.R & 107, 2021). The updates to Part 107 require the following safety standards to be met:

To operate over people and moving vehicle, UAS operator must meet the following safety standards:

- UAS must not have any exposed mechanical components that could cause severe injury upon impact with people;
- UAS components may not contain any safety defects
- UAS must have a label informing the vehicle is permitted to fly above people;

To operate during nighttime, UAS operator must meet the following safety standards:

- UAS must be equipped with an anti-collision lighting that allows the visibility for at least three statute miles;
- to assure acquaintance with the dangers and necessary mitigations of nocturnal operations, the remote pilot operating the vehicle must pass a current knowledge test;

UAS operators that wish to fly over people, moving vehicles or at night must provide the FAA with a declaration of conformity stating that their aircraft meets the criteria mentioned above.

As was mentioned above, to operate within controlled airspace, UAS operators need to gain airspace authorization from ATC. Such authorization permits the operator to operate in certain airspace provided that they comply with the rules of the airspace. Finally, Part 107 incorporates a waiver mechanism for enabling UAS operations beyond what is presently permitted by the rules to enable versatility and facilitate new and creative UAS applications (National Safe Skies Alliance, 2019). Accordingly, the following sections of Part 107 can be waived:

- 107.25: Operations from a vehicle or aircraft in motion.
- 107.29: Anti-collision lights are necessary for night and civil twilight operations.

- 107.31: Visual line of sight operations.
- 107.33: Visual Observer.
- 107.35: Simultaneous operations of multiple UAS.
- 107.37: Yielding the right of way.
- 107.39: Operations over civilians.
- 107.41: Operations in controlled airspace.

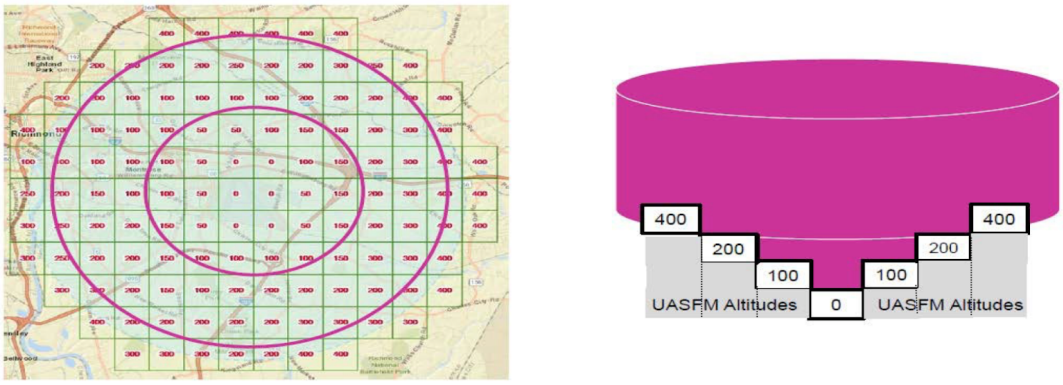
To submit a waiver, an airport must examine its internal safety and risk management plans. Applicants use the FAA's Drone Zone online portal to submit their requests with a detailed explanation of the intended operations and risk mitigation strategies. It usually takes between 60 and 90 days to get the go-ahead. According to the FAA official website, for short-term operations lasting less than six months, airspace authorizations are issued; whereas, airspace waivers can be provided for ongoing operations lasting up to two years. To address the risks associated with UAS operations, the FAA uses Safety Risk Management (SRM) methods - one of the main components of the Safety Management System approach to managing safety risk and ensuring the effectiveness of safety risk controls (see FAA, 2019, for more).

To make the application process easier for the users to apply for the authorizations and waivers, the FAA has implemented systems such as Low-Altitude Approval and Notification Capabilities (LAANC) and UAS Facility Maps (UASFM) (National Safe Skies Alliance, 2019). Remote pilots with current certificates can obtain airspace authorization to fly in controlled airspace through the LAANC system. When approving the request, consideration is given to UASFM provided by the air traffic control tower

with jurisdiction over the airspace. The example of UASFM can be seen in Figure 2; these maps identify restrictions within airspace surrounding the vicinity of airports. As can be seen from the picture, the airspace over airports typically has an acceptable height of zero, which indicates that UAS must not operate within this area. While applying through LAANC can be convenient for gaining immediate authorizations below a defined altitude ceiling, the system will automatically dismiss the requests within zero-altitude locations. The applicants seeking to obtain waivers to deviate from current rules must apply through the FAA Drone Zone portal.

Figure 2

UAS Facility Map Illustration



Note. From FAA Unmanned Aircraft Systems Integration Pilot Program, by the FAA, 2021 (https://www.faa.gov/uas/programs_partnerships/completed/integration_pilot_program/media/IPP_Final_Report_20210712.pdf)

SUMMARY OF FINDINGS

Because these systems are planned to operate autonomously, equipping airports with Security Support UASs would significantly boost productivity. Percepto Sparrow Automated Drone Systems is one candidate for providing perimeter security support. The system's components include an unmanned vehicle, a base station, and equipment for managing the vehicle. With a maximum takeoff weight of 22 lbs., it is classified as a small UAS. According to the National Safe Skies Alliance (2019), the proposed concept of operations describes simultaneous operations of multiple UASs launching from base stations installed around the airport perimeter. Considering these complex specifications, such operations are not possible under current regulations, and obtaining waivers is the only feasible method for permitting these flights. The following paragraphs will discuss the sections of Part 107 applicable to a Security Support UAS operator who apply for a waiver from the FAA (FAA, 2021a).

&107.31 Visual line of Sight Aircraft Operations (VLOS). According to this section, a remote pilot must have continuous positive visual contact with the vehicle throughout its entire flight. When the area to be covered is too broad for one observer to maintain visual line of sight, an additional person is required to serve as a visual observer and maintain visual line of sight with the vehicle. Airport operators may submit a waiver request to deviate from this rule. It is challenging to apply for VLOS waivers because of the need to submit technical information about the equipment used during the operation. An operator has to be able to ensure the reliability of the UAS and its system components. For example, as it pertains to communications requirements, the description

of the UAS command and control link as well as equipment licenses must be included in the application. The FAA is primarily interested in how the operator intends to manage the risks associated with beyond VLOS operations when evaluating these waivers. Waiver approval may be granted provided that the applicant addresses the following questions in a detailed manner:

- Explain how the remote pilot can maintain constant awareness of the UAS's location and altitude; and what actions will the pilot take if the existing method of retaining awareness fails.
- Discuss the pilot's methods for determining potential collision hazards, and how the separation with other conflicting traffic will be ensured.
- In the event of a UAS equipment outage, explain how the pilot is alerted to the problem and how they would respond.
- Describe procedures during adverse weather conditions.

& 107.35 Operation of Multiple Small Unmanned Aircraft. This section states that no more than one UAS may be controlled by a single person at a time. Security Support UAS users may need to waive this section to allow numerous UAS to conduct perimeter inspections simultaneously around the airport. The waiver application must include the following considerations:

- The applicant must explain how the operations will remain safe if one or more UAS malfunction at the same time while airborne; and describe a pilot's response to malfunctioning UASs.

- The applicant must describe how they will ensure an individual UAS remains confined within the pre-programmed route.

& 107.39 Operation Over Human Beings. Rulemaking has recently been issued to allow operations over civilians without a waiver, as was previously mentioned above. Operators who cannot meet the criteria of the new rules may seek a waiver under the rule. Airport Security Support UASs may occasionally fly above airport personnel while conducting routine tasks. Therefore, the operator must ensure either their drone complies with section 107.39 or they have secured a waiver to allow flights over people on the ground. The waiver application should include the following considerations:

- The operator must disclose the results of UAS testing including established harm levels it may cause if it impacts a human.
- The operator must specify the parts of the UAS that may cause harm to a person in the event of a collision and any safety features they have implemented to lessen the impact.

& 107.41 Operations in Certain Airspace. According to this section of Part 107, no person may operate a small UAS in Class B, Class C, or Class D airspace unless a prior authorization was obtained from the servicing ATC unit. The primary worry for UAS operations over airports is how to ensure they do not interfere with the flights of manned aircraft. When applying for a 107.41 section waiver, an operator must be able to explain the following points:

- How local ATC or pilots of manned aircraft will be advised of the whereabouts of the UAS when it is dispatched to conduct regular perimeter inspection or respond to an alarm.
- How ATC - Remote Pilot communication will be facilitated; and what procedures they must follow in non-routine scenarios such as loss of command-and-control link with the airborne UAS.

According to an analysis of prior waiver requests approved by the FAA (FAA, 2022), the waiver requests containing the following information are the most likely to be approved: as part of their waiver application, applicants were able to offer detailed information on each system element's performance capabilities; in addition to describing known hazards, applicants offered specific instructions on reducing the risk of those hazards; the applicant supplied specific operational restrictions in the event of inclement weather; when a system malfunctions, the applicant explains what steps will be taken as a backup; finally, the applicant provides a description of the qualifications and knowledge of the staff involved with the UAS operation.

The FAA's "operations first" strategy for incorporating new UAS operations into the National Airspace System is also worth noting. The Administration’s officials have been particularly supportive of testing new and complicated UAS operations, noting that any further use of UAS delivers significant insights on technological capabilities and best practices and other vital lessons that drive future rulemaking and other policy efforts. In this sense, the FAA has gained a lot of expertise through examining applicants’ waiver requests because of the insight gained regarding the demands of the industry and the wide

variety of applications capable of being performed by this technology. Therefore, the airports interested in using this innovative tool should not back away from the challenging process of applying for waivers because the more applications received in unique operating environments, the more likely it is that such complex UAS operations will eventually become normalized in the regulatory framework.

In summary, waivers to existing rules and effective safety risk mitigation strategies allow for complex UAS operations to occur. Although the FAA has progressed in leveraging and adapting existing regulations, relying only on waivers to enable complex UAS flights cannot be a long-term solution. Issuing waivers on a case-by-case basis is time-consuming and laborious for both the Administration and the applicants. To promote scalable complex unmanned aircraft operations in the NAS, long-term solutions such as new regulations will be needed. In crafting new legislation, there is a a "Goldilocks spot" for the Administration to find, as it was nicely put by Graboyes and his colleagues (2020), which means that they need a reasonable amount of regulation, but not so much that it suffocates the technology before it can even fly.

Future Work

Integrating UAS into airfield operations would introduce new risks and require changes to the current airport environment. Investigating the hazards UAS may pose to airport infrastructure and personnel is a critical step in building effective risk mitigation methods and properly managing safety. In future work, investigating the overall impacts of UAS introduction into airport operations and infrastructure might prove important.

CONCLUSION

This paper has explored a range of Unmanned Aircraft Systems applications in the airport environment. These systems have the potential to become an integral part of airport security programs and support security forces by enhancing their surveillance and response capabilities. Having such a mobile security camera in the airport arsenal would simplify the airport security operations in many ways. In particular, UAS can allow faster response to security alarms, threat identification and tracking as necessary. More importantly, they can be deployed in dangerous situations to provide much-needed situational awareness to security personnel without compromising their safety. The capabilities of UAS will be enhanced with the proliferation of artificial intelligence technologies such as object and facial recognition software. Eventually, drones can be used as an additional capability to provide data to airport's AI technologies which can be used for predictive analytics to warn the security team of suspicious activity in the vicinity of an airport.

The FAA's decision to implement Part 107 was a monumental one, allowing the growth and expansion of small UAS operations in various industries. The Administration was able to modify and apply the current legal framework to allow a wide range of UAS operations in the US airspace by utilising its Part 107 waiver process. Waivers for complex UAS operations are challenging to get and necessitate a thorough examination of an airport's safety program and risk mitigation strategies. The existing regulations allow for the use of Security Support UAS; however, petitioning for a waiver can be lengthy and complicated. A more tailored regulatory strategy for complex UAS

operations will be required to accommodate the needs of increasing numbers of UAS users in the vicinity of airports, including those intended for airport security purposes.

REFERENCES

14 C.F.R & 107. (2021). Small Unmanned Aircraft Systems. *Federal Register*. Retrieved from https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107

Bartholomew, E. (2010). *Airport and Aviation Security: U.S. Policy and Strategy in the Age of Global Terrorism*. Auerbach Publications.

Beake, N. (2015, April 23). London airport police to use surveillance drones. *BBC News*. https://doi.org/https://www.bbc.com/news/uk-england-london-32431630

Benny, D. (2013). *General Aviation Security*. *Airport, Aircraft, and Airline Security*.

Chao, H., & Chen, Y. Q. (2012). *Remote Sensing and Actuation Using Unmanned Vehicles*. *Remote Sensing and Actuation Using Unmanned Vehicles*.

FAA. (2016). *SUMMARY OF SMALL UNMANNED AIRCRAFT RULE (PART 107)*. Retrieved from http://www.faa.gov/uas/media/Part_107_Summary.pdf

FAA. (2019). *Unmanned Aircraft Systems Safety Risk Management Policy*. Retrieved from https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8040.6.pdf

FAA. (2021a). *Part 107 Waiver Section Specifc Evaluation Information*. Retrieved from https://www.faa.gov/uas/commercial_operators/part_107_waivers/media/Part-107-Waiver-Section-Specific-Evaluation-Information.pdf

FAA. (2021b). *Pilot's Handbook of Aeronautical Knowledge. Chapter 15: Airspace*. Retrieved from https://www.faa.gov/sites/faa.gov/files/regulations_policies/handbooks_manuals/aviation/phak/17_phak_ch15.pdf

FAA. (2022). *Part 107 Waivers Issued*. Retrieved from https://www.faa.gov/uas/commercial_operators/part_107_waivers/waivers_issued/

GAO. (2016). Aviation security: airport perimeter and access control security would benefit from risk assessment and strategy updates. Retrieved from https://www.gao.gov/products/gao-16-632

Graboyes, R. F., Bryan, D., & Coglianese, J. M. (2020). Overcoming Technological and Policy Challenges to Medical Uses of Unmanned Aerial Vehicles. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3561743

Griffiths, D., & Boehm, J. (2018). Rapid object detection systems, utilising deep learning and unmanned aerial systems (UAS) for civil engineering applications. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*

- *ISPRS Archives*, *42*(2), 391–398. https://doi.org/10.5194/isprs-archives-XLII-2-391-2018

Hubbart, S., Pak, A., Gu, Y., & Jin, Y. (2017). UAS to Support Airport Safety and Operations: Opportunities and Challenges. *Journal of Unmanned Vehicle Systems*. Retrieved from https://mc06.manuscriptcentral.com/juvs-pubs

Korecki, Z., Janosek, M., & Pechacek, T. (2021). Use of Unmanned Aerial Systems in Airport Operations. *2021 8th International Conference on Military Technologies, ICMT 2021 - Proceedings*. https://doi.org/10.1109/ICMT52455.2021.9502756

Mackie, T., & Lawrence, A. (2019). Integrating unmanned aircraft systems into airport operations: From buy-in to public safety. *Journal of Airport Management*, *13*(4), 380–390.

Mendoza, M., & Pritchard, J. (2015, April 9). AP Investigation Details Perimeter Breaches at US Airports. *NBC New York*. https://doi.org/https://www.nbcnewyork.com/news/local/ap-investigation-details-perimeter-breaches-at-us-airports/2018468/

National Institute of Justice. (2016). *Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program*. *National Institute of Justice*. Retrieved from https://www.dropbox.com/sh/mgsbtd9qh4qn6r8/AAC0MT_TUFq8ud3Jl1g6w8mka?dl=0&preview=NIJ+Recommendations+for+Implementing+a+UAS+Program.pdf

National Safe Skies Alliance. (2019). *Guidance for Integrating UAS into Airport Security ii*. Retrieved from www.sskies.org/paras.

Price, J., & Forrest, J. (2016). *Practical Aviation Security: Predicting and Preventing Future Threats*.

Sichko, P. (2019). Integrating UAS into Dallas airport .pdf. *Journal of Airport Management*, *13*, 206–214.

Sweet, K. (2008). *Aviation and Airport Security*. *Aviation and Airport Security*. CRC Press.

The Associated Press. (2015). *Breaches of perimeter fencing at airports in the United States* (Vol. II). Retrieved from http://data.ap.org/projects/2016/airport-security-breaches/

TSA Hearing. (2011). *TSA oversight Part 2: Airport Perimeter Security*. Retrieved from https://www.govinfo.gov/content/pkg/CHRG-112hhrg71820/html/CHRG-

112hhrg71820.htm