NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SYSTEM ANALYSIS OF COUNTER UNMANNED AERIAL SYSTEMS' KILL CHAIN IN AN OPERATIONAL ENVIRONMENT

by

Choon S. Tan

September 2021

Thesis Advisor: Douglas L. Van Bossuyt
Co-Advisor: Britta Hale

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
SYSTEM ANALYSIS OF COUNTER UNMANNED AERIAL SYSTEMS' KILL CHAIN IN AN OPERATIONAL ENVIRONMENT

5. FUNDING NUMBERS

6. AUTHOR(S) Choon S. Tan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The proliferation of unmanned aerial system (UAS) capabilities in the commercial sector is posing potentially significant threats to the traditional perimeter defense of civilian and military facilities. In particular, commercial-off-the-shelf UASs, which are small, cheap, and come with many functions, have sparked growing interest among hobbyists and raised risks to facilities. Consequently, facility commanders now need a methodology to conduct quick evaluation and analysis of immediate threats to their facility to determine effectiveness of their facility's counter unmanned aerial system (CUAS). Following a systems engineering approach, this research proposes a methodology that provides a step-by-step process to conduct evaluation and analysis of a facility, and employs model based systems engineering (MBSE) tools to assess a CUAS's effectiveness and limitations. The methodology analyzes the CUAS's operating environment and the ways CUASs may impact other stakeholders (e.g., adjacent allied forces, civilians, etc.) within the area of operation. We then identify configuration candidates for optimizing the CUAS's performance to meet the requirements of the stakeholders. A case study of a hypothetical airport with an existing CUAS is presented to demonstrate the usability of the methodology, explore the candidates, and justify the implementation of a candidate that fits the facility's and the stakeholders' requirements.

14. SUBJECT TERMS
system analysis, risk analysis, airport security, base security, unmanned aerial system, UAS, counter unmanned aerial system, CUAS, model based systems engineering, MBSE

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SYSTEM ANALYSIS OF COUNTER UNMANNED AERIAL SYSTEMS' KILL CHAIN IN AN OPERATIONAL ENVIRONMENT

Choon S. Tan
Major, Singapore Army
BSEE, Newcastle Upon Tyne, 2015

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Douglas L. Van Bossuyt
Advisor

Britta Hale
Co-Advisor

Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The proliferation of unmanned aerial system (UAS) capabilities in the commercial sector is posing potentially significant threats to the traditional perimeter defense of civilian and military facilities. In particular, commercial-off-the-shelf UASs, which are small, cheap, and come with many functions, have sparked growing interest among hobbyists and raised risks to facilities. Consequently, facility commanders now need a methodology to conduct quick evaluation and analysis of immediate threats to their facility to determine effectiveness of their facility's counter unmanned aerial system (CUAS). Following a systems engineering approach, this research proposes a methodology that provides a step-by-step process to conduct evaluation and analysis of a facility, and employs model based systems engineering (MBSE) tools to assess a CUAS's effectiveness and limitations. The methodology analyzes the CUAS's operating environment and the ways CUASs may impact other stakeholders (e.g., adjacent allied forces, civilians, etc.) within the area of operation. We then identify configuration candidates for optimizing the CUAS's performance to meet the requirements of the stakeholders. A case study of a hypothetical airport with an existing CUAS is presented to demonstrate the usability of the methodology, explore the candidates, and justify the implementation of a candidate that fits the facility's and the stakeholders' requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

AGL	Above Ground Level
AI	Artificial Intelligence
C2	Command and Control
CBRE	Chemical, Biological, Radiological and Explosives
COTS	Commercial Off The Shelf
CUAS	Counter Unmanned Aerial System
DOD	Department of Defense
DOE	Design of Experiment
EFFBD	Enhanced Function Flow Block Diagram
EO	Electro Optical
F2T2EA	Find, Fix, Track, Target, Engage, Assess
FL	Flight Level
GNSS	Global Navigation Satellite System
HADR	Humanitarian Assistance and Disaster Relief
HFE	Human Factors Engineering
HUD	Heads-Up Display
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
LIDAR	Light Detection and Ranging

LOS	Line-Of-Sight
MBSE	Model Based Systems Engineering
MGTOW	Max Gross Take-Off Weight
MIO	Maritime Interdiction Operations
ML	Machine Learning
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
OEM	Original Equipment Manufacturer
OV-1	Operational Viewpoint - 1
RF	Radio Frequency
SAF	Singapore Armed Forces
SAR	Search And Rescue
SI	Swarm Intelligence
TRL	Technology Readiness Level
TTP	Tactics, Techniques, and Procedures
UAS	Unmanned Aerial System
VTOL	Vertical Take-Off and Landing

Executive Summary

The continuous growth in Unmanned Aerial System (UAS) technological advancement and adoption rates across industry and the hobbyist community pose significant security and safety concerns to facilities such as airports, critical infrastructure, and military camps and bases. Among such potential risks is an intruder UAS colliding with an asset, personnel, or infrastructure that results in damage to aircraft or infrastructure, or injuries to personnel. Additionally, recovery efforts at an airport, for instance, usually require the affected runway to be temporarily shutdown or an aircraft pulled out of service which then can cause huge interruptions to daily operations [1]. The consequences are potentially catastrophic for facilities left unguarded against UAS threats. To keep pace with the rapid proliferation and expansion of UAS capabilities, the defense industry must act quickly to implement updated methods to safeguard critical infrastructures and operations against possible UAS intrusion. Furthermore, the defense industry may find it challenging to keep up with emerging UAS threats that make the design and implementation of a Counter Unmanned Aerial System (CUAS) extremely complex.

This research employs a systems engineering method and perspective to develop an approach for the evaluation and analysis of a CUAS for a specific facility in order to better identify the facility's potential weak points and to balance the CUAS capabilities with adjacent stakeholders' needs. The proposed methodology is iterative and allows designers to compare performance parameters across the sub-systems of the CUAS and at different Technology Readiness Levels (TRLs). The use of Model Based Systems Engineering (MBSE) and simulation tools aids in verification and validation of candidate CUAS configurations [2]. Candidate CUAS configurations are narrowed down to one design through the use of a Pugh matrix. Then the down-selected CUAS is analyzed for effectiveness.

The method proposed in this research is as follows with additional sub-steps detailed in the body of the thesis:

- Pre-Step: Collect System Information
- Step 1: Define Threats
- Step 2: Re-evaluate the Current System

- Step 3: Perform Evaluation and Analysis
- Step 4: Generate Design Recommendations

This methodology serves as a guide for the designer to adopt an evaluation and analysis approach in the design and implementation of a CUAS. A case study of a hypothetical airport is also provided to demonstrate the methodology in reviewing and choosing a candidate configuration that is resource-optimized and suits the facility's needs in a timely manner.

List of References

[1] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies," *Sensors*, vol. 20, no. 12, May 2020. [Online]. Available: https://doi.org/10.3390/s20123537

[2] J. Shevchenko. "An introduction to Model-Based Systems Engineering (MBSE)," Accessed May 30, 2021. [Online]. Available: https://insights.sei.cmu.edu/blog/introduction-model-based-systems-engineering-mbse/

Acknowledgments

I would like to thank my thesis advisors, Dr. Douglas Van Bossuyt and Dr. Britta Hale, for providing guidance and support as I put my thoughts into this thesis. You both taught me the importance of the instruction “to start writing” that pulled me through the struggle.

To my wife, thank you for taking care of the house and allowing me to deep dive with my writing. I would not have been able to complete this thesis without your unwavering support. For my Abby, finally, I can have more playtime with you. I love you both.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

In recent years, the rapid advancement of Unmanned Aerial System (UAS) technologies has sparked interest in and spurred the adoption of UASs for recreational uses by hobbyist communities. Further, UASs have become affordable and accessible for every nation or militant organization. While flying regulations are being implemented to require UAS operators to provide attribution for all UASs in operation, many hobbyists still do not provide such information, and nefarious actors can be expected to provide no identification of UAS origin. Thus, merely requiring UAS identification is not sufficient to protect most facilities, such as airports, from UAS intrusion. Further, if the facility were to be left unguarded, the consequences of a UAS intrusion could be catastrophic. For example, if a UAS were to be ingested into an aircraft engine during departure or to crash into a fuel tank, such an event could cause loss of life, huge disruption to operations, and costly repairs to infrastructure or assets.

UAS are designed to conduct various tasks that are "dull, dirty or dangerous" to humans [1]. The primary capability driver for UAS technological growth is the increasing interest in military force preservation efforts while conducting dangerous tasks such as Intelligence, Surveillance, and Reconnaissance (ISR), Humanitarian Assistance and Disaster Relief (HADR), and precision strike. As UAS technology matured over the last several decades, the commercial sector saw opportunities for UAS to be applied in commercial operations such as infrastructure inspection, traffic surveillance, delivery, and meteorology. Beneficial to both military and commercial sectors, the implementation of open architecture in the UAS community has garnered significant innovations which continue to speed up UAS technological advancement with revolutionary potential. Commercial Off The Shelf (COTS) UAS or small group UAS often provide functions such as photography, videography and self-assembly kits that attract hobbyists of all domains to adopt UAS for recreational purposes [2]. Nonetheless, with the technological growth and widespread adoption of UAS, there is a significant risk to the both military and commercial sectors [3], [4].

The key risks from non-nefarious UAS to facilities, bases, airports, critical infrastructure,

and similar installations are loss of control and collisions. Loss of control may cause major damage to critical assets or injury to humans, and may incur high costs to repair infrastructure damage and heal severe injuries. For instance, a hobbyist UAS operator could attempt to take videos of parked airliners as part of her hobby and inadvertently lose control due to an out of signal range issue which could cause a collision with a departing airliner. As the majority of UAS owners are hobbyists, many of them are untrained or inexperienced in controlling an UAS. Existing regulation and policy are unable to track hobbyists' operating proficiency before allowing them to fly smaller UAS. Although there are no-fly zones around sensitive areas, a handful of incidents still occur every year as hobbyists may not understand the damage they could cause. Facilities such as airports, military camps and bases, and government buildings and prisons are already experiencing the security dilemmas just described in dealing with UAS [5]. Further, nefarious UAS activities pose an even greater threat, although so far there have been relatively few such incidents globally outside of active war zones.

Facilities have a compelling need to adopt Counter Unmanned Aerial Systems (CUASs) to proactively safeguard their assets and security. To effectively counter UAS, a CUAS require multiple sensors to detect, identify, and classify the UAS before engaging an interceptor to take down a UAS. There are multiple factors both internal and external to the CUAS system, however, that can diminish the effectiveness of a CUAS and for which the facility commander is required to adopt mitigation efforts against [6]–[8]. A big challenge facility commanders face is to stay ahead of the technological race against UAS.

Existing research has primarily focused on the technical capabilities of CUAS and UAS systems in isolation of a broader systems engineering perspective. The research in this thesis adopts a systems engineering perspective to support facility commanders in understanding a facility's potential weak points against current and emerging UAS threats, and to balance a CUAS capabilities against adjacent stakeholders' needs [9]. The proposed methodology in Chapter 2 allows the facility commander to explore the possible CUAS trade-space through evaluation and analysis to ensure that the CUAS is optimized and relevant against the fast emerging threat of UAS.

This thesis conforms to the Naval Postgraduate School (NPS) "manuscript option" that requires a manuscript be submitted to a peer-reviewed journal [10]. Chapter 2 of this thesis

is currently in review with the Multidisciplinary Digital Publishing Institute's Systems journal. Chapter 1 of this thesis has provided broader context for the work while Chapter 3 provides a summary of the work and recommends potential future directions for research on this topic beyond what is found in Chapter 2.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Manuscript Submission

2.1 System Analysis of a Counter Unmanned Aerial Systems Kill Chain in an Operational Environment

A version of this chapter was submitted in August 2021 to the *Multidisciplinary Digital Publishing Institute's Systems journal* as: C.S. Tan, D.L. Van Bossuyt, and B. Hale, "System Analysis of Counter Unmanned Aerial Systems Kill Chain in an Operational Environment."

2.2 Introduction

The fast growth in commercial Unmanned Aerial System (UAS) capabilities poses significant threats related to safety, security, and privacy in perimeter defense [11]. The defense industry sector has had to quickly implement methods to safeguard critical infrastructures against UAS, both from adversaries and civilians. Many methods found to be effective in dealing with UAS, however, can also cause disruption to other authorized operations, which makes the operation of a Counter Unmanned Aerial System (CUAS) extremely complex. For instance, an airport with an actively operating CUAS can disrupt communication signals (e.g., mobile phones, control tower, etc.) and radar signals, which can limit ground crew communications and disrupt control tower operation for critical coordinated activities such as debris reports or runway clearance for landing or taking off [12]. Yet, the consequence of not deploying CUAS can be catastrophic if a facility's perimeter were breached by a UAS. For instance, the UAS could collide with an airplane, causing a shutdown of the runway. Moreover, a UAS used by someone with ill-intent, could conduct reconnaissance and surveillance, conduct strikes on targets with weaponized UAS capabilities, or deliver a payload that contains explosives or chemicals [13]. The situations just mentioned represent only a few of the security dilemmas that facility commanders face today in dealing with UAS.

Existing research and implementation of CUAS has focused largely on the technical capabilities of CUAS and UAS systems such as detection, identification, and classification of UAS, the study of CUAS kill chains with or without a human in the loop, and the limitations of passive or active counter measures. Research has not focused on the broader systems perspective. Although there is research on the adoption of UAS and CUAS in military and perimeter security operations (e.g., airports, camps, and bases), only limited work examines the full impacts on adjacent stakeholders and civilians within the perimeter vicinity during the activation of CUAS interceptor systems in order to counter UAS threats or intrusions.

Developing a systems perspective on CUAS effectiveness in addressing current and emerging UAS threats may help facility commanders to better identify potential weak points in their defenses. A systems perspective on mitigation measures to reduce the risk of a successful UAS attack through a variety of means (e.g., new CUAS systems, progressive levels of defense approaching sensitive assets, etc.) to counter UAS threats is also needed to help facility commanders make decisions on potential CUAS upgrades. At the same time,

a systems perspective on how CUAS operations may affect adjacent stakeholders (e.g., allied forces operations and civilians) is needed to aid in balancing CUAS capabilities with adjacent stakeholders' needs.

2.2.1 Specific Contributions

This research presents a systems engineering evaluation and analysis process to review the effectiveness of currently deployed CUAS in supporting facility operations. The proposed process is intended for facility commanders to understand CUAS vulnerabilities and consider the possible effects their current CUAS may have on adjacent allied forces and civilians (e.g., jamming, spoofing, etc.). A trade-off study can be completed through the proposed evaluation and analysis method. This approach can then be used to develop an upgrade or implementation plan to better defend facilities against the evolving UAS threat while reducing impacts to adjacent stakeholders' operations. The Singapore Armed Forces (SAF), Department of Defense (DOD), civilian airports, and other facilities that may be targets of UAS can benefit from this research.

2.3 Background and Related Research

This section provides the required background knowledge and describes related research on CUAS and UAS technical capabilities to assist in understanding the discussion and the step-by-step process proposed in Section 2.4. Additionally, a review of the existing literature on evaluation and analysis of CUAS is presented.

2.3.1 Specific Threats from UAS

The concept of the UAS was adopted by the military in 1849, when Austria used unmanned balloons stuffed with explosives to attack Venice [14]. The unmanned balloons blew off course, however, and were unable to reach their target. This failure motivated further UAS technological development. Today, the U.S. military and many other defense forces have successfully adopted UAS to conduct operations such as precision strikes; electronic attacks; and intelligence, surveillance and reconnaissance (ISR). UAS have proven effective during military operations such as Operation Enduring Freedom and Operation Iraqi Freedom [15], [16].

Beyond the military, the commercial sector is investing in UAS development, as they see potential economic growth from UAS deployment in the next few years ushering in the Fourth Industrial Revolution [17], [18]. The rise in UAS-related patent submissions over the last 30 years (from about 20 to about 12,000) demonstrates the explosive growth in this sector, as shown in Figure 2.1, Developments over the last 30 years have included sophisticated capabilities such as motion tracking, visual projection, thermal scanning, light detection and ranging, 3D environment mapping, facial recognition, and obstacle avoidance. UAS support many uses in agriculture, mining, manufacturing, logistics, security firms, marketing, construction, and infrastructure. These capabilities have also attracted hobbyists who have formed a community to adopt UAS for recreational uses [2] such as taking pictures of scenery, videos, or racing. At the same time, unapproved media recordings may lead to security concerns among respective stakeholders. Hence, the recent growth in both the capabilities and the adoption rate of small Commercial Off The Shelf (COTS) UAS poses a significant threat to security facilities as well as civilian facilities [3], [4].

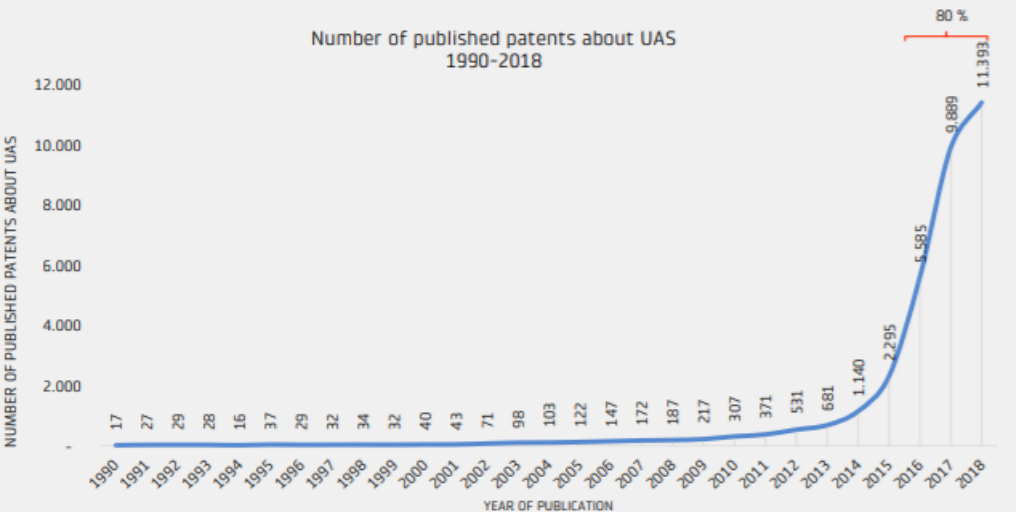

Figure 2.1. Number of Published Patents About UAS between 1990 and 2018. Source: [19].

UAS Group Classification

UAS are often classified by top speed, Max Gross Take-Off Weight (MGTOW), and maximum operating altitude. The groupings of UAS by basic capabilities and weight are given in **Table 2.1**.

Table 2.1. UAS Groupings. Source: [3].

UAS Group	Weight Range (lbs.) MGTOW	Nominal Operating Altitude	Speed (knots)	Representative UAS
Group 1	0 – 20	<1,200 Above Ground Level (AGL)	100	Raven (RQ-11), WASP DJI Phantom, Solo, Typhoon H, Ghostdrone 2.0
Group 2	21 – 55	<3,500 AGL	<250	ScanEagle
Group 3	<1,320	<Flight Level (FL) 180	<250	Shadow (RQ-7B) Tier II / STUAS
Group 4	>1,320	<FL 180	Any	Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warrior ERMP (MQ-1C)
Group 5	>1,320	>FL 180	Any	Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)

Capabilities of UAS

UAS classification provides a quick guide to what a particular group of UAS can be used for and the type of capabilities the UAS can employ. In this research, the UAS capabilities of concern are payload-enabled capabilities, self-modification capabilities, and swarm capabilities.

Payload-Enabled Capabilities The MGTOW is the payload weight limit that the UAS can carry, which narrows down the type of capabilities the UAS has. The most common low-cost payloads are non-sensing payloads that do not gather or transmit any type of information to the operator. Such payloads can be anything from homemade explosives to biological or radiological payloads (e.g., Chemical, Biological, Radiological and Explosives (CBRE)). Delivery of such payloads requires the target to be in the operator's line-of-sight. By contrast, COTS payloads with capabilities such as live video feeds enable the conduct of Intelligence, Surveillance, and Reconnaissance (ISR) operations and precision strikes. These capabilities, however, are limited by the energy consumption of the UAS. Finally, a countermeasures payload can disrupt a wide range of operations using Radio Frequency (RF) jamming or electromagnetic systems. Like sensing payloads, countermeasures payloads are limited by UAS energy consumption. A list of payload enabled capabilities is shown in **Table 2.2**.

Table 2.2. Types of Payload-Enabled Capabilities

Type	Capabilities
Non-Sensing Payload	
Kamikaze	Both the payload and UAS crashes into the target.
Payload Release	The payload is carried to a certain altitude and is released upon hovering above the target.
Sensing Payload	
Electro-Optic	The payload provides imagery and video recording functions to support ISR operations.
Light Detection and Ranging (LIDAR)	The pulsing of a laser for a given time that enables distance measurements.
Countermeasure Payload	
Spoofers	The spoofing capability payload disrupts navigational or command and control receiver systems, such as those that rely on the Global Navigation Satellite System (GNSS).
Jammers	The payload overloads sensor inputs which cause disruption to operations.

Self-Modification Capabilities Another unique feature some COTS UAS have is that they are packed in kit boxes and require self-assembly of premade components [20]. This feature enables hobbyists with a certain level of knowledge in model aircraft and basic electrical engineering, or with online learning resources to mix and match components to achieve

desired capabilities.

With the proliferation of low-cost materials and available design templates online, additive manufacturing (3D printing) enables the creation of parts, which makes UAS design and assembly customizable and enables rapid experimentation [21]. Such one-off designs are harder to track by authorities as they lack a paper trail, which allows users with malicious intent to adapt devices for nefarious purposes.

Swarm Capabilities As the complexity of military missions increase, the need to complete more and complex high-risk tasks increases and drives the study of UAS deployment. Within the defense community, on going research efforts focus on designing UAS to operate in swarms, which can improve the efficiency of ISR, Maritime Interdiction Operations (MIO), Humanitarian Assistance and Disaster Relief (HADR), and Search And Rescue (SAR) missions [22].

The commercial sector has found use for swarm technology as a means for entertainment at large scale events. Commercial swarm technology can be seen in recent publicized events, where a swarm of UAS was coordinated for lighting displays that switched between different formations [23]–[26]. For instance, in China, swarm UAS were recently used for marketing purposes in which QR codes were illuminated in the sky. Displaying QR codes can raise several cyber-security concerns that are beyond the scope of this research [27], [28].

UAS swarm capabilities are achieved by adopting an automation architecture or utilizing Artificial Intelligence (AI) and Machine Learning (ML) to support UAS in basic self-organized maneuvers and assist an individual operator in controlling multiple UASs for a common mission. These decentralized and self-organized approaches are commonly known as Swarm Intelligence (SI), which direct flocking, herding, and schooling that resemble collective behavior found in animals. SI supports UAS in solving complex issues through cooperation and operating within a set of rules embedded in the system [29]. History consistency of flocking coordination decisions may be assisted through application of blockchain [30]–[33]. As operations are decentralized to swarm UASs, there is the increased possibility of cyber-vulnerabilities.

Although there is the possibility of a UAS swarm intruding into a facility, the likelihood of such an attack may be low, as the cost and space required to mount such a coordinated attack

is most likely affordable only for a state actor or large organization with its own fleet of UAS. This reduces the probability of a large-scale swarm UAS occurrence. Moreover, with currently available CUAS, it is highly unlikely that the simultaneous launch of multiple UASs would not be detected early, as the signature created at the launch site would be significant. Nevertheless, the risk should not be completely ruled out, as the fast growth in swarm technology could support future grey zone warfare in the event of rising tensions between nations.

The direct threat of concern to many facilities is small COTS UAS (Group 1 and 2) and modified UAS, which are inexpensive, easily acquired, and difficult to detect and intercept [5]. As the adoption of UAS by the public has increased, there are increasing reports of UAS intrusions and sightings that have disrupted facility operations and caused monetary losses, flights delays, and unnecessary risks (e.g., the2018 Gatwick drone incident and the 2019 Changi Airport drone incident [34], [35]). A 2018 study by the CUAS capabilities analysis working group established the most probable nefarious uses of UAS by non-state actors are for ISR, conveyance of contraband, kamikaze explosive attacks, and CBRE attacks.

2.3.2 Counter Unmanned Aerial System

Currently, a wide range of CUAS solutions with various configurations can be purchased as separate systems or suites of systems that can be adopted directly [36]–[38]. The concept behind the proposed system solution composed of products from different companies is similar – namely, the ability to detect and intercept UAS.

Several considerations influence the CUAS system configuration and performance such as the level of facility security required, the expected time needed from initial detection UAS intrusion until interdiction of the UAS occurs, and the type of deployed interceptor system (e.g., kinetic, RF jamming, energy pulse, etc.). Given the need for flexibility in system configurations, the cost of deploying CUAS is relatively high for a sophisticated solution. As a complex system of systems, this solution requires detailed study of the environment in which the CUAS operates (e.g., nearby tall buildings, terrain, weather, other environmental behavior factors, etc.) to mitigate possible interference that may cause poor system performance. A typical CUAS Operational Viewpoint - 1 (OV-1) is shown in **Figure 2.2**.

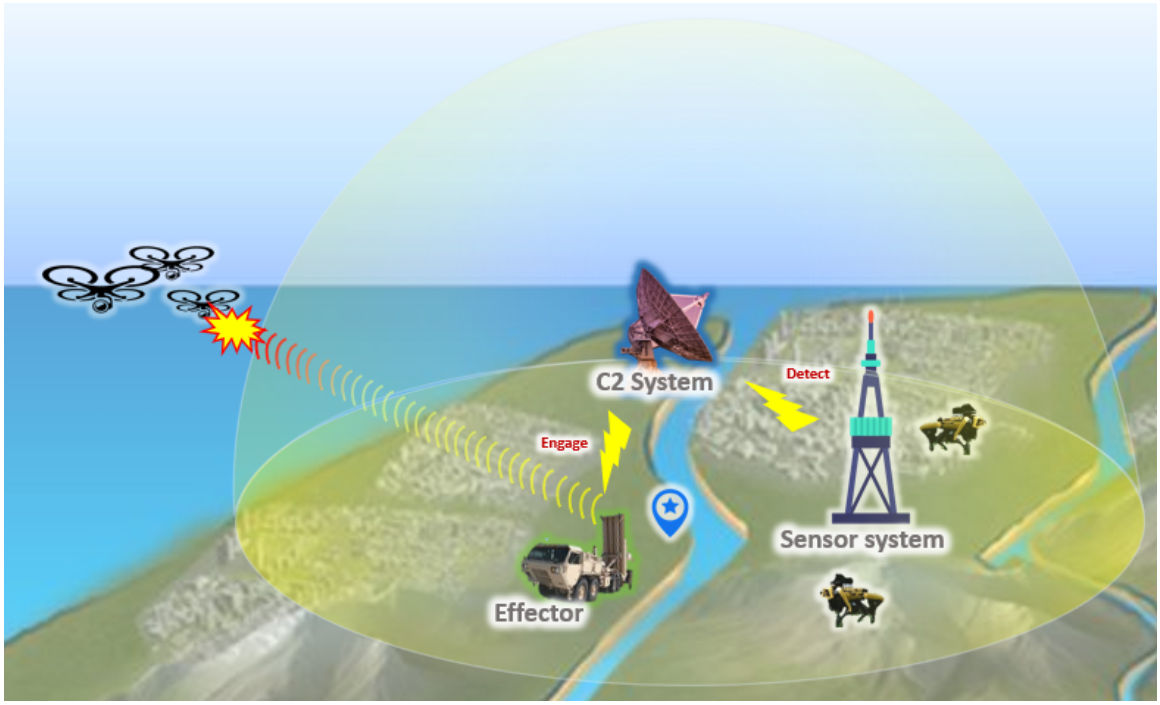

Figure 2.2. OV-1 of Typical CUAS Operation

System Kill Chain

The CUAS kill chain model is similar to the generic military application of Find, Fix, Track, Target, Engage, Assess (F2T2EA), and the definition of each process is given in **Table 2.3**.

With an understanding of the F2T2EA kill chain, we suggest that the CUAS kill chain can then be simplified for the purposes of this research from F2T2EA to detection and interception only. Detection consists of find, fix, track; and the remaining processes fall under interception. This simplification helps in associating the kill chain process with physical subsystem capabilities and key performance metrics that are discussed in Section 2.3.2 and Section 2.4.

Subsystem Capabilities

The proposed CUAS requires three key subsystems to effectively counter incoming UAS.

Table 2.3. Definition of F2T2EA Kill Chain. Adapted from [39]

Kill Chain	Definition
Find	Identify a target. Find a target within surveillance or reconnaissance data or via intelligence means.
Fix	Fix the target's location. Obtain specific coordinates for the target either from existing data or by collecting additional data.
Track	Monitor the target's movement. Keep track of the target until either a decision is made not to engage the target or the target is successfully engaged.
Target	Select an appropriate weapon or asset to use on the target to create desired effects. Apply command and control capabilities to assess the value of the target and the availability of appropriate weapons to engage it.
Engage	Apply the weapon to the target.
Assess	Evaluate effects of the attack, including any intelligence gathered at the location.

The first subsystem is the sensor system which performs the initial detection of the kill chain process and conducts sensing only and investigates the cause of a potential UAS detection. The sensor system consists of multiple sensors that can sense, maintain track, and identify an incoming UAS. A list of typical CUAS sensors is given in **Table 2.4**.

Table 2.4. Sensor Systems.

Systems	Capabilities
Radar	Some UAS may be identified via radar signature. Radar may also be applied to device tracking. Unlike RF, the radar signature of a UAS must be distinguished from radar signatures for birds, etc.
Radio-frequency (RF)	RF scanning supports the detection and geolocation of UAS based on communication link frequencies. The UAS may also be identified by RF behavior in some cases.
Acoustic	UASs can be identified by acoustic signatures generated from operating motors.
Electro-optical (EO)	Identifies and tracks the UAS based on its visual signature.
Infrared (IR)	IR uses heat signatures for identifying and tracking the UAS.

The second subsystem is the Command and Control (C2) system that performs the second part of the detection kill chain process. The C2 system classifies and assesses the situation, and subsequently provides decision-making assistance to the CUAS operator. The C2 system can fuse multiple sensors' data, map the situation, confirm the threat, and provide decision-making assistance and dissemination of information to the onsite response team. As there are many different types of software that can be used to fulfill these requirements, this research stays at a generic level with regards to software.

The third subsystem is the interceptor system, which performs the interception function of the kill chain process. The interceptor system may consist of soft kill [40] and/or hard kill [41]–[44] systems (see Table 2.5 for details) that can temporarily or permanently disable or disrupt the UAS from continuing its mission.

Table 2.5. Soft and Hard Kill Interceptor Capabilities.

Systems	Capabilities
Soft Kill Interceptor	
RF Jamming	Radio frequencies are susceptible to frequency jamming, where RF interference is generated to effectively block the RF connection between the UAS and the operator or between more than oneUAS.
GNSS Jamming	As with RF jamming, GNSS jamming blocks connection to the device. In the case of GNSS, jamming is against the satellite link to the UAS, e.g. GPS or GLONASS, which provides essential navigation information.
Spoofing	Spoofing often implies a break in the cryptographic entity authentication between the device and the operator/GNSS satellite. Spoofing an operator allows the attacker to impersonate the operator to the UAS, taking control of the device or redirecting it. If spoofing the GNSS link, the attacker may feed false navigation information to the device. Spoofing may also be used by some researchers to imply a break in the channel (data confidentiality or authenticity) providing information on the UAS and operator link, or the GNSS link.
Dazzling	High-intensity lasers or light beams can be used to render UAS camera use ineffective.
Hard Kill Interceptor	
Laser	High-intensity lasers can be used for directed energy against a UAS, melting or weakening key components.
Microwave	Like lasers, directed high-intensity microwaves can be used to disable the UAS' electronic systems.
Nets	Physical nets can entangle and trap a UAS.
Projectile	Physical projectiles, including ammunition, can be used to kinetically take down a UAS.
Collision UAS	A custom UAS may be flown against the target UAS with the intent to collide with it and produce a kinetic take-down.

Challenges

Although the CUAS may consist of multiple subsystems that have overlapping capabilities in order to ensure a high level of success intercepting UASs, a number of external factors

and challenges remain that are not within the controls of the system and can diminish overall effectiveness in addressing a UAS intrusion.

The first challenge relates to the detection effectiveness of the sensors, which can be greatly affected by some UAS capabilities [6]. For instance, a UAS with high maneuverability enables close-to-the-ground and sea flying that can dampen a radar's ability to detect the UAS. Similarly, a UAS entering a facility from a direction with backlighting by strong light sources such as the sun or from beyond tall buildings with a limited Line-Of-Sight (LOS) will reduce the Electro Optical (EO) and Infrared (IR) sensors' detection effectiveness. Another factor is adverse weather, which can cause attenuation of RF signals and reduce RF sensor effectiveness. Therefore, detection effectiveness is based on the specific ability of each type of sensor to investigate intrusion throughout the environment and the available LOS between the CUAS sensors and the UAS. In addition, the UAS MGTOW may also contribute to detection interference, as it allows the UAS to carry payloads such as electromagnetic devices that can cause interference or damage to the sensors' capabilities. In the near future, it is likely that many operating environments will include the use of friendly UAS within the area of operation [45]–[47]. Thus, there is a strong need to ensure that the CUAS possesses the capabilities to identify, classify, and differentiate between friends and foes in detected UASs to avoid missed or unintentional engagements. These limitations pose a crucial requirement to have a sufficient buffer to compensate for errors during the short and complex response window in which to deal with both authorized and unauthorized UASs, as the effectiveness of the CUAS interceptor system can decrease rapidly as time passes and an unauthorized UAS approaches an intended target.

The second challenge relates to the facility's legal rights and public image when applying passive or active countermeasures during a UAS intrusion [7]. There are rising concerns about the application of CUAS interceptors in operating environments including the possibility of causing collateral damage such as a disrupted UAS falling out of the sky and causing injury to bystanders and damage to infrastructure [5].Ongoing debates are already focused on whether the application of an interceptor should be limited and used only as a last resort, a prospect that would greatly reduce the effectiveness of a CUAS [7], [8].

The third challenge relates to the emerging requirement of forensic study of intercepted UASs. Forensic study processes are known to be labor intensive and require much effort

to find evidence of an operator's intention through examination of media storage [48]. Nonetheless, the benefit of forensic study is high as it will assist in the vulnerability assessment of a facility and in establishing improvement requirements for a CUAS. This extracted data can include flight path coordinates, pictures, and videos that will provide data to aid in the enhancement of base security such as extending fenceline boundaries, increased foot patrol in an area, etc. [48]–[51]. With this in mind, it should be noted that forensic study requires more resources and technical expertise among responding personnel to prevent unintentional tampering with or destruction of evidence while extracting data from the intercepted UAS's media storage. The debate is, therefore, whether a dedicated team of technical experts is required to conduct forensic study on detained UASs.

The last challenge concerns the consequences of engaging a misidentified target. There are few studies on the consequences of misidentified UAS; however, multiple broadly publicized incidents involving passenger aircraft being misidentified and subsequently shot down by air defense systems due to mis-identification exist [52]–[55]. For instance, the incident involving Flight PS752 which was shot down due to mis-identification by an air defense unit in the suburbs of Tehran [55] provides an example of what a CUAS system could do if it were to misidentify an incoming object. Per investigations into Flight PS752, the air defense targeting system unit failed to re-calibrate and deemed that the aircraft was flying toward Tehran at a low altitude. The defense unit operator attempted to inform the C2 center of the suspected incoming threat, but the message was unable to be transmitted for unknown reasons. The operator violated standard procedures by firing at the presumed hostile target without receiving approval. With that in mind, the design of CUAS solutions should include remediation to immediately hold or stop such an action and prevent a catastrophic outcome.

2.3.3 Existing Methods of Developing and Deploying a CUAS

Several methods exist to develop and deploy a CUAS and related physical protection systems. Such approaches include Garcia's physical protection design and evaluation method, which begins with the determination of the physical protection system objectives that characterize the physical facility, define threats, and develop target identification. Next, the design of the system splits into three broad categories of *detection*, *delay*, and *response*. The analysis is then carried out on the system design to determine whether the system design has met the requirements, and lastly, whether it is ready to be output as a final design or iterated back to

the redesign loop.

A related method is the National Institute of Standards and Technology (NIST) risk management framework, which provides a generic process that can be applied to any type of system [56]. The processes within this framework are *prepare*, *categorize*, *select*, *implement*, *assess*, *authorize* and *monitor*. Each process must meet a certain objective that guides an organization in adopting a more comprehensive risk management plan. The *prepare* step identifies the key risk management roles and an established strategy that can be adopted organization-wide. The *categorize* step ranks the risk according to the impact level and appoints an appropriate approving authority. Then the *selection* of control measures to be allocated to specific system components is made. The *implement* step applies the controls for the system and the organization. The next step, *assessment*, assesses whether the controls have met the intended outcome. The approving authority then reviews the assessment to see whether the risk management plan is acceptable. The final step is the continuous monitoring of the risk on the control implementation to allow timely review or intervention.

In general, the concepts and principles of the two methods just described are relevant and applicable for adoption in conducting the analysis of a CUAS system. While they do not directly address the need of a CUAS design method, these principles do provide inspiration for this research.

2.4 Methodology

Rapidly developing UAS technology has disrupted the design and implementation of CUAS systems. Consequently, scope creep and new requirements are often introduced late in the CUAS system design cycle, which can lead to higher overall project cost or a failed CUAS deployment. In order to successfully deliver CUAS solutions to facilities, it is essential to develop a cost-effective and comprehensive system analysis method that can ensure the designed CUAS stays relevant against emerging UAS technology and threats. This section proposes a systems perspective analysis method that can guide a facility commander in developing new CUAS capabilities and augmenting an existing CUAS. The proposed methodology provides insights for how the CUAS system can be optimized to achieve required system effectiveness and allow timely intervention to propose CUAS system redesign solutions. The proposed methodology illustrated in Figure 2.3 is not dependent on

any specific CUAS technology and can be adopted by any facility to conduct analysis and evaluation of potential and existing CUAS systems.

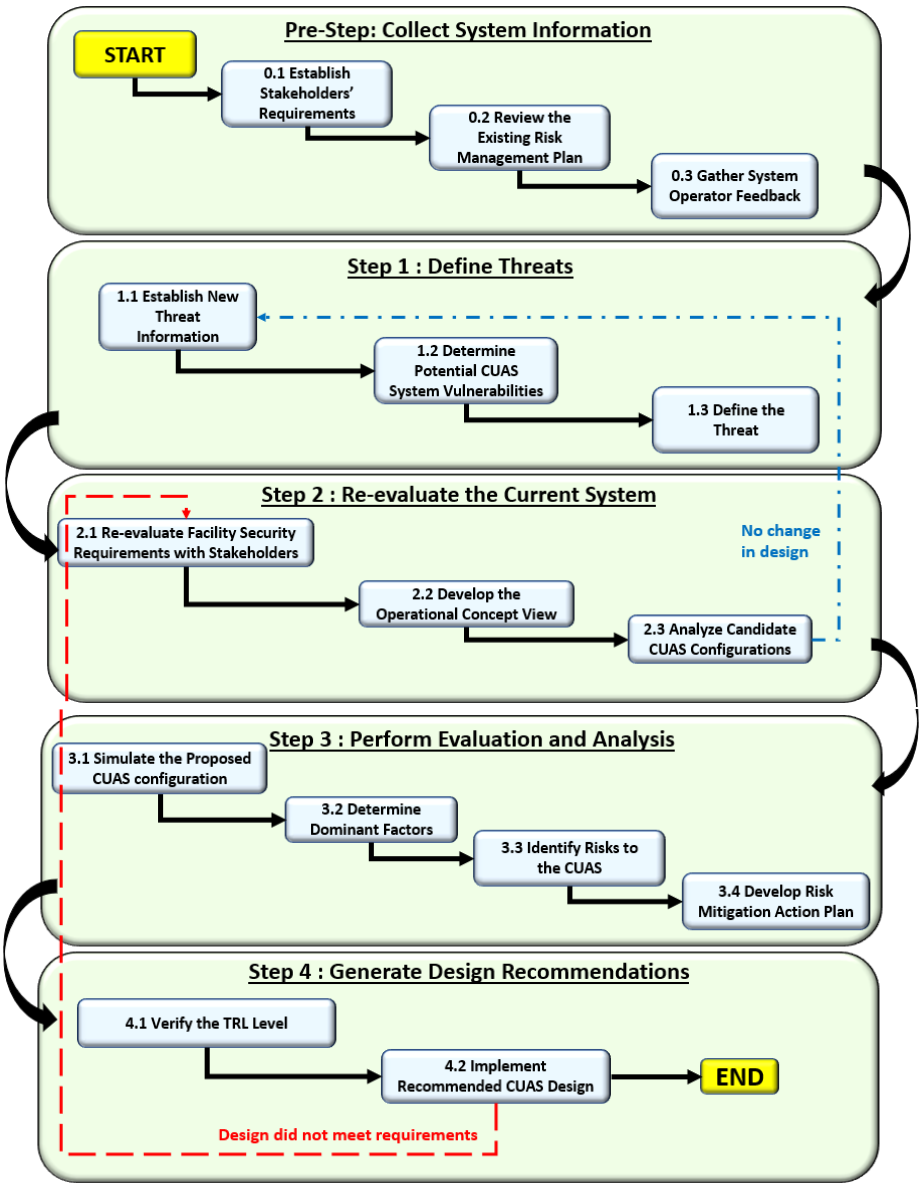

Figure 2.3. Overview of the Proposed Methodology. The methodology is intended for use by facility commanders to analyze existing CUAS effectiveness, identify CUAS capabilities gaps, produce CUAS upgrade recommendations, and provide CUAS system design reviews.

2.4.1 Pre-Step: Collect System Information

There are two events that can trigger the pre-step process. The first event is the identification of emerging UAS capabilities that pose a new threat to the currently deployed CUAS at a facility, creating a technological gap between the CUAS and the threat. It is assumed that the pre-step has not been completed for the facility before and thus must now be done. The second event is the availability of newly developed CUAS capabilities, and that can address the existing outstanding CUAS threats a facility faces. These two events are iterated upon throughout the design process and even after the system is delivered to ensure timely intervention to maintain the intended CUAS requirements for the facility. Without either of these events occurring, there is likely no need to use the proposed methodology.

The objective of the pre-step is to gather current and historical data about the CUAS. The gathered data establishes the current state of the CUAS for further investigation and analysis work by facility commanders. It is recommended to use Model Based Systems Engineering (MBSE) tools such as Core, Innoslate, and others to assist in performing analysis and evaluation work [57]. However, it is not mandatory and the analysis can still be carried out without the use of MBSE tools.

Step 0.1: Establish Stakeholders' Requirements

The initial data required from the stakeholders should detail the (1) daily activities within the facility, (2) expected environmental conditions, and (3) facility security requirements.

The daily activities data can be human or asset (e.g., planes, cargo vessels, etc.) traffic flow, routine operations, and possible ad-hoc operations that need to be carried out by the respective stakeholders. This information can provide a baseline of the types of daily activities that will be in operation alongside the CUAS at the facility.

Next, to understand the expected environmental conditions in which the system needs to operate, it is important to gather facility blueprints, identify the maximum and minimum boundaries of the facility (some facilities have zones of protection that extend beyond the site boundary), conduct a direct LOS study, identify possible wildlife activity, and collect historical weather condition data. This effort identifies the environment's "noise" that could interfere with CUAS system performance.

Finally, the stakeholders are to determine their expectations for the CUAS security requirements. This requires the stakeholders to list their critical assets with the expected level of protection and security classification of the assets.

The objective in this step is to determine the expected CUAS operation conditions and acceptable security level so that the system can be configured to meet all stakeholder requirements.

Step 0.2: Review the Existing Risk Management Plan

In this step, it is important to understand the current risk management plan to determine and address the inherent vulnerability of the existing CUAS. The inherent vulnerability can be associated with any of these three areas: the first is physical system failures such as electrical faults, inclement weather, fires, and accidents. The second is potential infrastructure damage and injuries to personnel caused by falling intercepted UAS. The third type are the risks posed by cyber security itself, which may have catastrophic outcomes such as if an attacker successfully gains control of either the CUAS's detection or interception systems.

The review of the existing risk management plan helps to determine whether there is any impact on existing vulnerabilities introduced by a new CUAS design solution. Ideally, a new CUAS design solution should cut down on the number of risks that the existing risk management plan must address. Otherwise, there is a need to identify new mitigation measures that may overlap with the existing risk management plan.

The objective in this step is to allow the facility commander to have a thorough and accurate view of the impact of CUAS activities on daily operations. This will be achieved by garnering collective agreement from the various stakeholders about the mitigation plans that will be in place to manage the identified inherent risks [58].

Step 0.3: Gather System Operator Feedback

The last step of the pre-step phase is to gather feedback from the personnel who interact with the CUAS. To achieve high overall CUAS effectiveness, it is good practice to include current operators or personnel who interact with the CUAS during design reviews, as these users may uncover constraints or beneficial concepts that otherwise would not be recognized.

These data can then support Human Factors Engineering (HFE) design efforts that improve the interaction between the operator and the system [59]. This interaction improvement implies a better response time and reduction in human errors, as the interaction is more intuitive for the operator, which also increases the overall system effectiveness.

2.4.2 Step 1: Define Threats

In Step 1, the objective is to assemble current technical specifications of the Group 1 and Group 2 UASs. A static list of technical specifications cannot be used because UAS development is constantly advancing which translates into new capabilities frequently emerging [60].

Step 1.1: Establish New Threat Information

As discussed in Section 2.3.1, the facility commander must understand UAS capabilities that are of concern to the facility. Such concerns can be payload enabled capabilities, self-modification capabilities, and swarm capabilities among others. For instance, if any of the aforementioned capabilities have been made available to COTS UAS, the facility commander should review the existing CUAS and determine whether the current CUAS design solution is still relevant to manage the new threat. Hence, the facility commander needs to collect both UAS and CUAS capability parameters to conduct the system analysis.

Step 1.2: Determine Potential CUAS System Vulnerabilities

To determine potential CUAS system vulnerabilities, it is essential to develop an understanding of baseline system performance. We recommend that the CUAS system's baseline performance be established through the listing of expected daily operations and be based on possible UAS intrusion scenarios that may occur at the facility. Furthermore, potential future scenarios should also be considered. The subsequent CUAS evaluation can then harness the insights on vulnerabilities of the CUAS.

Given the identified vulnerabilities and data developed in the previous steps, it is now possible to provide tangible measurements of the CUAS's effectiveness. To this end, we derive a generic mathematical representation of the probability of CUAS effectiveness from Kouhestani [61]. CUAS effectiveness can be determined by Equation 2.1, which is the

product of probability of detection and probability of interception. The breakdown of the two sub-functions' equations is explained in subsequent sections.

$$P(Effectiveness) = P(Detection) \times P(Interception) \tag{2.1}$$

The probability of detection functions refers to the probability of the sensor detecting the presence of a UAS. This includes the element of accurate identification and classification of the UAS, which can also be implied as the false alarm rate. The three sub-performance metrics of detection effectiveness in terms of probability are; sensing, tracking, and data transmission. The relationship between each of the sub-performance metrics and their definitions are given in **Equation 2.2** and **Table 2.6**, respectively.

$$P(Detection) = P(Sense) \times P(Track) \times P(Transmission) \tag{2.2}$$

Table 2.6. Performance Metrics and Definitions of Detection

Performance Metrics	Definitions
Detection Effectiveness	
Probability of Sensing	The probability of the sensors being able to detect the presence of UAS and initiate an alarm. A higher probability of sensing will increase the CUAS success rate of accurately detecting UAS.
Probability of Tracking	The probability of accurately tracking the UAS's geolocation. A lower rate of drops in tracking increases the CUAS's accuracy in acquiring the UAS's position.
Probability of Transmission	The probability of data being transferred over a specific period such data might include UAS models and coordinates that will be successfully transmitted to the response team or interceptor. If the analysis is to omit or have a perfect transmission rate, the value of probability of transmission is kept as 1.

The probability of interception refers to the likelihood that the CUAS system can deny or disable a UAS from continuing its intended mission. The sub-performance metrics that make up the interception effectiveness in terms of probability are; hit, kill/deny, and risk. The relationship between each sub-performance metric and their definitions are given in **Equation 2.3** and **Table 2.7**, respectively.

$$P(interception) = P(Hit) \times P(Kill/Deny) \times P(Risk) \tag{2.3}$$

Table 2.7. Performance Metrics and Definitions of Interception

Performance Metrics	Definitions
Interception Effectiveness	
Probability of Hit	The probability of successful contact being made by the interceptor to the UAS by either hard (e.g., projectiles) or soft (e.g., electromagnetic waves) kill method. A higher probability correlates with better effectiveness.
Probability of Kill/Deny	The probability of successful denial or destruction of the UAS after being contacted by the interceptor. A higher probability correlates with better effectiveness.
Probability of Risk	The probability of possible injury to a person or damage to infrastructure due to a UAS falling or accidentally colliding with an obstacle following interceptor action. Based on a study conducted by [5], the probability that a Group 1 or Group 2 UAS can cause that impact is about 2-6% and it can remain in this state throughout the evaluation.

In addition to the aforementioned mathematical relationship, it is also important to consider any of the existing mitigation measures that will be applied to reduce collateral damage. These mitigation measures are then evaluated as part of system vulnerability reduction in a subsequent step.

Step 1.3: Define the Threat

With the vulnerabilities identified, the facility commander should next associate specific threats with specific risk levels and then link the risk levels to respective system vulnerabilities. A threat can be defined by measuring the severity of the threat and how this could cause the associated system vulnerability.

2.4.3 Step 2: Re-evaluate the Current System

In Step 1, the process focused on the CUAS's technical performance. In Step 2, the process focuses on human factors that may affect CUAS performance from the perspectives of adaptability and usability. The aim is to optimize and choose only changes that reduce the CUAS's impact on the people and operations within the facility.

To better understand the current system, more data such as building blueprints, existing surveillance systems, perimeter environmental behavior, and standard operating procedure documents are reviewed in detail. These documents should provide a good starting point for a systems perspective of the overall effectiveness of the current CUAS that the facility commander can use for analysis.

Step 2.1: Re-evaluate Facility Security Requirements with Stakeholders

With an understanding of current CUAS system capabilities in mind, it is important to conduct a meeting with the respective stakeholders to verify whether the current CUAS performance meets facility requirements. This includes the identification of the respective stakeholders' critical assets and critical asset locations within the facility, which will determine the level of protection within that zone. This requirement provides the criteria for the baseline of needed CUAS performance. The stakeholders must collectively agree and commit to the operational requirements and safety constraints identified in this and previous steps. If there is dispute over requirements, the facility commander will decide and direct the stakeholders to accept compromises between their operation and security needs.

Step 2.2: Develop the Operational Concept View

At this point, a variety of OV-1s and accompanying system architectural products should be developed to demonstrate multiple potential CUAS system configurations. These CUAS configurations will be used in subsequent steps for comparison against requirements and eventually determine that the current CUAS is sufficient or that the CUAS should be either upgraded or replaced.

We suggest that it is particularly important to develop the OV-1 view because it allows the facility commander and stakeholders to have a visualization of the CUAS system perspective. This helps to clarify interactions or identify missing interactions between portions of the

base and its surrounding community and the CUAS. The case study in a subsequent section provides an example of OV-1.

Step 2.3: Analyze Candidate CUAS Configurations

Now that several CUAS configuration candidates have been developed, a trade-off analysis of requirements can be conducted. We recommend the Pugh Matrix approach because it provides a method for scoring in terms of positive or negative impacts on specific requirements based on the facility commander's best intuition according to the available data [62].

The Pugh Matrix analysis results can identify which CUAS configurations are the most preferred. The CUAS configurations are ranked based on the stakeholders' requirements and translated into a decision to improve an existing CUAS (or build a new CUAS if none already exists) or to remain with the existing CUAS.

If the prospective' CUAS configuration solution's benefit is lower or matches the current CUAS, the recommendation is that no change to the current CUAS be undertaken. In this case, return to Step 1 for continued monitoring of the situation for future emerging UAS threats. Otherwise, if there are technological gaps found in the capabilities of the existing CUAS against a UAS, proceed to Step 3.

2.4.4 Step 3: Perform Evaluation and Analysis

In Step 3, a more in-depth evaluation and analysis is conducted to assess the effectiveness of the proposed CUAS solution from Step 2.3. This step includes generating the workflow of the proposed solution and using MBSE software to conduct simulation work.

Step 3.1: Simulate the Proposed CUAS Configuration

In this step, MBSE software is used to conduct detailed evaluations of the proposed CUAS configuration. In the case study presented in this research, CORE software is used to conduct the simulation of the CUAS's functions which allows the facility commander to assess the feasibility of the function's interactions. That said, many other MBSE software packages are available and have similar functionality.

Step 3.2: Determine Dominant Factors

The objective in this step is to identify the dominant factors that have the most impact on overall CUAS performance by simulating the down-selected CUAS configuration identified in Step 3.1. This approach reduces the cost and time required to assess the new CUAS configuration that may not otherwise have sufficient real-world data points for detailed analysis. Another benefit of conducting simulations is that they can explore high risk scenarios involving personnel, hazardous payloads, and other threats which would be dangerous to conduct physically. We suggest conducting a Design of Experiment (DOE) as part of this step using software such as Minitab, ExtendSim, or CORE to generate time-based simulations. Doing so can produce results such as outcome probability distributions, identify delays and bottlenecks in the CUAS response, and implement probabilistic decision making that can improve realism in the simulations [3], [63].

The interaction between the UAS and CUAS capabilities generates certain important interaction effects; the relationship of those interaction effects is illustrated in Table 2.8.

Table 2.8. Effects of the UAS and CUAS Capabilities Interactions

System	Capability Parameter	Effects	Rationale
UAS	Maximum Range	Detection Range	To make earlier detection possible, the detection coverage should include the UAS maximum distance outwards starting from the facility's outer perimeter.
UAS	Maximum Speed	Response Time	Required to intercept before the UAS achieves the objective.
CUAS	Identification and Classification Time	Reaction Time	This duration must be much shorter and within the response time. This could also be used to determine whether this process should be managed by human-in-the-loop or full automation.
CUAS	Tracking Capacity	Software Algorithm and Sensors Capabilities	This will determine the CUAS's ability to deal with a UAS swarm.
CUAS	Maximum Interceptor Range	Engagement Window	It will be ideal for the interceptor to be able to engage as soon as possible.

Step 3.3: Identify Risks to the CUAS

In this step, risks to the CUAS are identified to allow for mitigation strategies to be developed in the subsequent step. In this context, we are interested in risk of the CUAS not performing as intended.

CUAS system risks can be caused by limitations that are inherent to some CUAS subsystems such as sensors and interceptors requiring LOS with the UAS, no sun glare, and other related interferences. The CUAS is designed as a system of systems which aims to address the individual sensor's and interceptor's vulnerabilities and eliminate such single points of failure. Additional risks may be present such as bypassing (e.g., through blind spots, via saturating or overloading a sensor, etc.) or spoofing sensors. Interceptors can be vulnerable if they are unable to activate in a timely manner which can lead to missed UAS engagement opportunities. Additionally, the risks to facility personnel and nearby communities caused by the CUAS must be considered. For example, an adversary's UAS that loses control due to CUAS interception may fall or crash into nearby communities.

We suggest identifying and categorizing the risk level of the aforementioned risks into high, moderate and low risk categories based on the severity of each risk outcome. We define high risk as the possibility to cause significant damage to the CUAS or severe degradation of its performance, to the facility, and/or to the surrounding community; moderate risk has the possibility to cause moderate damage to the CUAS or degradation of its performance, to the facility, and/or to the surrounding community; and low risk as the potential to cause minor damage to the CUAS or degradation in its performance, to the facility, and/or to the surrounding community.

Step 3.4: Develop Risk Mitigation Action Plans

Next, mitigation plans for each identified risk can be developed.

The aims of the mitigation plans are to increase the probability of CUAS success and reduce potential collateral damage. We suggest that this can be achieved through a review of policy, practices, and procedures associated with the CUAS. In order to reduce the likelihood of CUAS system failure, the emphasis here is to develop and implement controls over the risks. This can be done by strengthening the identified weak points of the system or by accepting the risk and creating layers of processes to neutralize it if the CUAS system cannot be

strengthened. While a variety of mitigation strategies are discussed subsequently, we assert that the main consideration for risk mitigation should be to provide ample time for the CUAS system to react safely to UAS intrusion while ensuring the safety of people operating within the vicinity. We assert that this is a conservative and safer approach than others.

The first mitigation strategy is to achieve early detection so as to increase the duration of the CUAS engagement window. Detection coverage should be as far out as can be reasonably accommodated from the facility. The probability of successful detection can be further increased by eliminating detection blind spots and reducing false alarm rates. If there is LOS blockage by tall buildings or trees, this can be mitigated by employing patrols to cover blind spots, pruning vegetation, or establishing satellite sensor locations atop the tall buildings that otherwise would block CUAS sensors. This also involves adding layers of procedures and a revamp of policy to allow installation of sensors on buildings that may not be controlled by the facility. To reduce the false alarm rate, we recommend the mitigation efforts include employing environmental studies, as discussed in previous steps, to understand the visibility conditions at different periods of the day, such as possible sun glare during sunrise and sunset, reduced visibility during inclement weather, and blockages by wildlife activities.

The second mitigation strategy is to have interceptors that are effective and will not cause disruption to facility operations or neighboring communities. The time taken to react and neutralize a UAS intrusion is expected to be swift, and the result is expected to be decisive. This mitigation strategy aims to intercept the UAS before it enters the facility or at least prior to encountering sensitive areas of the facility. We suggest employing multiple layers of interceptors to allow CUAS engagement at different distances and with different interception methods in order to eliminate the possibility of a single point of failure.

2.4.5 Step 4: Generate Design Recommendations

In the final step, the stakeholders collectively decide on CUAS upgrades and implementation.

Step 4.1: Verify the TRL Level

In this step, checks must be performed to ensure that selected CUAS technologies and configurations meet appropriate Technology Readiness Level (TRL) levels. We advocate

using Kouhestani's CUAS TRL levels where Level 1 is scenario-based testing (e.g., "red-teaming" [64]–[66]), Level 2 is exploratory testing, Level 3 is baseline characterization testing, Level 4 is performance testing (statistical confidence levels), Level 5 is degradation/vulnerability testing, and Post-Install is certification and periodic performance testing [61]. Note that Kouhestani's TRL is significantly different than other TRLs. We prefer Kouhestani's TRL levels over other approaches to TRL because it focuses on elements that are more relevant to the rapid development of technologies associated with CUAS and UAS. For the purposes of this research, we suggest that TRL Level 1 is the minimum level that any specific system or subsystem must be at within the CUAS for consideration. We recommend not evaluating TRL earlier in the methodology beyond ensuring that CUAS technologies are on track to be at TRL Level 1 by the time Step 4 is reached. This is because of the rapid development of CUAS technology, which must keep pace with the rapid development of UAS technology. If a facility was constrained to evaluate only TRL Level 5, then in our opinion, the facility would have little hope of ever countering the latest UAS threats and instead would be protected only against old and outmoded UAS threats.

After confirming the TRL levels, the results can be bundled into a package for stakeholder review.

Step 4.2: Implement Recommended CUAS Design

In this step, the stakeholders review all CUAS information compiled and developed over the previous steps. Stakeholders review the CUAS information to ensure that all requirements are met satisfactorily. If that any requirements are not met, the stakeholders must either accept that some requirements will not be met or the CUAS design needs to be revised to meet requirements. If the CUAS does not meet requirements, the method returns to Step 2 and repeats until a suitable design solution is found or the stakeholders accept the CUAS limitations.

If the CUAS meets all requirements, the facility commander can proceed with implementing CUAS capability upgrades or deploying an entirely new CUAS depending upon the situation. In parallel, the method returns to Step 2 to continuously monitor emerging UAS and CUAS technologies and capabilities that can pose threats to and create solutions for the facility. The proposed method never truly ends because the threats posed by UAS innovations are ever evolving.

2.5 Case Study

This section demonstrates the usability of the proposed methodology applied to a hypothetical airport and CUAS in a dense urban area within a tropical environment. Although the case study's hypothetical airport and environment may bear a passing resemblance to some airports, the details have been intentionally changed to retain realism while ensuring that no unintended disclosure of sensitive information could occur because of this paper. The case study assumes that a CUAS is already in operation and the expected threat is from hobby UASs consisting of COTS systems. The analysis provides evidence to determine whether emerging UAS capabilities require an upgrade to the existing CUAS's capabilities. In this case study we use the MBSE software CORE to illustrate the proposed methodology.

2.5.1 Pre-Step: Collect System Information

Step 0.1: Establish Stakeholders' Requirements

The identified key stakeholders are the facility commander, personnel working within the facility, and the CUAS operator. In a real facility, there could be multiple entities for personnel working within the facility, and ideally, they would be listed separately as they may have different levels of authority over the design solution.

The list of key stakeholders, their respective concerns, and their influence over the system design is illustrated in **Table 2.9**.

Table 2.9. Stakeholder List.

Stakeholder	Design Influence Level	Concerns
Facility Commander	High	System Cost Delivery Schedule Efficiency of the System Safety Exposure Hazard Legality
CUAS Operator	Medium	System Usability System Interface Efficiency of the System Safety Legalization
Flight Controller	Low	Safety Exposure Hazard Adjustment to Operation
Luggage Transport Team	Low	Safety Exposure Hazard Adjustment to Operation
Runaway Clearance Team	Low	Efficiency of the System Safety Exposure Hazard Adjustment to Operation
Maintenance Team	Low	Efficiency of the System Safety Exposure Hazard Adjustment to Operation

Along with the list highlighting the stakeholders' concerns, the list of daily activities provides a sense of the baseline operations within the vicinity. A sample list of daily activities is provided in **Table 2.10**.

Table 2.10. List of Daily Activities. Adapted from [67].

Activity	Number of personnel	Frequency
Airplane entering or exiting facility airspace	500	Estimated 200 flights per month (Based on Changi Airport Group's Data [68])
Luggage Transportation	6	Estimated handling 200 flights per month
Runway Clearance	4	Every 3 hours per day to clean up Precision Obstacle Free Zone
Runway Maintenance	3	Twice a month

The next step is to gather expected environmental conditions using historical data of the weather over the past several years. The average year round weather historical data can be accessed from Weather Spark's website [69] and many other data repositories. The parameters of interest to the designer are the temperature and weather conditions. These parameters determine the expected operating temperature range that the CUAS is required to withstand and the expected inclement weather such as haze, snow, and rain which will affect the sensors' sensitivity and visibility. The temperature in Singapore throughout the year is estimated to be above 24°C at the lowest and below 33°C at the highest. For the daily chance of precipitation, the lowest probability is 25% in February and the highest is 65% in November.

Lastly, the stakeholders are to determine the boundaries of their respective assets and the level of security required to guard their assets. The assets identified in this case study are

the aircraft, the "critical repelling zone" where the airplane parks, and the runway where airplane takeoffs and landings occur.

Step 0.2: Review the Existing Risk Management Plan

The existing risk management plan adopted the "isolation approach" for the physical system and operating procedure to segregate the potential risks into layers for better management. The physical system of the CUAS, like many other military systems, must have the redundancy to ensure the mission can still be carried out. The existing risk management plan is illustrated in **Table 2.11**.

Table 2.11. Risk Type, Mitigation Action, and Simulation Model Approach.

Risk Type	Mitigation Action	Simulation Model Approach
Full System Failure	Activation of soldiers to be deployed as sentry until the CUAS is back online	Increase processing time and reduce the layer defense to Last Mile layer only
Detection System Failure	Use of stand-alone portable aeroscope to manage the detection until system is back online	Increase system processing time
Interceptor System Failure	Adoption of Physical Interceptor gun by the patrol until system is back online	Reduce the layer defense to remaining the Last Mile layer
Crashing UAS	1) Segregation of engagement area into Outer, Inner, and Last Mile layers. Based on personnel concentration, Outer Layer with lesser personnel will be given the highest priority to engage the UAS followed by Inner Layer then Last Mile layer 2) Interception after dispersal of personnel within the vicinity	Increase probability of Outer Layer Engagement Delay engagement time
Cyber-attack	1) Isolation of communication link and network 2) Separation of super user account from operator account	Unable to model in Simulation Unable to model in Simulation

Step 0.3: Gather System Operator Feedback

The current CUAS is operating in human delegated mode where the system gathers and generates a situation map that displays all the relevant information to the operator. The system's decision making tools will analyze the information from the sensors and provide decisions of the pre-programmed actions to the operator. Nonetheless, the operator is still responsible for interpreting the data and deciding which action to execute [70].

The primarily use of this HFE feedback is to ensure the virtual environment (Situational Map) generated by the CUAS matches the actual environment as much as possible so as not to cause any misjudgment in operator communication or decision making [71]. Other factors to be considered for the design review include the sound level of the alarm, and the Heads-Up Display (HUD), such as color of the threat, size of the text, legends to label the icons, and confirmation messages. Other factors can be subjective and may vary with different individual inputs. The best way is to use common colors for the display, such as red for threat, blue for own forces, and so forth [72].

2.5.2 Step 1: Define Threats

Step 1.1: Establish New Threat Information

As the anticipated intrusion will be hobby UASs which are COTS and modified systems, their specifications are mostly within the maximum endurance of one hour, the payload of 5 to 15kg, a maximum speed of 68km/h, and have a size of approximately 50cm to 2m in width, with the ability to withstand strong wind speeds of 39 to 61 km/h [19], [73]. The technologies found on the COTS UAS are usually electric propulsion, Vertical Take-Off and Landing (VTOL), and a navigation system, all of which are radio-controlled but require LOS to maintain the link. Although the specifications just mentioned may not be applicable to a modified UAS, for now it can be safely assumed that the differences are minimal.

These capabilities are then recorded and set as the new baseline threat capabilities. Further, the presented COTS UAS generally have the option to be configured into a swarm.

Step 1.2: Determine Potential CUAS System Vulnerabilities

The overall potential system vulnerabilities are investigated and segregated into two parts, which are the detection system and interception system.

The detection system vulnerabilities are defined by their sub-system weaknesses. However, each sub-system, given its unique capabilities, addresses the weaknesses of the others, as shown in **Table 2.12**.

Table 2.12. List of Detection Sub-System Strengths and Weaknesses.

Capability	Strength	Weakness
Acoustic	No LOS required	Limited Detection Range
Passive Radio-Frequency	Long Detection Range can identify specific protocols and intercept video	Potential Latency and subject to signal interference that can cause false alarms
Radar	Long Detection Range and multiple target tracking with no latency	Birds and weather can cause false alarms
Electro-Optical	Easy to investigate for human decision-making	Required to couple with another technology for better reliability

Understanding the detection sub-system strengths and weaknesses, in this analysis, it is assumed that the system has a land link and it is frequently maintained. Therefore, for the purposes of this case study, the probability of transmission can be considered 100% successful. As for the parameters such as probability of sensing and tracking, they can be gathered through the review of Original Equipment Manufacturer (OEM) data or individual conduct of conditional testing. In this case, with the assumption that the probability of sensing and tracking are at 75% and 90% respectively, the overall probability of detection can be determined using **Equation 2.2**, resulting in an efficiency of 67.5%.

Next, the interception system vulnerabilities are dependent on the composite parameters of

individual probability of hit, kill/deny, and risk. For the case study, we adopt commonly used countermeasures, including RF Jamming and GNSS Jamming, as they have the least negative collateral impact and work against most current COTS UAS. On the other hand, they may have issues dealing with a modified UAS operating in a unknown RF band or a with modified navigation system such as an EO payload that utilizes a live feed for maneuvers. In this case, with the assumption that the composite parameters of the probability for hit, kill/deny, and risk are at 80%, 85%, and 6% respectively, the overall probability of interception effectiveness can be determined using Equation 2.3, resulting in 63.9%. Note that the probability of risk is inverted to get the non-risk probability for the calculation of interception efficiency.

The overall CUAS effectiveness is then computed using Equation 2.1 and is 43.13% which may not meet stakeholders' requirements.

Step 1.3: Define the Threat

Based on the previous computation of CUAS effectiveness, there is a strong need to improve both detection and interception effectiveness in order to raise the CUAS's overall effectiveness against the UAS. With the assumption that the adversary UAS's objective is to complete a path to a target with the least chance of being detected or intercepted, the biggest threat that the CUAS will face is UAS speed, where the UAS's speed reduces the engagement window, which can be implied as a lack of time for the CUAS to process and intercept.

2.5.3 Step 2: Re-evaluate the Current System

Step 2.1: Re-evaluate Facility Security Requirements with Stakeholders

With the threat defined, the stakeholders now need to decide what type of security is needed to protect their assets. The first is to determine the maximum line of exploitation within the facility that allows the UAS to roam freely after it intrudes the facility. Anything after the maximum line of exploitation will be deemed the danger zone. With these boundaries mapped out, the stakeholders need to identify locations for the detection or interception system to be deployed, keeping in mind that the system deployed must be compatible with the existing facility operations and procedures. Lastly, the stakeholders are to review

the procedure of activating the response team and where the response team stands during the CUAS's down-time to consider the changes needed to support the system mitigation measures. These details include the response team's expected time to be ready, the rest area, the mobility means, issued equipment, and the rules of engagement.

The outcome of the discussion is stakeholders accepting and approving the security level that was presented in the proposed CUASs to kick start the candidate system exploration with an in-depth study. This includes clarification of possible interference to the stakeholders' operations that the candidate systems may cause.

Step 2.2: Develop the Operational Concept View

A graphical operational concept view of the hypothetical airport is shown in Figure 2.4. The hypothetical airport is a relatively flat area consisting of three runways and generally low buildings, except of one significantly tall control tower. On a daily basis, there will be some ground operating crews onsite to direct aircraft traffic, transport luggage and clear debris off the runway, and wildlife activity such as bird flocks around the trees and fence line. The general assumption of the facility condition is that there are environmental effects which may cause intermediate levels of interference. These conditions need to be accounted for in the analysis as they may have some degrading effects on the subsystems' performance.

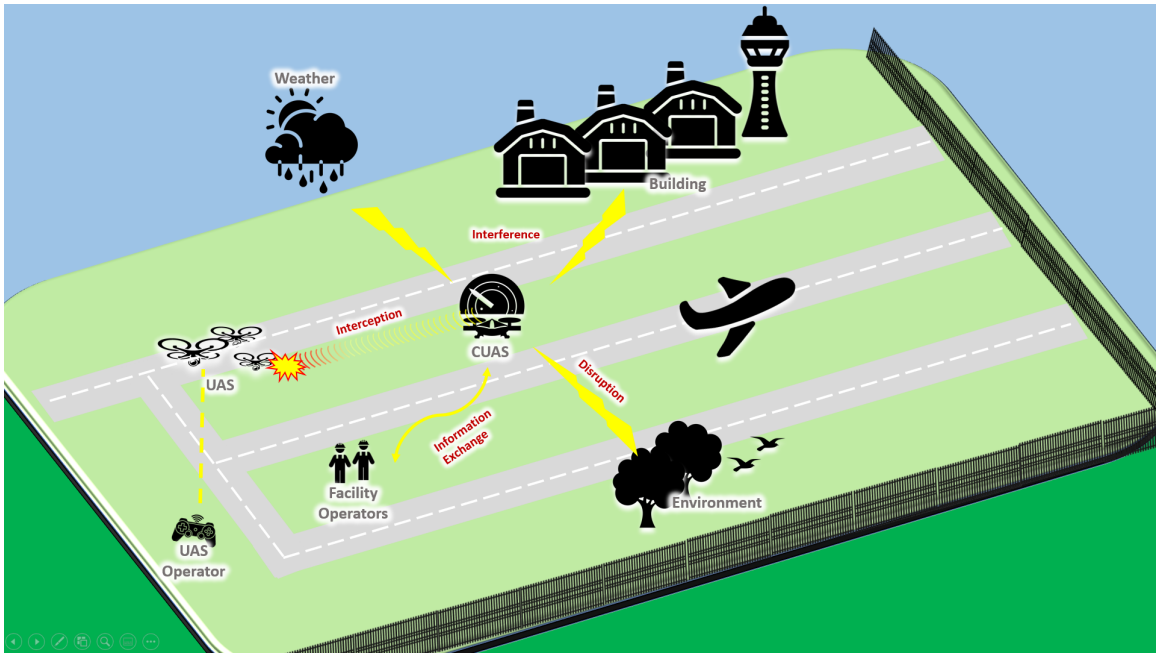

Figure 2.4. OV-1 – A Graphical View of Hypothetical Airport's Operations.

Step 2.3: Analyze Candidate CUAS Configurations

The evaluation measures for the CUAS are based on the key design drivers described earlier. There are numerous evaluation measures that can be adopted, but to have a reasonable evaluation of the candidate configurations, four evaluation measures are created.

- **High Detection Rate:** The high detection rate will increase the success rate of the mission. This measurement can be derived from the detection range, type of sensors overlapping, and false alarm rate.
- **Total System Cost:** The cost of the overall system must be prudent. This measurement can be derived from the per system cost, maintenance cost, testing cost, etc.
- **Flexibility for Layer Deployment:** The system must have the ability to deploy in layers for in-depth defense.
- **High Interception Rate:** The high interception rate will increase the success of the mission. This measurement can be derived from the probability of hit and kill.

The Pugh Matrix is an effective way to evaluate candidates as it allows the comparison

of several design concepts against the existing system (Datum). This uses qualitative techniques, and each criterion listed in Table 2.13 and Table 2.14 has a quantifiable comparison.

Table 2.13. Pugh Matrix.

Criteria	**Candidates**			
	Soft Interceptor Only	Further Detection Range	Combination of Soft and Hard Interceptors	Medium Detection Range with combined Soft and Hard Interceptors
High Detection Rate	Datum	+	S	+
Total System Cost		-	-	-
Layer Approach		-	+	+
High Interception Rate		-	+	+
Sum of Positives		1	**2**	**3**
Sum of Same		0	1	0
Sum of Negatives		**3**	1	1

The Pugh Matrix may provide enough evidence for the designer to gather consensus from the stakeholders to move forward to explore the candidate configuration more deeply.

The results illustrated in Table 2.13 suggest that the CUAS candidate that provides medium detection range and a combination of soft and hard interceptors will be better as the sum of positives score is the highest. With that, the designer can proceed to Section 2.5.4 for further study of the CUAS candidate configuration.

2.5.4 Step 3: Perform Evaluation and Analysis

Step 3.1: Simulate the Proposed CUAS Configuration

Conducting simulations can reduce project cost by exploring innovative ideas or feasibility checks prior to actual live testing on the system. The feasibility check includes the testing of system functions and their interaction through simulations, as illustrated in Figure 2.5. This exploration can streamline the number of physical tests required and generally reduces testing costs. The baseline simulation was conducted using CORE, and the result is shown in Figure 2.6.

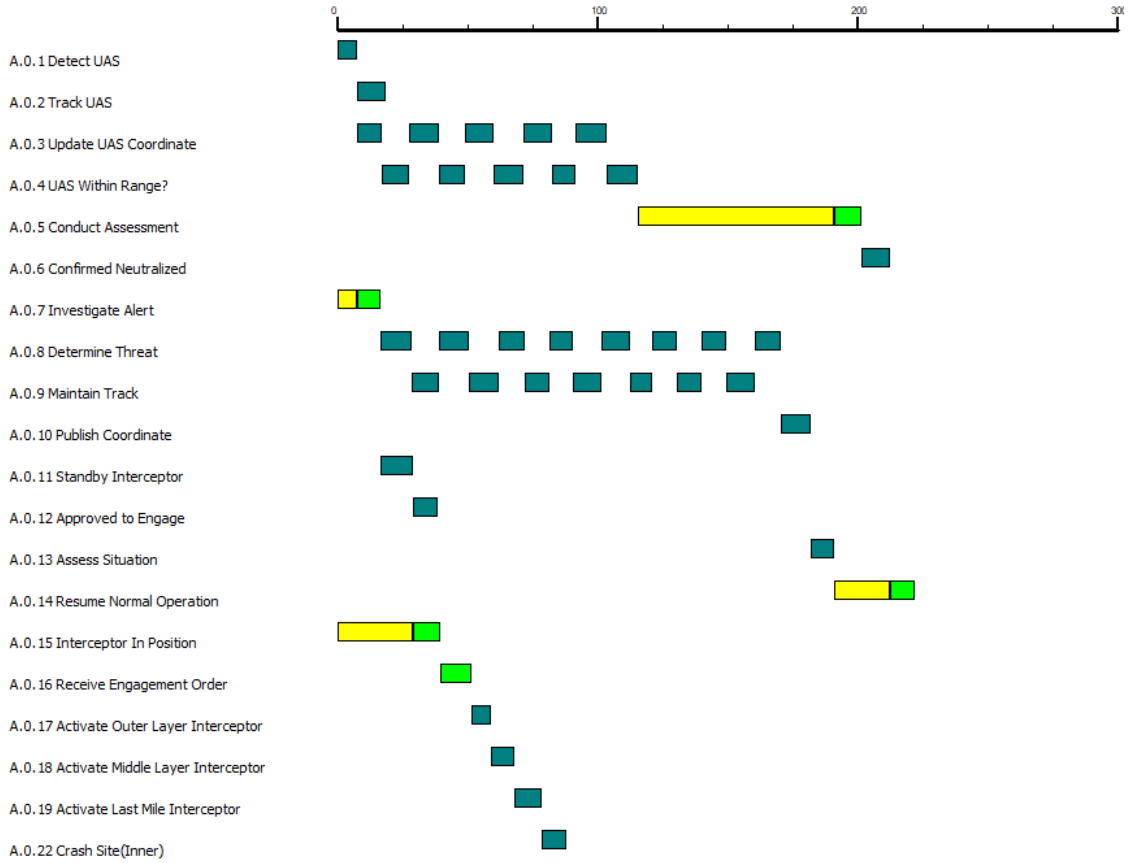

Figure 2.5. Simulation of Proposed CUAS Function.

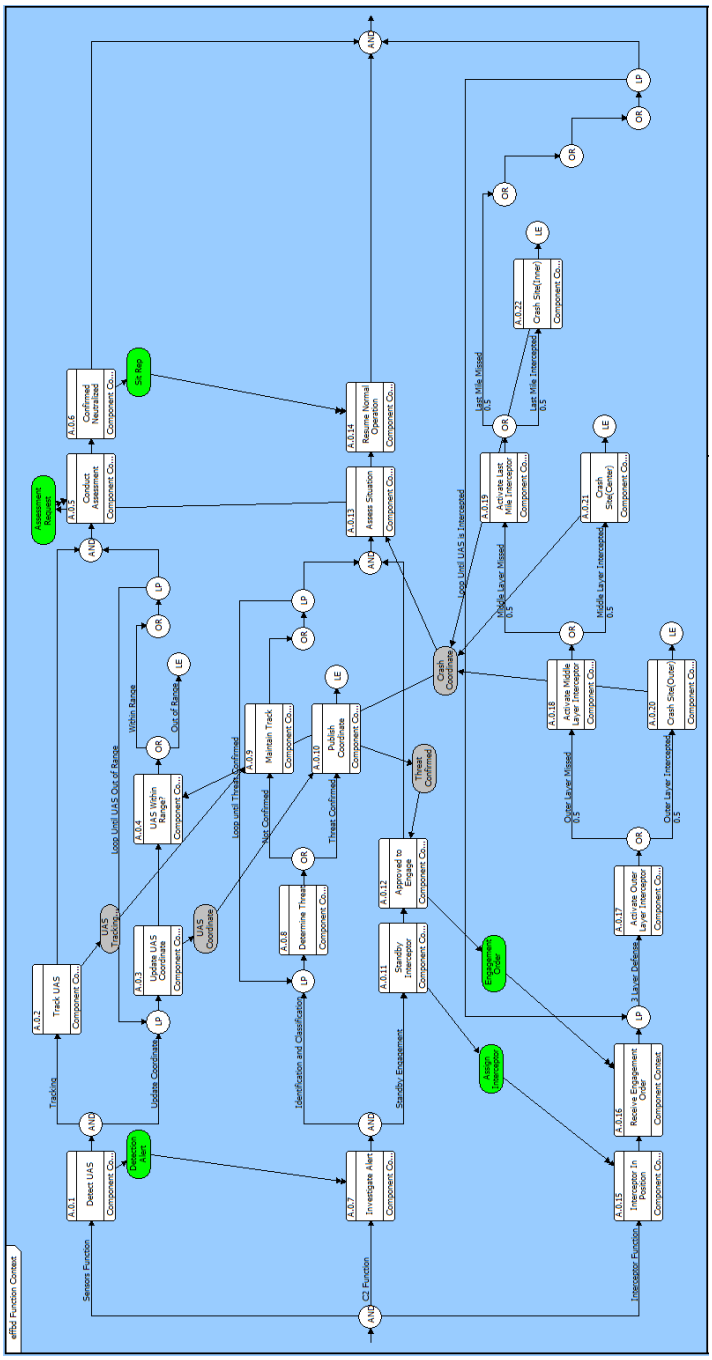

Figure 2.6. The Enhanced Function Flow Block Diagram (EFFBD) of Proposed CUAS.

Based on Figure 2.5, it is feasible to implement the chosen candidate CUAS that consists of a medium detection range and combination of soft and hard interceptors. The next step is to determine the dominant factors to optimize the improvement design to meet the requirements.

Step 3.2: Determine Dominant Factors

The results based on the DOE show the dominant factors that have significant impact to the respective probabilities: The CUAS's target initial range (maximum detection range) exponentially increases the probability of kill as it increases; the target speed (the UAS's maximum speed) decreases the probability of kill significantly as it increases; and any of the process, response, and neutralization times that require more than 10 seconds to carry out will cause an exponential decline in the probability of kill. From the results presented, the key dominant factors that have an impact on system effectiveness are the target initial range (maximum detection range) and system response time.

Step 3.3: Identify Risks to the CUAS

With the dominant factors identified, the system designer then creates a list of risks according to their severity and the likelihood of occurrences that will affect them, as illustrated in Table 2.14.

Table 2.14. Risks and Their Associated Severity and Likelihood of Occurrence.

Risk	Severity	Likelihood of Occurrence
Detection Blind Spot	High	High
Misidentification of Target	High	High
Wrongly Activation of Interception	High	High
Long Process Time	High	Moderate
Long Response Time	High	Moderate

Step 3.4: Develop Risk Mitigation Action Plan

Next, the level of risk severity is addressed as it was identified as high risk through the DOE. The mitigation actions' aims are to reduce the likelihood of occurrences of the possible identified risks. The list of mitigation recommendations and the new likelihood of occurrences are shown in Table 2.15.

Table 2.15. Mitigation Recommendations and Updated Likelihood of Occurrence.

Risk	Mitigation	Severity	Revised Likelihood of Occurrence
Detection Blind Spot	Create different types of sensors overlapping Employ foot patrol to the blind spot area	High	Moderate
Mis-Identification of Target	Include human in the loop Stitch together multiple sensors input	High	Moderate
Wrongly Activation of Interception	Issue confirmation prompt Place plastic shield over activation button	High	Low
Long Process Time	Use AI to assist Increase early detection range	High	Low
Long Response Time	Increase early detection range Practice response protocol periodically	High	Low

2.5.5 Step 4: Generate Design Recommendations

2.5.6 Step 4.1: Verify the TRL Level

Based on the findings in **Chapter 2.5.4**, the proposed CUAS possesses feasible functionality and meets most of the stakeholders' requirements.

The following step is to apply the mitigation measures to address the identified risk. The candidate design increases the CUAS's detection distance and adopts a combination of soft and hard interceptors which can effectively improve probability of sensing, probability of hit, and probability of kill/deny, respectively. The results are illustrated **Table 2.16**.

Table 2.16. Expected Probability Improvement by the Proposed Design.

Probability of	**Datum**	**Proposed Design**
Sensing	75%	90%
Tracking	90%	95%
Hit	80%	95%
Kill/Deny	85%	99%
No-Risk	94%	96%

With the applied mitigation measures, the CUAS's expected effectiveness increases from 43.13% to 77.19%. Based on the current sub-system's TRL against the UAS's TRL, this percentage of efficiency is acceptable for implementation. Hence, the case study proceeds to Section 2.5.6.

Step 4.2: Implement Recommended CUAS Design

To proceed with the recommendation, the stakeholders now make an informed decision to accept the unaddressed requirements and agree to discuss those requirements in the future when opportunities arise, and make necessary reviews of their Tactics, Techniques, and Procedures (TTP) to ensure they will maintain system cohesiveness to support implementation efforts. This includes reassessment of project funding and reallocation of resources

to support the new design configuration efforts.

While the implementation process is underway and after the new CUAS is deployed, the facility commander continues to monitor emerging UAS capabilities. As new threats emerge, the process is repeated to respond in a timely manner to the new threats.

2.6 Discussion

With the anticipation of deploying UAS to support the facility's daily operation, there is some key insight that will be applicable in reviewing the design solution. Rapidly emerging UAS capabilities are known to quickly reduce the effectiveness of a CUAS. Through minor tweaks to the UAS, a UAS can avoid detection and interception by a CUAS. The proposed methodology guides the designer through a structured systems engineering approach that is repetitive and consistent and allows the designer to compare the performance parameters across different sub-systems of the CUAS. The design principles are generic where peoples' interactions with the system are explored and leverage the collaboration effort across the stakeholders to ensure the chosen CUAS is effective.

The use of MBSE and simulation tools assist in the verification and validation of the system to further explore innovative ideas and conduct a feasibility study in a cost-saving and safe environment. Furthermore, the DOE can determine the dominant factors which then provide better insight to improve the system in a resource-optimized approach.

Although the data about the CUAS and the environment used in the case study are intentionally fictitious, the proposed methodology provides a generic guide to the facility commander for understanding the critical requirements of a CUAS's deployment through the proposed systems engineering approach. The proposed methodology is specifically useful for resolving projects with design uncertainty due to unknown parameters and projects with limited resources.

A word of caution, this methodology is proven effective in theory only. IT is not known whether more complex issues will arise when the actual system data sets are presented. The challenging portion of the methodology will be the development of a consistent parameter for performance comparison. This challenge could be due to limited testing facilities or because the capability is at low TRL. To overcome this, the data set must be generated

through live testing of a wide variety of scenarios, but this will entail an increase in the project's overall budget. It is worth nothing, however, the method of acquiring realistic and usable consistent parameters is not within the scope of this research. We assert that different types of facilities, different countries, and different stakeholders will find different parameters of most utility to their specific situations. Thus, we do not recommend a specific performance parameter here.

The proposed methodology can address threats from a single UAS up to UAS with swarm capabilities. The research did not include UAS capability that allows a UAS to travel through air and underwater, which may have a huge impact on the detection capability of the CUAS, as the UAS will be able to travel stealthily underwater and strike with agility in the air [74], [75]. Although the re-evaluation of design principles will be similar, the need to include underwater sensors such as sonar or proximity or new types of underwater countermeasures will generate integration issues such as increased false alarm rate, incompatible output, and target hand-over between ground sensors and underwater sensors.

The recommended expansion of this work is to include methods for generating consistent parameters through the conduct of designing a live test to support the evaluation through validation and also to conduct research on the new UASs that can travel both in the air and underwater. The expansion of the study will support this analysis by providing realistic results and include analysis of the emerging technology.

2.7 Conclusions

In conclusion, the results of the case study demonstrate that the adoption of an iterative learning and data sharing approach such as the methodology proposed in this study can consistently ensure that the CUAS is reviewed in a timely manner. The battle against the rapidly emerging capabilities of UASs that threaten the relevancy of deployed CUASs may be a thing of the past by enabling modular upgrades to strengthen a CUAS's systems and test system performance even at low TRL, and reduces the possibility of a UAS exploiting inherent weaknesses in facility security.

CHAPTER 3:
Conclusion

This chapter summarizes the research findings and highlights potential areas for future work. The journal manuscript presented in Chapter 2 can be used to address challenges that DOD, SAF, and civilian facility commanders face when conducting tests and evaluation of existing and anticipated CUAS capabilities to counter a UAS threat.

3.1 Conclusions

It is essential to develop a resource-optimized evaluation and analysis methodology to rapidly assess CUAS effectiveness through the assessment of the technological gaps between existing CUASs and emerging UAS threats and capabilities. The traditional CUAS system acquisition and development process may not suit efforts to counter the rapid growth in UAS capabilities. The focus of the methodology proposed in this thesis is on iterative learning and data sharing that supports the modular upgrade of an existing CUAS. The modular approach allows performance testing of capabilities even at low TRL, which is beneficial for generating data points and understanding the relationships of the dominant factors in CUAS systems being effective against UAS threats. The timely review of a CUAS may then reduce the possibility of UAS with the latest capabilities exploiting the inherent weaknesses of a facility's security, because such a review enables the application of mitigation measures before such exploits happen. The methodology demonstrated in the case study provides a process to gather data from both emerging UAS and CUAS systems to conduct evaluation and analysis. While the data used in the case study are intentionally fictitious, the case study does provide a good indication that the proposed methodology is valid and useful.

With the anticipation that in the future more industries will employ UASs to support their daily operations and tasks, the increase in UAS activities around facilities will require specific security and safety measures to reduce potential risks. The proposed methodology provides some key insights that will be applicable in reviewing the a CUAS's configuration and focuses on two key functions: detection and interception. The design principles used in the methodology are generic where it explores peoples' interactions with the CUAS and

leverages collaboration across the stakeholders to ensure the chosen CUAS configuration is effective at meet emerging UAS threats. The proposed methodology is specifically useful for resolving CUAS projects with design uncertainty due to unknown parameters, CUAS projects that have limited resources, and the methodology can also address threats posed by a single UAS as well as a UAS swarm.

3.2 Future Work

Adopting a systems engineering approach, the proposed methodology provides a guide to facility commanders for understanding the critical requirements of a CUAS deployment. It is important to note, however, that this methodology is proven effective in theory only, via the case study. It is not known whether more complex issues may arise when real system data sets are used. The most challenging portion of the methodology will be the development of consistent parameters for performance comparison. This challenge could be due to limited testing facilities or specific needed capabilities being at low TRL. To overcome such challenges, data sets must be generated through live testing of a wide variety of scenarios albeit with accompanying increases in overall project budget. Nevertheless, acquiring consistent parameters and data sets that are realistic and usable is beyond the scope of this research.

Recommended future expansions of this work include:

- Developing methods that produce useful data sets from live tests to support CUAS evaluation through validation of said data sets
- Increasing the autonomy of CUAS operations
- Improving the CUAS's cyber resilience

It may be tempting to introduce more higher quality sensors and interceptors to existing CUAS but many existing CUAS configurations are currently sufficient and cost-effective to deal with current UAS threats. Building from current CUAS configurations, a systems engineer should explore how to increase the uses of autonomy to make quicker decisions and further improve CUAS effectiveness. Understand that there will be uncertainty and constant searching of use-cases to justify the need for CUAS autonomy, and there must be the willingness to go through proper review and structured evaluation to reap more benefits

from a less conservative approach in design [76]. On the other hand, increasing autonomy in CUASs may increase inherent cyber security risks and requires in-depth analysis to constantly improve cyber-resilience and evolve mitigation plans [77]. An exploration into system "self-recovery" may be beneficial to support increased autonomy, as the reduction of having a human in the loop may not allow timely response to the immediate cyber-threats and implies that the system needs to have the means to automatically detect abnormalities or anticipate cyber-threats and activate protocols such as an immediate reboot or change in security pin [78], [79]. The suggested future work may support the proposed methodology by providing realistic results and include building a future-proof system against potential emerging technology. This may support the study of military and high-risk facilities (e.g., airports, oil plants, chemical plants and the like) with the focus of using parameters that will minimize the cost required to conduct testing. The success of this methodology will benefit DOD, SAF, and facility security in dealing with constantly evolving UAS threats.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

[1] S. G. Gupta, M. M. Ghonge, and D. P. M. Jawandhiya, "Review of unmanned aircraft system (UAS)," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 2, Apr. 2013. [Online]. Available: https://www.researchgate.net/profile/Mangesh-Ghonge/publication/249998592_Review_of_Unmanned_Aircraft_System_UAS/links/02e7e51e8ef1668ce8000000/Review-of-Unmanned-Aircraft-System-UAS.pdf

[2] K. Cho, M. Cho, and J. Jeon, "Fly a drone safely: Evaluation of an embodied egocentric drone controller interface," *Interacting with Computers*, vol. 29, no. 3, Sep. 2016. [Online]. Available: https://doi.org/10.1093/iwc/iww027

[3] D. Arteche, K. Chivers, B. Howard, T. Long, W. Merriman, A. Padilla, A. Pinto, S. Smith, and V. Thoma, "Drone defense system architecture for U.S. Navy strategic facilities," Capstone, Dept. of Systems Engineering., NPS, Monterey, CA, USA, Sep. 2017. [Online]. Available: https://calhoun.nps.edu/handle/10945/56172

[4] P. T. S. and G. J. P. I.I., "Defeating small civilian unmanned aerial systems to maintain air superiority," *Air & Space Power Journal*, vol. 31, no. 2, June 2017. [Online]. Available: http://libproxy.nps.edu/login?url:https://www.proquest.com/scholarly-journals/defeating-small-civilian-unmanned-aerial-systems/docview/1910739147/se-2?accountid=12702

[5] A. la Cour-Harbo, "Mass threshold for 'harmless' drones," *International Journal of Micro Air Vehicles*, vol. 9, no. 2, Apr. 2017. [Online]. Available: https://doi.org/10.1177/1756829317691991

[6] A. Michel, *Counter-drone Systems*. Center for the Study of the Drone at Bard College, Dec. 2019. [Online]. Available: https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[7] J. Knight, "Countering unmanned aircraft systems," Master's thesis, NPS, Dec. 2019. [Online]. Available: https://calhoun.nps.edu/handle/10945/63997

[8] J. S. J. Snead and D. Inserra, "Establishing a legal framework for counter-drone technologies," The Heritage Foundation, 214 Massachusetts Ave NE Washington DC 20002-4999, USA, Tech. Rep. 12, 2018. [Online]. Available: https://www.heritage.org/technology/report/establishing-legal-framework-counter-drone-technologies

[9] G. Mary Lynn, *Design and Evaluation of Physical Protection Systems*. Burlington, MA, USA: Butterworth-Heinemann, 2007.

[10] B. O'Halloran, "System engineering theses: A manuscript option," Dept. of Systems Engineering, Naval Postgraduate School, Monterey, CA, USA, Tech. Rep., Jul 2017. [Online]. Available: http://hdl.handle.net/10945/63841

[11] J. Desjardins, "Here's how commercial drones grew out of the battlefield," Dec 2016. [Online]. Available: http://www.businessinsider.com/a-history-of-commercialdrones-2016-12

[12] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies," *Sensors*, vol. 20, no. 12, May 2020. [Online]. Available: https://doi.org/10.3390/s20123537

[13] R. J. Wallace and J. M. Loffi, "Examining unmanned aerial system threats & defenses: A conceptual analysis," *International Journal of Aviation, Aeronautics, and Aerospace*, vol. 2, no. 4, Oct. 2015. [Online]. Available: https://doi.org/10.15394/ijaaa.2015.1084

[14] V. Kashyap, "A brief history of drones: The remote controlled unmanned aerial vehicles (UAVs)," interestingengineering.com, Jun. 29, 2020. [Online]. Available: https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs

[15] A. N. Stulberg, "Managing the unmanned revolution in the U.S. Air Force," *Orbis*, vol. 51, no. 2, pp. 251–265, May 2007. [Online]. Available: https://doi.org/10.1016/j.orbis.2007.01.005

[16] A. Etzioni, "The great drone debate," *Military Review*, May 2013. [Online]. Available: https://web.archive.org/web/20130522061025/http://icps.gwu.edu/files/2013/03/Etzioni_DroneDebate.pdf5

[17] W. E. Forum. "The Fourth Industrial Revolution: What it means, how to respond," Accessed May. 26, 2021. [Online]. Available: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[18] C. Tsekeris, "Industry 4.0 and the digitalisation of society: Curse or cure?" *Homo Virtualis*, vol. 1, no. 1, pp. 4–12, June 2018. [Online]. Available: https://doi.org/10.12681/homvir.18622

[19] Danish Technological Institute and Association for Unmanned Vehicle Systems International, "Global trends of unmanned aerial systems," Danish Technological Institute [DTI], Denmark, Tech. Rep., 2019. [Online]. Available: https://02f09e7.netsolhost.com/AUVSIDocs/Global%20Trends%20for%20UAS.pdf

[20] N. Vargas-Ramírez and J. Paneque-Gálvez, “The global emergence of community drones (2012–2017),” *Drones*, vol. 3, no. 4, June 2019. [Online]. Available: https://doi.org/10.3390/drones3040076

[21] A. C. Mckinnon, “The possible impact of 3d printing and drones on last-mile logistics: An exploratory study,” *Built Environment*, vol. 42, no. 4, pp. 617–629, Dec. 2016. [Online]. Available: https://doi.org/10.2148/benv.42.4.617

[22] K. Giles and K. Giammarco, “Mission-based architecture for swarm composability (masc),” 2017. [Online]. Available: https://calhoun.nps.edu/handle/10945/63785

[23] M. Cummings, S. Bruni, S. Mercier, and P. J. Mitchell, “Automation architecture for single operator, multiple UAV command and control,” *The International C2 Journal*, vol. 1, no. 2, pp. 1–24, Apr. 2007. [Online]. Available: http://hdl.handle.net/1721.1/90285

[24] W. Markus, K. Bill, and A. Federico, “Drone shows: Creative potential and best practices,” *ETH Zürich*, p. 18, Sep. 2017. [Online]. Available: https://doi.org/10.3929/ethz-a-010831954

[25] P. Kardasz, J. Doskocz, M. Hejduk, P. Wiejkut, and H. Zarzycki, “Drones and possibilities of their using,” *Journal of Civil & Environmental Engineering*, vol. 6, no. 3, Apr. 2016. [Online]. Available: http://dx.doi.org/10.4172/2165-784X.1000233

[26] K. Chih-ming, Y. Wei-Sheng, W. Ting-Ying, and C. Shu-Tsung, “The fast flight trajectory verification algorithm for drone dance system,” in *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, Jul 2020. [Online]. pp.97-101. Available: http://dx.doi.org/10.1109/IAICT50021.2020.9172016

[27] Vice. "Drones Light Up Shanghai’s Sky With a QR Code (That You Can Scan)," Accessed May. 17, 2021. [Online]. Available: https://www.vice.com/en/article/88n9vb/shanghai-drone-show-qr-code

[28] H. Ahn, D.-T. Le, D. T. Nguyen, and H. Choo, “Real-time drone formation control for group display,” *Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, vol. 935, pp. 778–785, May 2019. [Online]. Available: https://doi.org/10.1007/978-3-030-19063-7_63

[29] A. K. Dutta, “Fuzzy clustering with particle swarm intelligence for large dataset classification,” *TEM Journal*, vol. 7, no. 4, pp. 738–743, Nov. 2018. [Online]. Available: https://dx.doi.org/10.18421/TEM74-06

[30] M. E. Duntz, “Counter autonomy defense for aerial autonomous systems,” Master’s thesis, Purdue, Apr 2020. [Online]. Available: https://doi.org/10.25394/PGS.12174420.v14

[31] B. Basudeb, S. Sourav, D. A. Kumar, K. Neeraj, L. Pascal, and A. Mamoun, “Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, June 2020. [Online]. Available: https://doi.org/10.1109/TVT.2020.3000576

[32] B. Bera, D. Chattaraj, and A. K. Das, “Designing secure blockchain-based access control scheme in iot-enabled internet of drones deployment,” *Computer Communications*, vol. 153, pp. 229–249, Mar. 2020. [Online]. Available: https://doi.org/10.1016/j.comcom.2020.02.011

[33] R. P. Pratim and N. Kien, “A review on blockchain for medical delivery drones in 5G-IoT era: Progress and challenges,” in *2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, 2020. [Online]., pp. 29–34. Available: https://doi.org/10.1109/ICCCWorkshops49972.2020.9209931

[34] “Gatwick airport: Drones ground flights,” BBC, Dec. 20, 2018. [Online]. Available: https://www.bbc.com/news/uk-england-sussex-46623754

[35] “Drone sightings at changi airport force closure of one runway, nearly 40 flights affected,” CNA, Jun. 19, 2019. [Online]. Available: https://www.channelnewsasia.com/news/singapore/changi-airport-drone-sightings-one-runway-closed-11641920

[36] Aaronia. "AARTOS- Drone Detection System," Accessed May. 17, 2021. [Online]. Available: http://www.sarahespino.com/pdf/aaronia/Aaronia_AARTOS-Drone-Detection-System_broshure.pdf

[37] Blighter Surveillance Systems. "AUDS anti-UAV Defence System," Accessed May. 17, 2021. [Online]. Available: https://www.blighter.com/products/auds-anti-uav-defence-system/

[38] Raytheon Missiles & Defense. "Counter-UAS," Accessed May. 17, 2021. [Online]. Available: https://www.raytheonmissilesanddefense.com/capabilities/counter-uas

[39] *Dynamic Targeting and the Tasking Process*, Air Force Doctrine Publication (AFDP), Curtis E. Lemay Center, Montgomery, AL, USA, Mar. 2019. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-D17-Target-Dynamic-Task.pdf

[40] Battelle. “DroneDefender® Counter-UAS Device” Accessed Apr. 18, 2021. [Online]. Available: https://www.battelle.org/government-offerings/national-security/payloads-platforms-controls/counter-UAS-technologies/dronedefender

[41] Boeing. “Boeing’s Compact Laser Weapons System tracks and disables UAVs” Accessed Apr. 18, 2021. [Online]. Available: https://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page

[42] J. Carlini. “The anti-drone revolution: 22 companies building killer drone tech today from DronesX, Drone defence,” Accessed Apr. 18, 2021. [Online]. Available: https://www.dronedefence.co.uk/the-anti-drone-revolution-22-companies-building-killer-drone-tech-today-from-dronesx/

[43] R. Williams. “Tokyo police are using drones with nets to catch other drones,” The Telegraph. Accessed Apr. 18, 2021. [Online]. Available: https://www.telegraph.co.uk/technology/2016/01/21/tokyo-police-are-using-drones-with-nets-to-catch-other-drones/

[44] RAPERE. “Anti-drone interceptor,” Accessed Apr. 18, 2021. [Online]. Available: https://www.droneality.com/rapere-anti-drone-interceptor

[45] B. B. Chauhan, “Unmanned aerial system integration into national airspace system and airports: Risk mitigation using content analysis methodology,” Master’s thesis, FIT, May 2019. [Online]. Available: http://hdl.handle.net/11141/2909

[46] C. Kyrkou, S. Timotheou, P. Kolios, T. Theocharides, and C. Panayiotou, “Drones: Augmenting our quality of life,” *IEEE Potentials*, vol. 38, no. 1, Jan. 2019. [Online]. Available: https://doi.org/10.1109/MPOT.2018.2850386

[47] M. Thomas and L. Aaron, “Integrating unmanned aircraft systems into airport operations: From buy-in to public safety,” *Journal of Airport Management*, vol. 13, no. 4, Sep. 2019. [Online]. Available: https://www.ingentaconnect.com/content/hsp/cam/2019/00000013/00000004/art00008#expand/collapse

[48] T. Wierzbicki, “Investigating drones using open-source forensic software,” Master’s thesis, NPS, June 2020. [Online]. Available: https://calhoun.nps.edu/handle/10945/65468

[49] A. Roder, K. R. Choo, and N. Le-Khac, “Unmanned aerial vehicle forensic investigation process: DJI phantom 3 drone as A case study,” *CoRR*, vol. abs/1804.08649, Aug. 2018. [Online]. Available: http://arxiv.org/abs/1804.08649

[50] H. Moon, E. Jin, H. Kwon, S. Lee, and K. Gibum, "Digital forensic methodology for detection of abnormal flight of drones," *Journal of Information Security & Cybercrimes Research*, vol. 4, no. 1, Dec. 2021. [Online]. Available: https://journals.nauss.edu.sa/index.php/JISCR

[51] S. Viswanathan and Z. Baig, "Digital forensics for drones: A study of tools and techniques," in *Applications and Techniques in Information Security*, L. Batina and G. Li, Eds. Singapore: Springer Singapore, 2020, pp. 29–41.

[52] A. M. in Nairobi, "Cargo plane shot down in somalia, all occupants killed," Garowe Online, May 04, 2020. [Online]. Available: https://www.garoweonline.com/en/news/somalia/a-cargo-plane-shot-down-in-somalia-all-on-board-are-dead

[53] N. Karimi and J. Krauss, "Under pressure, iran admits it shot down jetliner by mistake," AP News, Jan 11, 2020. [Online]. Available: https://apnews.com/article/europe-accidents-ap-top-news-tehran-international-news-21f4a92a2dfbc38581719664bdf6f38e

[54] P. Cain, "Mistaken identity: Three times passenger airliners have been shot down in error," Global News, Jan. 09, 2020. [Online]. Available: https://globalnews.ca/news/6389887/iran-plane-crash-three-times-passenger-planes-shot-down-error/

[55] R. P. Jones and A. Burke, "Flight PS752 shot down after being misidentified as hostile target, Iran's final report says," CBC, Mar. 17, 2021. [Online]. Available: https://www.cbc.ca/news/politics/final-report-flight-ps752-1.5953340

[56] NIST. NIST risk management framework. [Online]. Available: https://csrc.nist.gov/projects/risk-management/about-rmf

[57] J. Shevchenko. "An introduction to Model-Based Systems Engineering (MBSE)," Accessed May 30, 2021. [Online]. Available: https://insights.sei.cmu.edu/blog/introduction-model-based-systems-engineering-mbse/

[58] V. Tiurin, O. Martyniuk, V. Mirenenko, and P. Openko, "General approach to counter unmanned aerial vehicles," *Safety & Defense*, vol. 5, no. 1, pp. 6–12, Oct. 2019. [Online]. Available: https://doi.org/10.1109/APUAVD47061.2019.8943859

[59] C. Wickens, *Introduction to Human Factors Engineering*, 2nd ed. 330 Hudson in New York City, New York: Pearson, 2004.

[60] W. Müller, F. Reinert, and D. Pallmer, "Open architecture of a counter UAV system," in *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2018*, R. Suresh, Ed., International Society for Optics and Photonics. SPIE, 2018. [Online]., vol. 10651, pp. 34 – 41. Available: https://doi.org/10.1117/12.2305606

[61] C. Kouhestani, B. Woo, and G. Birch, "Counter unmanned aerial system testing and evaluation methodology," in *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement Applications XVI*, E. M. Carapezza, Ed., International Society for Optics and Photonics. SPIE, May 2017. [Online]., vol. 10184, pp. 1 – 7. Available: https://doi.org/10.1117/12.2262538

[62] H. F. Cervone, "Using pugh matrix analysis in complex decision-making situations," *Applied digital library project management*, vol. 25, no. 4, pp. 228–232, Oct. 2009. [Online]. Available: https://doi.org/10.1108/10650750911001815

[63] C. J. Boyd, J. Harris, Roderick E., C. L. Kleparek, and J. W. Taylor, "A study of how unmanned aerial vehicle systems can improve over-the-horizon targeting and strike missions," Master's thesis, NPS, Mar. 2020. [Online]. Available: https://calhoun.nps.edu/handle/10945/64868

[64] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Journal on Applied Analytics*, vol. 36, no. 1, pp. 530–544, Dec. 2006. [Online]. Available: https://doi.org/10.1287/inte.1060.0252

[65] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Analyzing the vulnerability of critical infrastructure to attack and planning defenses," in *TutORial in Operations Research*. INFORMS, Oct. 2005. [Online]., pp. 102 – 123. Available: https://doi.org/10.1287/educ.1053.0018

[66] S. Marrone, R. Nardone, A. Tedesco, P. D'Amore, V. Vittorini, R. Setola, F. De Cillis, and N. Mazzocca, "Vulnerability modeling and analysis for critical infrastructure protection applications," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 3, pp. 217–227, Dec. 2013. [Online]. Available: https://doi.org/10.1016/j.ijcip.2013.10.001

[67] M. A. A. Makhloof, M. E. Waheed, and U. A. E.-R. Badawi, "Real-time aircraft turnaround operations manager," *Production Planning & Control*, vol. 25, no. 1, Feb. 2014. [Online]. Available: https://doi.org/10.1080/09537287.2012.655800

[68] Changi Airport Group. [Online]. Available: https://www.changiairport.com/corporate/our-expertise/air-hub/traffic-statistics.html. Accessed Jul. 16, 2021.

[69] W. Spark. "Average weather in Singapore," Accessed Jul. 18, 2021. [Online]. Available: https://weatherspark.com/y/114655/Average-Weather-in-Singapore-Year-Round

[70] A. P. Williams and P. D. Scharre, "Defining autonomy in systems: Challenges and solutions," in *Autonomous Systems: Issues for Defence Policymakers. Norfolk, VA: NATO Allied Command Transformation.*, 2008, pp. 41–42.

[71] R. Martin-Emerson and C. D. Wickens, "Superimposition, symbology, visual attention, and the head-up display," *Human Factors*, vol. 39, no. 4, pp. 581–601, Dec. 1994. [Online]. Available: https://doi.org/10.1518/001872097778667933

[72] A. J. Erjavac, R. Iammartinos, and J. Fossaceca, "An evaluation of human factors failure data in relation to system readiness assessment," in *Proceedings of the World Congress on Engineering and Computer Science 2016 Vol II*, 2016. [Online]. Available: https://www.semanticscholar.org/paper/An-Evaluation-of-Human-Factors-Failure-Data-in-to-Erjavac-Iammartino/bdbd17583f246039b5e47eda603cd29cdda0f1b4

[73] DJI. DJI drone comparison. Accessed Jul. 18, 2021. [Online]. Available: https://www.dji.com/products/comparison-consumer-drones?from=store-product-page

[74] "How China's flying submarine drone could change the way sea battles are fought," SCMP, Jul. 22, 2021. [Online]. Available: https://www.scmp.com/news/china/science/article/3141856/how-chinas-flying-submarine-drone-could-change-way-sea-battles?utm_content=article&utm_medium=Social&utm_source=Facebook&fbclid=IwAR2SfX2GhXfgH1w3vICBnlmgV5R5tUvYRhesm0LibFZdHwqw6Myl1b9SZdE#Echobox=1626811605

[75] SwellPro. SplashDrone3+. Accessed Jul. 18, 2021. [Online]. Available: https://www.swellpro.com/waterproof-splash-drone.html

[76] L. Matsuyama, R. Zimmerman, C. Eaton, K. Weger, B. Mesmer, N. Tenhundfeld, D. L. Van Bossuyt, and R. Semmens, "Determinants that are believed to influence the acceptance and adoption of mission critical autonomous systems," in *AIAA Scitech 2021 Forum*, Jan 2021. [Online]., p. 1156. Available: https://doi.org/10.2514/6.2021-1156

[77] J. Scrofani, C. Bollmann, J. Roth, and B. Hale, "Cyber systems: Their science, engineering, and security," in *Proceedings of the 54th Hawaii International Conference on System Sciences*. HICSS, Jan 2021. [Online]. Available: https://calhoun.nps.edu/handle/10945/66976

[78] D. Van Bossuyt and B. O'Halloran, "A method to choose between automation and human operators for recovery actions during a cyber attack," in *Procedia Computer Science*. Elsevier, Apr 2019, vol. 153, pp. 352–360.

[79] N. Papakonstantinou, D. L. Van Bossuyt, J. Linnosmaa, B. Hale, and B. O'Halloran, "A zero trust hybrid security and safety risk analysis method," *Journal of Computing and Information Science in Engineering*, vol. 21, no. 5, May 2021. [Online]., 050907. Available: https://doi.org/10.1115/1.4050685

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California