MITIGATING DRONE ATTACKS FOR LARGE, HIGH-DENSITY EVENTS

by

Travis L. Cline

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

College of Technology

West Lafayette, Indiana

December 2020

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. J. Eric Dietz, Co-chair

Computer and Information Technology

Dr. Umit Karabiyik, Co-chair

Computer and Information Technology

Dr. James Lerums

Computer and Information Technology

Dr. Damon Lercel

Aviation Technology

Approved by:

Dr. Kathryne Newton

This dissertation is dedicated to my children Dallas and Luke. I miss you every day we are apart. Always know your father loves you – no matter how far apart we are in this world.

ACKNOWLEDGMENTS

I would not have been able to make this much progress academically without a wealth of support from my dear friends and family. I would like to thank my parents, Ed Cline and Cindy Swenson, for raising me to have an academic work ethic, and for stressing the importance of academic excellence at an early age. I would like to thank my brother, Vincent Cline, for always being an example and setting a high standard for me to compete with.

To my friends, Krassimir Tzvetanov and Austin Reigsecker, thank you for your patience as I desperately tried to learn programming basics with zero experience. You provided a foundation and expertise to develop and execute this research. Krassimir, thank you for all the troubleshooting and coding expertise to build an operational model. The method for this research would not have been completed without your help. Gozdem Kilaz, thank you for planting the seeds in my head for attempting a Ph.D. It is not something I would have thought to pursue on my own. I appreciate all of your help getting me accepted into Purdue University. Jae Lee, thank you for helping me with my first simulation research project. Your expertise in this field set the standard for work quality and helped me get my first publication. Kaleb Gould and William Weldon, thank you for opening up your lab for this research. I appreciate the opportunity to build a drone from wires and parts as well as all of the help for flight testing.

To Kristle Cline, I appreciate the support you gave me during the first year of this endeavor and making sure the children were well taken care of. To Jessica Caballero, thank you for your continued support throughout the last six months. I would not have been able to remain as productive without your assistance and care.

To my graduate committee, thank you for your continued support over the last three years. I appreciate the directive guidance when I needed it and the flexibility to 'chose my own adventure.' Your thoughtful insight proved invaluable to my academic career.

To Dr. Eric Dietz and Dave Hankins, thank you for founding and managing the Purdue Military Research Institute. I would not have had the opportunity to continue my education in this manner had this program not been created and superbly managed.

TABLE OF CONTENTS

LIST OF TABLES 8
LIST OF FIGURES 9
LIST OF ABBREVIATIONS 11
LIST OF DEFINITIONS 12
ABSTRACT 14
CHAPTER 1. INTRODUCTION 15
1.1 Introduction to the Problem 15
1.2 Statement of the Problem 17
1.3 Purpose of Research 18
1.4 Research Questions 18
1.5 Hypothesis 18
1.6 Assumptions 19
1.7 Limitations 19
1.8 Delimitations 19
CHAPTER 2. LITERATURE REVIEW 21
2.1 Exploring the sUAS Threat 21
2.1.1 Intent-based categories of sUAS incursions 21
2.1.2 Types of threat sUAS operations 23
2.1.3 FAA sUAS guidelines affecting manufacture 25
2.1.4 Popular sUAS performance characteristics 26
2.2 Relevant C-UAS Systems and Elements 27
2.2.1 Detection, Identification, Tracking, Cueing, and Interdiction 28
2.2.2 DroneNet Concept and Characteristics 30
2.2.3 sUAS detection sensors 31
2.2.4 Interdiction Agents 32
2.3 The State of C-UAS within the U.S. 33
2.3.1 C-UAS Technical Standards 33
2.3.2 C-UAS Legal Implications 34
2.3.3 Legal C-UAS Implementation 35

2.4 An Overview of Agent-based Simulation Modeling 38
2.4.1 AnyLogic® agent-based modeling 38
2.4.2 Exploring Validity in Simulation Modeling 39
2.4.3 Agent-based Modeling for Emergency Management 40
2.4.4 Agent-based Modeling for C-UAS 41
CHAPTER 3. METHODOLOGY 43
3.1 Model characteristics 45
3.1.1 Threat UAS characteristics 45
3.1.2 Facility characteristics 50
3.2 Reliability 60
3.3 Validity 60
CHAPTER 4. RESULTS & ANALYSIS 62
4.1 Experiment Group Data Summary 62
4.2 Analysis of Casualties by Time Categories 65
4.3 Effects of Time on Specific Interventions 70
4.4 Inferential Statistics for Best Practices 74
CHAPTER 5. DISCUSSION 75
5.1 Research Questions Addressed 75
5.2 Hypothesis Revisited 75
5.3 Experiment Insights 76
5.4 Considerations for Mitigation System Development 77
5.5 Implications 80
5.6 Further Investigation 81
CHAPTER 6. CONCLUSION 83
REFERENCES 84
APPENDIX A: THE STATE OF C-UAS IN THE U.S. 90
APPENDIX B: AGENT BASED MODELING FOR LOW-COST COUNTER UAS PROTOCOL IN PRISONS 103
APPENDIX C: SAMPLE DATA FOR EXPERIMENT GROUPS 120
APPENDIX D: PARK MODEL ATTRACTIONS AND EXITS METRICS 124

APPENDIX E: SAS OUTPUT FOR MULTIPLE COMPARISONS TEST : INTERVENTION SAMPLES 125
APPENDIX F: CROWD MANAGEMENT SYSTEM 129

LIST OF TABLES

Table 1 Types of Detection Sensors and Descriptions 27
Table 2 Types of Interdiction Methods Currently Employed 28
Table 3 Federal C-UAS Authorized Activity 37
Table 4 Operational Validity Techniques for Simulation Models 40
Table 5 Summary of Casualty Sample Data from Experiment Results 63
Table 6 Summary of Casualties by Time Category 70
Table 7 Summary of Casualty averages by Time and Intervention 73

LIST OF FIGURES

Figure 1. Intent-based incursion categories 22

Figure 2. Drone mitigation process 29

Figure 3. Experiment matrix 44

Figure 4. A DJI Phantom 4 used by insurgents in Iraq with a makeshift 40 mm grenade launcher attachment (Llenas, 2017). 46

Figure 5. Phantom 4 flight test area macro (Google Maps, 2020) 47

Figure 6. weight-bearing platform used in testing 48

Figure 7. Threat agent state chart 49

Figure 8. A = Main Gate, B = Yellow River Adventure, C = Fountain Pavilion, D = Backstage and Concessions, E = Arcade (Tzvetanov et al., In press) 51

Figure 9. A = Main Gate, B = Yellow River Adventure, C = Fountain Pavilion, D = Backstage and Concessions, E = Arcade (Tzvetanov et al., In press) 51

Figure 10. Location of park exits (Tzvetanov et al., In press) 52

Figure 11. Yellow River Adventure serpentine queue modified to the right configuration to test study interventions 53

Figure 12. Patron state chart 54

Figure 13. Pedestrian logic for movement and exiting 54

Figure 14. Main exit evacuation example with casualties indicated in red. Some casualties remain bound by groupings and are pulled outside of the casualty rings. 57

Figure 15. A seven-exit evacuation with *Threat 1* casualties and *Threat 2* about to inflict casualties on a high-density patron group. Exits 2 and 5 are shown on the top left and right respectively. 58

Figure 16. Patrons approximately 30 seconds after a 2-meter separation interval. 59

Figure 17. Sample data from all experiment groups 64

Figure 18. Casualties for 30-second interventions 66

Figure 19. Casualties for 60-second interventions 67

Figure 20. Patrons re-coalescing at a hard corner while evacuating for the main exit in EG6 68

Figure 21. Casualties for 90-second interventions 69

Figure 22. Evacuation interventions compared 71

Figure 23. Separation interventions compared 73

Figure 24. Scale model of the radius required for two timed intervention categories explored in this study. Blue represents a 30” threat warning and 0.5-mile radius, while red represents a 60” threat warning and a 0.83-mile radius requiring a network of 26 and 43 sensors respectively…. 79

LIST OF ABBREVIATIONS

§	Section (used primarily concerning regulations and statues)
C-UAS	Counter Unmanned Aerial System(s)
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
NAS	National Airspace System
NAVAID	Aerospace Navigational Aid
POTUS	President of the United States
UAS	Unmanned Aerial System
UASSC	Unmanned Aircraft Systems Standardization Collaborative
UAV	Unmanned Aerial Vehicle
sUAS	Small Unmanned Aircraft System
SECDEF	Secretary of Defense
VPOTUS	Vice President of the United States

LIST OF DEFINITIONS

Agent-based modeling – a computer modeling based concept in which agents (which may represent people, systems, organizations, and objects) are programmed with set behaviors to interact with a virtual environment and other agents to gather data on complex environments (Grigoryev, 2018).

Counter Unmanned Aerial Systems (C-UAS) – associated systems, procedures, hardware, and software that contribute to the purpose of identifying, detecting, classifying, tracking, and interdicting UAS threats. Also known as counter-UAS or counter-UAV (Michel, 2018, p. 1).

Drone – colloquial reference to small unmanned aerial systems (sUAS). This may be used interchangeably with sUAS and UAS in this manuscript. *Operational definition*

Fixed-facility – refers to a rather large facility spanning several acres that is representative of prisons, military forward operating bases, compounds, and public sporting arenas.

High-tech offender – the term used to distinguish a higher sUAS threat category when compared to *low-tech offenders.* Primary differences include the ability of the high-tech offender to design nefarious purpose-built sUAS capable of autonomous flight and devoid of other sUAS characteristics that may otherwise be exploited for security purposes. *Operational definition*

Low-tech offender – the term used to distinguish the primary sUAS threat category explored within this study. A low-tech offender will use commercially available sUAS and modify them for nefarious purposes. These systems retain most of the characteristics of the commercially available versions of the sUAS which may be exploited for security purposes. *Operational definition*

Patron – a term used to designate a person or agent in a high-density outdoor event. This term is used synonymously with the term 'pedestrian,' in which the simulation modeling libraries were used to generate *patron* behavior. *Operational definition*

Small unmanned aircraft – "an unmanned aircraft weighing less than 55 pounds on takeoff, including everything that is on board or otherwise attached to the aircraft" C.F.R Title 14 §107.3 (2019)

Small unmanned aircraft system (sUAS) – "a small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the national airspace system" C.F.R Title 14 §107.3 (2019)

Security protocol – the sum of methods, procedures, equipment, and manning employed to provide security for a fixed facility. *Operational definition*

Support Vector Machines (SVM) – discussed as a tool in which machine learning is used in combination with software and an sUAS sensor to support the improvement of regression algorithms and overall sensor effectiveness. *Operational definition*

ABSTRACT

Advances in technology have given rise to the widespread use of small unmanned aerial systems (sUAS), more commonly known as 'drones.' The sUAS market is expected to continue to increase at a rapid pace, with the FAA forecasting around 8,000 registrations monthly (FAA, 2019). High profile drone incidents include use in an attack on the Venezuelan president, an undetected landing on the property of the White House, and use in dropping crude explosives on troops in the Middle East (Gramer, 2017; Grossman, 2018; Wallace & Loffi, 2015). The rate of proliferation and high-performance characteristics of these drones has raised serious concerns for safety in high-density outdoor events. Counter-unmanned aerial systems are currently illegal for all but a few Federal entities within the U.S., leaving private and public entities at risk. This exploratory research investigates several legal facility and patron behavioral interventions to reduce possible casualties during a drone attack by using AnyLogic simulation modeling in an amusement park scenario. Data from this experiment suggest that behavioral interventions implemented 30 seconds before a drone attack can reduce casualties by more than 55%, and up to 62% casualty reductions can be realized with a 60-second implementation time. Testing suggests that venue design considerations, such as a reduction in hard corners, covered high-density areas, and smoother area transitions can synergistically reduce casualties when used in conjunction with a warning system. While casualty mitigation did occur throughout the study, active threat interdiction methods would be necessary to design a system that may prevent casualties overall.

CHAPTER 1. INTRODUCTION

1.1 Introduction to the Problem

The unlawful and criminal use of sUAS is becoming more frequently reported with a range of nefarious uses. Current security protocols are proving to be ineffective as this new blending of technology has some unique characteristics that allow a rapid bypass of current systems and procedures. Many private and corporate entities are unable to protect themselves from sUAS threats due to current laws within the United States.

sUAS are defined by the Federal Aviation Administration (FAA) in Title 14 of the Code of Federal Regulations (CFR) Section (§) 107.3 as "a small unmanned aircraft and its associated elements," and weigh between .55 and 55 pounds (FAA, 2019, p. 43). The sUAS market is expected to continue to increase at a rapid pace, with the FAA reporting over 900,000 unmanned aerial systems (UAS) registered as of September 2018, and the expected average increases are forecast around 8,000 monthly (FAA, 2019). While there are many beneficial uses of sUAS including, building and tower surveys, farming analytics, search and rescue applications, photography, and geospatial uses, there are more nefarious uses that will need to be considered by security planners. The rapid proliferation of these devices necessitates new changes to the way facilities are secured in the future.

In 2018, a DJI Matrice 600 was used to attack the Venezuelan president in an outdoor high-density venue, marking the first assassination attempt on a head of state with a commercial unmanned aerial vehicle (UAV) (Grossman, 2018). In 2015, an allegedly drunk government employee had landed a quadcopter undetected on the White House lawn. The intrusion was reported by an on-duty police officer and was completely undetected by the aerial defense radar

of the White House (Wallace & Loffi, 2015). Insurgents in Afghanistan and Syria have been using crudely modified commercial drones to accurately drop crude explosives on troops and other targets in the Middle East (Gramer, 2017). Indeed, current physical security protocols have proven too costly or ineffective to stop unwanted sUAS activity.

Sporting venues and other high-density events have become increasingly concerned about drone intrusions. In England, a commercial drone pilot was legally threatening horse racing revenue by broadcasting a live feed of the race, bypassing the venue's control of advertising and built-in two-second delay (*Cerbair*, 2019). In 2018 the NFL had seen "about a dozen drone intrusions" by the time that Cathy Lanier, the Vice President for Security in the NFL, had testified before Congress on the safety concerns of drones over large events (Dukowitz, 2018). In the U.S., Disney Parks have had a permanent flight restriction in place shortly after the events of September 11, 2001. These no-fly zones were established to protect the high-patron concentrations in the amusement parks and the "most visited tourist destination in the world" (Jones, 2020). The no-fly zones apply to manned and unmanned aviation, including drones, but have been breached on several occasions in the past. One incident involved a 16-year-old Canadian who uploaded videos of the parks during the day, limited access construction areas, and footage of New Year's fireworks displays (*Unauthorized Drone Flies over Disney, Universal*, 2015). While there was no ill intent by this pilot, the incident served to highlight how vulnerable the properties are to drone attacks and how easily drones could be used as a medium for more dangerous criminal activity.

The popularity of sUAS for criminal use has come about from the ease of access, relatively low cost, and low risk for criminals due to the remote nature of drones. The high fidelity of the positioning systems and a range of up to 7 kilometers for some models allow for remote precision and high situational awareness (*DJI Phantom 4 Pro Specs*, 2019). Current detection and

deterrence methods have proven either inadequate to counter the threat or are often illegal. This research will consider explosive drone attacks for high-density outdoor events.

1.2 Statement of the Problem

This research project intends to address the problem that many high-density outdoor events are ill-equipped to address an attack from a small unmanned aerial vehicle. A contributing factor to this problem is the general lack of research on what constitutes an effective C-UAS protocol. Current C-UAS systems consist of expensive and often integrated sensors and interdiction methods that are illegal to implement with few federal government exceptions (covered in section 2.3.3).

C-UAS system manufacturers are not currently held to any standards when making product declarations. There are currently no international standards for the design, implementation, and testing of C-UAS (Michel, 2019). While preparing a comprehensive report of C-UAS manufacturers and available products, Michel (2019) found manufacturers unable or unwilling to provide performance details in real-world trials. This has led to a rapidly growing industry that advertises based on untested marketing claims, which may fall short of actual system performance.

This research project intends to address this security problem by using AnyLogic agent-based modeling software to replicate a few of the threat, facility, and pedestrian characteristics and behaviors in hopes to develop a legal set of interventions and associated pedestrian emergency actions that may mitigate the number of casualties in a drone attack event. This research aims to develop a feasible starting point for a C-UAS protocol for fixed facilities in a risk-free environment using simulation modeling.

1.3 Purpose of Research

The purpose of this research is to identify if there are emergency actions that can be taken by patrons of high-density outdoor events that may minimize the number of casualties in a drone attack involving an explosive payload. If successful mitigation is possible, C-UAS sensor requirements may be established that allow the proper identification of a threat UAS and warn pedestrians in an appropriate time to act.

1.4 Research Questions

The proposed research is intended to provide insights into the following questions:

1. Is there a feasible behavior that patrons can adopt that will minimize total casualties in the event of a weaponized drone attack, given appropriate warning of a threat?
2. What is the appropriate warning time to alert a crowd of an impending drone attack to allow for a mitigating behavioral action to be taken?

1.5 Hypothesis

This research will use simulation modeling to test the effects of different warning times and associated pedestrian behaviors on casualties in the event of an explosive drone attack within an amusement park. The control group will consist of a pedestrian group that will have no warning of an impending attack and will continue normal park behavior.

The hypothesis is that the simulations where pedestrians try to exit the park through the main exit upon warning of a threat UAS will have more casualties than the control group. This situation will present a high density, slow-moving crowd that is a lucrative target for an explosive attack. Additionally, the hypothesis also maintains that the simulations where pedestrians strive to keep a separation interval upon warning of a threat UAS will have lower casualties than the

control group. The more dispersed the pedestrians are, the less likely they are to becoming a casualty. The method used to test this hypothesis will be explained in detail in Section 3.

1.6 Assumptions

The following assumptions are made in the pursuit of this study:

1. Simulation modeling may serve as a valid tool to abstract the complexities of the real world and garner meaningful data.
2. AnyLogic pedestrian libraries and implementation mechanics can be used to simulate patron behavior effectively.
3. Different types of high-density events share enough characteristics to generalize conclusions regarding facility interventions and pedestrian behaviors' effects on an attack.

1.7 Limitations

The following limitations are used in the pursuit of this study:

1. Simulation modeling does not represent the real world but may offer an abstracted reality to garner insights.
2. The researcher is unable to adjust the social force model application programming interface (API) from AnyLogic's pedestrian library.

1.8 Delimitations

The following delimitations are used in pursuit of this study:

1. *Category II and III* trespassers will constitute the primary focus of the sUAS threat (see Section 2.1.1).
2. Threats modeled will replicate quad-copter type sUAS.

3. Only two common threat drone aircraft payloads will be modeled.
4. This study will only model one geographic map for testing interventions.
5. Only three time categories will be tested.
6. Only four intervention behaviors will be tested.

CHAPTER 2. LITERATURE REVIEW

This chapter serves to review literature related to the problem and purpose statements. It is broken into several sections with relevant topics exploring: the sUAS security threat; the state of C-UAS policy and law within the U.S.; relevant C-UAS sensors, systems, and interdiction methods; and an overview of agent-based simulation modeling. These topics will serve as concepts to be synthesized for further analysis.

2.1 Exploring the sUAS Threat

The C-UAS industry has been rapidly growing due to increasing security concerns with sUAS, more commonly known as 'drones.' Drones can quickly bypass traditional two-dimensional security measures with little risk to the drone operator, who can be up to several miles away. This has resulted in fixed facilities, such as prisons, sporting arenas, airports, compounds, and critical infrastructure being at risk for different types of attacks. Threat sUAS operations and incursions can generally be divided into several categories, which may help security managers design C-UAS systems and protocols to mitigate the types of threat behavior most likely to be encountered. This section is intended to identify and document categories of sUAS threats so that their behaviors may be replicated in testing C-UAS protocols through simulation modeling.

2.1.1 Intent-based categories of sUAS incursions

T. Humphreys (2015) breaks sUAS incursions into three categories based on the skills and intent of the drone operator. The first category involves accidental trespassing. Either the sUAS pilot is unaware they are near a restricted or otherwise sensitive area, or become disoriented to the aircraft's location and fly into a sensitive area unintentionally. The second category is intentional

trespassing by ‘unsophisticated’ operators. These operators usually use off-the-shelf products as is or with minimal modification. The third category of sUAS incursions involves intentional trespassing by sophisticated operators. This would consist of potentially self-made sUAS or heavily modified off-the-shelf products with modified software.

It is important to note that Geofencing may serve as the first line of defense against some incursions within the first two categories. Currently, geofencing is an added feature within manufacturers' flight control software and is only an FAA recommendation to sUAS manufacturers. This feature is largely reliant on up-to-date databases of sensitive buildings and infrastructure being pushed to manufacturers, which then have to be voluntarily updated by drone operators (*FAA Drone Advisory Committee*, 2019). While this may serve as a scalable first line of defense for protecting fixed facilities, and large events, not all drones have geofencing features, and the manufacturer controls geofences instead of the facilities needing protection. In addition to this, users can opt for third-party flight software which may make it easier to bypass geofenced areas. *Figure 1* provides a summary of intent-based incursion categories.

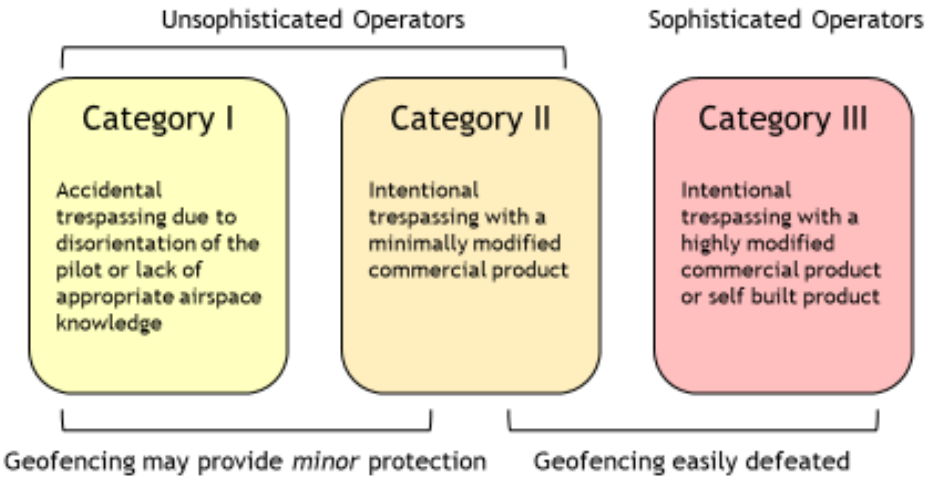

Figure 1. Intent-based incursion categories

2.1.2 Types of threat sUAS operations

When exploring the types of sUAS incidents that generally are reported, four distinct operational categories become prevalent. Threat sUAS operations tend to fall into either general disruption, physical attacks, surveillance, and reconnaissance, or smuggling. Each of these types of operations may have a distinct type of flight profile associated with it, that can be examined and modeled in future works to test C-UAS protocols.

General Disruption

Disruption occurs when the presence of an sUAS disrupts the normal flow or processes of a facility or event. It can be a disruption in the behavior of personnel at an event, or an electronic disruption potentially caused by the RF and other signals output by the aircraft or control inputs. In August 2014, the University of Texas at Austin Police watched helplessly as an sUAS was hovering above a packed football stadium with an estimated 100,000 personnel. Luckily, this was not an attack, and simply a fan in the parking lot wanting to see the game (Humphreys, 2015). This event highlighted the woefully inadequate security countermeasures in place to detect and mitigate an aerial attack. While there was no physical harm done, the incident did divert the attention of attendees at the event as well as the attention of security assets that may have introduced other weaknesses to the security as a whole. In addition to event disruption, the Cybersecurity and Infrastructure Security Agency (CISA) highlights that sUAS operation around, but not targeted at, critical infrastructure could disrupt operations if the facility has interdependencies.

An example of this is an sUAS disrupting operations at a power grid and affecting a nearby critical water facility operations (*UAS - Critical Infrastructure | CISA*, 2020). Another example of a general disruption was the incident that shut down the Gatwick airport in December 2018.

Around 1,000 flights were canceled over three days resulting in over 120,000 passengers being affected by the incident ("Drones Ground Flights at Gatwick," 2018). This was a security measure put in place to reduce the risk of catastrophic accidents caused by a potential mid-air collision between a drone and commercial airplanes.

Physical Attacks

Physical attacks involve using drones to purposely injure or maim personnel, whether through flying directly into targets, using explosives, carrying hazardous cargo, or outfitting drones with firearms or other projectiles. In August of 2018, in one of the more publicized drone attacks, Venezuelan President Maduro was attacked by a DJI Matrice laden with explosives in an outdoor event (Grossman, 2018). While Maduro was not injured, some audience members were, and it was apparent his security team was in a reactive state in responding to the incident. In 2015, a Japanese man was arrested for flying a drone with trace levels of radiation onto the roof of the Japanese Prime Minister's office. There are many examples of commercial drones being used in attacks that include near precision explosives being dropped on unsuspecting targets. An example of this includes a strategic attack on a Ukrainian ammunition depot by Russian-backed rebels resulting in over $1 billion in damage (*Drone Wars*, 2018). Additionally, ISIS terrorists in the middle east have been modifying commercial drone products to drop M67 hand grenades, as well as 40mm grenades that are traditionally fired from grenade launchers (Llenas, 2017).

Surveillance and Reconnaissance

GPS navigation, inertial navigation units, and calibrated camera gimbals make modern commercially available drones excellent options for surveillance and reconnaissance. This technology allows for high definition photos and video, which can be digitally stitched into 3D

models with a high level of accuracy (*UAS - Critical Infrastructure | CISA*, 2020). In this same spirit, insurgents in Afghanistan have been reported to use drones to adjust artillery fire for better accuracy (Gramer, 2017). Drones can also be used to monitor the actions of individuals, security, or law enforcement in real-time. In 2018, a French prisoner was suspected of using drones to surveil prison security and develop an elaborate escape plan involving a helicopter get-away vehicle and a staged diversion. Several drones were spotted over the correctional facility leading up to the incident and were likely used to identify weaknesses in the facility's security protocol (Shayanian, 2018).

Smuggling

Probably the most documented illegal use of sUAS in the US involves smuggling contraband into prison systems. Reports from Maryland, Ohio, Oklahoma, Tennessee, South Carolina, and other states have described the use of these systems to air-drop heroin, cell phones, and blades to prisoners ("United States: drones pose new contraband, smuggling challenge for prisons," 2016). Recently, there have been reports that sUASs are being used to drop opiates and other contraband into an Indiana State Prison (J. E. Dietz, personal communication, September 20, 2018). In California, 45 "unauthorized drone intrusions" were recorded between July 2017 and May 2018, some of which were found to have dropped in cell phones, drugs, and saw blades putting correctional officers and other inmates at risk (Harvey, 2018; Kotowski, 2018).

2.1.3 FAA sUAS guidelines affecting manufacture

Title 14 C.F.R §107.31 requires that an unmanned aircraft must remain in the visual line of sight of the remote pilot at all times and that the pilot is in a position to re-direct the aircraft if necessary (E-CFR, 2019). Obstacle avoidance and visual tracking become very challenging for

remote pilots in distances over one mile, even in clear weather conditions (*Drone Pilot Ground School*, 2020). Additionally, the remote pilot needs to maintain a visual line of sight to ensure a good connection between the controller and the unmanned aircraft. The typical control architecture for commercial drones involves directional controls being broadcast on the 2.4 GHz wavelength, and image transmission is broadcast back from the aircraft to the control station over the 5.8 GHz wavelength. This is common for DJI and Yuneec products as well as other manufacturers and may be used to interdict trespassing sUAS by monitoring, jamming, or hijacking communications within these wavelengths. The FAA 'line of sight' requirement excludes the possibility of legal autonomous flight and requires that a remote controller can control the aircraft, as opposed to the capability of "high-tech" or Category III trespassers to use pre-programmed GPS waypoints and flight routes for autonomous flight.

Title 14 C.F.R. §107.29 restricts sUAS operation during night hours. Commercial drones can fly at night, but at a reduced performance capacity, due to the majority of products relying heavily on visual sensors for flight orientation, navigation, and obstacle avoidance. Therefore, night flight is difficult for Category I and II trespassing without upgrading to expensive night visual optics and possible aircraft modifications, which would push the offender into Category III.

2.1.4 Popular sUAS performance characteristics

DJI currently holds the majority of the market share within the U.S. at 76.8% (Schroth, 2019). DJI's Phantom series drones are often seen in cases where trespassing has occurred and has been used by ISIS to deliver explosives due to the powerful motors and ease of modifying the landing gear to accept a small payload. The DJI Phantom 4 Pro can fly up to a maximum of 45 mph in calm air and without a payload (*DJI Phantom 4 Pro Specs*, 2019). This particular sUAS has a retail price of $1,700 and requires a smartphone or tablet to operate. Additionally, DJI is

known for its robust and powerful flight control software that is intuitive and ideal for low experience sUAS pilots. This aircraft will be used to model the threat sUAS behavior.

2.2 Relevant C-UAS Systems and Elements

A comprehensive December 2019 report noted 277 different companies offering 537 C-UAS products that ranged from detection only, to interdiction, to a mix of both (Michel, 2019). Methods of detecting and tracking UAS include radar, radio-frequency tracking, electro-optical, infrared, acoustic, and mixed sensors. Each detection method has its weaknesses, and no single method has proven to always be effective; therefore, most integrated systems use a mix of sensors to detect UAS. Table 1 briefly describes the general categories of sUAS detection sensors.

Table 1 Types of Detection Sensors and Descriptions

Detection Type	Description
Radar	Detects radar signature by emitting radio wave pulses and analyzing return energy to determine the range, angle, and velocity
Radio-Frequency	Detect UAS presence by scanning commonly used UAS bands such as 2.4 GHz and 5.8 GHz, may be able to determine location with complex antennas and multiple sensor locations
Electro-Optical	Detect UAS based on the visual signature of the UAS aircraft
Infrared	Detect UAS based on the infrared signature emitted by the UAS aircraft
Acoustic	Detect changes in sound by using microphones and software filters to match data from a database of UAS audio signatures

Note. Descriptions are adapted from Michel (2018, p. 4).

Michael's (2019) comprehensive report noted that of the 537 products currently, 214 systems are designed for interdiction alone, and at least 138 systems claim to provide both detection and interdiction capabilities (Michel, 2019). C-UAS interdiction involves limiting unwanted sUAS activity through the use of projectiles, nets, signal spoofing, global positioning

system (GPS) jamming, radio-frequency jamming, and other methods. Table 2 represents a summary of interdiction methods used to limit unwanted sUAS activity over a protected area.

Table 2 Types of Interdiction Methods Currently Employed

Interdiction Type	Description
Radio Frequency Jamming	Interrupts the RF link between UAV and operator by generating large amounts of RF output. Once the RF link is disturbed, the UAV may land or return to the operator
GNSS Jamming	Interrupts the satellite link used for navigating. Once the satellite link is lost, UAV will hover or land.
Spoof	Taking control of the UAV by hijacking the communications link
Kinetic	Destroys portions of the airframe with directed energy, causing a crash
Net	Entangles the UAV or its rotors
Projectile	Employs ammunition to destroy UAV
Combination	Several C-UAS employ a combination of interdiction elements—most commonly, tandem RF and GNSS jamming systems

Note. Descriptions are adapted from Michel (2018, p. 4)

2.2.1 Detection, Identification, Tracking, Cueing, and Interdiction

There is an inherently logical progression of activities involved in an integrated C-UAS that is not significantly different than an engagement process for military weapons systems. First, a potential threat needs to be detected for its existence within or near a protected area. This would be considered a coarse detection and may not discriminate between a bird or other non-threat entity. Coarse detection is often done by passive electro-optical or acoustic sensors and may recruit a higher fidelity sensor to assist with the next step.

After the potential threat is detected, the system will need to identify if the object is indeed a threat or something more harmless like a bird or large insect. Coarse directional data will cue in higher fidelity sensors that usually are linked with higher processing power and a smaller field of

view. Once this directional handoff is complete, the system tries to identify if the object is a potential threat. This is usually automated with software that uses machine learning algorithms that have sUAS been trained with audio, visual, or infrared profiles based on the sensors connected to the system. However, this is easier said than done, as it can be challenging to have a high probability of true positives without false negatives and false positives in cluttered environments (Michel, 2019).

After a threat is identified and confirmed, the system will need to track the sUAS threat to maintain situational awareness and manage the incident. When interdiction methods are available as part of the C-UAS, the three-dimensional position and velocity will need to be sent to the interdiction agent through a process known as cueing. This allows interdiction efforts to be focused on the threat and minimize unnecessary risk for the interdiction process. Figure 2 illustrates the broad concepts an integrated C-UAS must perform.

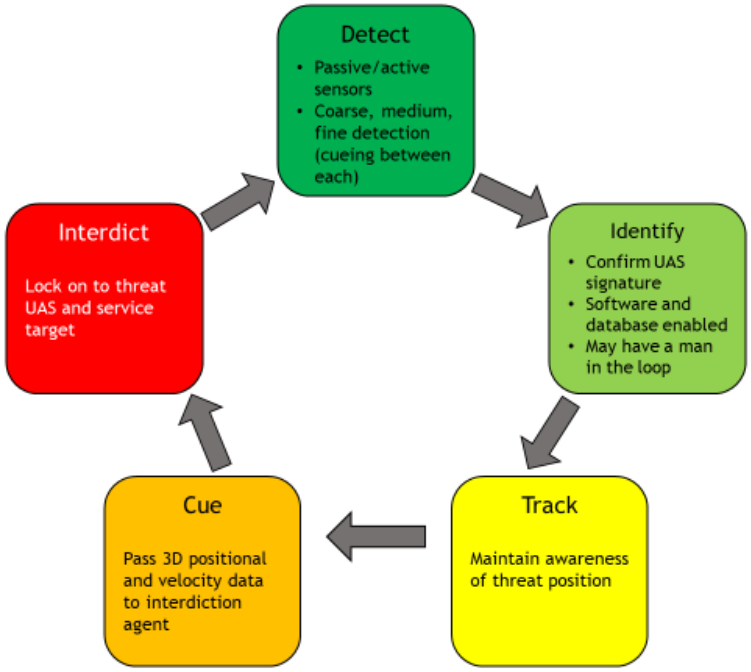

Figure 2. Drone mitigation process

An example of this concept can be found in the open-source DroneNet research project designed to help identify and mitigate sUAS threats to aviation near airports. This system uses an array of sky-view cameras in conjunction with acoustic sensors as a coarse detect "tripwire" to cue higher fidelity optical sensors to the potential drone location (Siewert et al., 2018).

An additional example of this framework can be found in an experiment by the French-German Research Institute of Saint-Louis (ISL) where the research team leveraged their expertise in gun-shot direction-finding using tetrahedral microphone arrays. The research team developed a system that could accurately determine the azimuth and elevation of different drone sound profiles from their microphone array to accurately cue a high-fidelity visual sensor for drone identification and active tracking (Christnacher et al., 2016).

2.2.2 DroneNet Concept and Characteristics

A previously mentioned and promising practical solution to the sUAS security problem involves a team of researchers at Embry Riddle is in the process of developing and validating an open-source architecture using comparatively cheap arrays of sensors to identify and track small unmanned aerial vehicles (sUAS) (Siewert et al., 2018). This research looks at tracking sUAS with a long-term goal of UAS traffic management (UTM) that can be used to provide timely updates and mitigation procedures to assist with manned aviation and deconfliction with non-radioed and non-compliant sUAS.

The goal of the team's research is to establish an open-source framework made up of a ground network of sUAS sensors, supplemented with aerial sensors affixed to an sUAS (Siewert et al., 2018). The primary sensors the team is relying on are passive and designed to compete with more expensive active sensors such as light detection and ranging (LiDAR) and radio detection and ranging (RADAR) when appropriate machine learning algorithms are applied. Passive ground

sensors for this system include the combination of electro-optical and infrared sensors (EO/IR), acoustic sensors, and 180º sky-view cameras.

The hypothesis the research team ultimately wants to test is whether a low-cost network of ground and flight sensors are more effective than ground RADAR for managing the traffic of sUAS. To test their methods, the researchers set a hypothetical architecture of software and hardware linkages and set to test a prototype sensor array and compare results to the on-board inertial data of the sUAS to be tracked. The truth analysis combined three separate high-fidelity 'truth' models and combined them into a MATLAB simulation. The truth models consisted of visual positioning of the sUAS, the inertial logs from the sUAS, and Automatic Dependent Surveillance-Broadcast (ADS-B) a system that transmits global positioning system locations and timestamps. The geometric flight models were compiled and correlated to the ground-based sensor recordings and classified by a human to train the machine learning algorithm.

This method's feasibility was demonstrated, and a path forward was discussed for acoustic testing and further EO/IR refinement. This research may prove beneficial as many C-UAS elements' technical specifications are not available to the public, and this project aims to make methods, hardware, and software open source to expedite the practical results of the system.

2.2.3 sUAS detection sensors

Operational data is severely limited to C-UAS sensor performance due to a lack of regulations which will be discussed in section 2.3.1. For this research, sensors and systems that provided operational data for commercial drone products that had ranges and probabilities of detection will be included.

French-German Research Institute of Saint-Louis (ISL) tested a real-world acoustic system for UAS leveraging previous work's success involving acoustic sensors being used to cue and focus

optical sensors on locating and recording the point of origin for gunshots (Christnacher et al., 2016). Upon testing a specific system using an array of meteorological microphones, the research team was able to accurately estimate the azimuth and elevation of an approaching drone approximately 20 seconds before overflight of the sensor with a custom-built UAS, and as far as 300 meters for a louder DJI Phantom 2 at altitudes approximately 120 to 150 feet (Christnacher et al., 2016). The ISL researchers suggest a network of sensors to monitor an area more effectively for overflight following appropriate site surveys to determine sensor placement. This will allow multiple sensor bearings to triangulate a potential threat UAS in three dimensions. The ISL research team utilized the three-dimensional data to cue a sophisticated electro-optical system onto the UAS for real-time identification and automatic algorithm-based tracking (Christnacher et al., 2016).

In addition to ISLs successes with acoustic sensors, the Army Research Lab conducted a 2014 study in which a tetrahedral array of microphones was used at varying distances to determine the probabilities of UAS detection and false alarm (Benyamin & Goldman, 2014). Some notable figures extrapolated from graphs provided in the study included a 99% probability of UAS detection with a 3% probability of false alarm at distances between 450-600m using a bandpass filter of 800-1700 Hz. The research team demonstrated some success with elevation tracking over four test flights and found higher altitudes and lower ambient noises aided in the accuracy of their beamforming tracking method (Benyamin & Goldman, 2014).

2.2.4 Interdiction Agents

While there are many types of interdiction methods, as introduced in Table 2, hunter type drones with affixed drone-catching nets seem to violate the fewest laws (covered in section 2.3.2) and provide the most flexibility for interdicting drones over a large fixed facility. One such system was developed in 2016 by a Michigan Tech research team that demonstrated the effectiveness of

a proof-of-concept anti-UAS net-launcher mounted on what appears to be a DJI Matrice 600 (Goodrich, 2016). This team later filed for and received a patent for their system, which can aim the net projectile and carry the intruding UAS to a safe location for handling, mitigating human risk due to explosives or other potentially hazardous cargo (Aagaah et al., 2018).

In 2017, another research team from Purdue University demonstrated the effectiveness of a completely autonomous C-UAS detection and interdiction system involving a radar tracking system and autonomous hunter drone equipped with an ultra-light carbon-framed conical net (Goppert et al., 2017). The hanging net design was selected to allow multiple attempts at interdiction of a threat if the autonomous positional data was too imprecise for a launched-net entanglement. The threat UAS was flown at a set altitude over a set path toward a protected object. The radar in use was described as a "high-precision" and "military" radar (Goppert et al., 2017, pp. 236, 238). This high-fidelity radar would be excellent for proving autonomous interdiction is possible but is mostly outside of the budget and workforce available to many fixed facilities.

2.3 The State of C-UAS within the U.S.

Previous works took a more in-depth look at the state of C-UAS within the United States from regulatory, legal, and operational employment perspectives. The full submitted version of this document can be found in Appendix A. This section will serve as a summary of the previously mentioned work.

2.3.1 C-UAS Technical Standards

The deployment of counter unmanned aerial systems within the United States has been very limited despite the growing concern of UAS threats. While there are companies that are manufacturing and testing these systems, there are no agreed-upon standards to which they

conform. This has led to an environment in which marketing claims make operational and performance data difficult to find. Major standards organizations such as the American National Standards Institute (ANSI) and ASTM International (formerly the American Society for Testing and Materials) regularly establish and implement standards adopted by industries and governments as best practices and ultimately to protect the end consumer of ineffective or unsafe products and services. Despite the highly technical nature of C-UAS, no standards currently exist.

ANSI established the Unmanned Aircraft Systems Standardization Collaborative (UASSC) in September 2017 in conjunction with ASTM, the Department of Homeland Security (DHS), the Department of Defense (DoD), the FAA, and others to guide research, policy, and standardization efforts concerning unmanned aerial systems (*ANSI UASSC*, 2020). The UASSC established and updated a standardization roadmap, which identifies, prioritizes, and defines elements of the UAS ecosystem that needs research and standardization. Of note, the standardization roadmap noted that no standards currently exist for UAS mitigation (or C-UAS), and topics regarding this were assigned as a Tier 1 or high priority (McCabe, 2020).

2.3.2 C-UAS Legal Implications

Small unmanned aircraft are required to register with the FAA and adopt the Title 49 U.S.C. § 40102 definition of 'aircraft' as "any contrivance invented, used, or designed to navigate, or fly in the air." This adoption of the term means interference with the flight path or destruction of an sUAS carries the same criminal penalties as if it were done to general aviation (GA) aircraft and can include up to a 20-year prison sentence for destruction or disablement of the aircraft. This effectively precludes the use of many of the interdiction methods to include kinetic, projectile, and signal spoofing and signal jamming options (Cline et al., 2020).

The Federal Communications Commission (FCC) requires licenses to operate radio transmitters and prohibits the sale of any devices that interfere with radio reception. Per FCC regulations, it is also illegal to interfere with radio communications with a licensed station. This would preclude the use of spoofing and jamming interdiction methods (Cline et al., 2020). The FAA also has regulations that would make a potential spoofer (taking control of a nefarious aircraft) legally liable for the remainder of the flight, including the safety and payload of the threat UAS. In addition to this, a 2019 letter to airports from the FAA dissuades the use of C-UAS sensors due to potential unintended consequences on the national airspace system. Specifically, they discuss the unknown impacts to navigational aids or highly sensitive radio beacons used by airplanes to navigate across the country. Navigational aids are heavily relied upon for flight and approaches in inclement weather (Cline et al., 2020).

2.3.3 Legal C-UAS Implementation

Four federal entities are legally allowed to conduct C-UAS activities within a specified scope related to the entities' mission. The National Defense Authorization Act (NDAA) of 2017 allows the DoD and the Department of Energy (DOE) certain C-UAS provisions while Division H of The FAA Reauthorization Act of 2018, also known as the Preventing Emerging Threats Act of 2018 grants C-UAS provisions in a more limited scope to the DHS and the Department of Justice (DOJ) (Cline et al., 2020).

The DoD, DOE, DHS, and DOJ are allowed to perform the following broad actions to mitigate a threat to a "protected facility or asset."

- Detect, identify, monitor, and track UAS
- Warn the UAS operator
- Disrupt control of the UAS

- Seize or exercise control of the UAS
- Use reasonable force to disable, damage, or destroy the UAS

The primary difference between the justification for the C-UAS actions listed above is how each "protected facility or asset" is defined through the law, and within each organization. Table 3 summarizes the grounds on which C-UAS actions may be conducted and the justifications by each department. The United States Coast Guard (USCG) falls under the DHS, but has separate and explicitly listed grounds and justifications for conducting C-UAS activities (Cline et al., 2020).

Table 3 Federal C-UAS Authorized Activity

	Department				
	DoD	DOE	DOJ	DHS	USCG*
Grounds	Facility or asset identified by the Secretary of Defense	Facility or asset identified by the Secretary of Energy	Facility, asset, or persons identified by the Attorney General (DOJ) or Secretary of Homeland Security (DHS) as high-risk and a potential target of unlawful unmanned aircraft activity		Facility under control of the Commandant or a vessel or aircraft operated by, assisted by, or otherwise involved in a mission with the USCG
Location	Located within the United States or one of its territories				Not explicitly bound by location
Justifications	1) Nuclear deterrence mission 2) Missile defense mission 3) National security space mission	1) Storage or use of nuclear material	1) National Security Special Event 2) Special Event Assessment Rating 3) At the request of a Governor 4) Protect active Federal investigation 5) FBI: protection of POTUS and AG 6) Marshals: protection of personnel involved in Federal trial 7) Protection of correctional facilities, courts, and other DOJ buildings	5) U.S. Customs and Border Protection 6) Secret Service protection operations 7) Protection of Federal buildings	1) Assistance or escort mission for DoD 2) Assistance or escort mission for a vessel of national security significance, or a high interest, capacity, or value vessel 3) Protection of the POTUS and VPOTUS 4) National Security Special Event 5) Special Event Assessment Rating 6) Air Defense of US 7) Search and rescue mission

Note. United States Coast Guard (USCG) falls under DHS but has separate grounds and authorized C-UAS justifications This table is presented in the author's previous work (Cline et al., 2020, p. 9)

Policies and regulations in the future will need to allow public agencies and private industry to utilize C-UAS technology to mitigate the increasing threat posed by drones. The UASSC will be managing this process, and critical research and development required by the DOJ and DHS by law may aid in developing the operational and equipment standards needed in C-UAS (Cline et al., 2020).

2.4 An Overview of Agent-based Simulation Modeling

2.4.1 AnyLogic® agent-based modeling

AnyLogic® is a computer simulation program used to identify and solve problems across multiple industries. The software is unique in that it can operate in one or more of the following simultaneously; discrete event modeling, agent-based modeling, and system dynamics (Grigoryev, 2018). In agent-based modeling, the user can add multiple different agents into a two or three-dimensional space and set agent behavior. Agents can simulate the behavior of a wide range of things to include; people, ideas, vehicles, and organizations. Agent-based simulation modeling attempts to replicate the whole of a system by defining the individual objects and their associated behavior within a system to see how the whole of the system works (Grigoryev, 2018). Once the model is built, an object (or agent) behavior can be modified, and results on the system can be recorded. This allows organizations to rapidly gather data and optimize a key output on a given system. AnyLogic has a wide pedestrian library that simulates pedestrian behavior and has been used in different industries to manage the flow of traffic and simulate pedestrian behavior. Agent-based modeling features will be primarily used in pursuit of this study as well as some of the system dynamics and discrete event modeling features.

Agent-based modeling has been gaining traction in a wide variety of different sectors to find efficiency in processes, test new ideas, provide estimates, and test policy implications, and

inform decisions. AnyLogic has many demo walk-through models to showcase the flexibility of their software (*AnyLogic*, 2020). Their website lists use in the following industries:

- Supply chains
- Manufacturing
- Transportation
- Warehouse operations
- Rail logistics
- Mining
- Oil and gas
- Ports and terminals
- Healthcare
- Business processes
- Asset management
- Marketing
- Social processes
- Defense

2.4.2 Exploring Validity in Simulation Modeling

Sargent (2011) acknowledges the need for validation of simulation models to solve real-world problems and support appropriate decision-making following the analysis of model results and data. Models should be purpose-built and validity assessed on the model's ability to provide relevant data to the specific purpose in which the model is built (Sargent, 2011).

Four basic approaches are used in the validation of simulation modeling. The first and potentially weakest approach is for the validity to be subjectively assessed by the modeling team. This method is typically more useful when a large and diverse modeling team is involved with the project. The second basic validation approach is to have the intended user of the model and subsequent analysis to be involved in the modeling process so that outputs more accurately reflect the needs of the user (Sargent, 2011). The third approach is more resource-intensive and involves the addition of an "independent verification and validation" (IV&V) entity that is separate from the modeling team and the intended user, and has extensive knowledge of the problem being addressed in the model (Sargent, 2011). The final approach involves scoring the model from a score-weighted score sheet and determining if the model receives a subjective passing score (Sargent, 2011).

From these basic approaches for validation, Sargent (2011) defines several validation techniques used within these approaches. Techniques relevant to this research or referenced research will be introduced and summarized in Table 4.

Table 4 Operational Validity Techniques for Simulation Models

Type	Description
Face validity	Knowledgeable individuals assess whether the conceptual model seems reasonable.
Animation validity	The operational behavior of the model appears to replicate an abstract version of reality.
Event validity	Events in reality are compared to the occurrences within the model.
Historical data validation	The model is compared to a historical event to gauge the accuracy of the model.
Internal validity	Modeling experiments are monitored for extreme variances.
Extreme conditions test	Tests the outputs for plausibility for extreme and usually unlikely factors within the model system

Note. Descriptions are adapted from Sargent (2011, pp. 186–187)

2.4.3 Agent-based Modeling for Emergency Management

Kirby (2016) used agent-based modeling in a study to determine the effects different policy decisions have in mitigating an active shooter situation in schools and businesses. Studies were developed with the dependent variables of time to shooter engaged (stopped), and the number of casualties inflicted. Various combinations of independent variables were used to simulate policy and determine the best outcome. It was determined that the police would take 300 seconds to arrive on the scene and track down the shooter in a generic building model. In 1000 simulation runs, the average time till shooter engagement was 355 seconds with 5 casualties. It was determined the best single measure to minimize casualties was to have a security officer on-site, followed by a 10% concealed carry population and door locks (Kirby, 2016). This serves as an excellent example of using agent-based modeling to gather data on emergency management policy.

Another example of simulation for emergency management is when Lee (2019) established validity in agent-based modeling as a tool when he recreated the1999 Columbine High School massacre scenario in AnyLogic, to study the effectiveness of the RUN.HIDE.FIGHT.® methodology developed in 2012 when compared against the shelter-in-place response that was used during the tragic incident. After various experiments to establish historical validity, it was determined that the RUN.HIDE.FIGHT.® methodology may have greatly reduced casualties (Lee, 2019).

In a similar type of study, Tzvetanov et al., (In press) utilized agent-based modeling to determine the most efficient methods to evacuate an amusement park and emergency response. The amusement park layout used for this study represents an actual project in the design phases slated to be built overseas. In one series of tests, the research team determined that pedestrian movement throughout an amusement park is minimized if pedestrians were re-directed to seven emergency exits evacuation times would decrease by an average of 24% when compared to leaving through the large main exit toward the parking lot (Tzvetanov et al., In press). Further, the study showed the importance of multi-exit evacuations regarding the impact of police response times to arrive at one of three incident locations, as well as the potential negative impact on hard corners and pedestrian flow in an evacuation (Tzvetanov et al., In press).

2.4.4 Agent-based Modeling for C-UAS

Our previous work suggests that agent-based modeling may serve as an appropriate venue to test C-UAS policy and techniques. Technical data was collected to model agents to closely match a threat UAS, C-UAS sensors, an interdiction "hunter" drone, and a 40-acre facility footprint representing a prison (Cline & Dietz, 2020). The submitted version of this manuscript can be found in Appendix B. The goal of the study was to determine if there is a critical threat speed in which

a hypothetical C-UAS is more easily defeated (Cline & Dietz, 2020). The study was framed with the prison smuggling problem in mind, and any threat overflights were counted as a system failure. A hunter drone was modeled with a fixed speed of 40 mph, and threat speed was varied. The hunter drone would only deploy when a hypothetical sensor was able to detect the threat UAS. The hypothetical system failed 4% of the time with a threat speed of 35 mph and failed 56% of the time at 36 mph. The study suggests that there is a critical threat speed in which a C-UAS system would fail, and it may be beneficial to limit commercial products' top speed to mitigate the risk of potential threat UAS (Cline & Dietz, 2020).

CHAPTER 3. METHODOLOGY

UAS interdiction is currently illegal for many reasons, but the threat from a UAS attack remains a genuine concern for security managers of large, high-density events. This research explores behaviors that event patrons can implement in high-density venues that may reduce the casualty rate of an attack and determine the amount of warning time necessary to execute the behavior. The purpose of this is to provide operational characteristics necessary to appropriately warn a large group of an impending threat in enough time to act. Modeling software has the unique ability to adjust parameters quickly and gather data and should provide insights that will transfer over to the real-world. AnyLogic modeling software is used to replicate a geometric space, threat UAS, explosive payloads, and pedestrian behaviors.

The methodology of this research is conducted in two phases. The first phase is to get real-world operational data and performance characteristics from likely threat UAS platforms by modifying a DJI Phantom 4 Pro to match the loading of historical or documented threat concerns. This data will be recorded and applied to the AnyLogic model in the second phase of the research.

Phase two is exploratory and involves a simulated model of the amusement park used in an experiment conducted by Tzvetanov et al., (In press), with a multitude of modifications for this study. Independent variables manipulated include the pedestrian behavior and the warning time in which the pedestrians are alerted to a threat before they begin a behavior.

Independent Variables

Facility interventions	Pedestrian behavior: No change	Main exit	7 exits	2m interval	5m interval
No threat warning	EG1	n/a	n/a	n/a	n/a
30-second warning	n/a	EG2	EG3	EG4	EG5
60-second warning	n/a	EG6	EG7	EG8	EG9
90-second warning	n/a	EG10	EG11	EG12	EG13

Dependent variable: Pedestrian Casualties

Figure 3. Experiment matrix

Experiments are broken up into different experiment groups (EG) to test the interventions depicted in *Figure 3.* The control group is EG1 where the pedestrians are not alerted to a threat, and they, therefore, do not change their behavior. Testing continues with different variations of behavior and warning times to gain insights, with a dependent variable output of total pedestrian casualties, expressed in a 5-number summary and graphed in a box-plot with 30 sample iterations for each EG. Facility interventions refer to the amount of time that patrons will be alerted before an identified drone threat arrives into the center of the park boundaries, while the pedestrian behavior outlines what actions the patrons will take during the impending threat warning. In the 'Main exit' and '7 exits' categories, the pedestrians stop their activity and either begin movement toward the main exit or the seven exits hidden around the park similar to the experiment by Tzvetanov et al., (In press), however, the two threat drones attack the highest densities of pedestrians at different time intervals within this process. Similarly, the two separation categories have the patrons stop activity within their attractions and attempt to separate at two and five-meter intervals once an impending threat alert is given. Two threat drones then proceed to attack the highest pedestrian densities within the park model. Two and five-meter intervals were selected to

match recent pandemic guidelines and the primary threat blast radius for both threat profiles tested in this study.

3.1 Model characteristics

3.1.1 Threat UAS characteristics

The DJI Phantom 4 Pro specifications are used to model the threat aircraft characteristics. While stated previously that this UAS is capable of speeds up to 45 mph, the model uses speeds that more accurately represent possible top speeds under less than ideal conditions while carrying small payloads based on testing. The field test notes and speeds are recorded later in this section.

Threat Payloads

Several incidents have been documented in the middle east and abroad of commercial drones being used to drop either traditional hand grenades, 40 mm rifle fired grenades, or explosives on unsuspecting targets (*Drone Wars*, 2018; Llenas, 2017). An example of this can be seen in *Figure 4*, depicting a Phantom 4 outfitted with a makeshift 40 mm grenade launcher. Additionally, the threat of a drone carrying a glass jar with common military hand grenades at a crowded venue remains a viable concern among government agencies (Matson, 2018). Once grenade arming pins are removed, fragmentation grenades could be placed in a mason jar, which would keep the spoon in place until the jar was dropped and broken from the resulting fall giving 4-5 seconds before detonation (Matson, 2018). Weighted flight tests at Purdue demonstrated a Phantom 4 pro was capable of carrying the weight of up to two grenades and retain a stable center of gravity at sustained speeds up to 40 mph.

Figure 4. A DJI Phantom 4 used by insurgents in Iraq with a makeshift 40 mm grenade launcher attachment (Llenas, 2017).

An M406 40 mm high explosive grenade is a common munition of the U.S. armed forces for use in grenade launchers. This grenade weighs in at about 8 ounces and has a casualty radius of 5 meters with a danger radius of 165 meters (*TM 3-22.31*, 2010). Documentation on the fragmentation patterns of the M406 round was unavailable, so a casualty percentage of 25% is assumed for pedestrians that are within a 5-meter radius of a *Threat 1* drone attack

An M67 fragmentation grenade is a common military hand grenade and weighs in at 14 ounces, has a killing radius of 5 meters, and an effective casualty producing radius of 15 meters and sending fragments as far as 230 meters (*TC 3-23.30*, 2013). Documentation on the fragmentation patterns of the M67 grenade was unavailable, so a casualty percentage of 50% is assumed for pedestrians within 5 meters, and a 25% casualty percentage is assumed for pedestrians out to 15 meters of a *Threat 2* drone attack. A drone threat is programmed to replicate the dropping of two M67 grenades over a crowded area. In the simulation *Threat 2* models a multiple M67 grenade hazard.

DJI Phantom 4 Loaded Speed Test

On September 15, 2020, flight tests were conducted to assess the feasibility of the previously mentioned threats by assessing the flight controllability, loading, and top speed of a Phantom 4 Pro (P4P) with different simulated threat payloads. Figure 5 represents an overview of the test flight area, as well as the one-mile test run flight path.

Figure 5. Phantom 4 flight test area macro (Google Maps, 2020)

An unloaded Phantom 4 Pro (P4P) maintained speeds averaging 43 mph at level flight along the mile course. A 3D printed platform was added to secure the weights behind the camera gimbal. Figure 6 shows the platform and weights used in the experiment.

Figure 6. weight-bearing platform used in testing

The P4P was able to maintain a 41-mph top speed with a one-pound payload, representative of a 40 mm grenade threat. A three-pound payload was used to represent a mason jar with two grenades as described by Matson (2018). The aircraft was unable to maintain a stable hover after takeoff and reached the maximum rotor speed at an unstable 1.5-foot hover. This threat concern may be feasible for another sUAS platform, such as an M600, but not for the P4P. Finally, a two-pound payload was used to represent two hand grenades that could be secured to the aircraft with a detachable line, and spoons that could be depressed by brittle 3D printed bands that would break upon landing. The P4P was able to maintain a 40-mph top speed with the two-pound payload with relatively normal flight control characteristics. *Threat 1* in the simulations corresponds to a P4P with a 40 mm HE grenade, and *Threat 2* corresponds to a P4P carrying two M67 hand grenades.

Threat Model Implementation

The threat model state chart implementation is depicted in *Figure 7*.

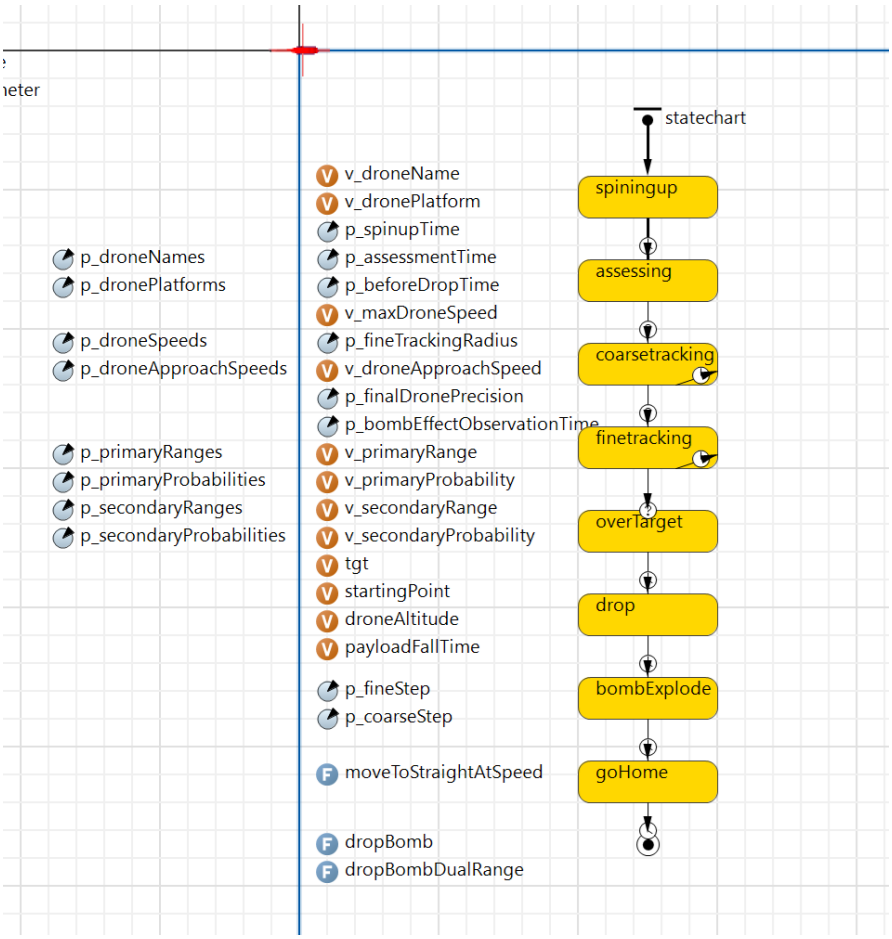

Figure 7. Threat agent state chart

The threat agent is designed using a modular approach to be easily tailorable in future works and encompass both *Threat 1* and *Threat 2* characteristics. The threats are programmed to spawn commensurate with the warning delay and render at the edge of the park at the end of the delay. Delays are set at 30, 60, and 90-second intervals, with the latter representing an approximate 1-mile distance at a speed of 40mph, which is near the maximum limit of visual observation for a drone pilot (*Drone Pilot Ground School*, 2020). After a brief warm-up, the *spinningup* state raises the agent to an altitude using a uniform distribution between 200-500'. The *assessing* and

coarsetracking phases are coded to mimic a distant visual assessment by a nefarious drone operator by locating what appears to be the largest density of pedestrians and establish that as the drone target and destination. This is done through the setting of *p_coarseStep,* which breaks down the map to measure pedestrian density into a large grid system of approximately 50 meters and sends the threat agent at maximum speed [41, 40] mph toward the center of the highest density area returned by the function. The method is written so that two or more threats can be activated at the same time and will attack the highest two pedestrian densities that do not contain more than approximately 5% overlap. At approximately 50 meters away from the course target, as dictated by *p_fineTrackingRadius,* the threat does another assessment and course correction down to 8-meter accuracy of the highest pedestrian density and slows to half of the maximum speed until over the target. Once *overTarget*, the threat *drop*s its payload which falls at the standard rate of gravity 9.81 m/s based on the threat altitude. *Threat 1*'s simulated 40mm detonates on impact making a 5-meter casualty radius, while Threat 2's simulated M67s have a 4-5 fuse delay and incur casualties out to 15 meters. The threat then returns to the point at which it was spawned at maximum speed.

3.1.2 Facility characteristics

A previous study for amusement park evacuation was conducted with AnyLogic to see the effects of evacuation time and first responder response time by manipulating the available exits to patrons (Tzvetanov et al., In press). Elements of this framework are modified for this study; however, the base geographic map will remain the same. See *Figure 8* for an artist's rendition of the amusement park map used in this study and the associated attractions. See *Figure 9* for a graphic representation of the modeling space in AnyLogic modeling software (Tzvetanov et al., In press). *Figure 10* depicts the exits throughout the park.

Figure 8. A = Main Gate, B = Yellow River Adventure, C = Fountain Pavilion, D = Backstage and Concessions, E = Arcade (Tzvetanov et al., In press)

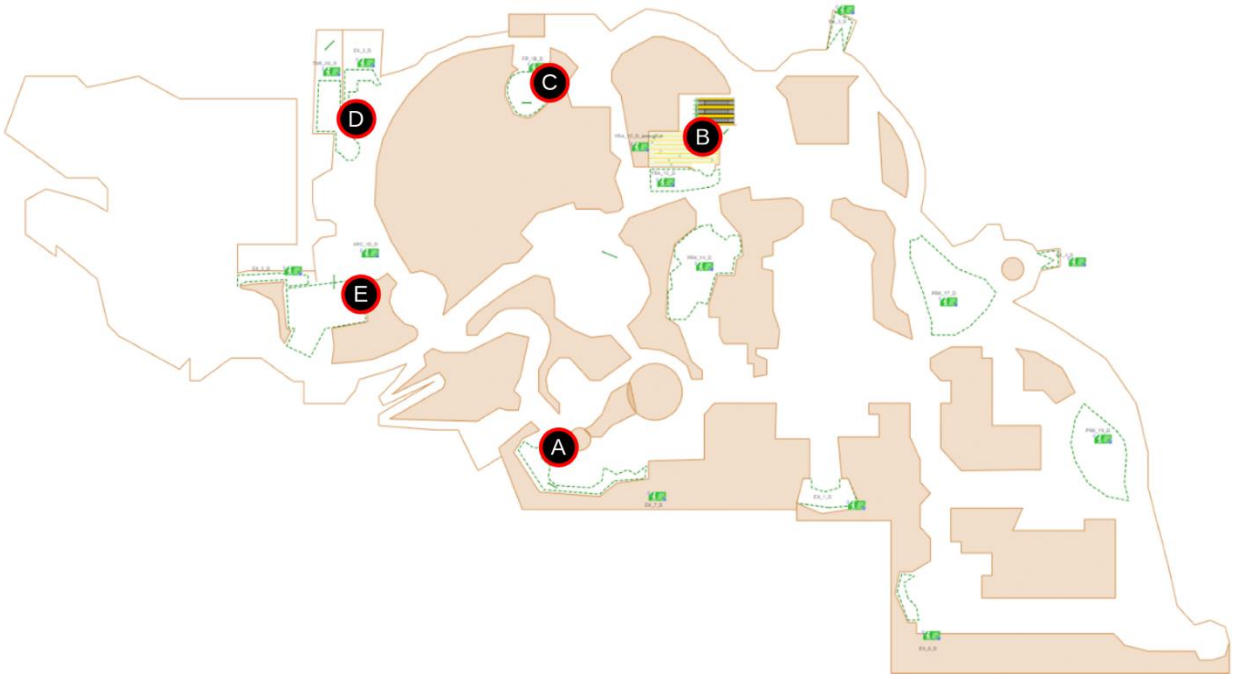

Figure 9. A = Main Gate, B = Yellow River Adventure, C = Fountain Pavilion, D = Backstage and Concessions, E = Arcade (Tzvetanov et al., In press)

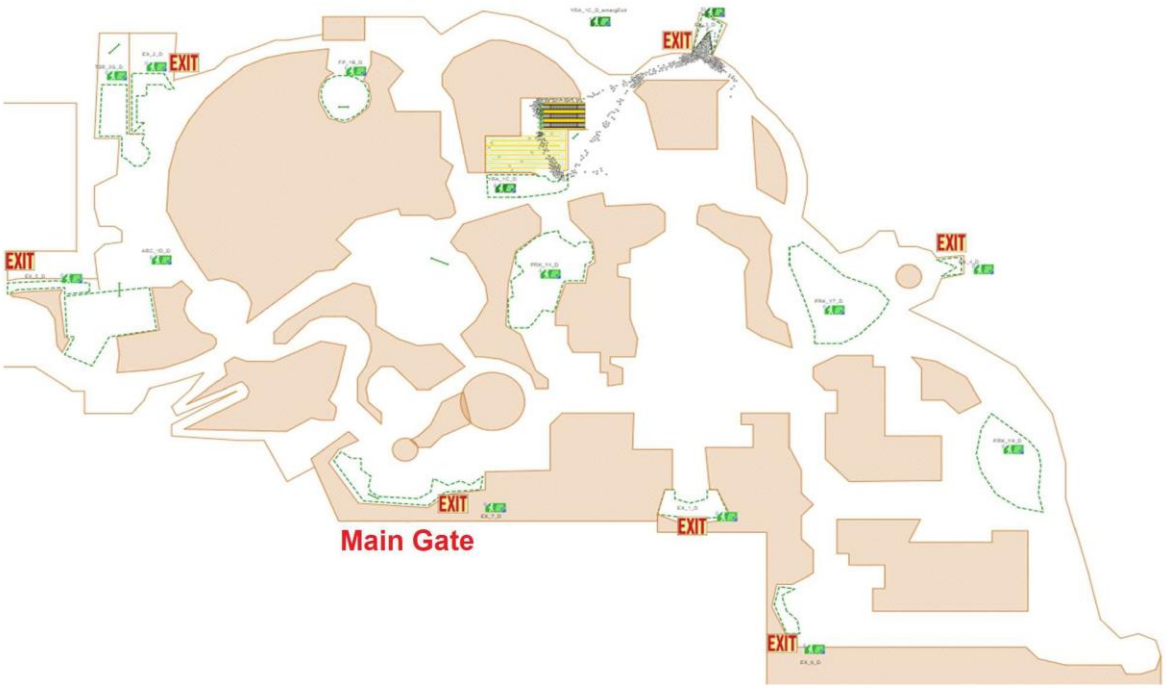

Figure 10. Location of park exits (Tzvetanov et al., In press)

Two small modifications are made to the physical space within the model to allow for the appropriate testing of the interventions discussed. The rigid serpentine queue at the Yellow River Adventure (item B in *Figure 9*) was opened into a free-form line as the serpentine queue would prevent any patrons in the queue from exiting the park or separating once the threat warning was declared. This resulted in threat attacks on strictly the serpentine queue in many of the initial test runs. Changes are shown in *Figure 10*. An additional minor change includes some wall edge

softening on the Fountain Pavilion (item C in *Figure 9*) allowing pedestrians that are conducting a spacing protocol to more naturally and effectively exit that area.

Figure 11. Yellow River Adventure serpentine queue modified to the right configuration to test study interventions

Pedestrian behavior

Appendix D shows the starting locations of the 2,443 pedestrians that are added into the park model with a 12-minute warm-up time to allow the dispersion throughout the park and the queues associated with attractions to be filled. The pedestrians are populated at different attractions and are organized into groups based on a distribution of census household sizes (*Historical Households Tables,* 2019). The pedestrians, alternately called 'patrons,' are programmed to spend a certain amount of time at an attraction before moving to another one. The attraction logic remains unchanged from Tzvetanov et al., (In press). The pedestrians move at speeds during normal activities following a uniform distribution between 0.5 and 1.0 m/s as dictated by AnyLogic's default pedestrian speeds. When an evacuation or threat warning occurs, the patrons increase their speed and began an intervention behavior

Patrons evacuate through the main gate following a threat detection and threat announcement on EG2, EG7, and EG12, and evacuate using the nearest of the park's seven exits

in EG3, EG8, and EG13. The patrons separate from each other at intervals of 2 meters in EG4, EG8, and EG12 and separate at 5-meter intervals on EG5, EG9, and EG13. *Figure 12* represents the state chart used in conjunction with the pedestrian logic represented in *Figure 13* that alert and govern the patron's actions.

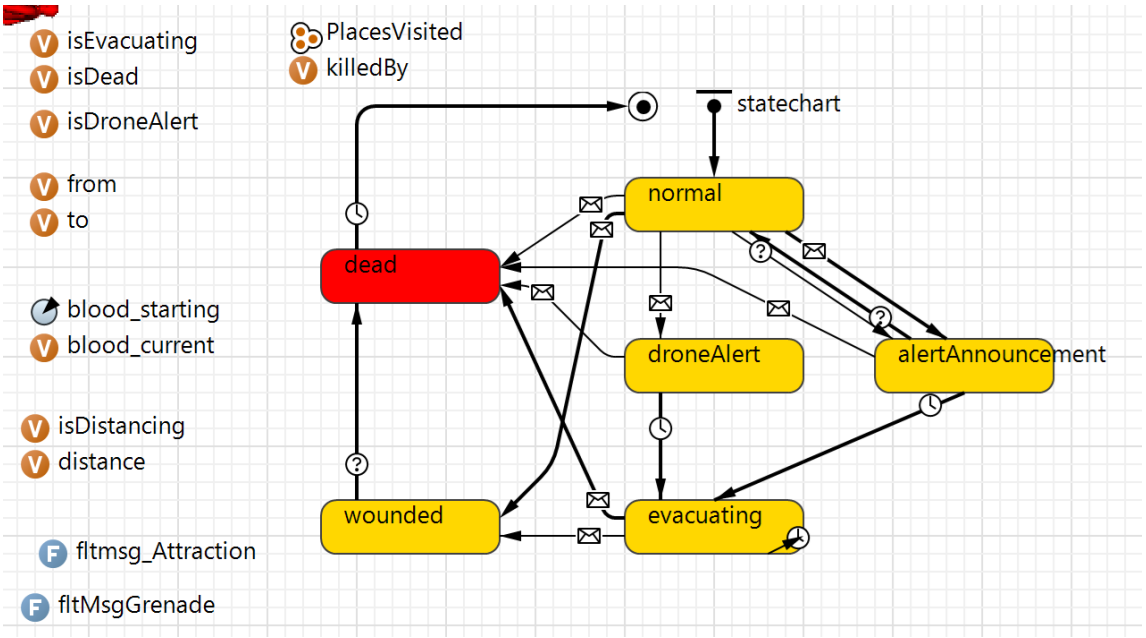

Figure 12. Patron state chart

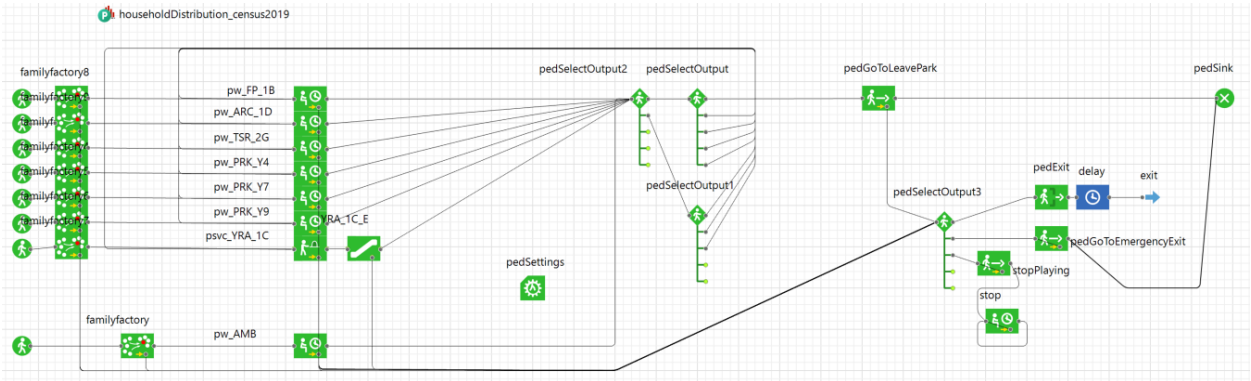

Figure 13. Pedestrian logic for movement and exiting

The statechart is used primarily for the purposes of rendering patrons and affecting behaviors while evacuating, separating, or being subject to a casualty radius from a drone threat attack. In the *normal* state, the patrons follow the chart blocking in *Figure 13.* This is very similar to the logic, and patron capacity numbers in Tzvetanov et al., (In press), with some minor modifications. Grouping blocks were added at each patron spawn point that matches the 2019 U.S. census data on household sizes (*Historical Households Tables*, 2019). Group size data for amusement parks were not readily available, so a distribution was made from the 2019 census data to govern the frequency and size of patron groups that stick together as they traverse the amusement park. Agent messaging can change the patron state from *normal* to *droneAlert* or *alertAnnouncement* based on the scenario that is selected at the start of each experiment. In both cases, the patron speeds will increase to simulate Rinne et al.,'s (2010, p. 22) evacuation "goal-oriented" mean horizontal walking speed of 2.1 m/s which is implemented using a uniform distribution between 1.9 and 2.3 m/s. In the case of *droneAlert*, the patron's diameter is manipulated to either 2 or 5 meters depending on the experiment group being tested, and the patrons are canceled from the attraction logic as they begin to separate throughout the park. In the case of *alertAnnouncement*, patrons are canceled from their attraction logic as they head to the nearest 'open' exits, which is either set to the main exit only, or all seven park exits as configured at the start of each experiment. The *wounded* state is not used in this study.

The drone agent, comprised of *Threat 1* and *Threat 2*, will send a message to each patron that lands within a casualty ring of the simulated ordinance. A probability is assigned as to whether the patron then enters the *dead* state and is considered a casualty. It is important to note that this study was designed to count casualties as a dependent variable and not deaths; however, the statechart is in development for other future research projects designed to account for the

degradation of health and eventual death following an injury from active shooter situations. *Figure 14* and *Figure 15* depict examples of evacuations with casualties inflicted, while *Figure 16* illustrates a separation interval before a drone attack.

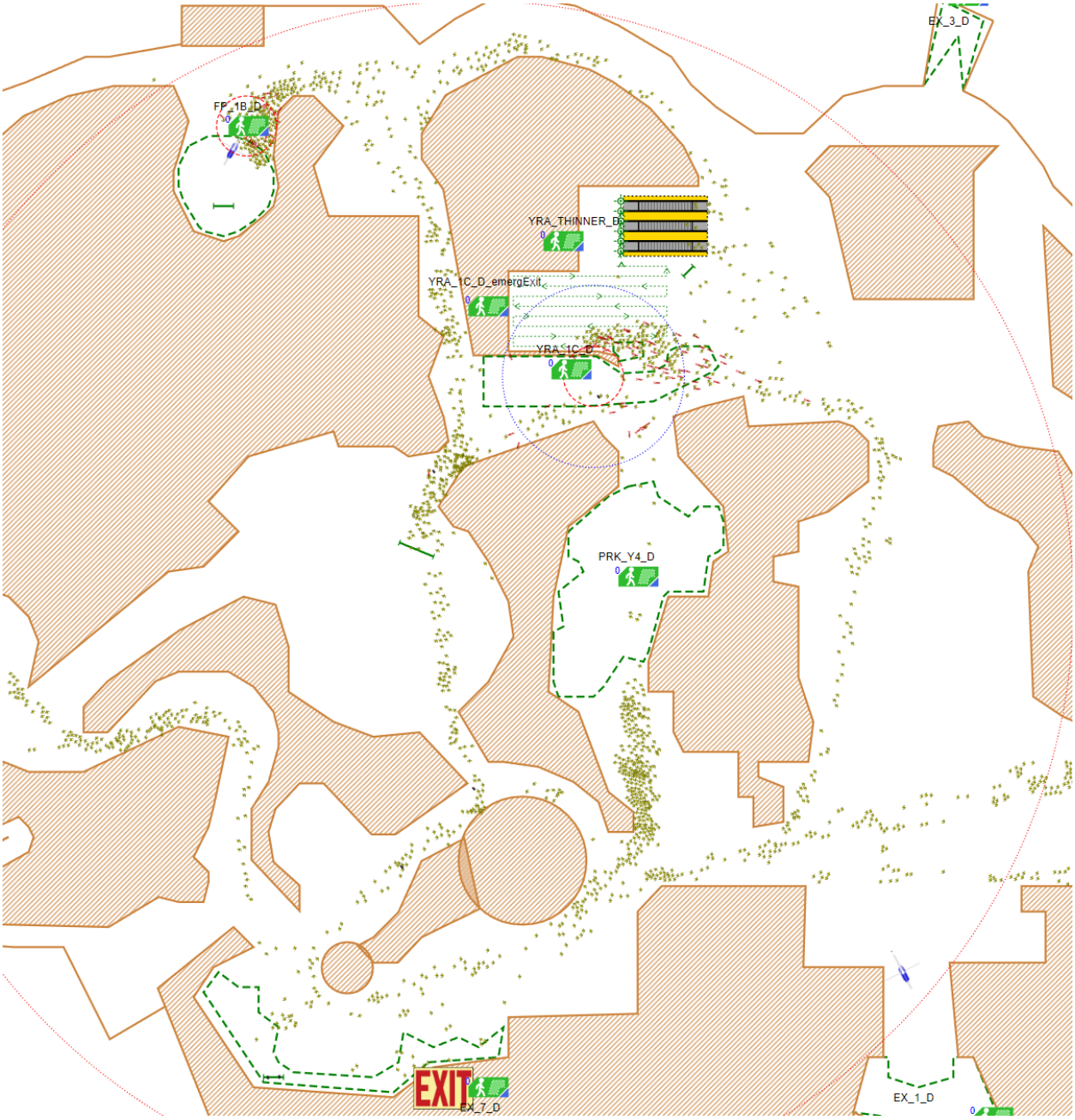

Figure 14. Main exit evacuation example with casualties indicated in red. Some casualties remain bound by groupings and are pulled outside of the casualty rings.

Figure 15. A seven-exit evacuation with *Threat 1* casualties and *Threat 2* about to inflict casualties on a high-density patron group. Exits 2 and 5 are shown on the top left and right respectively

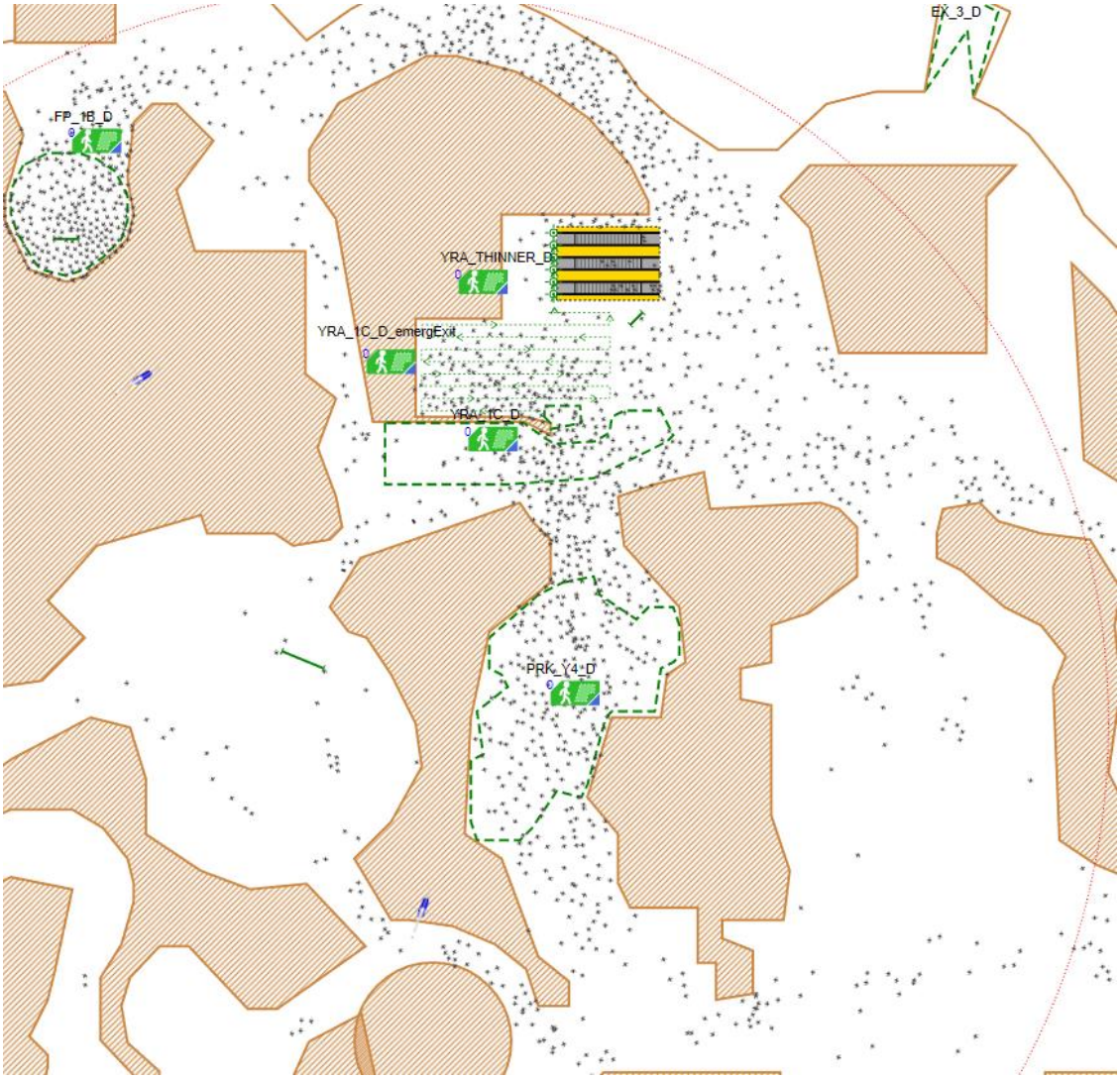

Figure 16. Patrons approximately 30 seconds after a 2-meter separation interval.

3.2 Reliability

Reliability was assessed throughout the development and testing of the model. Outliers within the data and variance were noted and assessed by the researcher during this process. Outliers in simulation modeling usually indicate an error in implementation, programming, or usage of the AnyLogic software. Outliers were identified using the following formulas and noted in Appendix C:

$$H.O. > Q3 + (IQR * 1.5)$$

$$L.O. < Q1 - (IQR * 1.5)$$

Note: H.O. is a high outlier, L.O. is a low outlier, Q1 and Q3 refer to quartiles, and IQR represents the interquartile range.

3.3 Validity

Agent-based modeling validity may be divided into several facets. The parameters selected to guide the behavior of each agent are discussed in previous sections involving agent behavior. These parameters are selected from available data and are intended to replicate an abstracted version of the real-world behavior of pedestrians, facility interventions, and threat UAS. The validity of AnyLogic as a tool has established historical validity in other settings to include the 1999 Columbine active shooter situation (Lee, 2019), and operational validity in the mitigation of active shooter incidents in "gun-free" zones (Kirby et al., 2016) and in establishing efficient methods and manning to operate a regional hub reception center for evacuees in the event of an emergency evacuation (Kirby et al., 2014). The model was continuously tested for simulation validity aspects first introduced in Section 2.4.2 throughout the creation, testing, and data

collection process. Specifically, the model has been screened for face, animation, event, and internal validity by the researcher, and backed up through the reliability and generally normal distributions of the testing results.

CHAPTER 4. RESULTS & ANALYSIS

This section will display and analyze the summarized results from the 390 sample iterations collected across the study's 13 experiment groups. The full data and sample information is included in Appendix C.

4.1 Experiment Group Data Summary

EG1 served as the control group in which patron behaviors and facility interventions are not manipulated and appears in multiple columns within Table 5 as a reference to casualty numbers without any interventions. The distributions for each experiment group followed a generally normal shape, and only two outlier test runs were recorded and replaced for EG1 (see Appendix C). The highest casualty sample mean was EG1, followed by EG3, and the lowest casualty sample was EG7 followed by EG9. In general, all intervention categories appeared to significantly reduce the number of casualties compared to the control group.

Table 5 Summary of Casualty Sample Data from Experiment Results

		30-second warning			
Group	EG1 Control	EG2 ME	EG3 7E	EG4 2M	EG5 5M
Mean	**189.4**	79.7	***117.7***	86.2	81.3
Std. dev.	9.0	23.9	16.2	13.1	13.1
Min	173.0	37.0	73.0	58.0	59.0
Q1	183.5	68.3	107.3	76.0	71.3
Median	**189.0**	75.5	***119.0***	84.0	80.0
Q3	194.8	99.3	129.5	95.0	89.5
Max	209.0	128.0	145.0	114.0	112.0
		60-second warning			
Group	EG1 Control	EG6 ME	EG7 7E	EG8 2M	EG9 5M
Mean	**189.4**	101.8	**72.0**	80.9	***74.4***
Std. dev.	9.0	19.3	15.9	18.6	14.1
Min	173.0	73.0	42.0	44.0	49.0
Q1	183.5	83.0	59.0	67.5	63.5
Median	**189.0**	101.5	**71.0**	77.5	***73.5***
Q3	194.8	122.5	81.3	101.5	81.8
Max	209.0	131.0	110.0	109.0	106.0
		90-second warning			
Group	EG1 Control	EG10 ME	EG11 7E	EG12 2M	EG13 5M
Mean	**189.4**	89.9	84.4	92.4	96.1
Std. dev.	9.0	21.4	25.6	14.9	16.7
Min	173.0	54.0	41.0	62.0	62.0
Q1	183.5	71.8	62.5	84.3	87.5
Median	**189.0**	86.0	89.5	95.0	93.5
Q3	194.8	108.8	104.5	102.0	105.8
Max	209.0	128.0	128.0	127.0	124.0

**Note. EG1 is listed in the left column of each time category for reference.*

The information in Table 5 is visualized in *Figure 17* and generally shows the effect of the interventions on the casualty count.

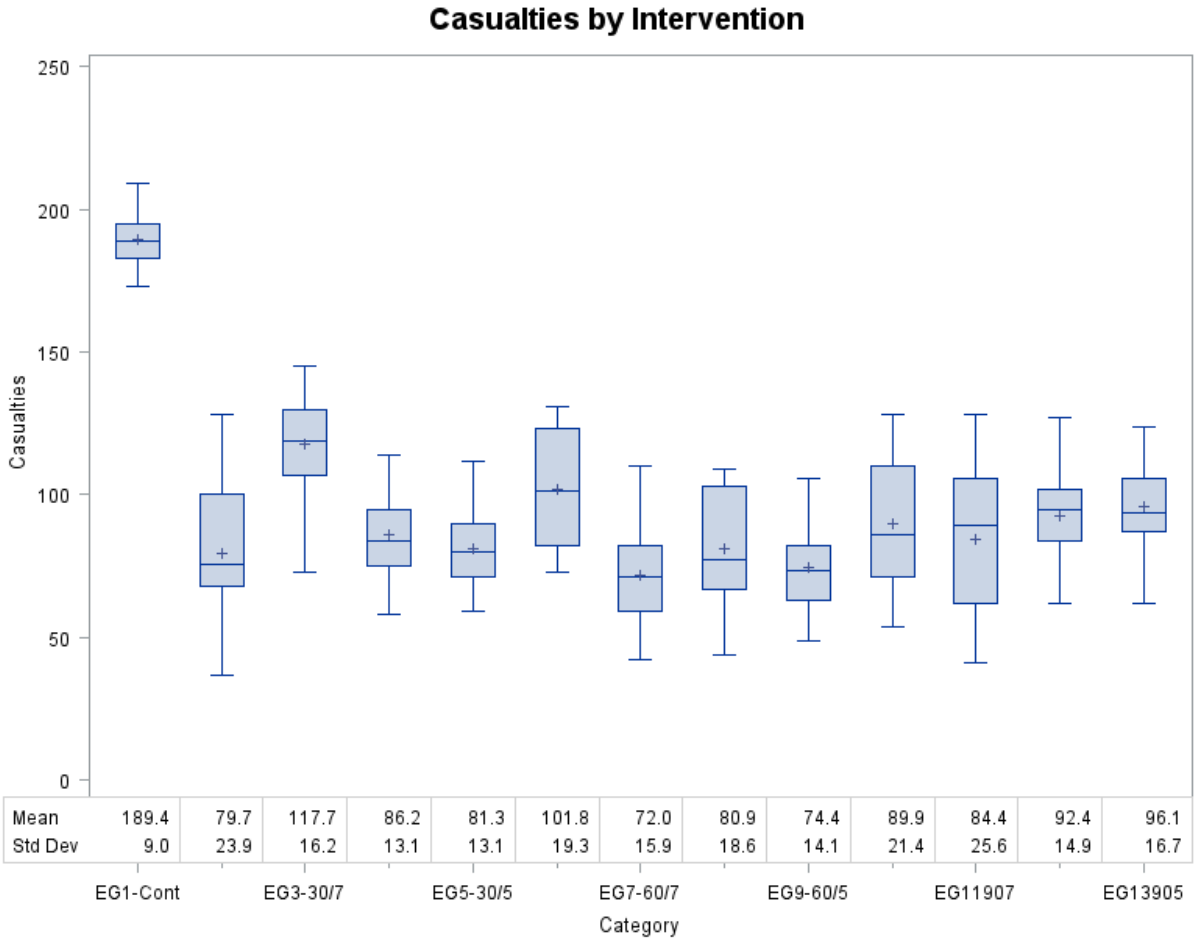

Figure 17. Sample data from all experiment groups

Further analysis requires divisions in the sample data compared. The samples will be divided into time-delay before interventions, and the effect of the time delay on a specific type of intervention to further analyze the effects of time for each type of intervention.

4.2 Analysis of Casualties by Time Categories

Figure 18 displays the results of the experiment for each of the behavioral interventions with the 30-second threat warning interval of patrons executing a mitigating behavior. In the '30-second' category, the 'main exit' intervention, or EG2, had the lowest casualty average but maintained the highest variance. EG2 and EG3 began to effectively move the highest density attraction areas to the park's main pathways. In EG2, there were few areas of high-density patron areas caused by the park design or the exit path taken, and the majority of the high-density targets were caused by patrons leaving attractions. EG3 had the highest casualty average for all intervention categories. This relatively short time delay resulted in high-density patron groups forming in the common area to the east of the Yellow River Adventure at the time of the attack, which was subsequently targeted by a majority of the drone threats in the sample runs.

The two separation intervals, EG4 and EG5, had similar results with the 5-meter separation interval having a slightly lower overall casualty average when compared to the 2-meter separation interval. The variances of the two separation intervals were a bit smaller when compared to the evacuation trials, which suggests a more reliable approach for mitigating casualties in the '30-second' category. Patron groups were often attacked at the Fountain Pavilion and just outside of the Yellow River Adventure during both EG4 and EG5.

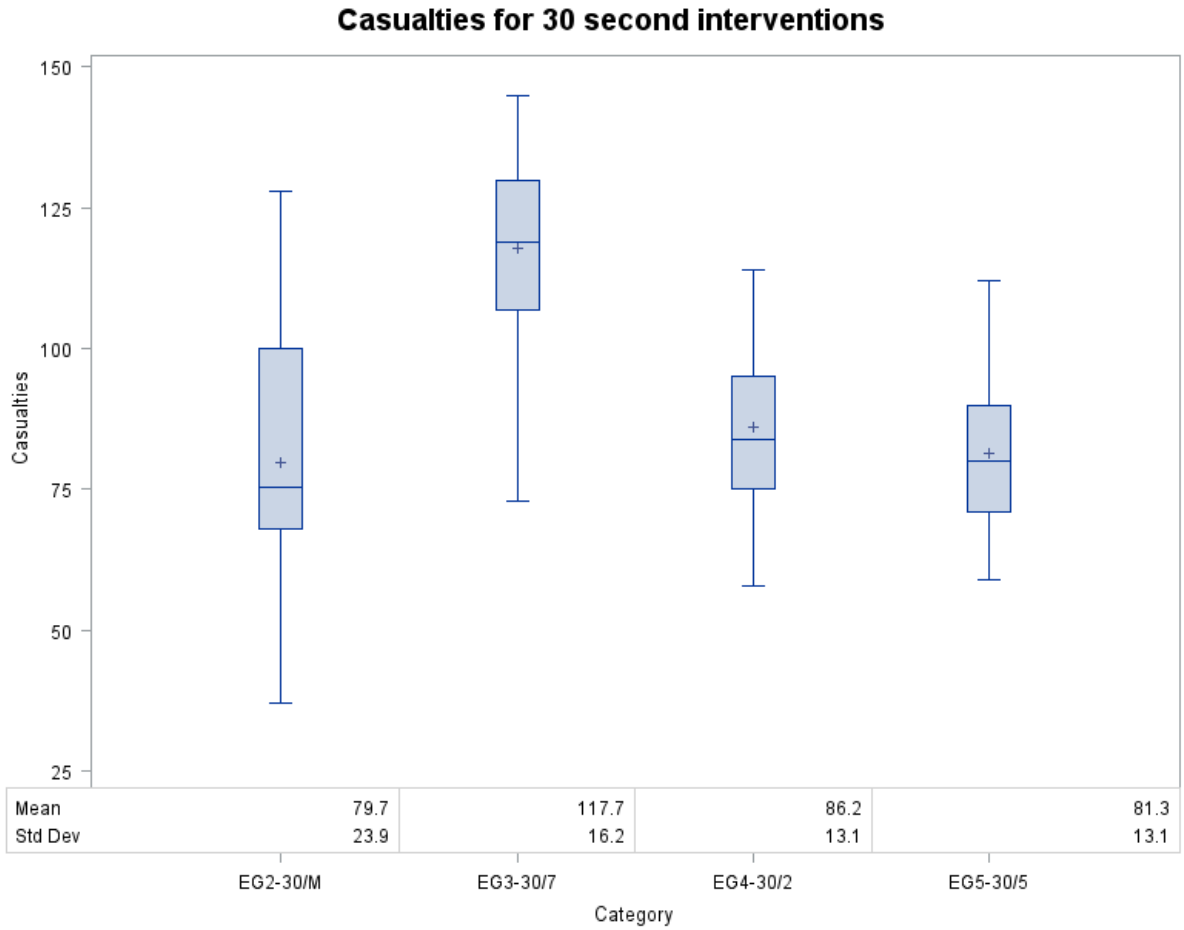

Figure 18. Casualties for 30-second interventions

Figure 19 displays the results of the experiment for each of the behavioral interventions with the 60-second threat warning interval of patrons executing a mitigating behavior. The 'main exit' intervention (EG6) held the second-highest casualty average for the intervention groups. After some dispersion from the main attraction areas, patrons began to re-coalesce in major pathways as they got closer to the main exit in EG6 as seen in *Figure 20.* EG7, in which patrons had a 60-second warning to go to the nearest of seven exits, had the lowest overall casualty average of all the 13 groups tested. This was due to the ability for patrons at high-density attraction areas to have enough time to disperse toward an exit, but not enough time to coalesce in large numbers at the emergency exits due to their limited throughputs.

The two and five-meter separation interventions fared significantly better than the control group with 80.9 and 74.4 average casualties compared to the control group's 189. The 60-second and 5-meter separation (EG9) had the second-lowest casualty average of all groups tested (+2.4 from EG7) and had a lower sample variance than EG7 (-54 casualties^2), potentially suggesting the most reliable intervention strategy. While more time was allowed for the separation intervals, many of the same areas were attacked as the patron agents seemed to have difficulty determining which direction to move to achieve the distance interval from other patrons. This would likely occur in a more realistic setting as patrons would have limited situational awareness for the park as a whole and only be aware of their immediate and likely chaotic surroundings.

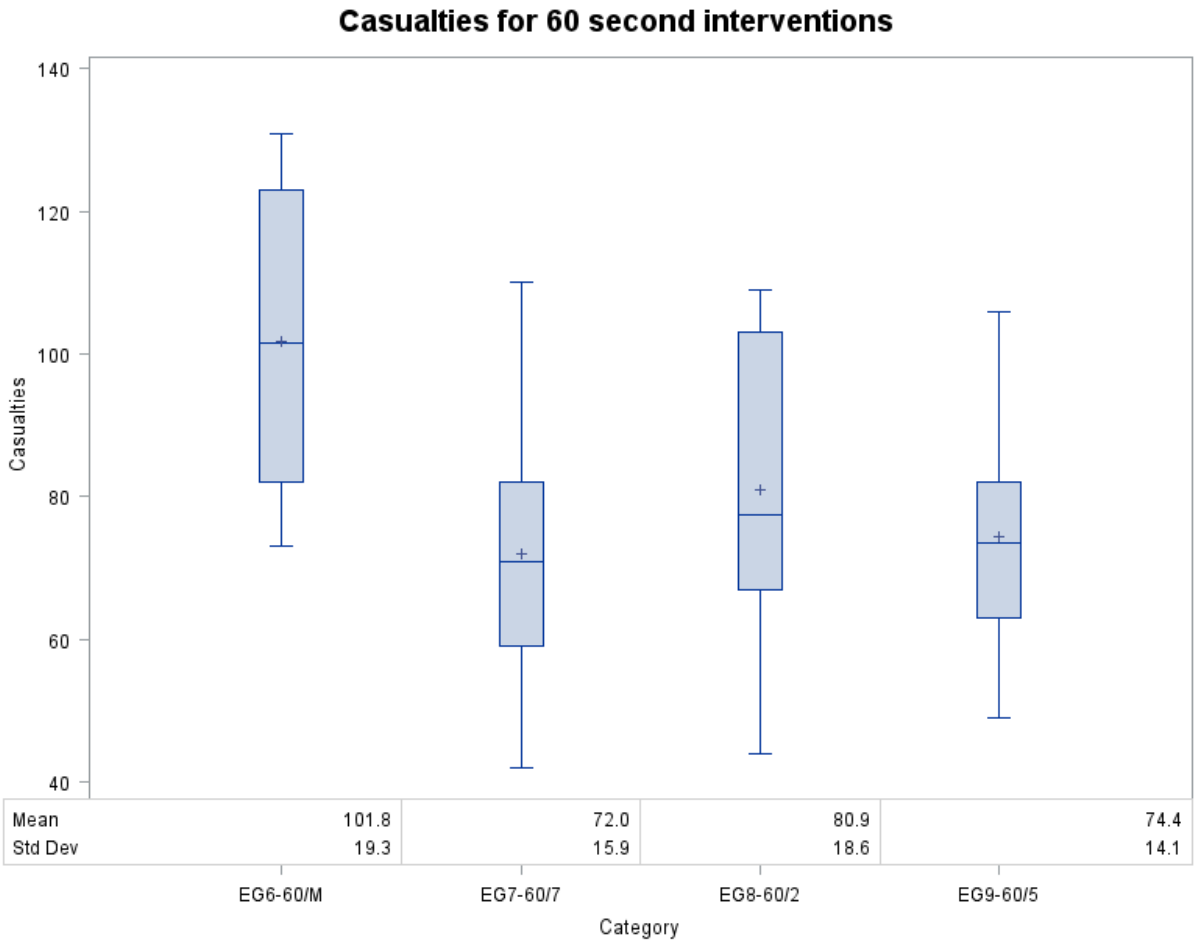

Figure 19. Casualties for 60-second interventions

Figure 20. Patrons re-coalescing at a hard corner while evacuating for the main exit in EG6

Figure 21 displays the results of the experiment for each of the behavioral interventions with the 90-second threat warning interval of patrons executing a mitigating behavior. The evacuation categories, EG10 and EG11, maintained a slightly lower casualty average and a higher variance than the separation categories, EG12 and EG13. The separation interval categories saw higher casualties than in the 60-second interventions due to the gridlock of expansion in tight corridors as patrons attempted to spread throughout the park. Interestingly, the 2-meter separation interval fared slightly better than the 5-meter interval due to the additional clearance to navigate the tighter areas. The '7-exit' category continued to have more patron coalescing near throughput-restricted exits, while the 'main exit' category saw less.

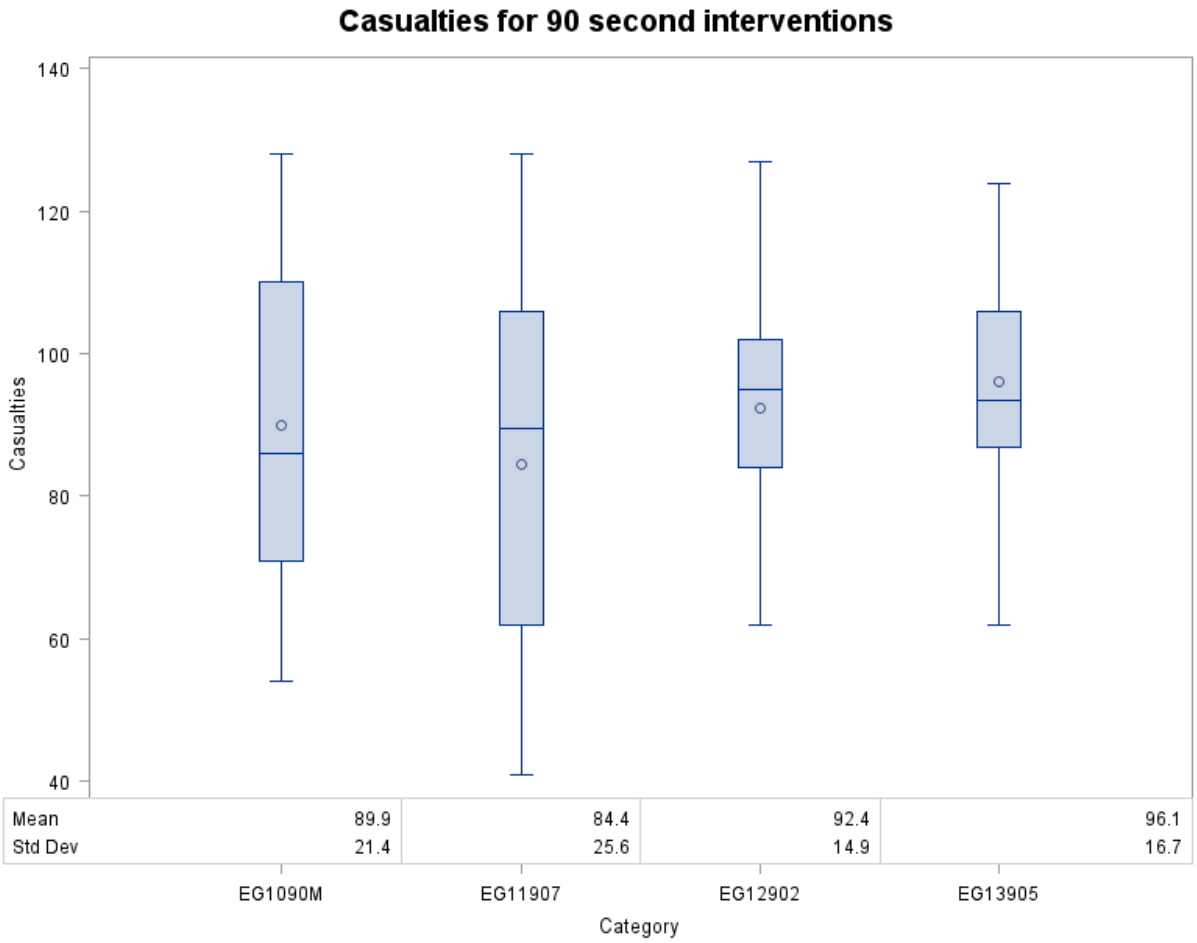

Figure 21. Casualties for 90-second interventions

Overall, the 60-second category had the lowest casualty average and median totals among the 4 intervention categories. The 30 and 90-second categories had similar casualty scores. The 30-second category had a lower median total among groups and the 90-second category had a lower average total among groups, as seen in Table 6.

Table 6 Summary of Casualties by Time Category

	30-second warning				**Totals**
Group	EG2 ME	EG3 7E	EG4 2M	EG5 5M	
Mean	79.7	117.7	86.2	81.3	**364.9**
Median	75.5	119.0	84.0	80.0	**358.5**
	60-second warning				
	EG6 ME	EG7 7E	EG8 2M	EG9 5M	
Mean	101.8	72.0	80.9	74.4	**329.10**
Median	101.5	71.0	77.5	73.5	**323.50**
	90-second warning				
	EG10 ME	EG11 7E	EG12 2M	EG13 5M	
Mean	89.9	84.4	92.4	96.1	**362.8**
Median	86.0	89.5	95.0	93.5	**364.0**

4.3 Effects of Time on Specific Interventions

The previous section focused on comparing the four interventions against each other in each time category. This section will discuss the effect time has on each specific intervention. The 'main exit' interventions, EG2, EG6, and EG10, and the '7 exits' interventions EG3, EG7, and EG11 are depicted in this order in *Figure 22* for comparison.

The 'main exit' intervention (EG2) held the lowest casualty average at a 30-second warning, the 'main exit' intervention (EG6) had the second-highest casualty average for the non-control sample groups. While the patrons were able to separate from the high-density attraction areas, lowering the EG2 casualties, the patrons began to re-coalesce in major pathways as they got closer to the main exit in EG6 as seen in *Figure 20.* This higher density group began to dissipate for EG10, as more patrons could exit the park or clear some of the restrictive pathways into larger open areas.

The '7 exits' intervention saw the highest casualty average at 30-seconds (EG3) among the twelve groups. This was due to the high patron densities leaving the Yellow River Adventure and Fountain Pavilion areas, creating prime target areas for the threat drones. The subsequent 60-

second ‘7 exits’ trial (EG7) saw the lowest casualty average among the intervention groups. The high-density patron group could further dissipate toward the emergency exits leaving smaller target groups for the threat drones. The 90-second ‘7 exits’ intervention (EG11) had a small increase in casualties over EG 7 due to throughput (rates can be found in Appendix D) grouping at the Yellow River Adventure emergency exit and small pathway leading to the Fountain Pavilion exit, both of which resulted in larger patron densities.

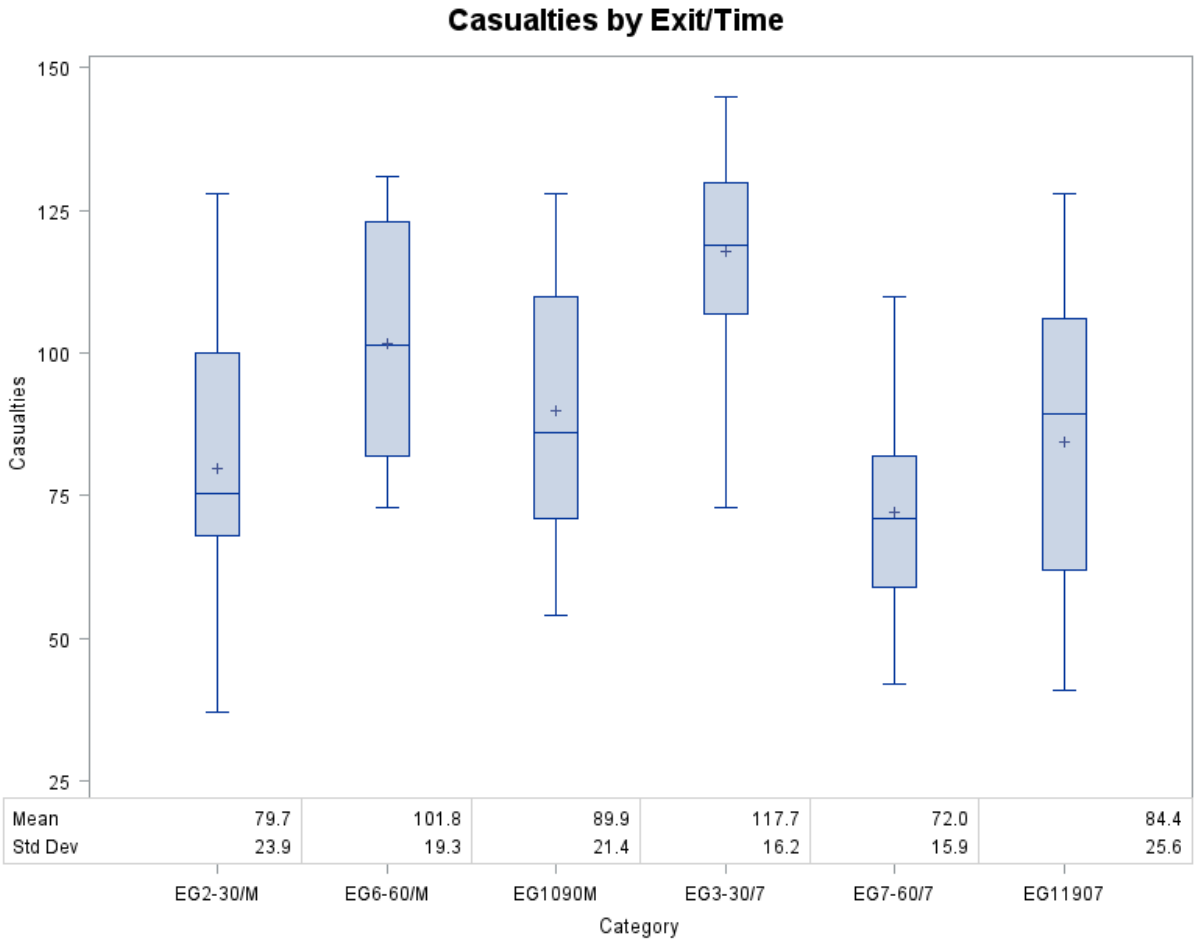

Figure 22. Evacuation interventions compared

The 2-meter separation interventions, EG4, EG8, and EG12, and the 5-meter separation interventions EG5, EG9, and EG13 are depicted in this order in *Figure 23* for comparison. Both

categories of separation interventions followed a similar pattern where casualties were greatly reduced from the control group, EG1, in EG4 and EG5, and further casualty reductions were seen in EG8 and EG9. The 5-meter separation interval had slightly lower casualty averages than the 2-meter interval in the 30 and 60-second categories. Interestingly, casualties increased for both separation intervals in the 90-second category due to 'deadlocking' in common areas and the additional time allowed for patrons to congregate and get 'stuck' in narrower pathways within the park. As one would expect in real life, true intervals were never maintained as patrons were attempting to account for and move away from multiple others around them. This appeared to simulate the confusion that would be encountered attempting to maintain an interval while not knowing patron densities outside one's immediate area. In the 90-second category, the 2-meter intervention had a slightly lower casualty average reflecting the more mobility gained through a smaller separation interval.

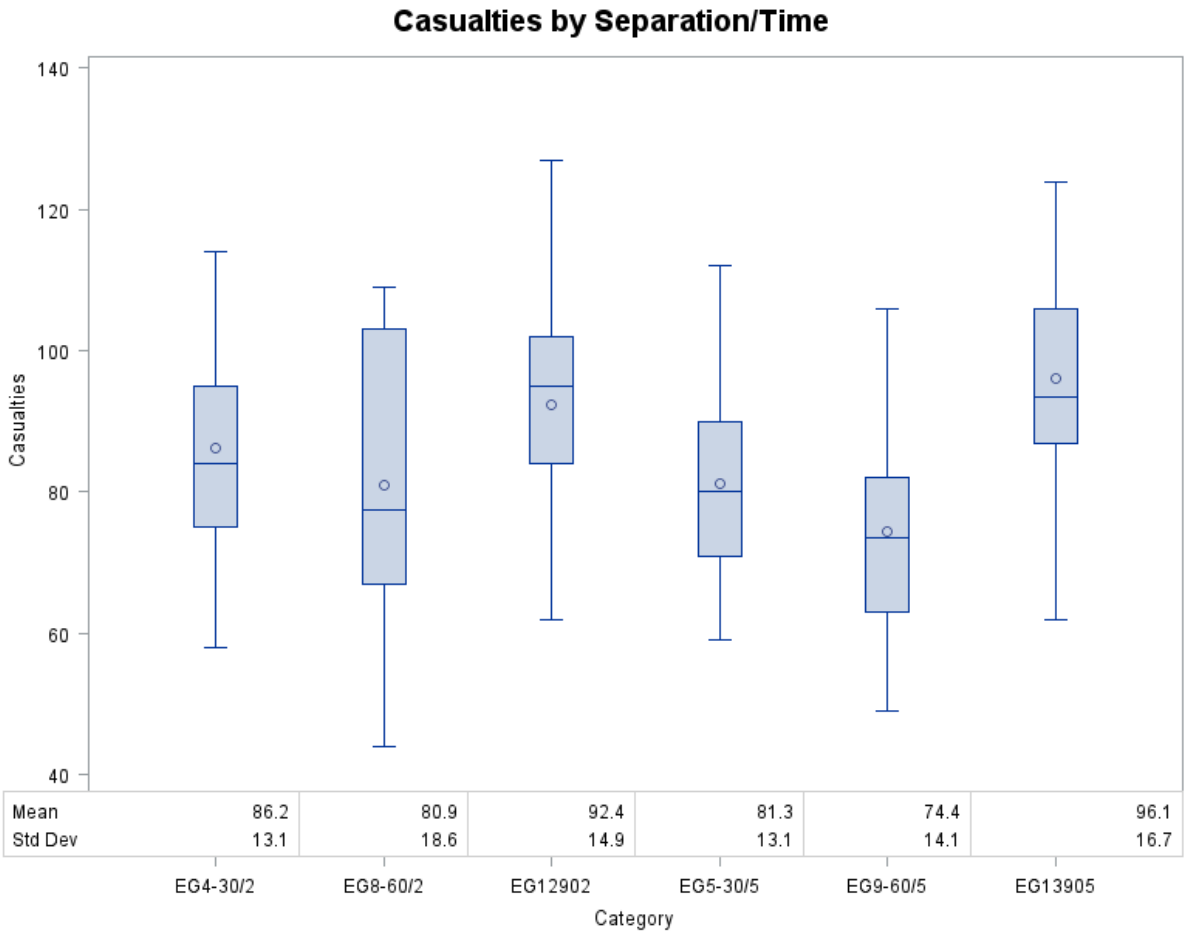

Figure 23. Separation interventions compared

Table 7 shows mean summary data and highlights that overall, the 5-meter separation interval was the most effective across the four mitigating behaviors. The most effective time interval for intervention was the 60-second time interval.

Table 7 Summary of Casualty averages by Time and Intervention

	ME		7E		2M		5M		**Totals**
30 s	*EG2*	79.7	*EG3*	117.7	*EG4*	86.2	*EG5*	81.3	**364.9**
60 s	*EG6*	101.8	*EG7*	72.0	*EG8*	80.9	*EG9*	74.4	**329.1**
90 s	*EG10*	89.9	*EG11*	84.4	*EG12*	92.4	*EG13*	96.1	**362.8**
Totals	**271.4**		**274.2**		**259.5**		**251.8**		**1056.8**

4.4 Inferential Statistics for Best Practices

From the previous analysis, it appears that the interventions in EG9 would be the most prudent to reduce the number of casualties involving a threat drone attack, as outlined in this study. While EG7 did have a lower casualty average, the same intervention had much higher casualties when the warning time was reduced. A 60-second warning provides the best time interval tested to apply any patron movement interventions for reducing casualties. The 5-meter separation interval proved to be the overall best behavior across each warning interval tested. Inferential statistics results are included in Appendix E to provide insights on any other experiment groups that did not have a statistically significantly different population casualty means per attack based on the sample data collected. EG5, EG8, EG2, and EG7 did not have a statistically different population mean of casualties per attack at the 95% confidence interval when conducting a multiple comparison T-test. These implications will be discussed in the next section.

CHAPTER 5. DISCUSSION

5.1 Research Questions Addressed

1. *Is there a feasible behavior that patrons can adopt that will minimize total casualties in the event of a weaponized drone attack, given appropriate warning of a threat?*

In this experiment, all categories of timed warnings and resultant behaviors resulted in a reduction of average casualties between 37.8% and 62% from the control group. These benefits were attributable to behaviors that have a dispersion effect on patron groups, thus making it more difficult to create casualties with explosive ordinance, chemical weapons, or biological contaminants.

2. *What is the appropriate warning time to alert a crowd of an impending drone attack to allow for a mitigating behavioral action to be taken?*

All experimental groups had fewer casualties with a 60-second threat warning, and similar results were observed between the 30-second and 90-second categories across all four behavioral interventions.

5.2 Hypothesis Revisited

There was no evidence to support the claim that evacuation interventions resulted in more casualties than the control group. In fact, the sample data suggested the opposite as evacuations had immediate dispersive effects and overall lower casualties. There was evidence to support the claim that separation intervals reduce the average casualties when compared to the control group.

However, there appeared to be a diminishing return on the amount of time allowed to disperse and the dispersion intervals due to constricting corridors and limited situational awareness of patrons.

5.3 Experiment Insights

Park design and exit throughput rate (Appendix D) played a large factor in the number of casualty reductions for the two evacuation intervention types. The timed threat warnings produced predictable high-density gatherings at certain times and locations during the evacuation that must be considered when developing a casualty mitigation protocol for high-density outdoor events. Similarly, casualty mitigation considerations should begin in the design phases of the venue, as tight corridors and sharp corners resulted in high-casualty target opportunities for the threat drone aircraft.

Separation intervals proved to be the most reliable overall behavior in mitigating casualties across the different timed warning intervals. The 5-meter interval produced slightly better results as a 60-second intervention but did not have a statistically significant mean difference between the 5-meter 30-second intervention or the 2-meter 60-second intervention. This is important to note when considering the development of a threat warning system. Separation intervals should be viewed as a 'goal' as the complicated dynamics of separation of a mass of patrons would result in confusion as patrons attempt to separate in different directions and at different speeds. True separation intervals were never seen in modeling and would likely be an impossibility without coaching from a large perspective over a lengthy amount of time. The separation intervals modeled would represent a behavioral cue rather than an absolute outcome. Separation intervals provide positive effects but would lead to confusion and prove to be difficult to implement in dense areas. The two and five-meter intervals had very similar results due to the most crowded and restrictive areas preventing the expansion of patrons which were subsequently targeted by the drone threats.

Larger separation intervals would be infeasible at best, as the complicated dynamics would not allow a true expansion throughout the park and no further casualty reduction would likely be seen.

Covered areas near known or expected high-density areas may provide additional casualty mitigation protections, as well as sufficient time to exit the open areas into modeled buildings or other entrances. Park designs should consider smoothing transitions to corridors and open areas as well as matching throughput rates at exits to accommodate the expected patron densities at nearby attractions in the event of an emergency. It is important to note that the serpentine queue was targeted often in the early testing phases of the study, resulting in modifications being made to the queue before data collection occurred. Park designers should consider queues that are easily and quickly exited during an emergency situation and should refrain from using traditional waist-high rigid fencing outdoors. Queues could be located inside buildings to provide additional protection from attacks, or alternately queues and corridors could be protected by netting that would prevent drone interference and create a distance barrier from some explosive attacks that would ultimately reduce casualties.

5.4 Considerations for Mitigation System Development

This section will discuss some of the requirements and planning factors involved in developing an sUAS threat detection and patron notification system similar to the one modeled in this study. The purpose of this study was to find alternative UAS mitigation strategies since C-UAS technology is illegal to implement in the U.S. A network of acoustic sensors may provide a cost-effective and reliable means to detect drones. Acoustic drone sensors demonstrated a 99% probability of detection at distances below 600 meters (1969 feet) with a 3% false-positive rate using bandpass filters of 800-1700 Hz and 4 second non-overlapping recorded data intervals (Benyamin & Goldman, 2014). Christnatcher et al. (2016) proposed a system of acoustical nodes,

separated by no more than 200 meters, around a protected facility with a short wave infrared gated-viewing device to locate, identify, and track threat UAS. The 200-meter interval was chosen so that any intruding drone could be located in three-dimensional space by tracking the vectors of three acoustic nodes to a singular point. Once the point is identified an optical sensor can be slewed and focused on the offending drone for tracking and classification.

For the discussion, the acoustic nodes will serve as detection trip-wire to direct an electro-optical device for the classification of an sUAS and determination of its threat status. Since no C-UAS interdiction will be deployed for this discussion, a buffer radius must be determined that allows for the desired time to implement a behavioral intervention. To determine a buffer radius, the threat speed must be considered in conjunction with the time of a threat announcement, the pre-movement time between when an announcement concludes and patrons begin an action, and the time desired for behavioral intervention.

While no specific data is available for amusement park evacuations, pre-movement times should be similar to patrons exiting a cinema, as opposed to schools and churches which have to account for additional time for the collection of belongings or clothing items not near their owner before going outside. A five-second delay will represent an audio warning, and a pre-movement following Rinne et al.'s (2010, p. 15) depicted cinema evacuation of approximately 5 seconds.

For this study, the protected area radius was 325 feet, equivalent to the main central area of the park layout. The anticipated threat speed is calculated at 40 mph or 58.68 fps. The alert time and pre-movement times are both 5 seconds, and the sensor node intervals are set to 200 meters or 656 feet. *Figure 24* represents a 30 and 60-second sensor radius of 0.5 and 0.83 miles requiring approximately 26 and 43 acoustic sensors respectively at 200-meter intervals using the formula below:

$$SN = \frac{2\pi(Pa + Ts(At + Mt + Bt))}{Ni}$$

SN = Number of sensors required
Pa = protected area radius
Ts = anticipated threat speed
At = alert or announcement time required
Mt = pre-movement time expected
Bt = behavioral intervention action time
Ni = sensor node interval required

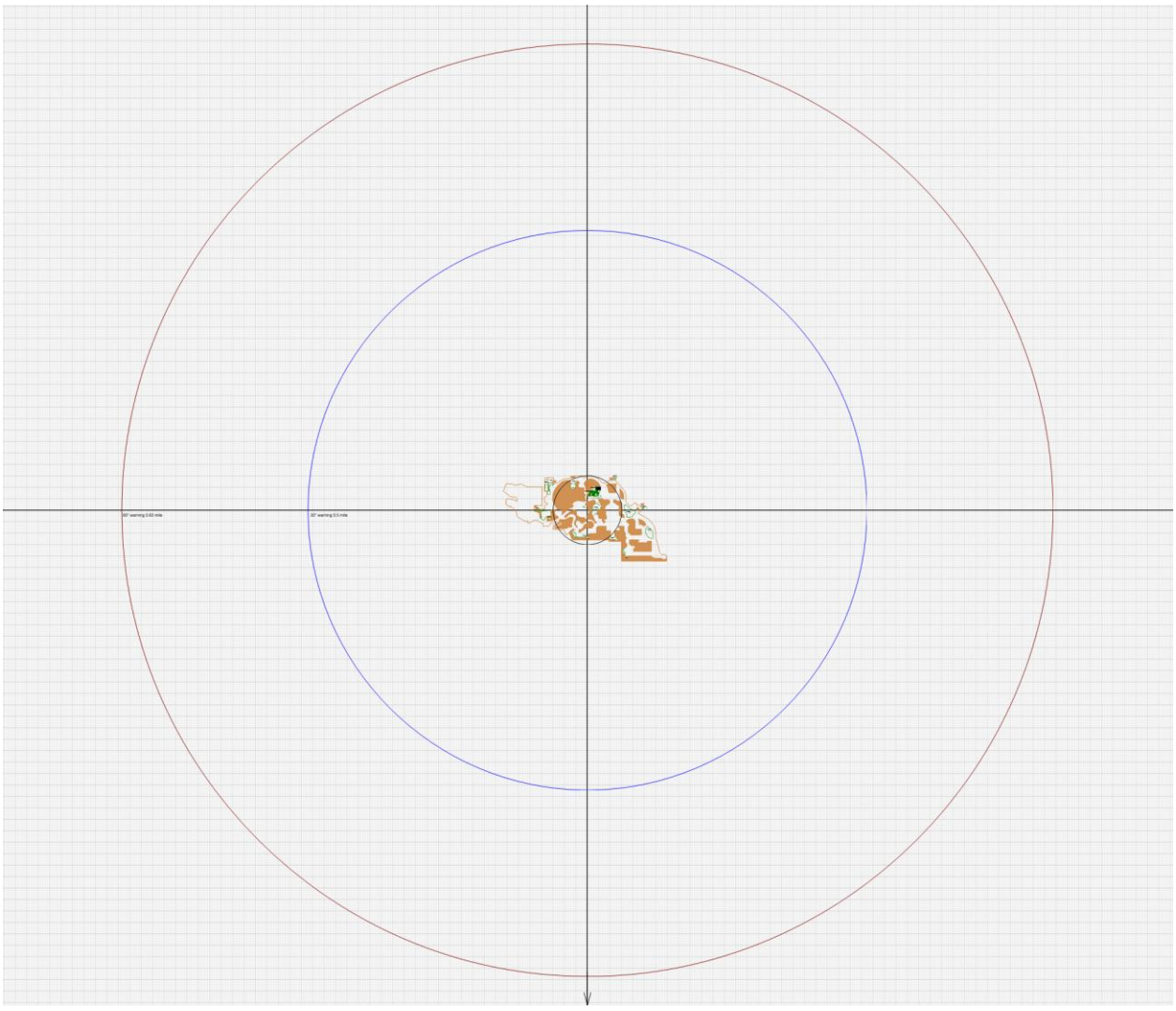

Figure 24. Scale model of the radius required for two timed intervention categories explored in this study. Blue represents a 30" threat warning and 0.5-mile radius, while red represents a 60" threat warning and a 0.83-mile radius requiring a network of 26 and 43 sensors respectively.

While the 60-second interventions were generally more effective at reducing casualties, the 30-second 5-meter separation group did not have a statistically significant difference in mean casualties at the 95% confidence level and would be more manageable to implement than a 60-second intervention.

5.5 Implications

Park design changes listed in Section 5.3 may work synergistically with warnings and behaviors to reduce casualties, but additional measures would be needed to reduce casualties to near zero. The implications of these interventions would apply to amusement parks, fairs, or outdoor concerts, but a different approach would be needed to account for high-density seated venues such as sports arenas, or stadium-seated concerts. The premovement times for seated venues would increase drastically, and netting or other mitigating barriers should be considered. The relationship between threat speed and sensor network footprint can be explored with the equation in Section 5.4. While regulating and lowering commercial sUAS speeds could greatly reduce a required sensor-network footprint, this would only account for Category II offenders, as Category III offenders would have the skills to build high-speed sUAS.

While a threat warning and behavioral interventions were successful at *mitigating* some casualties, it is clear that these two measures are not enough to reach a casualty *prevention* strategy. Active threat interdiction methods would need to be allowed to reach a true *prevention* strategy. Current U.S. law defines UAS as registered aircraft in the NAS and carries the same penalties for disrupting or destroying UAS and manned aircraft, precluding the use of C-UAS intervention technology. New definitions need to be adopted for UAS and separate laws need to be applied to the mistreatment and misuse of UAS platforms, as well as robust testing to minimize any ill effects to the NAS.

5.6 Further Investigation

Simulation models provide a valuable tool for testing theories or optimizing processes but must be designed at an appropriate level of abstraction to gather the insights desired without overcomplicating a project. This research base can be modified in a variety of different ways in the future to gain meaningful insights for further casualty mitigation strategies or amusement park design techniques. Buildings and doors could be modeled with set capacities to see if a mixture of going indoors and other interventions provides any additional benefit. Refinements of crowd panic effects could account for crushing and trampling injuries which could lead to improved park designs. Similarly, a tailorable signage system could be programmed and tested to direct patrons toward safe or low throughput areas to reduce casualties and maximize park safety. A crowd management system as proposed in Appendix F could allow for a greater patron situational awareness and help direct traffic to open exits or less dense areas for more effective separation interval implementation. Other types of hazards could be programmed into a model to determine parameters that lead to safer outdoor high-density event layouts. Additional testing of hunter-type drones or other illegal C-UAS interventions could be added to gauge the reduction of the required sensor footprint in future simulation studies.

The best interventions presented and modeled in this study were able to reduce casualties by as much as 63% when compared to the control group. A significant downside to the interventions proposed is the massive footprint required to implement. At the 30-second intervention interval, the sensor networks span 1 mile in diameter. Once specific C-UAS parameters are developed and standardized, their characteristics may be modeled to see if the casualty reducing benefit of this technology might necessitate a thorough review and subsequent legalization of these systems at high-density events. Hopefully, the future legal climate and C-

UAS solutions will reduce potential casualties further and reduce the span of the required sensor network to a more manageable size.

CHAPTER 6. CONCLUSION

This study sought to explore if there were alternative and legal threat sUAS mitigation strategies for high-density outdoor events since the use of C-UAS technology is mostly illegal for non-federal entities within the United States. This study provided evidence for several patron dispersive behaviors and time implementations that reduced casualties in an amusement park setting as tested through the method of simulation modeling. Patron separation intervals proved to be the overall best intervention strategy across three separate time domains and were most effective with a 60-second behavior implementation and a 5-meter goal separation interval – reducing casualties by 61% when compared to the control group.

There was evidence to suggest that evacuations may provide a casualty reduction in a drone attack sequence if proper threat warning is given to the patrons to act. The control group, which had no change in behavior before the drone attack, had the highest average casualties of all tested incidences. Park designs may affect casualty rates during an attack, as hard corners, limited throughput exits, tight corridors, and rigid serpentine queues were common threat target areas.

The footprint required to conduct the proposed interventions is massive, spanning 1 mile in diameter, largely to account for the high speeds of modern quad-copter style drones. The future use of C-UAS technology may provide additional benefits to casualty reduction as well as reducing the sensor network footprint to a more manageable size. Currently, the C-UAS industry lacks testing standards to verify the reliability of equipment and operations and is reserved for legal implementation by the DoD, DOE, DOJ, and DHS. This current climate makes advances and testing difficult, stifling meaningful growth, while current illegal drone threat concerns continue to advance unfettered by any legal recourse.

REFERENCES

Aagaah, M. R., Fleanha, E. M., & Mahmoudian, N. (2018). *Drone having drone-catching feature* (Patent No. US 10,005,556 B2).

ANSI unmanned aircraft systems standardization collaborative (UASSC). (2020, March). https://www.ansi.org/standards_activities/standards_boards_panels/uassc/overview?menuid=3

AnyLogic: Simulation Modeling Software Tools & Solutions for Business. (2020, July). https://www.anylogic.com/

Benyamin, M., & Goldman, G. H. (2014). *Acoustic Detection and Tracking of a Class I UAS with a Small Tetrahedral Microphone Array:* Defense Technical Information Center. https://doi.org/10.21236/ADA610599

Christnacher, F., Hengy, S., Laurenzis, M., Matwyshuck, A., Naz, P., Schertzer, S., & Schmitt, G. (2016). Optical and acoustical UAV detection. *SPIE*, *9988*(99880B). https://doi.org/10.1117/12.2240752

Cline, T. L., & Dietz, J. E. (2020). Agent Based Modeling for Low-cost Counter UAS Protocol in Prisons. *International Journal of Aviation, Aeronautics, and Aerospace*, *7*(2), 18.

Cline, T. L., Lercel, D., Karabiyik, U., & Dietz, J. E. (2020). *The Current State of Counter Unmanned Aerial System Policy in the U.S. 7*, 13.

Dietz, J. E. (2018, September 20). *Michigan City State Prison* [Personal communication].

DJI Phantom 4 Pro – Specs, Tutorials & Guides – DJI. (2019). DJI Official. https://www.dji.com/phantom-4-pro/info

Drone wars: How 'off-the-shelf' drones are changing the way wars are fought. (2018, May 28). Global News. https://globalnews.ca/news/4236518/the-new-drone-warfare/

Drones ground flights at Gatwick. (2018, December 20). *BBC News*. https://www.bbc.com/news/uk-england-sussex-46623754

Dukowitz, Z. (2018, September 28). *The NFL Makes a Case for Counter Drone (CUAS) Programs*. UAV Coach. https://uavcoach.com/nfl-cuas/

Electronic Code of Federal Regulations (eCFR). (2020). [Text]. Electronic Code of Federal Regulations (ECFR). https://www.ecfr.gov/

FAA aerospace forecast, fiscal years 2019-2039. (2019). [Aerospace Forecast]. Federal Aviation Administration. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/unmanned_aircraft_systems.pdf

FAA drone advisory committee (p. 148). (2019). [DAC 10/17/2019 Notes].

Goodrich, M. (2016, January 7). *Drone catcher: "robotic falcon" can capture, retrieve renegade drones*. Michigan Technological University. https://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html

Google Maps. (2020, September 16). Google Maps. https://www.google.com/maps/@40.4459074,-87.0385316,2971m/data=!3m1!1e3

Goppert, J. M., Wagoner, A. R., Schrader, D. K., Ghose, S., Kim, Y., Park, S., Gomez, M., Matson, E. T., & Hopmeier, M. J. (2017). Realization of an Autonomous, Air-to-Air Counter Unmanned Aerial System (CUAS). *2017 First IEEE International Conference on Robotic Computing (IRC)*, 235–240. https://doi.org/10.1109/IRC.2017.10

Gramer, R. (2017, January). *Afghan insurgents use drones in fight against U.S. – Foreign Policy*. Foreign Policy. https://foreignpolicy.com/2017/01/31/afghanistan-insurgents-use-drones-in-fight-against-u-s-nato-coalition-forces-unmanned-aerial-vehicles-future-warfare/

Grigoryev, I. (2018). *Anylogic in three days: A quick course in simulation modeling* (Fifth edition).

Grossman, N. (2018, August). *Analysis | Are drones the new terrorist weapon? Someone tried to kill Venezuela's president with one.* Washington Post. https://www.washingtonpost.com/news/monkey-cage/wp/2018/08/10/are-drones-the-new-terrorist-weapon-someone-just-tried-to-kill-venezuelas-president-with-a-drone/

Harvey, K. (2018, May 18). *State invests $35k on pilot program to keep unwanted drones out of prisons | KBAK*. https://bakersfieldnow.com/news/investigations/state-invests-35k-on-pilot-program-to-keep-unwanted-drones-out-of-prisons

Historical Households Tables. (2019). The United States Census Bureau. https://www.census.gov/data/tables/time-series/demo/families/households.html

Humphreys, T. (2015). *Statement on the security threat posed by unmanned aerial systems and possible countermeasures*.

Is there a specific distance implied when the FAA says "visual line-of-sight"? (2020). Drone Pilot Ground School. https://www.dronepilotgroundschool.com/kb/is-there-a-specific-distance-implied-when-the-faa-says-visual-line-of-sight/

Jones, M. (2020, January 14). This Is Why You Never Hear Airplanes in Disney Parks. *Reader's Digest*. https://www.rd.com/article/no-airplanes-in-disney/

Kirby, A. (2016). *Comparing Policy Decisions for Active Shooters Using SImulation Modeling*. Purdue University.

Kirby, A., Anklam, C. E., & Dietz, J. E. (2016). Active shooter mitigation for gun-free zones. *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, 1–6.

Kirby, A., Dietz, J., Matson, E., Pekny, J., & Wojtalewicz, C. (2014). Building Resilience in a Major City Evacuation Plan Using Simulation Modeling. *10th Annual Conference of the International Institute for Infrastructure Renewal and Reconstruction*, 114–120. https://doi.org/10.5703/1288284315350

Kotowski, J. (2018). Drones used to deliver drugs, cellphones and other contraband to Delano prison, documents say. *TCA Regional News*. http://search.proquest.com/docview/2015026811/

Lee, J. Y. (2019). *Agent-based modeling to assess the effectiveness of run hide fight*. Purdue University.

Llenas, B. (2017, April 6). *Terrorist drone threat: US unprepared for growing danger, experts say | Fox News*. https://www.foxnews.com/tech/terrorist-drone-threat-us-unprepared-for-growing-danger-experts-say

Matson, E. T. (2018, November 12). *Malicious use of autonomous technology threatens public safety—Dawn or Doom*. https://polytechnic.purdue.edu/newsroom/matson-malicious-use-of-autonomous-technology-threatens-public-safety

McCabe, J. (2020). *ANSI UASSC standardization roadmap for unmanned aircraft systems*. 412.

Michel, A. H. (2018). *Counter-drone systems* (p. 23). Bard College. https://dronecenter.bard.edu/publications/

Michel, A. H. (2019). *Counter-drone systems* (2nd Edition; p. 45). Bard College. https://dronecenter.bard.edu/publications/

OLRC USC. (2020, March). Office of the Law Revision Counsel United States Code. http://uscode.house.gov/browse/&edition=prelim

Rinne, T., Tillander, K., & Grönberg, P. (2010). Data collection and analysis of evacuation situations. *VTT Tiedotteita Research Notes 2562*, 145.

Sargent, R. G. (2011). Verification and validation of simulation models. *2011 Winter Simulation Conference*, 183–198.

Schroth, L. (2019, October). Drone Manufacturer Market Shares: DJI Leads the Way - DRONEII.com. *Drone Industry Insights*. https://www.droneii.com/drone-manufacturer-market-shares-dji-leads-the-way-in-the-us

Shayanian, S. (2018, July 2). *Gang may have used drones to help Redoine Faid escape prison—UPI.com*. UPI. https://www.upi.com/Top_News/World-News/2018/07/02/Gang-may-have-used-drones-to-help-Redoine-Faid-escape-prison/7801530538554/

Siewert, S., Andalibi, M., Bruder, S., Gentilini, I., & Buchholz, J. (2018). Drone net architecture for UAS traffic management multi-modal sensor networking experiments. *2018 IEEE Aerospace Conference*, 1–18. https://doi.org/10.1109/AERO.2018.8396716

Small Unmanned Aircraft Systems, 14 C.F.R.§ 107 (2019)., Electronic Code of Federal Regulations § Part 107—Small Unmanned Aircraft Systems (2019), Source: Docket FAA-2015-0150, Amdt. 107-1, 81 FR 42209, June 28, 2016, unless otherwise noted. https://www.ecfr.gov/cgi-bin/text-idx?SID=3f50729cff2b56a549c4515c703eda34&mc=true&node=pt14.2.107&rgn=div5

Stadiums vulnerable to drone attacks & intrusions | CERBAIR. (2019). https://www.cerbair.com/after-gatwick-could-sports-venues-be-the-next-great-drone-debacle-blog/

TC 3-23.30 Grenades and pyrotechnic signals. (2013). Department of the Army.

TM 3-22.31 40-mm Grenade launchers. (2010). Department of the Army.

Tzvetanov, K., Riegsecker, A., Frantz, B., Xiong, C., Bott, R., Cline, T., Dietz, J. E., & Dubiel, B. (In press). Agent-based modeling for theme park evacuation. *Journal of Emergency Management*.

UAS - Critical Infrastructure | CISA. (2020, April). https://www.cisa.gov/uas-critical-infrastructure

Unauthorized drone flies over Disney, Universal. (2015, January 30). WKMG. https://www.clickorlando.com/news/2015/01/30/unauthorized-drone-flies-over-disney-universal/

United states: Drones pose new contraband, smuggling challenge for prisons. (2016). *Asia News Monitor*.

Wallace, R., & Loffi, J. (2015). Examining unmanned aerial system threats & defenses: A conceptual analysis. *International Journal of Aviation, Aeronautics, and Aerospace*. https://doi.org/10.15394/ijaaa.2015.1084

APPENDIX A: THE STATE OF C-UAS IN THE U.S.

This section represents a manuscript that was submitted by the author to the International Journal of Aviation, Aeronautics, and Aerospace and published in October 2020.

Citation:

Cline, T. L., Lercel, D., Karabiyik, U., & Dietz, J. (2020). The Current State of Counter Unmanned Aerial System Policy in the U.S. *International Journal of Aviation, Aeronautics, and Aerospace, 7*(3). Retrieved from https://commons.erau.edu/ijaaa/vol7/iss3/11

Small unmanned aerial systems (UAS), more commonly known as 'drones,' are an increasing security risk to fixed facilities due to their ease of use, high performance, and increasing prevalence. Prison systems have experienced incidents where drones were used to introduce contraband, such as cell phones, drugs, and weapons (Harvey, 2018; Otte, 2017). In December 2018, drones disrupted flights for an estimated 110,000 people over several days at London's Gatwick Airport ("Drones Ground Flights at Gatwick," 2018). Systems to counter UAS are rapidly being developed but are often unattainable by a majority of organizations due to high cost, liability concerns, and regulatory restrictions.

The FAA Reauthorization Act of 2018 defines counter unmanned aerial system (C-UAS) technology as "a system or device capable of lawfully and safely disabling, disrupting or seizing control of an unmanned aircraft or unmanned aircraft system" (p. 100). For this paper, C-UAS will include active measures to detect and interdict unwanted UAS traffic by a facility or entity. While geofencing has proven beneficial in deterring casual drone users from overflying restricted or otherwise sensitive areas, it is largely dependent on the drone manufacturer to implement and may be easily disabled by the user. Since the protected facilities have no active control over geofencing it will not be considered a C-UAS.

Industry regulatory standards for C-UAS are in the process of being developed but are not yet implemented. Several governing bodies have been identified to develop technical standards within this field. A multitude of legal issues exist that prevent public and private organizations from conducting C-UAS operations due, largely, to a broad application of the term "aircraft" and subsequent measures to protect manned aviation. Currently, few Federal agencies are legally permitted to use C-UAS technology within the United States within the constraints outlined in

Public Law. This paper serves as a collective summary of the current state of C-UAS policy within the U.S. and highlights the current lack of industry standards and identifies major efforts to develop these standards.

Industry Regulatory Standards of C-UAS

As of December of 2019, the *Counter-Drone Systems* report highlighted that there are 537 C-UAS products and systems offered by over 277 different companies (Michel, 2019). It was noted that not a single manufacturer consulted in preparing the report was able or willing to provide operational or test data associated with their systems. This resultant C-UAS environment is one where manufacturers may publish performance specifications that are not established under a testing standard. From a consumer standpoint, this is concerning because manufacturer marketing claims may not match the operational performance of a system. In addition to this, many of the technical standards for drone technology are currently under development, making C-UAS more difficult to implement against the wide variety of methods being used by drone manufacturers (McCabe, 2020). Standardization of these technical aspects is one step toward the reliable performance that will help C-UAS become available outside of the Federal government.

Before a manufacturer sells a product within a market, the manufacturer must first determine if the product category is subject to any regulations or related industry standards. Regulations may require that a product adheres to certain technical specifications or testing standards (Standards Portal, 2020). Generally, these regulations are designed to protect the consumer. For example, a consumer purchasing gasoline that is not produced in accordance with approved specifications or standards could encounter costly vehicle repairs. Failing to adhere to the applicable laws and standards may result in manufacturers being subject to market denial, fines, imprisonment, or other penalties (Standards Portal, 2020). Governments rely on regulations and technical standards specifications generally established by professional bodies or standards organizations to ensure products follow industry best practices. Currently, no standards or regulations exist for C-UAS technology.

Standards Organizations

Several major standard-setting organizations within the U.S. oversee the development of standards within their respective areas of expertise. Examples of this include NSF International, which develops standards related to public health and safety, and the Society of Automotive Engineers International, which develop technical standards for self-propelled vehicles (Standards Developing Organizations, 2020). The American National Standards Institute (ANSI) is a non-profit standards organization that is made up of government, industry, and professional, technical, and trade societies. ANSI manages the establishment and implementation of thousands of standards across virtually all sectors of the economy (Grainger, 2020). ASTM International (formerly the American Society for Testing and Materials) serves similarly to ANSI and develops voluntary consensus standards for products, materials, systems, and services (Grainger, 2020).

Lack of C-UAS Technical Standards

In September 2017, ANSI stood up the Unmanned Aircraft Systems Standardization Collaborative (UASSC) in collaboration with the Federal Aviation Administration (FAA), the Department of Homeland Security (DHS), ASTM, and others, to help research and guide public policy and guidelines concerning the rapidly expanding UAS ecosystem (ANSI UASSC, 2020). The UASSC established a standardization roadmap to identify experts and stakeholders within facets of the UAS ecosystem and to guide efforts for standardization. The document acknowledges that "A comprehensive evaluation template for testing C-UAS systems is needed," and that "standards must be developed for user identification, design, performance, safety, and operations"(McCabe, 2020, p. 377). McCabe further reports that there is a general lack of standards within the C-UAS industry, noting a significant variance of effectiveness and reliability of these systems. "Detection and mitigation of unmanned aerial threats" was listed as a high priority, and noted that standards in-development are not generally known to the public, due to the sensitive nature of C-UAS implementation for entities entitled to mitigate UAS threats (McCabe, 2020). The USAAC has a comprehensive list of UAS related standards that are currently in development to meet the rapidly growing presence of UAS within the U.S.

Legal Issues Preventing C-UAS Implementation

Federal law prevents organizations from using C-UAS other than a few select federal agencies, such as the Department of Defense (DoD), the Department of Energy (DOE), the Department of Homeland Security (DHS), and the Department of Justice (DOJ). These specific use cases will be discussed in a later section. To better understand these legal concerns, it is important for one to know some of the current detection and interdiction methods. Generally, C-UAS systems work by identifying and potentially tracking an intrusive UAS with sensors designed to detect some characteristic of the UAS. Methods for detecting and tracking include radar, acoustic, electro-optical, radio-frequency, and infrared. Often two or more of these detection methods are used. For example, a coarse bearing and location can be used from a network of acoustic sensors to cue a fine-detect electro-optical sensor on to the target for classification and processing (Siewert et al., 2019).

Interdiction methods involve means to subdue, divert, or destroy an intrusive UAS and can be accomplished through a myriad of means. Table 1 represents a summary of some of the more popular methods employed to interdict a UAS. To successfully mitigate an unwanted UAS threat, a drone must first be detected by sensors, then interdicted by one of the methods discussed in Table 1. Many laws are currently in place that would prevent individuals and organizations from using these methods and carry heavy fines and potential prison time (Michel, 2019).

Table A.1 Types of Interdiction Methods Currently Employed

Sensor Type	Description
Radio Frequency (RF) Jamming	Interrupts the RF link between UAV and operator by generating large amounts of RF output. Once the RF link is disturbed, the UAV will land or return to the operator
GNSS Jamming	Interrupts the satellite link used for navigating. Once the satellite link is lost, UAV will hover or land
Spoof	Taking control of the UAV by hijacking the communications link
Kinetic	Destroys portions of the airframe with directed energy, causing a crash
Net	Entangles the UAV or its rotors
Projectile	Employs ammunition to destroy UAV
Combination	Several C-UAS methods employed – commonly tandem RF and GNSS jamming

Note. Descriptions are adapted from Michel (2018, p. 4)

The following represents several of the categories that carry legal implications for the use of C-UAS technology.

Federal Communications Commission (FCC)

The FCC is an independent Federal regulatory agency that regulates domestic and international communications within the U.S. and is the primary authority for communication law and regulation. The FCC is responsible for Title 47 of the Combined Federal Regulations (CFR) and is granted authority through Title 47 of the United States Code (U.S.C.) (FCC, 2010). Title 47 (U.S.C.) Section (§) 301 requires licenses for entities to operate radio transmitters and compliance with FCC regulations. This would require entities to acquire authorization and licenses for the use of any radar UAS detectors, and RF and GPS jamming equipment. Title 47 U.S.C. § 302(a) prohibits the sale and use of devices that interfere with radio reception. Similarly, Title 47 U.S.C. § 333 prohibits maliciously or willfully interfering with any radio communications with a licensed station. This would directly preclude the sale and use of applicable RF and GPS jamming and spoofing operations. In 2016, a Chinese company was ordered to pay over $34 million to the FCC for the sale of signal jammers on their website (Rupprecht Law, 2020). The FCC related laws preclude several of the more popular interdiction methods commonly used by the federal government to include spoofing and jamming.

Criminal Code

Small unmanned aircraft are required to register with the Federal Aviation Administration (FAA) per Title 14 C.F.R. § 48.15 in which the definition of "aircraft" is adopted from Title 49 U.S.C. § 40102 as "any contrivance invented, used, or designed to navigate, or fly in, the air." The application of this regulation to UAS inherently implies that small UAS are subject to many of the same laws that apply to larger manned aircraft. Therefore, any individual or organization that interdicts a small UAS may be subject to the same penalties imposed for larger manned aircraft.

Title 18 U.S.C. § 32 prohibits willful disablement, destruction, and damage to any aircraft within the jurisdiction of the United States, and carries a hefty fine and up to a 20-year prison sentence. This statute bans the use of kinetic, net, projectile, and other potentially destructive means of interdicting a small UAS. . Additionally, many Title 47 statutes that prevent C-UAS include a reference to Title 18 statutes, which carry fines or prison sentences as well. Title 18 U.S.C. § 1367 prohibits the interference with satellite transmissions and carries the penalty of a fine and a prison sentence of up to ten years.

Federal Aviation Administration (FAA)

The FAA established Title 14 C.F.R. § 107 to integrate UAS into the National Airspace System (NAS). Part 107 covers registration, certification, and operational regulations and procedures required to operate a civil small UAS within the U.S. From a legal perspective, an entity that successfully spoofs the UAS link and takes control of the aircraft is required to comply with Title 14 C.F.R. § 107. This requires a successful spoofer to have appropriate FAA certifications, airspace waivers (if applicable), and established a pilot in command for the flight. Additionally, the spoofer is responsible for the condition of the aircraft and the safety of the remaining flight (*Rupprecht Law*, 2020). In essence, the spoofer becomes completely liable for the aircraft and anything that happens for the remainder of the flight. Spoofing has possible additional penalties under Title 49 U.S.C. § 46308, in which a penalty of fines and up to 5 years imprisonment for a person with an intent to interfere with air navigation by interfering with a "true light or signal."

A 2019 FAA letter to airports reiterates some of the criminal penalties that could be leveraged from C-UAS implication and continues to cite some of the additional concerns with airport-specific implementation (FAA C-UAS letter to airports, 2019). This letter discusses the use

of UAS sensors as a potential point of contention due to the emissive properties of many of the sensors. For example, while audio sensors are typically considered passive, they are typically required to be networked to other sensors and processing stations to locate and identify threats properly. This is typically through wireless networking between components of the system. The FAA letter cites Title 14 C.F.R. § 77 which requires airports to notify the FAA for any planned airport alterations and sets standards for determining if they cause obstructions to air navigation (FAA C-UAS Letter to Airports, 2019). Additionally, the FAA cautions the use of UAS detection systems due to potential unknown effects on the navigational facilities and transmitters (NAVAIDs) used by pilots to navigate the national airspace. The letter also cites Title 14 C.F.R. § 139.333, requiring the protection of NAVAIDs as part of the airport certification process. While the FAA acknowledges the potential threat that UAS present, it certainly does not condone the casual use of even passive C-UAS technology for airports.

Legal C-UAS Implementation

Several federal entities are allowed to legally conduct C-UAS per public law. The National Defense Authorization Act (NDAA) FY 2017 allows C-UAS implementation to the Department of Energy (DOE) and the Department of Defense (DoD). Division H of The FAA Reauthorization Act of 2018, also cited as the Preventing Emerging Threats Act of 2018, subsequently grants similar C-UAS implementation to the Department of Justice (DOJ) and the Department of Homeland Security (DHS).

Authorized C-UAS Actions

Both the NDAA 2017 and FAA Reauthorization Act of 2018 use similar verbiage to authorize C-UAS actions to the DoD, DOE, DOJ, and DHS. However, the context and justifications in which C-UAS actions may be employed differ between departments. In general, the DoD and DOE have slightly more freedom to execute actions to "mitigate the threat… to the safety or security of a covered facility or asset" (NDAA, 2017, pp. 641, 758) when compared with the DHS and DOJ actions being limited executing actions to "mitigate a credible threat…to the safety or security of a covered facility or asset" (FAA Reauthorization Act of 2018, p. 339). All four agencies' respective Secretaries are required to consult with the Secretary of Transportation

for implementation of these C-UAS actions. This is primarily to mitigate and monitor negative impacts to the National Airspace System. The FAA Reauthorization Act of 2018 and the NDAA 2017 list the following broad actions permitted for UAS threat mitigation by the DoD, DOE, DHS, and DOJ:

- Detect, identify, monitor and track UAS
- Warn the UAS operator
- Disrupt control of the UAS
- Seize or exercise control of the UAS
- Use reasonable force to disable, damage, or destroy the UAS

Permitted DoD and DOE C-UAS Justifications

The primary difference between each of the respective agencies' ability to conduct C-UAS lies in how a 'covered facility or asset' is defined for each agency. Each of the respective agencies' secretary can define a covered asset or facility within the scope of the agency's responsibilities and under broad guidelines outlined in legislation. The NDAA 2017 (p. 759) defines a covered facility or asset for the DOE as one which is owned by the United States and is used to store or use special nuclear material. Essentially, nuclear facilities are covered and the DOE can take the listed actions above to protect these facilities.

The DoD's 'covered facility or asset' is one that the Secretary of Defense identifies, is within the United States (or territories), and relates to the DoD's nuclear deterrence mission, missile defense mission, or national security space mission NDAA 2017 (p. 642). It is important to note that these restrictions apply only within the United States, and there are tactical guidelines to dispatch unwanted UAVs in combat situations. These provisions allow the DoD to continue strategic missions and deal with potential UAS threats appropriately.

Permitted DOJ and DHS C-UAS Justifications and Additional Restrictions

The DOJ and DHS have more restrictions and additional requirements placed upon them for C-UAS activities as outlined in the FAA Reauthorization Act of 2018 when compared to the DOE and DoD, likely due to the immediate gravity of possible consequences from unmitigated UAS threats from the 'covered facilities or assets' overseen by the DOE and DoD. Both the DOJ

and DHS are authorized to take the common C-UAS actions for National Special Security Events and Special Event Assessment Rating events, at the request of the Governor for a specific time and specific event, and to protect active Federal law enforcement investigations, emergency response, or security functions that are also limited for a specific time and event (FAA Reauthorization Act of 2018, p. 344).

The DOJ is also permitted to take C-UAS action to protect the President of the United States and Attorney General, as well as federal detention centers, correctional facilities, and buildings, to include courts, that are owned or operated by the DOJ. The U.S. Marshals Service is somewhat unique in that it is specifically listed to protect certain persons instead of 'facilities or assets' and can take C-UAS action to protect "Federal jurists, court officers, witnesses and other threatened persons in the interest of justice" (FAA Reauthorization Act of 2018, p. 344). The U.S. Attorney General recently published department guidance on the implementation of this Act, describing the processes in which covered facilities will be identified, required risk-based assessments, and other measures designed to preserve First and Fourth Amendment rights (Barr, 2020).

The DHS has several other justifications for taking C-UAS action that are separate from the shared justifications with the DOJ. The DHS is authorized to use C-UAS actions for security and protection functions related to U.S. Customs and Border Protection, Secret Service protection operations, and to protect buildings and facilities occupied or secured by the Federal Government (FAA Reauthorization Act of 2018, p. 344).

The United States Coast Guard (USCG) falls under the purview of the DHS but has unique justifications for authorized use of C-UAS actions and is separately mentioned in the FAA Reauthorization Act of 2018. The 'covered facility' for the USCG is one that is under the administrative control of the Commandant USCG or a vessel or aircraft that is involved in a USCG mission. The USCG may execute C-UAS actions involving a mission escorting or assisting a DoD vessel, other high value or high personnel vessels, to protect the POTUS and VPOTUS, as well as in search and rescue operations (FAA Reauthorization Act of 2018, p. 347).

A summary of the C-UAS implementation for Federal entities can be found in Table 2.

Table A.2 Federal C-UAS Authorized Activity

	Department				
	DoD	DOE	DOJ	DHS	USCG*
Grounds	Facility or asset identified by the Secretary of Defense	Facility or asset identified by the Secretary of Energy	Facility, asset, or persons identified by the Attorney General (DOJ) or Secretary of Homeland Security (DHS) as high-risk and a potential target of unlawful unmanned aircraft activity		Facility under control of the Commandant or a vessel or aircraft operated by, assisted by, or otherwise involved in a mission with the USCG
Location	Located within the United States or one of its territories				Not explicitly bound by location
Justifications	1) Nuclear deterrence mission 2) Missile defense mission 3) National security space mission	1) Storage or use of nuclear material	1) National Security Special Event 2) Special Event Assessment Rating 3) At the request of a Governor 4) Protect active Federal investigation 5) FBI: protection of POTUS and AG 6) Marshals: protection of personnel involved in Federal trial 7) Protection of correctional facilities, courts, and other DOJ buildings	5) U.S. Customs and Border Protection 6) Secret Service protection operations 7) Protection of Federal buildings USCG	1) Assistance or escort mission for DoD 2) Assistance or escort mission for a vessel of national security significance, or a high interest, capacity, or value vessel 3) Protection of the POTUS and VPOTUS 4) National Security Special Event 5) Special Event Assessment Rating 6) Air Defense of US 7) Search and rescue mission

Note. United States Coast Guard (USCG) falls under DHS but has separate grounds and authorized C-UAS justifications

In addition to the necessary coordination with the Department of Transportation and the FAA for all C-UAS activities, both the DOJ and DHS have additional requirements and restrictions placed upon them. Both departments are required to "establish research, testing, training on, and evaluation of" equipment used for C-UAS before its implementation in the field (FAA Reauthorization Act of 2018, p. 340). Other restrictions on the two departments include civil privacy protections to preserve First and Fourth Amendment rights. Both the DOJ and DHS are only allowed to keep electronic communications and data regarding C-UAS actions for up to 180 days and are prohibited from sharing such information outside of their respective departments unless the Secretary of Homeland Security or Attorney General determines that the information is

necessary for prosecution or purposes of ongoing litigation (some exclusions apply to both of these rules). Additionally, semi-annual briefings are required to appropriate Congressional subcommittees regarding any previously mentioned exclusions and activities related to C-UAS policy and efforts (FAA Reauthorization Act of 2018, p. 341-342).

Conclusion

C-UAS implementation and policy are still in the early stages within the United States. As the UAS threat becomes more prevalent, reliable and accessible C-UAS options will need to be available to public agencies and private industry most at risk for drone threats. For this industry to mature, performance standards and testing metrics will need to be developed and adopted that pose minimal adverse effects to the National Airspace System. Once standards are set, new legal definitions can be applied to the equipment in use for manufacturer compliance, and implementation by non-federal entities. The required DHS and DOJ research and testing, coupled with the required semi-annual briefings to the appropriate Congressional committees, may serve as a responsible way to gather insights and data for wider C-UAS adoption. New legal definitions may be needed for UAS to prevent the hefty penalties that may be imposed for their interdiction.

References

7 big problems with counter drone technology (drone jammer, anti drone gun, etc.). (2020, March). https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems

ANSI unmanned aircraft systems standardization collaborative (UASSC). (2020, March). https://www.ansi.org/standards_activities/standards_boards_panels/uassc/overview?menuid=3

Barr, W. (2020). *Department activities to protect certain facilities or assets from unmanned aircraft and unmanned aircraft systems*. Retreived from https://www.justice.gov/ag/page/file/1268401/download

Drones ground flights at Gatwick. (2018, December 20). *BBC News*. https://www.bbc.com/news/uk-england-sussex-46623754

Electronic Code of Federal Regulations (eCFR). (2020). [Text]. Electronic Code of Federal Regulations (ECFR). https://www.ecfr.gov/

FAA Reauthorization Act of 2018, Pub. L. No. 115–254, 463 (2018).

Harvey, K. (2018, May 18). *State invests $35k on pilot program to keep unwanted drones out of prisons | KBAK*. https://bakersfieldnow.com/news/ investigations/state-invests-35k-on-pilot-program-to-keep-unwanted-drones-out-of-prisons

McCabe, J. (2020). *ANSI UASSC standardization roadmap for unmanned aircraft systems*. 412.

Michel, A. H. (2019). *Counter-drone systems* (2nd ed.). Bard College. https://dronecenter.bard.edu/publications/

National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114–328, 970 (2016).

Non-governmental agencies in the safety industry—Quick tips #100—Grainger industrial supply. (2020, March). Understanding ANSI, ASTM International, FM Global, NFPA, SEI, UL and CSA Group. https://www.grainger.com/content/qt-safety-ansi-astm-international-100

OLRC USC. (2020, March). Office of the law revision counsel United States Code. http://uscode.house.gov/browse/&edition=prelim

Otte, J. (2017, November 7). *Drones dropping drugs into prisons; Ohio fights back.* Dayton Daily News. https://www.daytondailynews.com/news/drones-dropping-drugs-into-prisons-ohio-fights-back/GSB3jLP3sy9VMVWiaO31KM/

Siewert, S. B., Andalibi, M., Bruder, S., & Rizor, S. (2019, January 7). Slew-to-cue electro-optical and infrared sensor network for small UAS detection, tracking and identification. *AIAA Scitech 2019 Forum*. AIAA Scitech 2019 Forum, San Diego, California. https://doi.org/10.2514/6.2019-2264

Standards Developing Organizations (SDOs). (2020). https://www.standardsportal.org/usa_en/resources/sdo.aspx

Steps to determine technical requirements for market access. (2020, March). https://www.standardsportal.org/usa_en/key_information/technical_requirements.aspx

UAS detection and countermeasures technology at airports. (2019, May 7). https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf

What we do. (2010, November 22). Federal Communications Commission. https://www.fcc.gov/about-fcc/what-we-do

Definitions

§	Section (generally used in reference to regulations and statutes)
C-UAS	Counter Unmanned Aerial System(s)
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
FAA	Federal Aviation Administration
NAVAID	Aerospace Navigational Aid
POTUS	President of the United States
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
SECDEF	Secretary of Defense
VPOTUS	Vice President of the United States

APPENDIX B: AGENT BASED MODELING FOR LOW-COST COUNTER UAS PROTOCOL IN PRISONS

This section represents a manuscript that was submitted by the author to the International Journal of Aviation, Aeronautics, and Aerospace and published in April, 2020.

Citation:

Cline, T. L., & Dietz, J. (2020). Agent Based Modeling for Low-cost Counter UAS Protocol in Prisons. International Journal of Aviation, Aeronautics, and Aerospace, 7 (2). https://doi.org/10.15394/ ijaaa.2020.1462

INTRODUCTION

Threat background

As technology advances and computing power continues to become more and more miniaturized, commercial small unmanned aerial systems (sUAS), more commonly known as "drones," are becoming more prevalent. These systems are defined by the Federal Aviation Administration (FAA) in Title 14 of the Code of Federal Regulations (C.F.R.) § 107.3 as a small unmanned aircraft and its associated elements. While there are many beneficial uses of sUAS including photography, building and tower surveys, search and rescue applications, and geospatial uses, there are more nefarious uses that are concerning from a physical security standpoint. Drones have been used to attack the Venezuelan president, land undetected on the property of the White House, and to deliver crude explosives to troops in the Middle East (Gramer, 2017; Grossman, 2018; Wallace & Loffi, 2015). Indeed, current physical security protocols are proving too costly or ineffective to stop unwanted sUAS activity.

Within the United States, an alarming number of prisons have reported use sUAS to drop contraband to inmates. Reports from Maryland, Ohio, Oklahoma, Tennessee, South Carolina, and other states have described the use of these systems to air-drop heroin, cell phones, and blades to prisoners ("United States," 2016). In California, 45 "unauthorized drone intrusions" were recorded between July 2017 and May 2018, some of which were found to have successfully smuggled cell phones, drugs, and saw blades putting correctional officers and other inmates at risk (Harvey, 2018; Kotowski, 2018). In South Carolina, a drone was used to give personnel locations and deliver wire-

cutters to assist a convict in a prison break. After a manhunt, the criminal was re-apprehended ("Dedrone," 2019).

Challenge

Many prisons struggle to implement an effective counter unmanned aerial systems (C-UAS) detection program tailored to the typical UAS threat they encounter and do not have enough funding for a robust C-UAS protocol (Otte, 2017). Additionally, even well-funded organizations are finding effective C-UAS solutions for fixed sites a challenge, as evidenced by a March 2019 solicitation by the Department of Defense admitting, "It has proven difficult to identify and mitigate threats," in regard to its bases, installations, and facilities (NC DefTech, 2019). Common characteristics of UAS intrusions to prisons include using minimally modified commercial off-the-shelf platforms from manufacturers such as DJI and Yuneec. This gives threat sUAS some unique characteristics that can be used to develop tailored and low-cost solutions that are specific to this problem.

Modeling and UAS Security

Currently, the ability to interdict drones is illegal outside of certain Federal entities. Agent-based modeling may serve as an appropriate venue to test counter UAS policies and techniques without legal consequences. Technical data can be programmed into a model to represent a geographical space, a sensor, an interdiction device, a threat UAS, and a facility footprint. Modeling may be an appropriate method to provide data to guide policy revisions involving counter UAS operations. Once a model is built, it can be used to validate the security procedures of a fixed site, while different scenarios can be used to test and refine the security policy and implementation. This data may provide lawmakers with insights to make legal revisions necessary for corporations and non-federal entities to protect themselves with C-UAS technology currently restricted from use.

Research Question

Given a hypothetical C-UAS sensor performance data and fixed C-UAS interdiction characteristics, what are the effects of a threat unmanned aerial vehicle's speed on detection and interdiction of a C-UAS designed to protect a 40-acre facility from threat UAS overflights?

LITERATURE REVIEW

Threat UAS Characteristics

FAA sUAS guidelines affecting manufacture.

Current threats to U.S. prison systems involve 'low-tech' offenders using commercially available sUAS from manufacturers such as DJI, Yuneec, and Parrot and minimally modifying them for the purposes of intrusive overflight and contraband smuggling. Manufacturers adhere to FAA regulations regarding the use of and operation of sUAS, which gives these threats several common characteristics that can be used in detecting, tracking, and integrating interdiction methods.

Title 14 C.F.R §107.31 requires that a remote pilot is within visual line of sight of the sUAS at all times and able to re-direct the aircraft (e-CFR, 2019). Typically this will place the remote pilot no further than one mile from the aircraft where visual tracking and obstacle avoidance becomes very challenging (UAV Coach, 2020). The control channel for DJI offerings, such as the Phantom 4, typically send control inputs from the radio control module on the 2.4 GHz wavelength, and image transmission is broadcast back from the aircraft to the control station over the 5.8 GHz wavelength (DJI, 2019). DJI reports the controllable signal strength of this UAS to be just over four miles. A similar Yuneec offering, the Typhoon 4K, transmits control inputs over the 2.4 GHz bandwidth and sends video signals back to the control system over the 5.8 GHz range as well (Yuneec, 2018). This control transmission architecture is not uncommon for commercial offerings and may be used to interdict trespassing sUAS. This also excludes the possibility of legal autonomous flight and requires that a remote controller can control the aircraft, as opposed to the capability of 'high-tech' offenders to use pre-programmed GPS waypoints and flight routes for autonomous flight.

Title 14 C.F.R. §107.29 restricts sUAS operation during night hours. While the flight performance characteristics are not different at night, most of the control systems for commercial sUAS involve visual sensors for flight orientation and obstacle navigation. Night flight is therefore difficult without upgrading to expensive night visual optics and possible aircraft modifications, which would push the offender into the 'high-tech' category as well. For the purposes of this paper, 'low-tech' threats will be considered and modeled, as they are the primary sUAS threat encountered by prisons.

Popular sUAS performance characteristics.

The primary threat and common thread in the reviewed cases of unwanted UAS intrusions involving prisons is using commercial-off-the-shelf platforms with slight modifications for accepting and jettisoning a payload. The DJI Phantom 4 Pro is a popular UAS and can fly up to a maximum of 45 mph in ideal atmospheric conditions and in a clean configuration with no payload (DJI, 2019). This UAS has a retail price of approximately $1,700 and requires an Apple iPhone or iPad to operate. Additionally, DJI offers a robust and powerful flight control software that is intuitive and ideal for low experience sUAS pilots. This aircraft is consistent with the price point, power and specifications of reported prison intrusions and will be used as an initial basis from which to model flight behavior (Rubens, 2018).

C-UAS Sensor Types and Characteristics

As of December of 2019 a report highlighted that there are 537 C-UAS products and systems offered by over 277 different companies (Michel, 2019). The products range from detection only, interdiction only, or a mix of both. Detection methods include radar, radio-frequency tracking, electro-optical, infrared, acoustic, and mixed sensors. No single detection method has proven to be without fault, so often integrated systems use a mix of detection sensors. Interdiction methods can include radio-frequency jamming, global positioning system (GPS) jamming, spoofing, laser, nets, and projectiles (Michel, 2019). Table 1 represents a brief summary of UAS detection sensors.

Table B.1 Types of Detection Sensors and Descriptions

Sensor Type	Description
Radar	Detects radar signature by emitting radio wave pulses and analyzing return energy to determine the range, angle, and velocity
Radio-Frequency	Detect UAS presence by scanning commonly used UAS bands such as 2.4 GHz and 5.8 GHz, may be able to determine location with complex antennas and multiple sensor locations
Electro-Optical	Detect UAS based on the visual signature of the UAS aircraft
Infrared	Detect UAS based on the infrared signature emitted by the UAS aircraft
Acoustic	Detect changes in sound by using microphones and software filters to match data from a database UAS audio signatures

Note. Descriptions are adapted from Michel (2018, p. 4).

For the purposes of this study, the hypothetical sensor used in modeling will be largely based on integrated acoustic UAS sensors since there is very limited data available with other sensors that can be used for simulation modeling, and this sensor type is typically lower in cost than other sensor types.

Acoustic sensor characteristics.

Acoustic means of sUAS detection typically rely on microphone arrays that are coupled with audio analysis software. Simply stated, a microphone array consists of several microphones positioned at a single site with positional offsets that allow for bearing and azimuth estimations based on the slight differences between the timing and intensity of the sound reaching each microphone. The detection range of these systems can be affected by multiple elements such as microphone quality and sensitivity, ambient noise, weather conditions, and software packages.

French-German Research Institute of Saint-Louis (ISL) conducted audio drone detection testing using four Brüel & Kjaer type 4189 metrological microphones (Christnacher et al., 2016). The research team was only able to accurately detect (in azimuth and elevation) a customized drone 20 seconds away from the sensors when the drone was directly traveling towards the sensor. However, the sensor array was able to continuously track the drone for 45 seconds when it was flying away. In ISL's 2016 experiment, the audio sensor array reached the longest detection range of up to 300 meters when testing against the DJI Phantom 2 at an altitude ranging from 120 to 150 feet. While there is no acoustic data specifically on the Phantom 4, the Phantom 2 is a close alternative.

Additionally, from data gathered by Guvenc, Koohifar, Singh, Sichitiu, & Matolak (2018), the detection range of different acoustic sensors ranges from 20 meters to 600 meters, mainly depending on drone types and sensor arrangement. According to Bernardini et al. (2017), their acoustic detection algorithms have accuracy ratings ranging from 0.964 to 0.992 when distinguishing UAS noises from different environmental noises. The lowest accuracy being in a crowd and street with traffic, while the highest rating was in natural daytime. These algorithms, however, do not account for limitations encountered by distance, ambient conditions and specifications of microphones.

The hypothetical sensor characteristics used for this study will be modeled largely after acoustic sensors as there is more available operational data for this sensor type than others, and it meets the intent for developing a low-cost solution for identifying threat sUAS.

Interdiction Agent Characteristics

UAS interdiction involves the disruption of the threat sUAS flight path by one or more methods, with a goal of threat mitigation or minimizing perceived risk from the unwanted activity. Table 2 represents a summary of different interdiction methods currently employed (Michel, 2018). It is important to note that currently UAS interdiction operations are illegal in the U.S. outside of the Department of Defense, Department of Energy, Department of Homeland Security, and Department of Justice.

Table B.2 Types of Interdiction Methods Currently Employed

Sensor Type	Description
Radio Frequency (RF) Jamming	Interrupts the RF link between UAV and operator by generating large amounts of RF output. Once the RF link is disturbed, the UAV will land or return to the operator.
GNSS Jamming	Interrupts the satellite link used for navigating. Once the satellite link is lost, UAV will hover, land, or return to the operator.
Spoof	Taking control of the UAV by hijacking the communications link
Kinetic	Destroys portions of the airframe with directed energy, causing a crash
Net	Entangles the UAV or its rotors
Projectile	Employs ammunition to destroy UAV
Combination	Several C-UAS methods employed – commonly tandem RF and GNSS jamming

Note. Descriptions are adapted from Michel (2018, p. 4)

In 2016, a Michigan Tech research team demonstrated the effectiveness of a proof-of-concept anti-UAS net-launcher mounted on what appears to be a DJI Matrice 600 (Goodrich, 2016). This team later filed for and received a patent for their system which is able to aim the net projectile and carry the intruding UAS to a safe location for handling, mitigating human risk due to explosives or other potentially hazardous cargo (Aagaah et al., 2018).

In 2017, another research team from Purdue University demonstrated the effectiveness of a completely autonomous C-UAS detection and interdiction system involving a radar tracking system and autonomous hunter drone equipped with an ultra-light carbon-framed conical net (Goppert et al., 2017). The net design was selected to allow multiple attempts at interdiction of a threat in the event the autonomous positional data was too imprecise for a launched-net entanglement. The threat UAS was flown at a set altitude over a set path toward a protected object. The radar in use was described as a “high-precision” and “military” radar (Goppert et al., 2017, pp. 236, 238). This high-fidelity radar would be excellent for proving autonomous interdiction is possible but is largely outside of the budget and manpower available to prisons and other fixed facilities. Hunter type drone characteristics will be modeled for the interdiction agent in this study.

Prison Characteristics for Modeling Consideration

Like many other prisons across the country, there have been reports drones have been used to smuggle contraband within the security perimeter of the Indiana State Prison (J. E. Dietz, personal communication, September 20, 2018). Indiana State prison is a level four maximum-security prison located in Michigan City, Indiana which houses approximately 2,400 inmates (State of Indiana, 2019). The walled area spans 24 acres and the adjacent field is approximately another 18 acres (see Figure 1). These dimensions will be used to geographically represent the protected facility within the simulation model.

Figure B.1. Indiana State Prison footprint of approximately 40 acres (Google Maps, 2020)

METHOD

This section discusses the research framework, approach, tools of measurement, variables, and assumptions used in this article.

Research Framework

This research paper explores the usefulness of agent-based modeling software for adjusting and determining parameters that could lead to a successful C-UAS detection system. Simulation

modeling software has the unique ability to quickly adjust parameters and gather data and should provide insights that should transfer over to real-world systems, and bypass current legal restrictions on testing and implementation of C-UAS interdiction. Later iterations are intended to refine threat, sensor, and system behaviors. This will be done with a goal of identifying parameters for recommending system specifications for a comprehensive detection, tracking, and interdiction system for common commercially manufactured threats. AnyLogic modeling software will be used to replicate the geometric space, threat UAS, hypothetical C-UAS sensors, and an interdiction agent.

This study is designed to test an abstracted fixed counter unmanned aerial system that is designed to prevent overflight of a fixed facility representing an abstracted prison or compound. Parameters for agents will be discussed in later sections and are designed to replicate probable integrations of equipment that may be purchased for these purposes. Data will be collected for 50 iterations of each varying threat speed, while all other C-UAS behaviors remain the same between iterations.

Model Characteristics

Threat UAS characteristics.

The DJI Phantom 4 Pro specifications will be used to model the threat aircraft characteristics. This UAS is capable of speeds up to 45 mph under ideal conditions with no other payload other than the integrated camera on-board. Adding a payload will lower the top speed and affect the center of gravity and other flight controllability characteristics. The modeled threat UAS was spawned .75 miles away from the protected facility outside of sensor detection range, and at the far end of feasible line-of-sight tracking (UAV Coach, 2020). The threat UAS was flown in a pattern as dictated by 100 “attractors” selected randomly, one after the other, as depicted in Figure 2. There were 50 attractors placed evenly within the bounds of the protected facility, and an additional 50 attractors spanning the remaining space surrounding the facility. The simulation was run with threat speeds set at 25, 27.5 30, 32.5, 35, 36, 37.5, and 40 mph to collect sample data in each speed category.

Facility characteristics.

The simulation model contains a .25 x .25-mile (40 acres) square that will be used to indicate the footprint of the protected facility. A 'failure' within an iteration is defined as the threat UAS overflying the footprint of the protected facility, regardless of the duration of overflight.

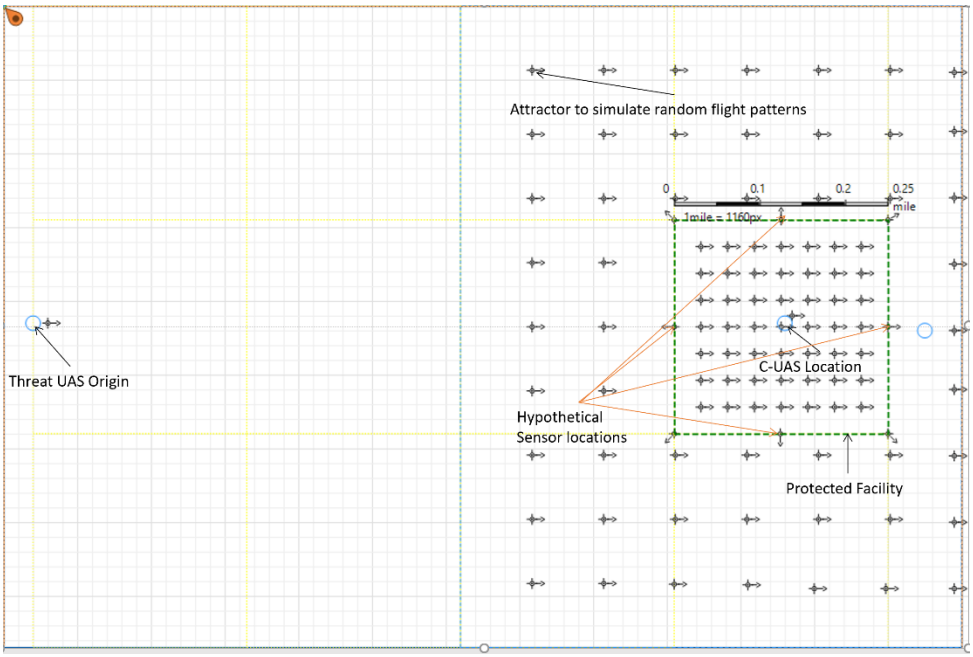

Figure B.2. The physical representation of the model space used in the experiment

Hypothetical sensor model characteristics.

A hypothetical sensor will be used for modeling based on an average of performance characteristics of Bernardini et al. (2017) and listed specifications of DroneSheild as reported by Birch et al. (2015) for ranging and success probability. The hypothetical sensor will be assumed to provide cueing to a higher fidelity electro-optical sensor. For the purposes of this study cueing and additional functionality will be abstracted into the specifications listed in Table 3.

Table B.3 Hypothetical sensor model parameters and values.

Sensor Type:	Omni-directional	Parabolic dish	Hypothetical
Effective Range	150 m / 495 ft	1000 m / 3280 ft	575 m / 1890 ft
Detection Angle	300°	30°	165°
Analysis Time Frame	-	-	5 second frames
SVM Success Rate	-	-	96.4%

Note. Analysis time and success rate derived from works by Bernardini et al. (2017, p. 63) and range and angle adapted from Birch et al. (2015, p. 27).

Interdiction agent model characteristics.

The DJI Matrice 600 Pro specifications will be used to model the interdiction aircraft characteristics. This UAS is capable of speeds up to 40 mph, no wind or excess payload (DJI, 2020). The simulation model will be using this as the fixed C-UAS interdiction speed. The model assumes that there will be an attached ultra-light net similar to the one used in a 2017 study by Goppert et al., in which a conical net and carbon-fiber housing were attached to a similar platform for the purposes of entangling threat UAS. The effects on top speed, the center of gravity, and other flight controllability characteristics have not been considered with the net attached for the purposes of this study. The C-UAS will be placed in the center of the protected facility and will track to the threat 10 seconds after the sensor detects the threat UAS. This will be the assumed time for cueing from the sensor to the interdiction agent.

RESULTS AND ANALYSIS

The model was built based on an abstracted facility footprint, hypothetical C-UAS sensor performance data and fixed C-UAS interdiction characteristics. After this framework was established and the agent behaviors set, the only variable manipulated in the model for each set of samples collected was the sUAS threat speed, which was set at the beginning of each iteration. These individual fixed-speed simulations were allowed 50 iterations of each run. The runs were documented and the threat UAS fixed speed was adjusted for the next set of simulations. Eight fixed-speed simulation sets were run, altering the threat UAS speed at 25 mph, 27.5 mph, 30 mph,

32.5 mph, 35 mph, 36 mph (added to explore the critical failure speed for this hypothetical system), 37.5 mph, and 40 mph and recorded each time. The results are recorded in Table 4.

Table B.4 Model Simulation Results

Threat Speed (MPH)	Avg I - D Time (s)	Std. Dev. (s)	Overflights	Avg overflight time (s)
40.0	59.2	30.4	72%	18.2
37.5	50.8	23.4	54%	14.0
36.0	*48.8*	*19.2*	*56%*	*13.0*
35.0	35.5	9.9	4%	1.5
32.5	32.0	5.9	0%	0
30.0	33.9	5.7	0%	0
27.5	33.0	4.4	0%	0
25.0	34.6	3.8	0%	0

Note. I-D Time represents the interdiction time minus the detection time in seconds. 36 MPH was added to further explore the relationship between speed and system failure.

Predictably, the amount of 'failures' or overflights of the protected facility increase as the threat speed increases. Interestingly, however, the overflights increase rapidly between 35 mph and 37.5 mph. Another 50 trials were run to determine if there was a linear relationship between the threat speed and failures of the system. From 35 mph to 36 mph the overflights increased from 4% to 56% of the trials respectively.

This is interesting in that there is a large jump in system "failures" within a very small increase in speed. Subsequent research may be needed to identify the critical speed delta between the interdiction agent and the threat UAS to better determine the point at which the system's effectiveness is degraded.

The data from this experiment suggest that a 5 MPH or greater speed delta is required between the expected threat UAS and a hypothetical system designed as outlined in this study. Figure 3 displays the large increase in variance present when the difference in speed changes from 5 mph to 4 mph to 2.5 mph and 0 mph between the threat sUAS and interdiction UAS respectively.

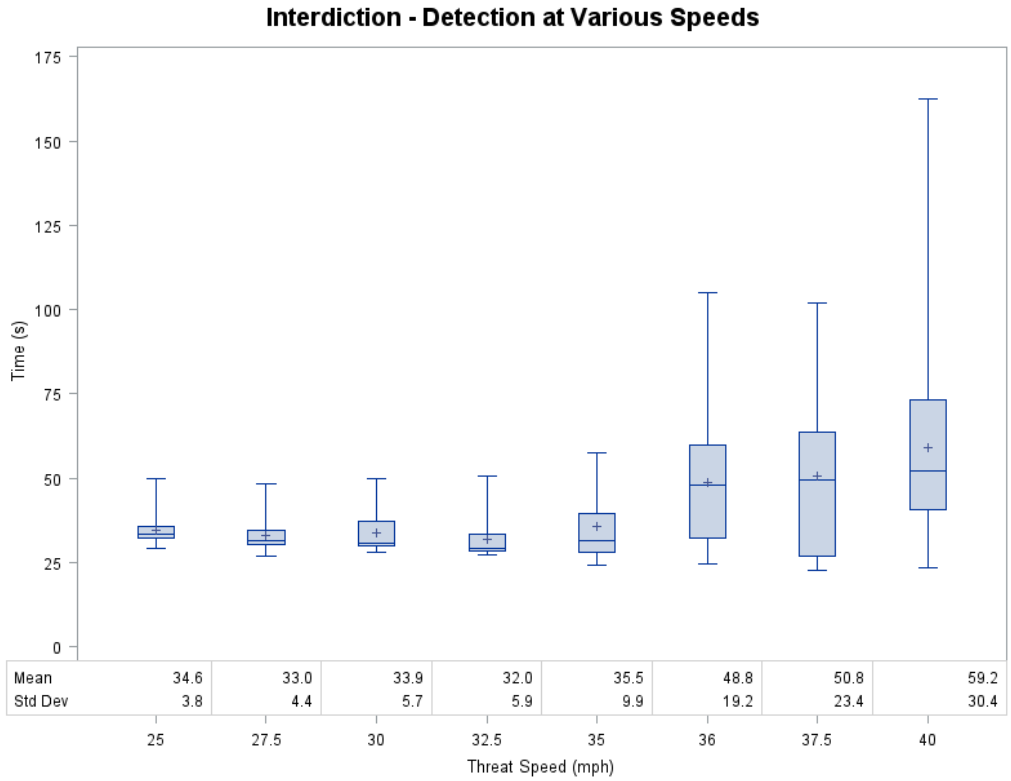

Figure B.3. Interdiction time - Detection time at Various Speeds

The distributions in each category are generally right skewed with very close lower limits. This is due to the high success rates of the hypothetical C-UAS system for threats that follow a straight flight path toward the protected facility. Since half of the attractor points were located within the protected facility, this type of flight pattern was common. As the threat speed increases, the variance increases, as can be seen by larger box areas in the graph for each speed category. The higher tail grows drastically larger in the categories that have less than a 5-mph difference between the interdiction or 'hunter' UAS and the threat UAS.

DISCUSSION

The purpose of this study was to explore the relationship threat UAS speed has on a set C-UAS system that might be typical for a fixed facility such as a prison. Additionally, the second goal of this study was to explore the usefulness of agent-based modeling software as a future tool for adjusting and determining parameters that could ultimately lead to a cost-effective C-UAS detection and interdiction system for fixed facilities. Data was gathered that provide insights that may apply to real-world systems.

This study suggests that there is a critical threat speed in which the variance between detection to interdiction times drastically increases along with subsequent system failures. The critical threat speed will depend on sensor performance, the geographic position of the sensors in relation to the protected facility, and interdiction characteristics. The goal of a fixed facility C-UAS system is to mitigate the threat, or in this case, prevent overflights of the facility. Agent-based simulation modeling may be a useful tool for establishing system parameters when careful consideration is applied in replicating the environment, threat, and parts of the whole C-UAS system.

The threat agent was given behavior based on commands to fly to a random sequence of attractors around the protected facility with the largest concentration within the facility. Further investigation will be conducted prior to future research if there are better methods to model this threat behavior. Threat speed was set initially at the start of each simulation. Future works may add in a speed variability into the behavior of the agent to replicate more real-world threats. The simulation took place primarily in a two-dimensional plane. The third dimension was replicated with a changing variable that was not fully accounted for within the interdiction behavior. Future research will try to integrate the third dimension more natively, which will have an added benefit of providing more visually appealing simulations. Additionally, although the threat UAS was given semi-random behavior based on attractors distributed around the facility, there was only one spawn point for the threat UAS, which will likely be addressed in further iterations.

Sensor data was based on a hypothetical sensor, since there is a general lack of real-world performance characteristics of C-UAS sensors. As better data becomes available, more realistic sensor data will be modeled in future works. A 96.4% probability seems rather high for an SVM accuracy rating, and perhaps a distance tiered probability would be appropriate for such sensors if data is available.

Interdiction ‘warm-up’ time may need to be lengthened past ten seconds to replicate more real-world conditions. Further investigation will be conducted on similar integrated systems as data becomes available. As system complexity increases, communication delays due to cueing and data transmission may be added into the model logic.

CONCLUSION

This study suggests that there is a critical threat speed for a hypothetical C-UAS system in which the variance of possible detection to interdiction sequences becomes so great that system failure becomes prevalent. This critical speed will be based on the geographic location and layout of the protected facility, the parameters of the sensor network, and the interdiction agents that make up the counter unmanned aerial system. Additionally, this study suggests that simulation modeling may be a useful tool for determining the system parameters required for the desired level of protection (i.e. notification of an overflight vs. prevention of an overflight) for a fixed facility, or can alternately suggest the appropriate makeup and placement of sensors and interdiction methods from tested and well-documented elements of a system. Simulation modeling may also be able to provide data to influence policy currently restricting UAS interdiction at the federal level.

References

Aagaah, M. R., Fleanha, E. M., & Mahmoudian, N. (2018). *Drone having drone-catching feature* (Patent No. US 10,005,556 B2).

Bernardini, A., Mangiatordi, F., Pallotti, E., & Capodiferro, L. (2017). Drone detection by acoustic signature identification. *Electronic Imaging*, *2017*(10), 60–64. https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-168

Birch, G. C., Griffin, J. C., & Erdman, M. K. (2015). *UAS detection classification and neutralization: Market survey 2015. - SAND2015-6365*. https://doi.org/10.2172/1222445

Christnacher, F., Hengy, S., Laurenzis, M., Matwyshuck, A., Naz, P., Schertzer, S., & Schmitt, G. (2016). Optical and acoustical UAV detection. *SPIE*, *9988*(99880B). https://doi.org/10.1117/12.2240752

Dedrone. *(2019). Dedrone corrections airspace security study*. http://web-assets.dedrone.com/collateral/Dedrone_Corrections_Airspace_Security_Study2019.pdf

DJI. (2019). *DJI phantom 4 pro – Specs, tutorials & guides – DJI*. https://www.dji.com/phantom-4-pro/info

DJI. (2020). *Matrice 600 specifications*. https://www.dji.com/matrice600-pro/info

Goodrich, M. (2016, January 7). *Drone catcher: "Robotic falcon" can capture, retrieve renegade drones*. Michigan Technological University. https://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html

Google Maps. (2020). Google Maps. https://www.google.com/maps/place/Indiana+State+Prison/@41.7036668,-86.9196084,835m/data=!3m1!1e3!4m5!3m4!1s0x8811a7eb3f091ba7:0x74a24ce0965df5b9!8m2!3d41.7036647!4d-86.9177619

Goppert, J. M., Wagoner, A. R., Schrader, D. K., Ghose, S., Kim, Y., Park, S., . . . Hopmeier, M. J. (2017). Realization of an autonomous, air-to-air counter unmanned aerial system (CUAS). *2017 First IEEE International Conference on Robotic Computing (IRC)*, 235–240. https://doi.org/10.1109/IRC.2017.10

Gramer, R. (2017, January). *Afghan insurgents use drones in fight against U.S. – Foreign Policy*. Foreign Policy. https://foreignpolicy.com/2017/01/31/ afghanistan-insurgents-use-drones-in-fight-against-u-s-nato-coalition-forces-unmanned-aerial-vehicles-future-warfare/

Grossman, N. (2018, August). *Analysis | Are drones the new terrorist weapon? Someone tried to kill Venezuela's president with one.* Washington Post. https://www.washingtonpost.com/news/monkey-cage/wp/2018/08/10/are-drones-the-new-terrorist-weapon-someone-just-tried-to-kill-venezuelas-president-with-a-drone/

Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M. L., & Matolak, D. (2018). Detection, tracking, and interdiction for amateur drones. *IEEE Communications Magazine*, *56*(4), 75–81. https://doi.org/10.1109/MCOM.2018.1700455

Harvey, K. (2018, May 18). *State invests $35k on pilot program to keep unwanted drones out of prisons | KBAK*. https://bakersfieldnow.com/news/ investigations/state-invests-35k-on-pilot-program-to-keep-unwanted-drones-out-of-prisons

Kotowski, J. (2018). Drones used to deliver drugs, cellphones and other contraband to Delano prison, documents say. *TCA Regional News*. http://search.proquest.com/docview/2015026811/

Michel, A. H. (2018). *Counter-drone systems* (p. 23). Bard College. https://dronecenter.bard.edu/publications/

Michel, A. H. (2019). *Counter-drone systems* (2nd ed). Bard College. https://dronecenter.bard.edu/publications/

Otte, J. (2017, November 7). *Drones dropping drugs into prisons; Ohio fights back.* Daytondailynews. https://www.daytondailynews.com/news/drones-dropping-drugs-into-prisons-ohio-fights-back/ GSB3jLP3sy9VMVWiaO31KM/

Rubens, T. (2018, February 8). *Drug-smuggling drones: How prisons are responding to the airborne security threat*. IFSEC Global. https://www.ifsecglobal.com/drones/drug-smuggling-drones-prisons-airborne-security-threat/

Small Unmanned Aircraft Systems, 14 C.F.R.§ 107 (2019)., Electronic Code of Federal Regulations § Part 107—Small Unmanned Aircraft Systems (2019), Source: Docket FAA-2015-0150, Amdt. 107-1, 81 FR 42209, June 28, 2016, unless otherwise noted. https://www.ecfr.gov/cgi-bin/text-idx?SID=3f50729cff2b56a549c4515c703eda34&mc=true&node=pt14.2.107&rgn=div5

State of Indiana. (2019). *Indiana state prison fact sheet*. https://www.in.gov/idoc/2413.htm

NC Def Tech. (2019, March 11). *Tech area of interest: Installation counter unmanned aerial systems (CUAS)*. https://deftech.nc.gov/ opportunities/ 2019-04-30/tech-area-interest-installation-counter-unmanned-aerial-systems-cuas

UAV Coach. *(2020). Is there a specific distance implied when the FAA says "visual line-of-sight"?* https://www.dronepilotgroundschool.com/ kb/is-there-a-specific-distance-implied-when-the-faa-says-visual-line-of-sight/

United States: Drones pose new contraband, smuggling challenge for prisons. (2016). *Asia News Monitor*.

Wallace, R., & Loffi, J. (2015). Examining unmanned aerial system threats & defenses: A conceptual analysis. *International Journal of Aviation, Aeronautics, and Aerospace*. https://doi.org/10.15394/ijaaa.2015.1084

Yuneec. (2018). *Typhoon 4K specs*. http://us.yuneec.com/typhoon-4k-specs

APPENDIX C: SAMPLE DATA FOR EXPERIMENT GROUPS

	EG1 - Control			EG2 -30sec/Main Exit			EG3 -30sec/7 Exits		
Iteration	T1	T2	Total	T1	T2	Total	T1	T2	Total
1	*24*	*159*	183	*10*	*87*	97	*10*	*63*	73
2	*30*	*150*	180	*14*	*62*	76	*26*	*91*	117
3	*37*	*137*	174	*6*	*32*	38	*31*	*79*	110
4	*32*	*177*	209	*8*	*61*	69	*28*	*93*	121
5	*40*	*145*	185	*5*	*73*	78	*21*	*87*	108
6	*33*	*145*	178	*11*	*48*	59	*29*	*79*	108
7	*35*	*163*	198	*15*	*57*	72	*22*	*79*	101
8	*46*	*148*	194	*9*	*41*	50	*24*	*89*	113
9	*41*	*152*	193	*17*	*98*	115	*27*	*103*	130
10	*39*	*142*	181	*15*	*60*	75	*30*	*76*	106
11	*36*	*153*	189	*8*	*29*	37	*40*	*58*	98
12	*33*	*160*	193	*10*	*61*	71	*33*	*95*	128
13	*32*	*154*	186	*17*	*89*	106	*28*	*112*	140
14	*47*	*148*	195	*6*	*40*	46	*23*	*76*	99
15	*42*	*167*	209	*13*	*56*	69	*33*	*71*	104
16	*32*	*157*	189	*20*	*50*	70	*28*	*117*	145
17	*36*	*159*	195	*12*	*45*	57	*36*	*87*	123
18	*37*	*161*	198	*5*	*71*	76	*29*	*85*	114
19	*39*	*139*	178	*19*	*87*	106	*11*	*111*	122
20	*34*	*155*	189	*12*	*88*	100	*43*	*94*	137
21	*31*	*166*	197	*25*	*87*	112	*11*	*102*	113
22	*40*	*139*	179	*19*	*101*	120	*39*	*95*	134
23	*38*	*153*	191	*25*	*79*	104	*42*	*80*	122
24	*45*	*147*	192	*26*	*61*	87	*31*	*93*	124
25	*37*	*149*	186	*45*	*83*	128	*30*	*106*	136
26	*25*	*148*	173	*11*	*62*	73	*21*	*78*	99
27	*32*	*153*	185	*17*	*71*	88	*30*	*106*	136
28	*39*	*150*	189	*14*	*66*	80	*29*	*93*	122
29	*41*	*153*	194	*20*	*43*	63	*33*	*109*	142
30	*42*	*157*	199	*14*	*54*	68	*37*	*70*	107
Mean	36.50	152.87	**189.37**	14.93	64.73	**79.67**	28.50	89.23	**117.73**
StdDev	5.56	8.92	8.99	8.13	19.42	23.89	8.33	14.94	16.23
StdErr	1.01	1.63	1.64	1.48	3.55	4.36	1.52	2.73	2.96

	Min	173		Min	37		Min	73	
	1st	183.5		1st	68.25		1st	107.25	
	2nd	189		2nd	75.5		2nd	119	
	3rd	194.75		3rd	99.25		3rd	129.5	
	Max	209		Max	128		Max	145	
	HO value	211.63		HO value	145.75		HO value	162.88	
	LO value	166.63		LO value	21.75		LO value	73.88	
	Outlier values - Discard								
	39	*79*	118						
	38	*191*	229						

replaced trial

EG4 - 30sec/2m			EG5 - 30sec/5m			EG6 -60sec/Main Exit		
T1	T2	Total	T1	T2	Total	T1	T2	Total
12	*92*	104	*13*	*75*	88	*20*	*101*	121
22	*71*	93	*10*	*78*	88	*11*	*114*	125
15	*81*	96	*16*	*64*	80	*27*	*87*	114
9	*64*	73	*19*	*68*	87	*40*	*33*	73
11	*92*	103	*10*	*92*	102	*30*	*77*	107
20	*87*	107	*4*	*62*	66	*20*	*95*	115
15	*68*	83	*6*	*64*	70	*17*	*69*	86
11	*64*	75	*14*	*61*	75	*23*	*66*	89
16	*69*	85	*14*	*71*	85	*43*	*59*	102
11	*63*	74	*17*	*95*	112	*30*	*93*	123
15	*78*	93	*9*	*50*	59	*28*	*59*	87
20	*59*	79	*12*	*52*	64	*18*	*106*	124
14	*83*	97	*11*	*69*	80	*29*	*98*	127
10	*78*	88	*15*	*59*	74	*43*	*59*	102
13	*82*	95	*8*	*55*	63	*40*	*35*	75
15	*89*	104	*15*	*64*	79	*35*	*90*	125
14	*74*	88	*15*	*57*	72	*24*	*101*	125
4	*65*	69	*13*	*58*	71	*19*	*108*	127
15	*99*	114	*9*	*56*	65	*29*	*46*	75
13	*55*	68	*16*	*57*	73	*4*	*78*	82
15	*58*	73	*8*	*91*	99	*26*	*54*	80
9	*72*	81	*17*	*67*	84	*25*	*71*	96
15	*58*	73	*10*	*82*	92	*23*	*108*	131
16	*67*	83	*19*	*71*	90	*29*	*59*	88
15	*67*	82	*7*	*69*	76	*38*	*61*	99
20	*69*	89	*16*	*81*	97	*22*	*89*	111
12	*69*	81	*15*	*71*	86	*5*	*77*	82
16	*66*	82	*6*	*84*	90	*33*	*48*	81
11	*47*	58	*14*	*57*	71	*6*	*95*	101
12	*83*	95	*19*	*82*	101	*30*	*50*	80
13.87	72.30	**86.17**	12.57	68.73	**81.30**	25.57	76.20	**101.77**
3.75	12.32	13.10	4.19	12.30	13.14	10.46	23.16	19.28
0.68	2.25	2.39	0.77	2.24	2.40	1.91	4.23	3.52

Min	58	Min	59	Min	73
1st	76	1st	71.25	1st	83
2nd	84	2nd	80	2nd	101.5
3rd	95	3rd	89.5	3rd	122.5
Max	114	Max	112	Max	131
HO value	123.5	HO value	116.88	HO value	181.75
LO value	47.5	LO value	43.88	LO value	23.75

EG7 -60sec/7 Exits			EG8 - 60sec/2m			EG9 - 60sec/5m		
T1	T2	Total	T1	T2	Total	T1	T2	Total
9	51	60	14	65	79	18	31	49
8	51	59	7	73	80	9	82	91
13	44	57	10	53	63	15	41	56
11	46	57	12	68	80	7	53	60
7	68	75	13	56	69	11	78	89
16	66	82	12	93	105	5	69	74
16	41	57	11	45	56	17	42	59
9	49	58	11	92	103	10	68	78
16	87	103	10	99	109	8	51	59
10	62	72	11	63	74	11	70	81
8	63	71	11	60	71	19	46	65
14	49	63	17	88	105	14	71	85
16	63	79	15	42	57	14	85	99
11	47	58	4	93	97	10	65	75
13	46	59	19	50	69	19	75	94
19	63	82	7	99	106	13	55	68
7	52	59	12	54	66	11	58	69
20	59	79	14	47	61	14	48	62
10	61	71	9	62	71	6	49	55
14	75	89	8	100	108	8	61	69
11	57	68	10	57	67	8	61	69
17	86	103	13	51	64	6	74	80
9	68	77	10	95	105	15	66	81
4	38	42	18	73	91	16	90	106
8	53	61	6	97	103	9	86	95
2	73	75	17	62	79	8	69	77
24	64	88	17	79	96	12	51	63
14	70	84	7	67	74	11	57	68
12	51	63	6	38	44	7	75	82
12	98	110	11	65	76	9	64	73
12.00	60.03	72.03	11.40	69.53	80.93	11.33	63.03	74.37
4.77	14.17	15.88	3.83	19.36	18.61	4.01	14.55	14.14
0.87	2.59	2.90	0.70	3.53	3.40	0.73	2.66	2.58

Min	42	Min	44	Min	49
1st	59	1st	67.5	1st	63.5
2nd	71	2nd	77.5	2nd	73.5
3rd	81.25	3rd	101.5	3rd	81.75
Max	110	Max	109	Max	106
HO value	114.625	HO value	152.5	HO value	109.125
LO value	25.625	LO value	16.5	LO value	36.125

EG10 -90sec/Main Exit			EG11 -90sec/7 Exits			EG12 - 90sec/2m			E13 - 90sec/5m		
T1	T2	Total	T1	T2	Total	T1	T2	Total	T1	T2	Total
27	*60*	87	*35*	*35*	70	*11*	*116*	127	*9*	*80*	89
29	*76*	105	*26*	*62*	88	*20*	*42*	62	*12*	*86*	98
22	*49*	71	*25*	*70*	95	*15*	*56*	71	*11*	*110*	121
27	*88*	115	*16*	*100*	116	*16*	*80*	96	*13*	*72*	85
26	*56*	82	*22*	*90*	112	*13*	*71*	84	*13*	*64*	77
19	*50*	69	*21*	*74*	95	*16*	*102*	118	*5*	*95*	100
19	*55*	74	*16*	*75*	91	*18*	*79*	97	*11*	*52*	63
31	*73*	104	*18*	*91*	109	*8*	*77*	85	*17*	*85*	102
25	*61*	86	*20*	*88*	108	*9*	*91*	100	*12*	*75*	87
11	*57*	68	*18*	*23*	41	*10*	*92*	102	*19*	*43*	62
24	*104*	128	*31*	*33*	64	*15*	*93*	108	*13*	*111*	124
24	*41*	65	*28*	*72*	100	*12*	*90*	102	*15*	*97*	112
22	*79*	101	*20*	*75*	95	*9*	*83*	92	*19*	*99*	118
14	*54*	68	*21*	*20*	41	*10*	*95*	105	*18*	*100*	118
13	*54*	67	*23*	*39*	62	*14*	*82*	96	*8*	*82*	90
19	*57*	76	*25*	*103*	128	*7*	*58*	65	*9*	*77*	86
11	*43*	54	*19*	*59*	78	*9*	*77*	86	*16*	*74*	90
33	*77*	110	*25*	*23*	48	*14*	*63*	77	*9*	*56*	65
28	*56*	84	*18*	*82*	100	*9*	*83*	92	*17*	*78*	95
27	*59*	86	*27*	*72*	99	*7*	*96*	103	*8*	*97*	105
23	*88*	111	*32*	*25*	57	*18*	*60*	78	*8*	*111*	119
19	*67*	86	*23*	*57*	80	*9*	*87*	96	*7*	*85*	92
16	*65*	81	*32*	*25*	57	*16*	*78*	94	*10*	*94*	104
25	*92*	117	*36*	*51*	87	*10*	*67*	77	*16*	*82*	98
35	*83*	118	*26*	*24*	50	*8*	*77*	85	*13*	*74*	87
22	*43*	65	*29*	*36*	65	*20*	*85*	105	*8*	*83*	91
37	*87*	124	*18*	*109*	127	*13*	*96*	109	*18*	*73*	91
34	*94*	128	*32*	*74*	106	*14*	*63*	77	*13*	*104*	117
26	*65*	91	*29*	*26*	55	*17*	*68*	85	*12*	*94*	106
19	*58*	77	*19*	*89*	108	*12*	*85*	97	*17*	*75*	92
23.57	66.37	89.93	24.33	60.07	84.40	12.63	79.73	92.37	12.53	83.60	96.13
6.83	16.83	21.39	5.77	28.01	25.57	3.86	15.62	14.92	3.95	16.92	16.67
1.25	3.07	3.91	1.05	5.11	4.67	0.71	2.85	2.72	0.72	3.09	3.04

Min	54	Min	41	Min	62	Min	62
1st	71.75	1st	62.5	1st	84.25	1st	87.5
2nd	86	2nd	89.5	2nd	95	2nd	93.5
3rd	108.75	3rd	104.5	3rd	102	3rd	105.75
Max	128	Max	128	Max	127	Max	124
HO value	164.25	HO value	167.5	HO value	128.625	HO value	133.125
LO value	16.25	LO value	-0.5	LO value	57.625	LO value	60.125

APPENDIX D: PARK MODEL ATTRACTIONS AND EXITS METRICS

Attraction	Patron in queue, count	Patron on attraction / in venue, count	Dwell time, minutes
Yellow River Adventure	900	60	
Fountain Pavilion	n/a	225	
Table Sit Restaurant	n/a	175	
Arcade	n/a	250	
Park Y4	n/a	350	triangular(10, 35, 20)
Park Y7	n/a	125	triangular(10, 35, 20)
Park Y9	n/a	100	triangular(10, 35, 20)
Ambient pedestrians	n/a	313	triangular(0.95*WT, <WT>, 1.05*WT) WT - warmup time
TOTALS:	2,443		

Note. WT = Warmup time 12 minutes

Exit Name	Throughput, ppm
Entrance (can become an exit during emergency)	120
Regular exit	360
Service entrance/exit (6 ft wide door)	240
Exit to water park	120
Exit to hotel	120
Exit to service area	120
Employee-only service exit	60

APPENDIX E: SAS OUTPUT FOR MULTIPLE COMPARISONS TEST : INTERVENTION SAMPLES

Multiple Sample Comparison Tests

The GLM Procedure

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	11	53516.733	4865.1576	14.74	<.0001
Error	348	114857.67	330.0508		
Corrected Total	359	168374.4			

R-Square	Coeff Var	Root MSE	Casualties Mean
0.317844	20.62903	18.1673	88.06667

Source	DF	Type I SS	Mean Square	F Value	Pr > F
Category	11	53516.733	4865.15758	14.74	<.0001

Source	DF	Type III SS	Mean Square	F Value	Pr > F
Category	11	53516.733	4865.15758	14.74	<.0001

t Tests (LSD) for Casualties

Alpha	0.05
Error Degrees of Freedom	348
Error Mean Square	330.0508
Critical Value of t	1.9668
Least Significant Difference	9.2258

Comparisons significant at the 0.05 level are indicated by ***.				
Category Comparison	**Difference between means**	**95% Confidence Limits**		
EG3-30/7 - EG6-60/M	15.967	6.741	25.193	***
EG3-30/7 - EG13905	21.6	12.374	30.826	***
EG3-30/7 - EG12902	25.367	16.141	34.593	***
EG3-30/7 - EG1090M	27.8	18.574	37.026	***
EG3-30/7 - EG4-30/2	31.567	22.341	40.793	***
EG3-30/7 - EG11907	33.333	24.107	42.559	***
EG3-30/7 - EG5-30/5	36.433	27.207	45.659	***

EG3-30/7 - EG8-60/2	36.8	27.574	46.026	***
EG3-30/7 - EG2-30/M	38.067	28.841	47.293	***
EG3-30/7 - EG9-60/5	43.367	34.141	52.593	***
EG3-30/7 - EG7-60/7	45.7	36.474	54.926	***
EG6-60/M - EG3-30/7	-15.967	-25.193	-6.741	***
EG6-60/M - EG13905	5.633	-3.593	14.859	
EG6-60/M - EG12902	9.4	0.174	18.626	***
EG6-60/M - EG1090M	11.833	2.607	21.059	***
EG6-60/M - EG4-30/2	15.6	6.374	24.826	***
EG6-60/M - EG11907	17.367	8.141	26.593	***
EG6-60/M - EG5-30/5	20.467	11.241	29.693	***
EG6-60/M - EG8-60/2	20.833	11.607	30.059	***
EG6-60/M - EG2-30/M	22.1	12.874	31.326	***
EG6-60/M - EG9-60/5	27.4	18.174	36.626	***
EG6-60/M - EG7-60/7	29.733	20.507	38.959	***
EG13905 - EG3-30/7	-21.6	-30.826	-12.374	***
EG13905 - EG6-60/M	-5.633	-14.859	3.593	
EG13905 - EG12902	3.767	-5.459	12.993	
EG13905 - EG1090M	6.2	-3.026	15.426	
EG13905 - EG4-30/2	9.967	0.741	19.193	***
EG13905 - EG11907	11.733	2.507	20.959	***
EG13905 - EG5-30/5	14.833	5.607	24.059	***
EG13905 - EG8-60/2	15.2	5.974	24.426	***
EG13905 - EG2-30/M	16.467	7.241	25.693	***
EG13905 - EG9-60/5	21.767	12.541	30.993	***
EG13905 - EG7-60/7	24.1	14.874	33.326	***
EG12902 - EG3-30/7	-25.367	-34.593	-16.141	***
EG12902 - EG6-60/M	-9.4	-18.626	-0.174	***
EG12902 - EG13905	-3.767	-12.993	5.459	
EG12902 - EG1090M	2.433	-6.793	11.659	
EG12902 - EG4-30/2	6.2	-3.026	15.426	
EG12902 - EG11907	7.967	-1.259	17.193	
EG12902 - EG5-30/5	11.067	1.841	20.293	***
EG12902 - EG8-60/2	11.433	2.207	20.659	***
EG12902 - EG2-30/M	12.7	3.474	21.926	***
EG12902 - EG9-60/5	18	8.774	27.226	***
EG12902 - EG7-60/7	20.333	11.107	29.559	***
EG1090M - EG3-30/7	-27.8	-37.026	-18.574	***
EG1090M - EG6-60/M	-11.833	-21.059	-2.607	***
EG1090M - EG13905	-6.2	-15.426	3.026	
EG1090M - EG12902	-2.433	-11.659	6.793	
EG1090M - EG4-30/2	3.767	-5.459	12.993	
EG1090M - EG11907	5.533	-3.693	14.759	
EG1090M - EG5-30/5	8.633	-0.593	17.859	
EG1090M - EG8-60/2	9	-0.226	18.226	
EG1090M - EG2-30/M	10.267	1.041	19.493	***

EG1090M - EG9-60/5	15.567	6.341	24.793	***
EG1090M - EG7-60/7	17.9	8.674	27.126	***
EG4-30/2 - EG3-30/7	-31.567	-40.793	-22.341	***
EG4-30/2 - EG6-60/M	-15.6	-24.826	-6.374	***
EG4-30/2 - EG13905	-9.967	-19.193	-0.741	***
EG4-30/2 - EG12902	-6.2	-15.426	3.026	
EG4-30/2 - EG1090M	-3.767	-12.993	5.459	
EG4-30/2 - EG11907	1.767	-7.459	10.993	
EG4-30/2 - EG5-30/5	4.867	-4.359	14.093	
EG4-30/2 - EG8-60/2	5.233	-3.993	14.459	
EG4-30/2 - EG2-30/M	6.5	-2.726	15.726	
EG4-30/2 - EG9-60/5	11.8	2.574	21.026	***
EG4-30/2 - EG7-60/7	14.133	4.907	23.359	***
EG11907 - EG3-30/7	-33.333	-42.559	-24.107	***
EG11907 - EG6-60/M	-17.367	-26.593	-8.141	***
EG11907 - EG13905	-11.733	-20.959	-2.507	***
EG11907 - EG12902	-7.967	-17.193	1.259	
EG11907 - EG1090M	-5.533	-14.759	3.693	
EG11907 - EG4-30/2	-1.767	-10.993	7.459	
EG11907 - EG5-30/5	3.1	-6.126	12.326	
EG11907 - EG8-60/2	3.467	-5.759	12.693	
EG11907 - EG2-30/M	4.733	-4.493	13.959	
EG11907 - EG9-60/5	10.033	0.807	19.259	***
EG11907 - EG7-60/7	12.367	3.141	21.593	***
EG5-30/5 - EG3-30/7	-36.433	-45.659	-27.207	***
EG5-30/5 - EG6-60/M	-20.467	-29.693	-11.241	***
EG5-30/5 - EG13905	-14.833	-24.059	-5.607	***
EG5-30/5 - EG12902	-11.067	-20.293	-1.841	***
EG5-30/5 - EG1090M	-8.633	-17.859	0.593	
EG5-30/5 - EG4-30/2	-4.867	-14.093	4.359	
EG5-30/5 - EG11907	-3.1	-12.326	6.126	
EG5-30/5 - EG8-60/2	0.367	-8.859	9.593	
EG5-30/5 - EG2-30/M	1.633	-7.593	10.859	
EG5-30/5 - EG9-60/5	6.933	-2.293	16.159	
EG5-30/5 - EG7-60/7	9.267	0.041	18.493	***
EG8-60/2 - EG3-30/7	-36.8	-46.026	-27.574	***
EG8-60/2 - EG6-60/M	-20.833	-30.059	-11.607	***
EG8-60/2 - EG13905	-15.2	-24.426	-5.974	***
EG8-60/2 - EG12902	-11.433	-20.659	-2.207	***
EG8-60/2 - EG1090M	-9	-18.226	0.226	
EG8-60/2 - EG4-30/2	-5.233	-14.459	3.993	
EG8-60/2 - EG11907	-3.467	-12.693	5.759	
EG8-60/2 - EG5-30/5	-0.367	-9.593	8.859	
EG8-60/2 - EG2-30/M	1.267	-7.959	10.493	
EG8-60/2 - EG9-60/5	6.567	-2.659	15.793	
EG8-60/2 - EG7-60/7	8.9	-0.326	18.126	

EG2-30/M - EG3-30/7	-38.067	-47.293	-28.841	***
EG2-30/M - EG6-60/M	-22.1	-31.326	-12.874	***
EG2-30/M - EG13905	-16.467	-25.693	-7.241	***
EG2-30/M - EG12902	-12.7	-21.926	-3.474	***
EG2-30/M - EG1090M	-10.267	-19.493	-1.041	***
EG2-30/M - EG4-30/2	-6.5	-15.726	2.726	
EG2-30/M - EG11907	-4.733	-13.959	4.493	
EG2-30/M - EG5-30/5	-1.633	-10.859	7.593	
EG2-30/M - EG8-60/2	-1.267	-10.493	7.959	
EG2-30/M - EG9-60/5	5.3	-3.926	14.526	
EG2-30/M - EG7-60/7	7.633	-1.593	16.859	
EG9-60/5 - EG3-30/7	-43.367	-52.593	-34.141	***
EG9-60/5 - EG6-60/M	-27.4	-36.626	-18.174	***
EG9-60/5 - EG13905	-21.767	-30.993	-12.541	***
EG9-60/5 - EG12902	-18	-27.226	-8.774	***
EG9-60/5 - EG1090M	-15.567	-24.793	-6.341	***
EG9-60/5 - EG4-30/2	-11.8	-21.026	-2.574	***
EG9-60/5 - EG11907	-10.033	-19.259	-0.807	***
EG9-60/5 - EG5-30/5	-6.933	-16.159	2.293	
EG9-60/5 - EG8-60/2	-6.567	-15.793	2.659	
EG9-60/5 - EG2-30/M	-5.3	-14.526	3.926	
EG9-60/5 - EG7-60/7	2.333	-6.893	11.559	
EG7-60/7 - EG3-30/7	-45.7	-54.926	-36.474	***
EG7-60/7 - EG6-60/M	-29.733	-38.959	-20.507	***
EG7-60/7 - EG13905	-24.1	-33.326	-14.874	***
EG7-60/7 - EG12902	-20.333	-29.559	-11.107	***
EG7-60/7 - EG1090M	-17.9	-27.126	-8.674	***
EG7-60/7 - EG4-30/2	-14.133	-23.359	-4.907	***
EG7-60/7 - EG11907	-12.367	-21.593	-3.141	***
EG7-60/7 - EG5-30/5	-9.267	-18.493	-0.041	***
EG7-60/7 - EG8-60/2	-8.9	-18.126	0.326	
EG7-60/7 - EG2-30/M	-7.633	-16.859	1.593	
EG7-60/7 - EG9-60/5	-2.333	-11.559	6.893	

APPENDIX F: CROWD MANAGEMENT SYSTEM

The following document was sent to the Purdue Office of Technology Commercialization to generate a patent proposal:

Travis Cline, M.S.

Braiden Frantz, M.S.

Krassimir Tzvetanov, M.S.

J Eric Dietz, Ph.D., PE

Purdue University

Last Updated: August 3, 2020

Crowd Management System for High-Density Outdoor Events

Introduction

Background

In a previous study by Tzvetanov et al., (In press), agent-based modeling was used to determine the most efficient methods in which to evacuate an amusement park in the event of an incident requiring patron evacuation and emergency response. The amusement park layout used for the study is an actual project in the design phases slated to be built overseas. In one series of tests, the research team determined that pedestrian movement throughout an amusement park is minimized if pedestrians were re-directed to seven emergency exits evacuation times would decrease by an average of 24% when compared to leaving through the large main exit toward the parking lot Tzvetanov et al., (In press). Further, the study showed the importance of multi-exit evacuations regarding the impact of police response times to arrive at one of three incident locations, as well as the potential negative impact on hard corners and pedestrian flow in an evacuation Tzvetanov et al., (In press). In addition, the study established that some exits may be disproportionately loaded with pedestrians due to their proximity to major attractions. In this case, there will be further

timesaving if the crowd exiting that attraction can be guided to different exits to balance the load. This study serves as a starting point to assess the potential effects of an operational evacuation system or crowd management system prior to its deployment.

Standards for Outdoor Signage

Standards in place for outdoor events are generally vague and call for generic protocols to be in place for mass evacuations. The NFPA 1616 (2017) outlines a public communication system to be present for the passage of warnings, notifications, and general mass communication to patrons. The communication system is intended to ensure the health and well-being of patrons and staff throughout the venue. The communication system should be tested regularly, and the U.S. Department of Homeland Security recommends a video surveillance system to bolster security (Risk Management Division, 2006).

Signage is also an important factor for any emergency situation involving densely populated areas. Strategically placed signs can direct patrons toward safety and reduce the risk of injury involved with a mass evacuation. However, when it comes to standardization or mandates for outdoor spaces, direction is lacking from governmental entities. The U.S. Department of Homeland Security has issued a few general guidelines of when to use signs, such as signs to restrict access to areas off-limits to the public and instructions to ensure that signage uses standard emergency verbiage (U.S. Department of Homeland Security, 2019). However, there is no guidance for sign placement, size, color, shape, etc. Many outdoor venues are in locations that do not host large masses of people regularly or attract patrons that are not familiar with the layout. There is a need to implement on-demand emergency evacuation signage in high-density outdoor venues to keep patrons safe as they exit and guide people away from dangerous or overcrowded exits.

Problem

Currently, no known outdoor signage standards or systems exist that would facilitate an efficient evacuation of high-density outdoor events (HDOE) such as amusement parks, concerts, sporting events, and fairs while being tailorable to the incident and prevents pedestrians from evacuating into the incident area.

Solution

The purpose of this proposal is to suggest a modular Crowd Management System (CMS) that may be in a fixed or deployable configuration and is used to direct pedestrian traffic in high-density outdoor events such as concerts, sports games, fairs, and amusement parks. The system would have several operational uses that contribute to the overall safety of the event in which it is employed.

Claims:

1. Emergency signage and systems can aid in the safe evacuation of high-density outdoor events (HDOE)
2. Signage and systems controlled within a command center provide real-time directional crowd control during emergency evacuations within HDOE
3. Crowd management devices (CMDs) can re-direct traffic away from one or more hazardous event such as a shooting, terrorist attack, or inclement weather conditions
4. Traffic can be directed toward alternate emergency exits, which may not be well labeled or known to pedestrians for outdoor spaces. Foot traffic can also be directed away from an overloaded exit to prevent stacking.
5. CMDs can maximize throughput at hidden emergency exits when coupled with active pedestrian monitoring through a network of sensors and interactive signs
6. Sensors can monitor pedestrian density and re-direct traffic from high-density bottlenecks that could potentially lead to trampling or crushing events

Funding

No funding has been sourced or given for this patent proposal.

Proposal

We propose a Crowd Management System (CMS) made up of several modular components to help solve this problem. The system will be comprised of three primary categories which will be explained in greater detail within this document:

Command and Control System (C2)
Sensors
Crowd Management Devices (CMDs)

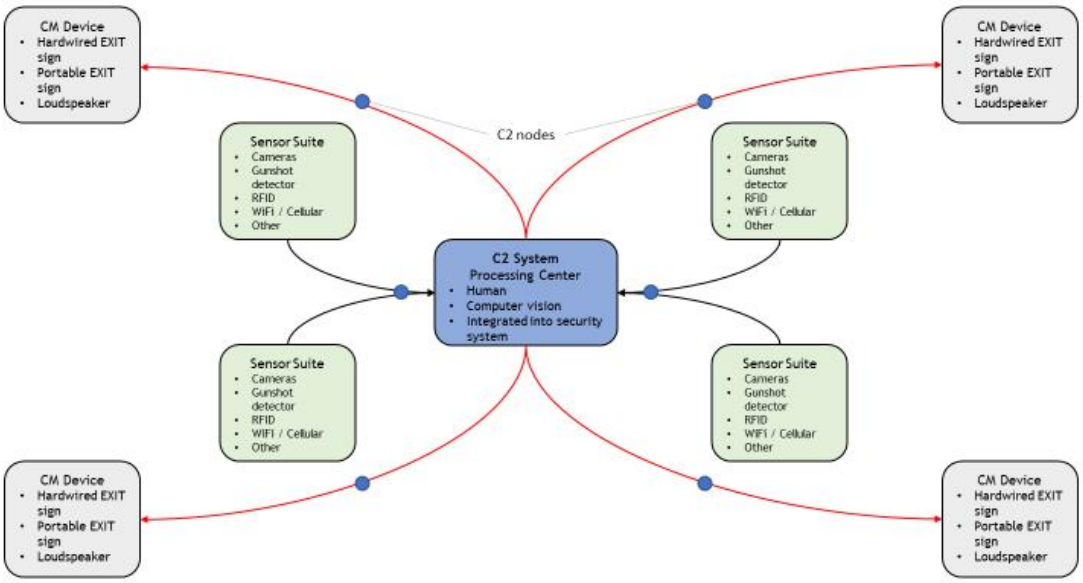

Figure 1. Concept Sketch of Crowd Management System

Command and Control System

The command and control (C2) system will connect data from the sensors to the traffic management devices, which include interactive signs and loudspeakers.

<u>Processing Center</u>

The data processing center receives data from the sensors and may form a computer model of the venue in which the system is employed. This will include a geographic representation of sensor data, traffic management devices, and exits. If equipped, this computer- model will have an approximation of the number of pedestrians per area, as processed from the specific sensors. The processing center will take input from the sensors and send signals to the traffic management devices in the event of an incident. This process can be monitored and actioned manually, or through automated software.

C2 Nodes (network)

The system will be connected in a mash or hub-and-spoke network, and primarily communicate wirelessly, through a variety of possible protocols, such as but not limited to, Zigbee, Bluetooth, Wi-Fi, etc. The network will automatically configure and will connect all sensors and traffic management devices. This will allow for a flexible mesh, or hub-and-spoke, network that can be rapidly deployed and healed if a singular node fails. Nodes will be added as necessary to cover an entire venue.

Sensors

The general purpose of the sensor category of the CMS is to monitor crowds for pedestrian count, density, movement, and behavior. Sensor data will be aggregated at the processing center to display a computer-generated representation of the event in real-time to provide situational awareness. Sensor data will be used to feed the following into the processing center:

- Pedestrian density broken up by area (unique to each event)
- Pedestrian movement and behavior
- Civil disturbance
- Gunshot monitoring
- General traffic patterns
- Distressed individuals

- Exit usage and flow
- Location of safety hazards

The CMS would be able to leverage the benefits of several different types of sensor technology to add to the overall situational awareness and safety of an HDOE.

Video Technology/Cameras

Video technology would likely be the primary sensor involved due to its low cost and proven history for manual monitoring. Additionally, over the past decade, video technology combined with computer vision has rapidly evolved. When paired with the right software, video technology can track specific individuals in crowds over multiple cameras. For the purposes of the CMS, the software could be integrated that can approximate the count of people in a particular area, or who have passed by a particular checkpoint (Li et al., 2012; Zaki & Sayed, 2014). Additionally, the video could be recorded and saved for law enforcement investigations if necessary.

Passive, Active Infrared and Radio Beam

Passive and active IR have similar characteristics as it pertains to the need to measure the pedestrian count in particular areas. In both cases, a checkpoint type of deployment could be used, similar to a digital turn style. This could be used to monitor entries and exits of an area or emergency exit.

Pressure Pads

Pressure pads appear to have fairly low accuracy comparable to active and passive IR (Ryus et al., 2014) but there is not a lot of data on them. Unlike other technologies, they need to be buried under the ground which makes it more challenging to deploy on temporary bases.

Cellphone Emissions

There are three types of cellphone emissions which can be useful in counting people in different areas in the park. The first one, WiFi, has become ubiquitous. Many venues even if they are temporary offer access to the Internet and in some cases, they provide information services about the venue which further incentivizes patrons to connect to the WiFi.

The second, and even more reliable method, is to track the presence of cell phones by passively monitoring their control channel communication with the cell phone towers. Note that this monitoring only covers the address of the phone and does not determine the phone number or the individual behind it.

Last, Bluetooth emissions can be passively monitored. Cellphones routinely emit Bluetooth signals even if they are not connected to other Bluetooth devices. These signals can be monitored for unique devices and produce a relative count of devices in an area.

In all cases, it is possible to collect signals passively without the need to acquire a permit. Furthermore, the MAC addresses of WiFi, Bluetooth, and cellphone radio do not directly identify users and there is not a privacy concern if they are not retained and mapped to users.

Environmental/Other Sensors

The scope of this system allows for specific sensors to be deployed that address the unique hazards that may be encountered at a specific venue. These may include but are not limited to; ambient temperature, humidity, flood/water sensors, inclement weather, light, gunshot detectors, smoke, carbon monoxide and other gases, etc. Additionally, pedestrian interactive sensors may be added that can alert attention to a specific area for monitoring. This would be similar to the emergency 'panic' buttons prevalent on campus walkways in the United States or fire alarm triggers.

Crowd Management Devices

Crowd management devices (CMDs) are those that are intended to change the behavior of a crowd in an incident to promote safety and good order. Crowd management devices can help direct pedestrians away from an active shooter, terrorist attack, or other hazardous event and efficiently direct them toward the nearest emergency exit, which may not otherwise be well known

or labeled for outdoor events. Crowd management devices can also be used in conjunction with the CMS to redirect evacuating pedestrians to less-congested exits or pathways, thus minimizing the risk of trampling or crushing by actively monitoring pedestrian density and managing pedestrian traffic.

Design

Crowd management devices are physical signs of a novel design that may be rapidly deployable or tailored to more fixed venues. The signs may or may not have an auditory component based on their intended venue and employment, which may be integrated into the venue public address system. The signs should be unassuming during normal operations, and very obvious and directive in the event of an incident. Two primary designs serve the same function. An inflatable sign in the shape of a column and arrow (see figure 1) and a collapsible mast and placard style sign for events in which the inflatable signs are impracticable.

Style 1: Inflatable Crowd Management Device

The approximate dimensions for this style will be a two-foot diameter cylinder with an opening for the actual inflatable sign connection. The base will also encompass a blower apparatus or compressed air to rapidly inflate the sign. The base will house a turntable style electric or hydraulic motor to change the sign's orientation to direct pedestrians away from an incident and toward an exit. The base will have a GPS receiver powered by a solar panel or shore power to communicate precise location and orientation to the processing center. See *Figure 2* for a concept drawing of the inflatable CMD.

Shape

The sign will have a large inflatable arrow oriented in the intended direction of crowd movement. The intended height at full deployment will be between 10-15 feet. The arrow will require material on both sides of the main inflation tube to offset the weight and add balance to the system.

Marking

Standard marking with “Evacuate” or another directive term will be on the arrow portion of the inflatable. The marking will not possess the ability to be changed in real-time, so if the exit is untenable, the arrow will orient toward a safe exit location. The marking will be made of reflective material for easier sight during low light conditions.

Lighting

LED lighting will line the inner chamber of the turning motor to illuminate the inflatable column in white, making it obvious in an incident, especially during nighttime conditions. A strobe light will be added to the end of the arrow to help draw attention during daylight hours.

Power

The rapidly deployable CMD will power the GPS receiver and networking components via mounted solar panels on top of the device. Excess power will trickle charge a battery. The battery will be designed to operate the blower motor, the turn-table motor, the lighting, and auxiliary systems, such as a loudspeaker for a short duration commensurate with evacuation or approximately 15-30 minutes. The system will have an external plug that is capable of powering the entire system, as well as a battery charger component to convert the AC power to DC power for charging the battery.

Auxiliary systems

Auxiliary systems may be added to match the needs of the venue or security team. They will include a loudspeaker with pre-recorded messages upon deployment and may include additional sensors or capabilities.

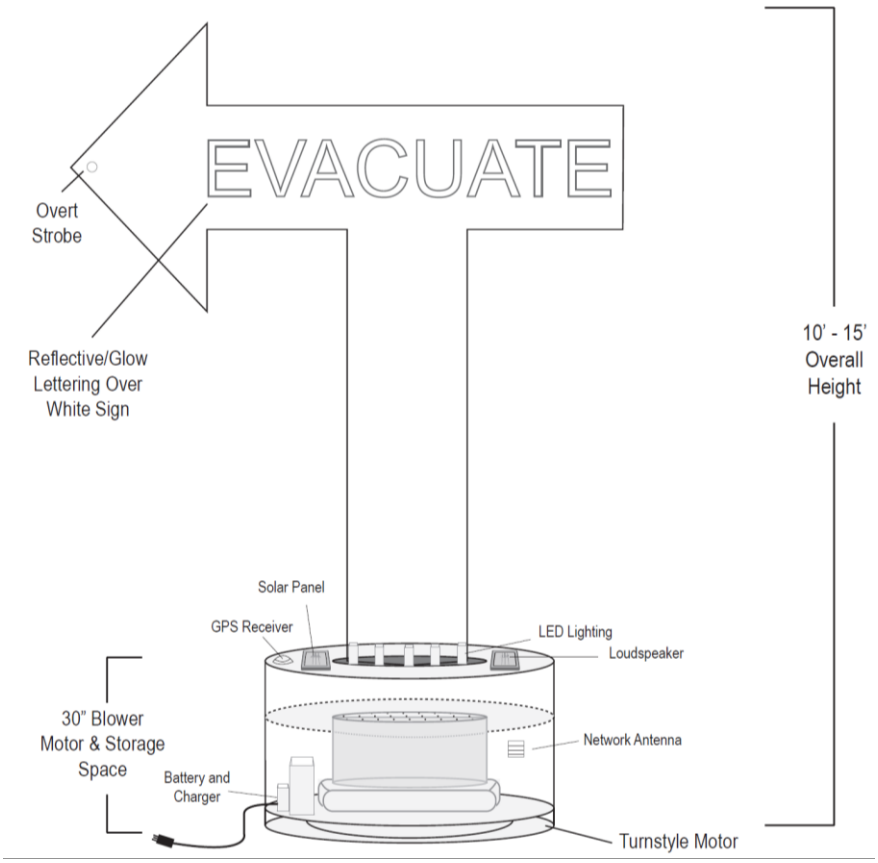

Figure 2. Inflatable Crowd Management Device

Style 2: Mast and Placard Crowd Management Device

The approximate dimensions for this style will be 96 inches at full extension. The base will house a turntable style electric or hydraulic motor to change the sign's orientation to direct pedestrians away from an incident and toward an exit. The base will have a GPS receiver and magnetic direction sensor powered by a solar panel or shore power to communicate precise location and orientation to the processing center. See *Figure 3* for a concept drawing of the mast type CMD.

Shape

The mast will have a base that is approximately 12 inches in diameter and 48 inches in height. It will be extendable to approximately 96 inches of total height, with two incremental extensions of 24 inches. The end of the mast will have a rectangular arrow sign attached, which extends perpendicular when the mast reaches its fully extended position.

Marking

Standard marking with “Evacuate” or another directive term will be on the rectangular arrow sign. The marking will not possess the ability to be changed in real-time, so if the exit is untenable, the mast base will orient the arrow toward a safe exit location.

Lighting

Only the rectangular arrow will be lit; the mast will be unlit. The sign will be illuminated green if the exit is permissible/safe or red if the exit is dangerous, with the light color controlled by the processing center. The ability will exist to adjust illumination color via the CMS. A small strobe light will also be affixed to the end of the arrow to draw attention during daylight hours.

Power

The fixed CMD will not require solar panels or batteries to operate and will be integrated into the facility's power grid.

Auxiliary systems

Auxiliary systems may be added to match the needs of the venue or security team. They will include a loudspeaker with pre-recorded messages upon deployment and may include additional sensors or capabilities.

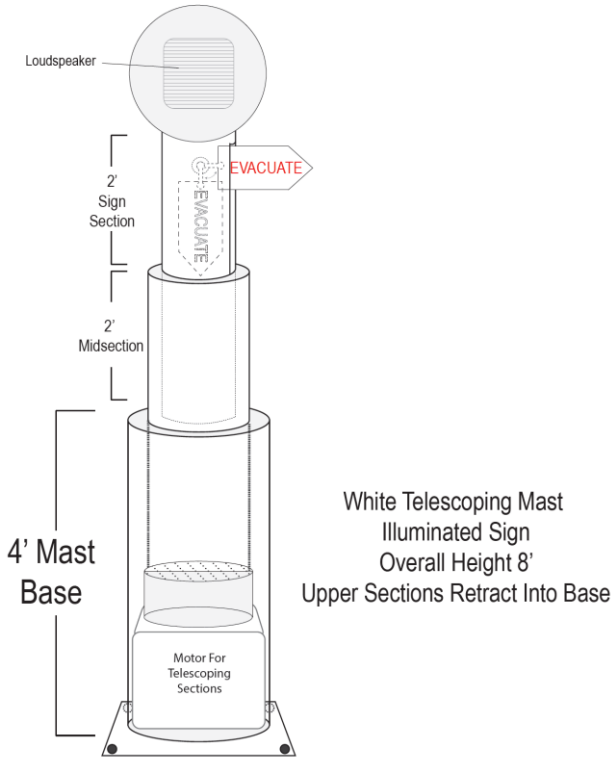

Figure 3. Telescoping Crowd Management Device for Permanent Outdoor Venues

Conclusion

Previous simulations have shown that utilizing multiple exits in the event of an incident for a HDOE result in faster evacuation times, and reduced emergency response time. A modular Crowd Management System (CMS) is proposed to monitor for hazardous situations in real-time, as well as actively direct pedestrians away from danger, and toward exits. Crowd Management Devices (CMD) are how the system interacts with pedestrians and consist of networked smart signs of an unassuming nature, that inflate or extend and rotate to highlight the best route away from danger. Signs are lit and clearly marked as to be easily understood at a glance and can be rotated in real-time to match the current state of the incident. A sensor network provides a computer-generated model of the HDOE and feeds information to a processing center that communicates with the CMDs.

References

Li, S., Sayed, T., Zaki, M. H., Mori, G., Stefanus, F., Khanloo, B., & Saunier, N. (2012). Automated Collection of Pedestrian Data through Computer Vision Techniques: *Transportation Research Record*. https://doi.org/10.3141/2299-13

National Fire Protection Association. (2017). *NFPA 1616: Standard on Mass Evacuation, Sheltering, and Re-Entry Programs 2017*.

Risk Management Division. (2006). *Infrastructure Protection Report: Amusement, Theme, and Water Parks*. Department of Homeland Security. https://info.publicintelligence.net/Commercial_ThemeParks.pdf

Ryus, P., Ferguson, E., Laustsen, K. M., Schneider, R. J., Proulx, F. R., Hull, T., Miranda-Moreno, L., National Cooperative Highway Research Program, Transportation Research Board, & National Academies of Sciences, Engineering, and Medicine. (2014). *Guidebook on Pedestrian and Bicycle Volume Data Collection* (p. 22223). Transportation Research Board. https://doi.org/10.17226/22223

Tzvetanov, K., Riegsecker, A., Frantz, B., Xiong, C., Bott, R., Cline, T., Dietz, J. E., & Dubiel, B. (In press). Agent-based modeling for theme park evacuation. *Journal of Emergency Management*.

U.S. Department of Homeland Security. (2019). *Planning Considerations: Evacuation and Shelter-in-Place*. FEMA. https://www.fema.gov/media-library-data/1564165488078-09ab4aac641f77fe7b7dd30bad21526b/Planning_Considerations_Evacuation_and_Shelter-in-Place.pdf

Zaki, M. H., & Sayed, T. (2014). Automated Analysis of Pedestrians' Nonconforming Behavior and Data Collection at an Urban Crossing. *Transportation Research Record*, *2443*(1), 123–133. https://doi.org/10.3141/2443-14