2022-12

COUNTER-UXS ENERGY AND OPERATIONAL ANALYSIS

Behling, Jason A.; Fuentes, Fernando; Mannings, Larry D.; Morgan, Golda R.; Schinowsky, Jonathan T.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/71593

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE REPORT

COUNTER-UXS ENERGY AND OPERATIONAL ANALYSIS

by

Jason A. Behling, Fernando Fuentes, Larry D. Mannings,
Golda R. Morgan, and Jonathan T. Schinowsky

December 2022

Advisor:	Douglas L. Van Bossuyt
Co-Advisor:	Britta Hale
Co-Advisor:	Corina L. White

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Systems Engineering Capstone Report

4. TITLE AND SUBTITLE COUNTER-UXS ENERGY AND OPERATIONAL ANALYSIS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jason A. Behling, Fernando Fuentes, Larry D. Mannings, Golda R. Morgan, and Jonathan T. Schinowsky	
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)

At present, there exists a prioritization of identifying novel and innovative approaches to managing the small Unmanned Aircraft Systems (sUAS) threat. The near-future sUAS threat to U.S. forces and infrastructure indicates that current Counter-UAS (C-UAS) capabilities and tactics, techniques, and procedures (TTPs) need to evolve to pace the threat. An alternative approach utilizes a networked squadron of unmanned aerial vehicles (UAVs) designed for sUAS threat interdiction. This approach leverages high performance and Size, Weight, and Power (SWaP) conformance to create less expensive, but more capable, C-UAS devices to augment existing capabilities.

This capstone report documents efforts to develop C-UAS technologies to reduce energy consumption and collaterally disruptive signal footprint while maintaining operational effectiveness. This project utilized Model Based System Engineering (MBSE) techniques to explore and assess these technologies within a mission context. A Concept of Operations was developed to provide the C-UAS Operational Concept. Operational analysis led to development of operational scenarios to define the System of Systems (SoS) concept, operating conditions, and required system capabilities. Resource architecture was developed to define the functional behaviors and system performance characteristics for C-UAS technologies. Lastly, a modeling and simulation (M&S) tool was developed to evaluate mission scenarios for C-UAS.

14. SUBJECT TERMS Concept of Operations; CONOPS; unmanned aerial vehicle; UAV; Model-Based Systems Engineering; MBSE; cyber attack; Counter Unmanned Aircraft System; C-UAS; small Unmanned Aircraft System; sUAS; modeling and simulation; M&S; Unmanned System; UxS; Counter Unmanned System; C-UxS; mission engineering; ME; Department of Defense Architecture Framework; DoDAF; tactics, techniques, and procedures; TTPs; agent-based modeling; ABM; energy optimization	**15. NUMBER OF PAGES** 223
	16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

COUNTER-UXS ENERGY AND OPERATIONAL ANALYSIS

Jason A. Behling, Fernando Fuentes, Larry D. Mannings,
Golda R. Morgan, and Jonathan T. Schinowsky

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Lead Editor: Golda R. Morgan

Reviewed by:

Douglas L. Van Bossuyt Advisor	Britta Hale Co-Advisor
Corina L. White Co-Advisor	

Accepted by:
Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

At present, there exists a prioritization of identifying novel and innovative approaches to managing the small Unmanned Aircraft Systems (sUAS) threat. The near-future sUAS threat to U.S. forces and infrastructure indicates that current Counter-UAS (C-UAS) capabilities and tactics, techniques, and procedures (TTPs) need to evolve to pace the threat. An alternative approach utilizes a networked squadron of unmanned aerial vehicles (UAVs) designed for sUAS threat interdiction. This approach leverages high performance and Size, Weight, and Power (SWaP) conformance to create less expensive, but more capable, C-UAS devices to augment existing capabilities.

This capstone report documents efforts to develop C-UAS technologies to reduce energy consumption and collaterally disruptive signal footprint while maintaining operational effectiveness. This project utilized Model Based System Engineering (MBSE) techniques to explore and assess these technologies within a mission context. A Concept of Operations was developed to provide the C-UAS Operational Concept. Operational analysis led to development of operational scenarios to define the System of Systems (SoS) concept, operating conditions, and required system capabilities. Resource architecture was developed to define the functional behaviors and system performance characteristics for C-UAS technologies. Lastly, a modeling and simulation (M&S) tool was developed to evaluate mission scenarios for C-UAS.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

ABM	Agent Based Model / Modeling
ADA	Air Domain Awareness
API	Application Programming Interface
ASW	Anti-Submarine Warfare
C2	Command and Control
C3	Command, Control, and Communications
CBRNE	Chemical, Biological, Radiological, Nuclear, and high-yield Explosives
CIWS	Close-in Weapon System
COG	Center of Gravity
CONOPS	Concept of Operations
COTS	Commercial/Consumer off-the-shelf
CRAM	Counter Rocket, Artillery, and Mortar
C-UAS	Counter UAS
C-UxS	Counter UxS
DASN-OE	Deputy Assistant Secretary of the Navy, Operational Energy
DC	Direct Current
DE	Directed Energy
DiD	Defense-in-Depth
DOD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DOF	Degrees of Freedom

DROSERA	Defense Reaction and Operational Strategy Evaluation, Response, and Analysis
EA	Enterprise Architecture
EMP	Electromagnetic Pulse
EO	Electro-Optical
EOS	Electro-Optics System
FAA	Federal Aviation Administration
FPCON	Force Protection Condition
FPCON C	Force Protection Condition CHARLIE
GCS	Ground Controls Station
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HPM	High-power Microwaves
HPM	High-Power Microwave
IFF	Identification Friend of Foe
IPOE	Intelligence Preparation of the Operational Environment
IR	Infrared
ISIS	Islamic State of Iraq and Syria
ISR	Intelligence, Surveillance, and Reconnaissance
JCO	Joint Counter-Small UAS Office
K9	Canine/Dog
LML	Life Cycle Modeling Language
LOE	Level Of Effort

LOS	Line of Sight
LVC	Live/Virtual/Constructive
MBSE	Model-Based Systems Engineering
MCTR	Missile Technology Control Regime
ME	Mission Engineering
MOE	Measures of Effectiveness
MOP	Measures of Performance
MSOSA	Magic Systems of Systems Architect
MSSE	Master of Science, Systems Engineering
NPS	Naval Postgraduate School
NRP	Naval Research Project
OOB	Order Of Battle
RCS	Radar Cross Section
RDT&E	Research, Development, Test and Evaluation
RF	Radio Frequency
ROE	Rules of Engagement
SoSE&I	System of Systems Engineering and Integration
sUAS	small UAS
SWaP	Size, Weight, and Power
TRL	Technology Readiness Level
TTPs	Tactics, Techniques, and Procedures
UAF	Unified Architecture Framework
UAS	Unmanned Aerial System

UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
USV	Unmanned Surface Vehicle
UxS	Unmanned System
VTOL	Vertical Take-Off and Land

EXECUTIVE SUMMARY

The Office of the Secretary of Defense acknowledges that the technology and the proliferation of small unmanned aerial systems (sUAS) continues to advance at a pace that challenges the Department of Defense's (DOD) ability to respond effectively within current paradigms (Department of Defense [DOD] 2020). Per the Government Accountability Office (GAO), with over 2 million sUAS drones projected in the U.S. by 2024, these risks are likely to grow (Bothwell 2022). Existing applications of C-UAS when compared to this growth highlights a significantly disproportionate relationship where many C-UAS infrastructures offer not only inadequate defense rendering a situation of asymmetric warfare, but also in many instances hinder operations further (Theissen 2022, 66). At present, there exists a prioritization of identifying novel and innovative approaches to managing this sUAS threat. However, as a perfect C-UAS system does not exist, a combination of these must be used for adequate coverage. Even further, there currently lacks an identification, concentration, and assessment of the effects chains of these individual systems regarding joint operations. This lack of understanding of what systems are available and how they could be best applied together to certain assets and situations has subsequently inhibited appropriate deployment, integration, and usage of C-UAS.

The anticipated threats to the Joint Services and the Department of Homeland Security (DHS) from sUAS attacks are varied and include some of the following:

- airport takeoffs and landings
- civilians within protected perimeters
- surface ships and submarines stationed in-port or in littoral waters
- dismounted infantry and Light Armored Vehicles
- first responders
- command and control centers
- critical infrastructure

As identified in a study on C-UAS capabilities for battalion-and-below operations (Division on Engineering and Physical Sciences [DEPS] 2018),

> Developing effective countermeasures to highly modified and customized sUASs is a difficult challenge. Effectively countering sUASs requires the rapid detection, identification, and neutralization of threat sUASs. Detection and identification are exceedingly difficult because sUASs are compact, can fly at low altitude, and can have highly irregular flight paths that can range in speed from zero (hover) to close to 54 mph. Additionally, sUASs can take advantage of the significant amount of background clutter close to the ground (e.g., birds and trees) affecting many variables, such as line of sight (LOS) and signal propagation. (DEPS 2018, 9)

Greater challenges are presented to C-UAS systems once the threat is detected and identified. For neutralization, the DOD has been developing capabilities to defeat UAS, but these are primarily focused on platforms larger than the hobby-sized aircraft within sUAS. Of these solutions, there are those that are classified as kinetic or are energy responses. Notably, while effective in addressing many of C-UAS challenges, usage of energy counters predominately requires a significant amount of energy to effectively operate.

In response to this concern, an alternative approach is to utilize a networked squadron of UAVs designed for aerial interdiction to counter adversarial sUAS. This architectural and strategic C-UAS approach leverages high-performance with minimal SWaP requirements to create less expensive, but more capable and scalable C-UAS devices to augment existing capabilities (DEPS 2018). Experiments have shown that it is possible for these networked UAVs to deliver a precision aerial cyber-attack against multiple UAVs using Wi-Fi communication protocols with minimal effect on the host device, drastically contrasting power requirements, as well as presenting minimal interruption to operationally adjacent systems.

The goal of this project is to provide a capability-based framework in which to recommend C-UAS architecture layering, configuration, Research, Development, Test and Evaluation (RDT&E), and deployment within an operational setting as well as a framework for evaluating current and future research projects that investigate energy requirements for existing C-UAS and proposed cyber-attack C-UAS methods. This is accomplished by developing a model-based environment that defines the C-UxS defense mechanisms explored by the Operational C-UxS Energy Optimization through Cybersecurity Strategy

(Hale and Van Bossuyt 2022) within a mission-engineering context and conducting performance analyses to ascertain mission effectiveness and energy needs. This project will maintain C-UAS as the primary use case but will expand its focus to other sub-categories of C-UxS as opportunities permit.

The systems engineering (SE) process used in in this project supported a mission-engineering (ME) focused analysis process based on model-based system engineering (MBSE) fundamentals. The team leveraged the System of Systems Engineering and Integration (SoSE&I) methodology, an extension of Systems Engineering "Vee" process. This project executed the entire left side of the "Vee" from Concept of Operations through Implementation. Equally critical to this project was architectural development and MBSE processes. Architectural Development helped to define and develop the important aspects of the project including views and details critical to stakeholders. MBSE is "the formalized application of modeling" in a cost-effective manner to support the classical SE process of "system requirements, design, analysis, verification, and validation activities" (INCOSE 2015, 189). Model-based processes provide the analytical framework to conduct the analysis of the system virtually defined in the model. This capstone report used Innoslate, a MBSE tool which supports architectural development and SE modeling. Innoslate allows users to model complex systems with DoDAF compliant diagrams. These diagrams were generated automatically from the project model and allow seamless translation between other modeling and analysis tools.

The CONOPS focuses on the use of sUAS as a means of enabling asymmetric warfare, where the primary threat employed in most cases is by a less capable adversary. The C-UAS operational concept will employ defense-in-depth (DiD) strategies to leverage multiple layers of defense in a dynamic threat landscape. While the C-UAS operational context will capture all phases of the warfighting effects chain, the CONOPS scenarios will specifically focus on the phases of the mission that uniquely challenges the C-UAS capability (Figure 1). These focus areas are denoted as: Sense (detect, classify, locate, and track), Assess (decide how to respond to threat and determine desired effect/targeting solution), and Neutralize (engage).

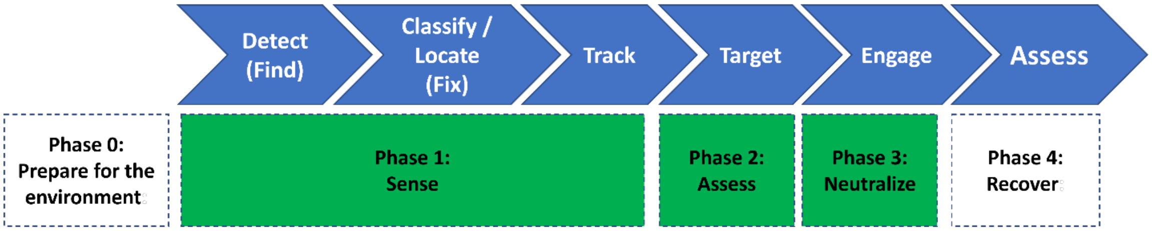


Figure 1. C-UAS Operational Scenario Priorities

Operational Analysis defined a conceptual idea for the C-UAS capability and determined the feasibility for operational mission success. An operational vignette for C-UAS Combat Patrol was developed using the C-UAS CONOPS. The mission definition summary was developed to describe both the entering conditions and boundaries such as the operational environment and the commander's desired intent. Next, the operational architecture was developed to describe the tasks, information exchanges, operational elements, and other entities required to accomplish the mission. Lastly, value systems design was conducted to establish performance and mission effectiveness metrics that represent stakeholder priorities. These products provided the necessary functionality to begin the development of the resource architecture.

The Resource Architecture derives system context and functions from the operational domain to develop the baseline System of Systems architecture. This included analyzing the scope of the system and linking together the operational and systems architecture by mapping system resource functions and data flows to operational performer activities and information exchanges. A key activity in this stage was a high-level functional analysis of the system. These analyses facilitated the development of a generic physical architecture. This architecture focuses on the main tasks determined by the functional analysis for mission success. The previously identified performance metrics from operational analysis were mapped to the identified systems functions. Finally, technical performance measures were captured for the system performers identified in the operational scenario to be simulated.

The SE process concludes with an Architectural Assessment that uses modeling and simulation techniques to assesses the C-UAS architecture in mission scenarios, investigating mission effectiveness as defined by operational analysis, with a specific focus on cyber-attack resilience, reliability, and energy usage. With the challenge of evaluating a growing number of sUAS, C-UAS systems, and other participants within a setting, a modeling and simulation (M&S) environment is needed. This project developed the DROSERA analysis tool as its C-UAS M&S environment. The DROSERA analysis tool relies on agent-based modeling (ABM) and aims to capture the mutual relationships of systems and the dynamic nature of these environments that will help illustrate mission effectiveness, asset preparedness, and projected resource requirements of capability deployment. Monte Carlo methods are applied to the ABM scenarios to generate non-deterministic behaviors associated with the operational scenario.

Next, an experimental design strategy was developed to ensure appropriate examination of the system performance characteristics within the mission context. The experimental design strategy presented is intended primarily to validate the feasibility of the DROSERA Analysis Tool in emulating the behaviors and exhibiting performance measures that are traceable to the C-UAS mission architecture model.

Finally, the DROSERA Analysis Tool performed simulations on six architecture variants that represented a unique vignette of the C-UAS Combat Patrol scenario, varied based on the C-UAS capability configuration and threat sUAS packages employed in each scenario. Monte Carlo analysis was performed running 100 iterations of the C-UAS Combat Deployment Operational Scenario for each vignette. Simulation results were tabulated and model analysis was performed. Statistical, output, and qualitative analysis of the simulation date revealed that C-UAS DiD configuration achieved the highest score based on unmatched performance across seven MOE categories, but the C-UAS Cyber-attack configuration is assessed to be a viable alternative to the DiD configuration because it offers comparable performance with DiD for radio-controlled sUAS threats, and it offers a low-cost, mobile solution.

In conclusion, the DROSERA project has successfully demonstrated, via proof of concept, that the C-UAS scenarios and vignettes implemented and analyzed were traceable to C-UAS strategic objectives, aligned with joint tasks, and could satisfactorily identify impacts on mission effectiveness and system performance. It is recommended that the C-

UAS Mission Model and the DROSERA Analysis Tool continue to be utilized and refined to support the definition and analysis of more specific research questions as pertaining to C-UxS. Recommendations for future improvements to the DROSERA project mission modeling and M&S environment are also presented.

References

Bothwell, Brian. 2022. *Science & Tech Spotlight: Counter-Drone Technologies*. GAO-22-105705. Washington, D.C.: Government Accountability Office. https://www.gao.gov/assets/gao-22-105705.pdf.

Department of Defense. 2020. *Counter-Small, Unmanned Aircraft Systems Strategy*. Washington, D.C.: U.S. Department of Defense. https://permanent.fdlp.gov/gpo150130/department-of-defense-counter-small-unmanned-aircraft-systems-strategy.pdf.

Hale, Britta, Douglas Van Bossuyt, 2022. *Operational C-UxS Energy Optimization through Cybersecurity Strategy*. White Paper. Monterey, CA: Naval Postgraduate School.

INCOSE. 2015. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, version 4.0. Hoboken, NJ, USA: John Wiley and Sons, Inc.

Theissen, Christian, 2022. "Redesigning the Counter Unmanned Systems Architecture" Master's Thesis, Naval Postgraduate School. http://hdl.handle.net/10945/70767.

ACKNOWLEDGMENTS

Team DROSERA would like to extend its gratitude and recognition for all of the support received during the completion of the Counter-UxS Energy and Operational Analysis capstone report.

Team DROSERA would like to show appreciation to our advisors, Dr. Douglas Van Bossuyt, Ms. Corina White, and Dr. Britta Hale, for their guidance and mentorship to ensure Team DROSERA succeeded in completing the capstone project required for graduation. In addition, a special thank you to Chee Hoe (Jason) Lee and Christian Thiessen for their sound advice throughout the early developmental stages of the capstone project.

Finally, and most importantly, we would like to recognize the families and friends of the team members for their unwavering support, patience, and encouragement during the past two years while navigating through the Naval Postgraduate School Systems Engineering master’s program. Your love and support through the many long nights of research and writing was critical to our academic success and accomplishments.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

1. Accessibility to Autonomy

Once a capability only available to near-peer competitors, the significant increase in consumer and industrial usage of unmanned systems (UxS) within the last decade has subsequently made the unparalleled dexterity and utility of drones accessible to all. This has been made possible because of three primary factors and has yielded an overall complicated situation. The first of these items is the increasing prevalence of information concerning these systems. From the increased popularity of UxS not only professionally, but also recreationally, more of the general populace are wanting to access autonomy. However, many of these individuals do not have the understanding concerning operations and manufacturing previously required to build and use their own systems. In response to this demand, a large community has arisen to create publicly digestible information for UxS. Individuals now have an immediate library of knowledge concerning the operation, construction, and development needed for their own UxS applications and most notably small Unmanned Aircraft Systems (sUAS) through a variety of walkthrough and open-source resources.

Second, due to the exponential growth of this development, materials needed to manufacture UxS have become both more affordable and ubiquitous. Previously, many components needed to create a capable system had to be developed and tailored for specific use cases. This would require an extensive amount of equipment, resources, skilled personnel, and time, as everything from chassis manufacturing to navigational software would need to be created. However, due to the commercialization of autonomy, most if not all components necessary for a UxS can be purchased at a fraction of the cost and generally with “next-day” delivery, subsequently expediting development, procurement, and deployment of UxS.

Lastly, the supply chain supporting UxS technologies has evolved to such a great degree that they are available commercially off-the-shelf (COTS). Many of these platforms exhibit state-of-the-art functionality, with most hosting several complex capabilities, such as autonomous maneuvering, waypoint planning, data recording, and payload ferrying. Access to a formidable system can now be purchased as conveniently as any smartphone.

Once a complex, longwinded, and overall difficult undertaking that generally required the involvement and assets of various parties, UxS has benefited from increases in information sharing and materials. The combination of these factors has widely enabled the obtainment of efficient and effective deployment of affordable, unique, and complex systems that are affordable and accessible to much of the populace.

2. Usages and the Classification of UAS

Concerning the topic of this capstone, primary discussion will be in reference to aerial drones, however many of the concepts are applicable to most of UxS as a whole. Notable nomenclature for this area begins with the identification of the Unmanned Aerial Vehicle (UAV). The UAV consists of an airframe and additional hardware and software components to allow the total platform to fly and operate, such as flight controller, radio receiver, and motors, to name a few.

Additionally, the outline concept of UAV platforms is an individual component that is part of a bigger collection called the Unmanned Aircraft Systems (UAS), which additionally includes radio transmitters, ground controls station (GCS), and any further required items needed for the UAV to function in an operational environment. A generic overview can be seen in Figure 1.

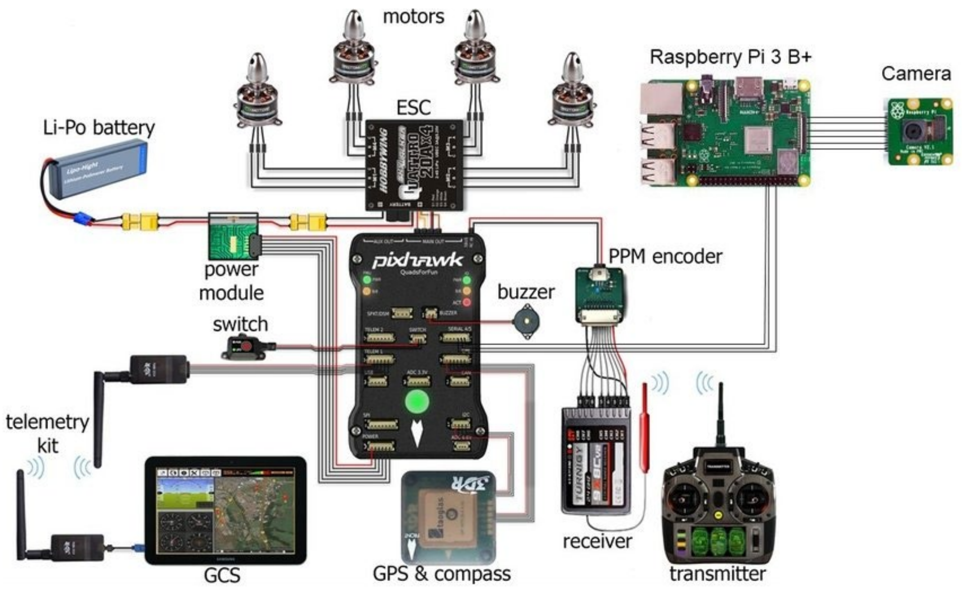
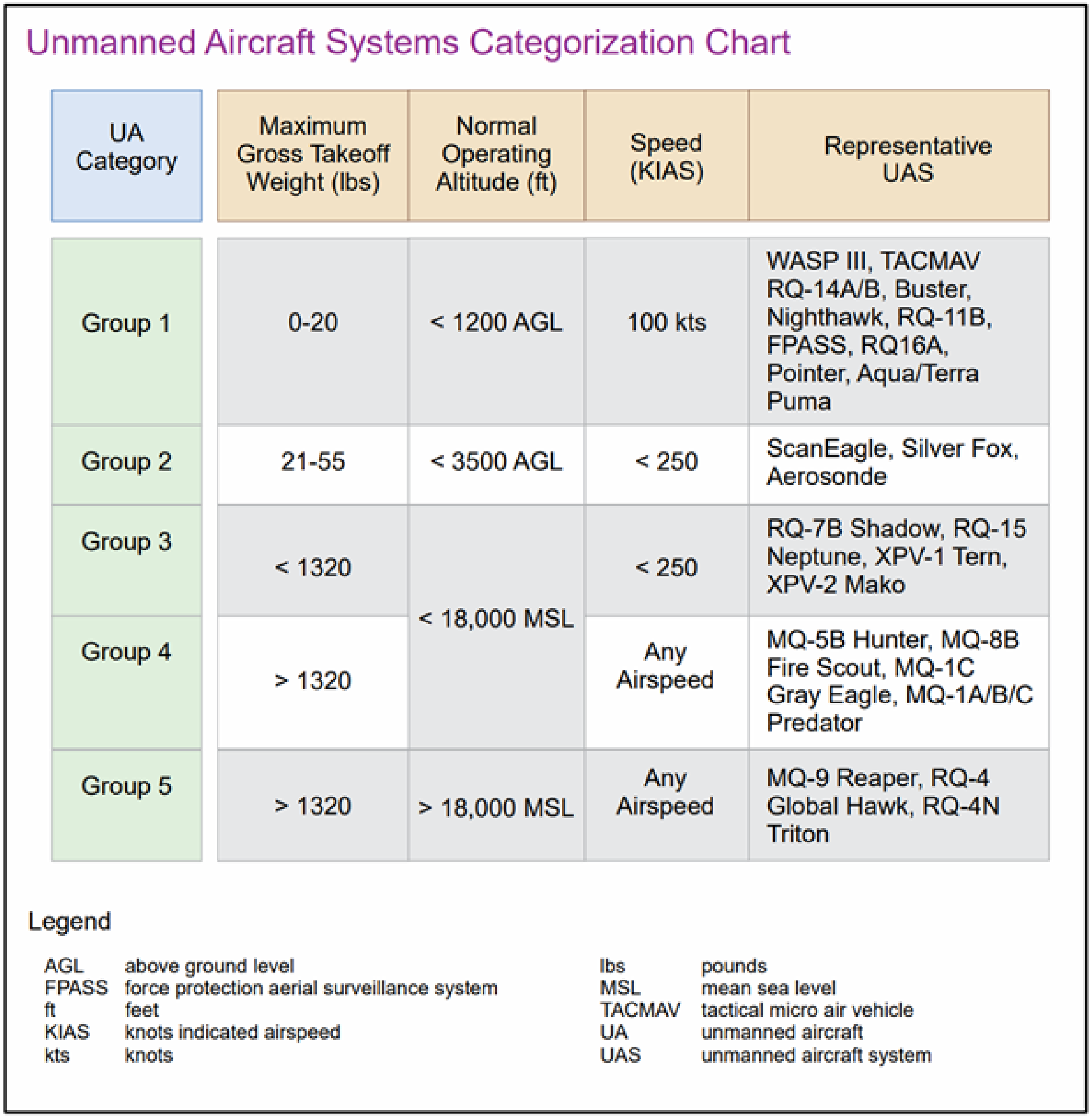


Figure 1. Wiring Overview for UAS.
Source: Wubben et. al. (2019).

Further, through understanding the delineation between UAS and UAV there exists even further specifications with which platforms are identified. A category of unmanned aircraft termed small UAS (sUAS) consists of UAVs that are categorized through Groups 1, 2, and 3 (Table 1) and are the primary topic covered for this capstone. It should also be noted that, for the purpose of this project, Group 1 should include commercially available hobby aircraft.

Table 1. Category of Unmanned Aircraft Systems in Groups. Source: Joint Chiefs of Staff [JCS] (2021).



Unmanned Aircraft Systems Categorization Chart

UA Category	Maximum Gross Takeoff Weight (lbs)	Normal Operating Altitude (ft)	Speed (KIAS)	Representative UAS
Group 1	0-20	< 1200 AGL	100 kts	WASP III, TACMAV RQ-14A/B, Buster, Nighthawk, RQ-11B, FPASS, RQ16A, Pointer, Aqua/Terra Puma
Group 2	21-55	< 3500 AGL	< 250	ScanEagle, Silver Fox, Aerosonde
Group 3	< 1320	< 18,000 MSL	< 250	RQ-7B Shadow, RQ-15 Neptune, XPV-1 Tern, XPV-2 Mako
Group 4	> 1320		Any Airspeed	MQ-5B Hunter, MQ-8B Fire Scout, MQ-1C Gray Eagle, MQ-1A/B/C Predator
Group 5	> 1320	> 18,000 MSL	Any Airspeed	MQ-9 Reaper, RQ-4 Global Hawk, RQ-4N Triton

Legend

AGL	above ground level	lbs	pounds
FPASS	force protection aerial surveillance system	MSL	mean sea level
ft	feet	TACMAV	tactical micro air vehicle
KIAS	knots indicated airspeed	UA	unmanned aircraft
kts	knots	UAS	unmanned aircraft system

3. The Challenges for Countering sUAS

With these sudden and recent emerging advancements within UxS, and more specifically sUAS, there exists a global lapse in response concerning appropriate regulation and defensive strategies. The existing infrastructure to combat these systems, known as counter-unmanned aerial systems (C-UAS), rely on a combination of techniques jointly integrated to best fit the needs of their assets. This practice is referred to as defense-in-depth. However, many of these current approaches for obtaining an effective defense-in-depth have innately flawed properties.

Many of these disadvantages originate from the fortress defensive model traditionally used in which protections are stagnant, inflexible, and consequently an incompatibility to address the fast-paced and dynamic needs of 21st century warfare. Implementation of these systems are in most cases cumbersome both given physical restraints and regarding infrastructure. Most UAS require regular maintenance and significant power, amongst other complications, to be operationally successful. Achieving sufficient defense-in-depth capabilities for C-UAS is also financially exorbitant as it requires the integration and operation of many independent systems. Lastly, the methodology employed for the most common of these systems operates primarily upon navigational and communication denial, interruption, or spoofing. This has been demonstrated to be effective against unmodified COTS C-UAS but has also yielded collateral repercussions from mutual interference from large signal denial footprints on communication systems of allied and uninvolved parties.

The near-future sUAS threat to U.S. forces and infrastructure indicates that current C-UAS capabilities and TTPs need to evolve to pace the threat. The widespread availability of UAS and the absence of adequate responsive measures amongst the international community has perpetuated and allowed for an opportunity for asymmetric warfare, or a conflict in which combat effectiveness is less reliant upon an entity’s resources but is instead characteristic of their weaknesses being exploited by non-comparable adversary through unconventional means. This can be seen given recent history in such events as the Islamic State of Iraq and Syria (ISIS) drone program, the Nagorno-Karabakh conflict, and the Russo-Ukraine war, where UAS had proved pivotal. In these situations, UAS were used within expected intelligence, surveillance, and reconnaissance (ISR) and opportunistic operations, but also demonstrated a continued evolution in use cases (Theissen 2022). From this, several factors and vulnerabilities can be highlighted that are fundamental to C-UAS. Given capabilities and strategies, a pursuit for resilient defense-in-depth with concentration on systems with near immediate, varied, cost-appropriate, and adaptive response, as well as broad, uninfluencing, and scalable coverage are necessary for improvements to C-UAS architecture for subsequently interested stakeholders.

B. OBJECTIVE

This Naval Postgraduate School (NPS) Master of Science in Systems Engineering (MSSE) Cohort 311 team has been assigned a capstone project that contributes to the Naval Research Project's (NRP) efforts in developing low-power Counter Unmanned Systems (C-UxS) technologies. These technologies strive to reduce energy consumption and establish a collaterally conscious disruptive signal footprint while maintaining operational effectiveness of C-UxS systems. Leveraged efforts in support of this NRP have assessed that the U.S. framework for countering unmanned systems through the utilization of stagnant centralized terrestrial equipment is insufficient because it lacks the robustness and flexibility needed to thwart a multi-pronged attack from an adversarial group. An alternative approach is to utilize a networked squadron of UAVs designed for aerial interdiction to counter the adversarial UAVs. This C-UAS approach leverages high-performance with low Size, Weight, and Power (SWaP) requirements to create less expensive, but more capable C-UAS devices to augment existing capabilities. Experiments have shown that it is possible for these networked UAVs to deliver an aerial cyber-attack against multiple UAVs using Wi-Fi communication protocols with minimal effect on the host device (Theissen 2022), as well as presenting minimal interruption to operationally adjacent systems. The focus of this capstone team will be to further explore and assess these low power, cyber-attack C-UxS technologies within a mission context and with joint operations with other C-UxS strategies.

The purpose of this project is to develop a model-based environment that defines the C-UxS defense mechanisms explored by the Operational C-UxS Energy Optimization through Cybersecurity Strategy within a mission-engineering context and conduct performance analyses to ascertain mission effectiveness and energy needs. This project will maintain C-UAS as the primary use case but will expand its focus to other sub-categories of C-UxS as opportunities permit. Further details about the scope of this project effort are addressed in Chapter II.

The completion of this project contributes directly to Deputy Assistant Secretary of the Navy, Operational Energy (DASN-OE) funded project, Operational C-UxS Energy Optimization through Cybersecurity Strategy (Hale and Van Bossuyt 2022). This research project is a multi-year effort that investigates energy requirements for existing C-UAS and proposed cyber-attack C-UAS solution. A successful outcome of this research will shape design and operation recommendations for C-UxS based on energy requirements, and explore cyber-attacks as a low energy, high impact alternative or addition to existing C-UxS systems, providing a defense-in-depth capability.

C. PROJECT TEAM

The members of the capstone project team, Team C-UxS Defense Reaction and Operational Strategy Evaluation, Response, and Analysis (DROSERA), possess a wide variety of skill sets and experience, which is well suited to support this research project. The overall success of the project, including accomplishing the goals and objectives set forth, is reliant on a diverse interdisciplinary team. Table 2 identifies the student team members and the organization that they support.

Table 2. Team DROSERA Members

Team Member	Organization
Behling, Jason	Naval Surface Warfare Center Crane Division (NSWC Crane), Chief Engineer, Specialized Munitions Division
Fuentes, Fernando	Naval Surface Warfare Center Dahlgren Division (NSWC Dahlgren), Software Engineer, Integrated Combat Systems Department
Mannings, Larry	Naval Undersea Warfare Center, Division Newport (NUWCDIVNPT). Mission Engineer, USW Mission Engineering and Analysis Department
Morgan, Golda	Naval Surface Warfare Center Corona Division (NSWC Corona), Engineer, Infrastructure Assessment Branch
Schinowsky, Jonathan	Naval Information Warfare Center Pacific (NIWC PAC), Robotics R&D Engineer and UAS Specialist and Air Vehicle Operator (AVO), Unmanned Systems

D. SYSTEMS ENGINEERING PROCESS

1. Overview

There are several textbooks available to NPS students (Blanchard and Fabrycky 2011, 19–43; Buede and Miller 2016, 27–41) that describe the process of developing a system whose development typically progresses as follows: identifying stakeholders, defining requirements, architecting the system, designing the system, prototyping, testing the system prototypes, refining the system, manufacturing the system, fielding the system, and maintaining the system. While these practices are sufficient for engineering and development activities associated with a typical systems-development program, the Mission Engineering (ME)-focused capstone projects assigned to NPS students will require the application of "an assessment framework to measure progress toward mission accomplishment through end-to-end system integration of test and evaluation of mission threads" (Gold 2016, 7). More specifically, the integration of the ME based on model-based system engineering (MBSE) fundamentals will permit the team to develop a "mission" systems architecture and conduct mission analysis. This integration enables and streamlines our understanding of the "tradeoffs available in the selection and integration of system configurations in a mission engineering context" (Beery and Paulo 2019, 1).

The team has reviewed various systems engineering processes in determining the best approach for implementation in this project. Examples include the waterfall process model, the spiral process model, and the "Vee" process model. The recommended SE approach for this ME-focused capstone project is the System of Systems Engineering and Integration (SoSE&I) methodology. SoSE&I is the "planning, analyzing, and integrating of constituent systems into a System of Systems (SoS) capability greater than the sum of those systems" (Vaneman 2016, 1), and would span the entirety of the project. The SoSE&I methodology is built on a Systems Engineering "Vee" process model as shown in Figure 2 (Shaffer 2017, 5). The upper-left side of the "Vee," referred to as SoS Architecture & Requirements Development, has a mission/capability focus and strives to define enterprise and SoS requirements and identify the greatest need/best opportunities for technology insertion. The bottom of the "Vee," referred to as "Systems Design & Development," includes the traditional systems engineering activities needed for the development of individual systems. Multiple "Vees" are depicted to represent that the individual systems are being developed iteratively and in parallel. The upper right side of the "Vee" includes certification activities. (Vaneman 2016, 1–7). For this project, the team does not expect to perform verification beyond the SoS Interoperability & Certification tier. Verification/ Validation in the Mission Assurance domain would require a Live/Virtual/Constructive (LVC) test environment. The systems defined in the Systems Design & Development domain are expected to be pre-defined at a level appropriate for SoS Engineering.

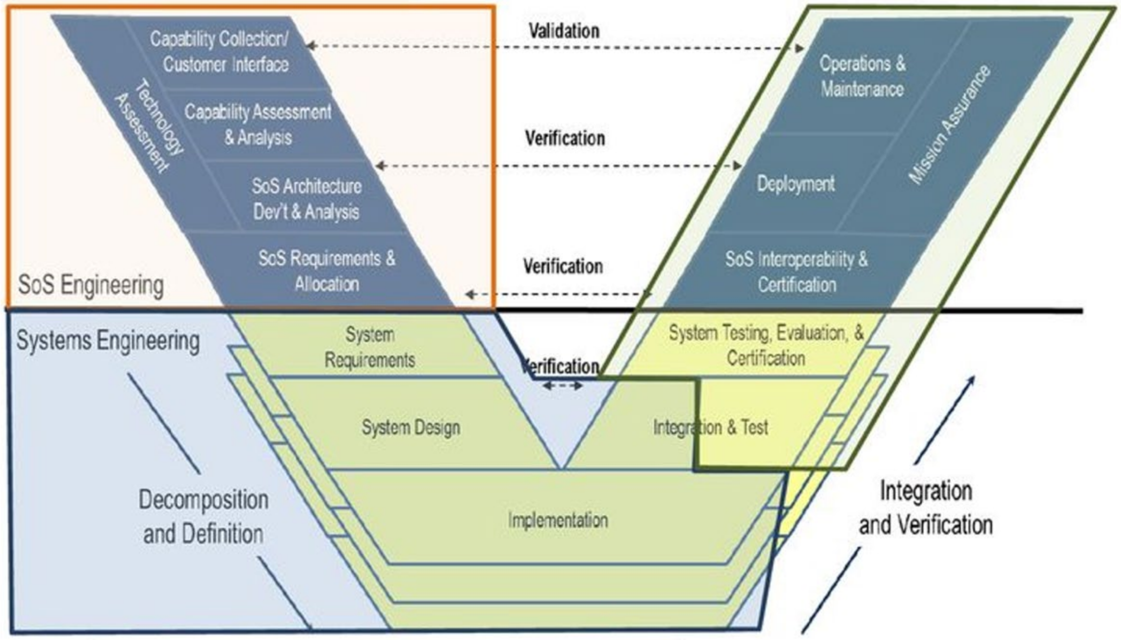

Capability Collection/ Customer Interface
Technology Assessment
Capability Assessment & Analysis
SoS Architecture Dev't & Analysis
SoS Requirements & Allocation
SoS Engineering
Validation
Verification
Verification
Operations & Maintenance
Mission Assurance
Deployment
SoS Interoperability & Certification
Systems Engineering
System Requirements
Verification
System Testing, Evaluation, & Certification
System Design
Integration & Test
Implementation
Decomposition and Definition
Integration and Verification

Figure 2. The SoSE&I "Vee".
Source: Shaffer (2017).

2. Architectural Development and MBSE Processes

Architecture is "a fundamental and unifying structure defines in terms of elements, information, interfaces, processes, constraints, and behaviors" (Dam 2014, 8). Architecture is a critical piece to this capstone project and to SoS integration in general. Architecture can serve as a method for deriving necessary requirements. This can include the system design, the test and evaluation plan, and the operations and support necessary. Dam states that, "The correct application of architecture gives us the basic requirements needed to pursue system development and acquisition" (Dam 2014, 4). This team will utilize the Department of Defense Architecture Framework (DoDAF) for classification schema and presentation frameworks. DoDAF is especially useful for enterprise-level projects such as acquisition of joint-defense capability systems with complex integration and interoperability challenges. The use of DoDAF operational views offer overview and details aimed at specific stakeholders across the spectrum of domains for which the system will be expected to operate. For this capstone project, the team will follow the DoDAF six-step process (Figure 3) in support of architectural development. In DoDAF 2.0, this process is defined as a "Methodology Based Approach to Architecture." The high-level, 6-step architecture development process emphasizes the overarching guiding principles for SoS architecture development (Department of Defense [DOD] Chief Information Officer [CIO] n.d.; Architectural Development).

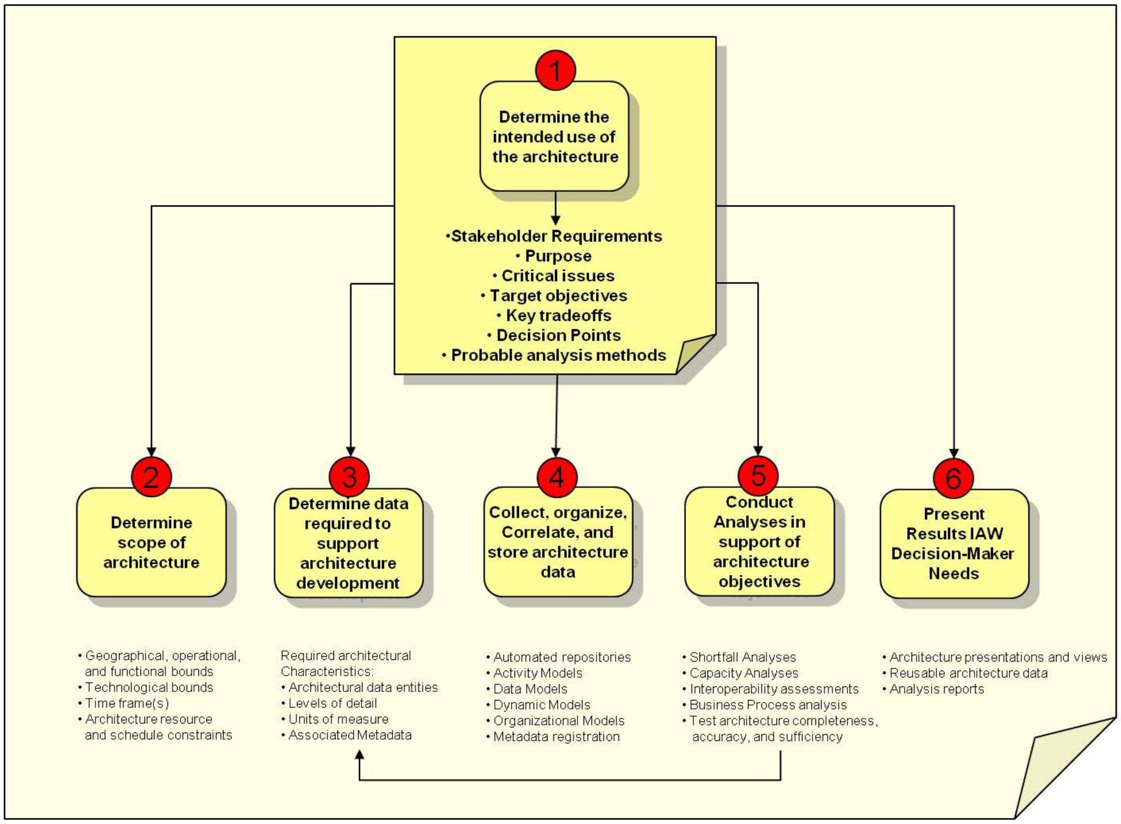

1
Determine the intended use of the architecture
•Stakeholder Requirements
• Purpose
• Critical issues
• Target objectives
• Key tradeoffs
• Decision Points
• Probable analysis methods
2
Determine scope of architecture
3
Determine data required to support architecture development
4
Collect, organize, Correlate, and store architecture data
5
Conduct Analyses in support of architecture objectives
6
Present Results IAW Decision-Maker Needs
• Geographical, operational, and functional bounds
• Technological bounds
• Time frame(s)
• Architecture resource and schedule constraints
Required architectural Characteristics:
• Architectural data entities
• Levels of detail
• Units of measure
• Associated Metadata
• Automated repositories
• Activity Models
• Data Models
• Dynamic Models
• Organizational Models
• Metadata registration
• Shortfall Analyses
• Capacity Analyses
• Interoperability assessments
• Business Process analysis
• Test architecture completeness, accuracy, and sufficiency
• Architecture presentations and views
• Reusable architecture data
• Analysis reports

Figure 3. DoDAF Architectural Development 6-Step Process.
Source: DOD CIO (n.d.).

Since the 6-step process does not specify below-the-line modeling processes for generating the models, viewpoints, and analyses specified for each step, additional tailored MBSE processes are required. For this capstone project, our team will use the middle-out MBSE process, as depicted in Figure 4. The "middle-out" MBSE process is described by Dam as an ideal SE approach when your goal is to develop a "to-be" type of architecture when you may have been given broad system requirements (Dam 2014, 88–89). The middle-out MBSE process is tailored to specifically support DoDAF-based architectures where most of the steps in the process overlap and are concurrent and iterative throughout the process (Dam 2014). The numbered steps indicate a nominal starting sequence and the overlapping of steps demonstrates the iterative nature of the process. The middle-out MBSE process is also color coded to depict the alignment with the classical 4-step SE process of requirements analysis, functional analysis, synthesis, and system analysis and control.

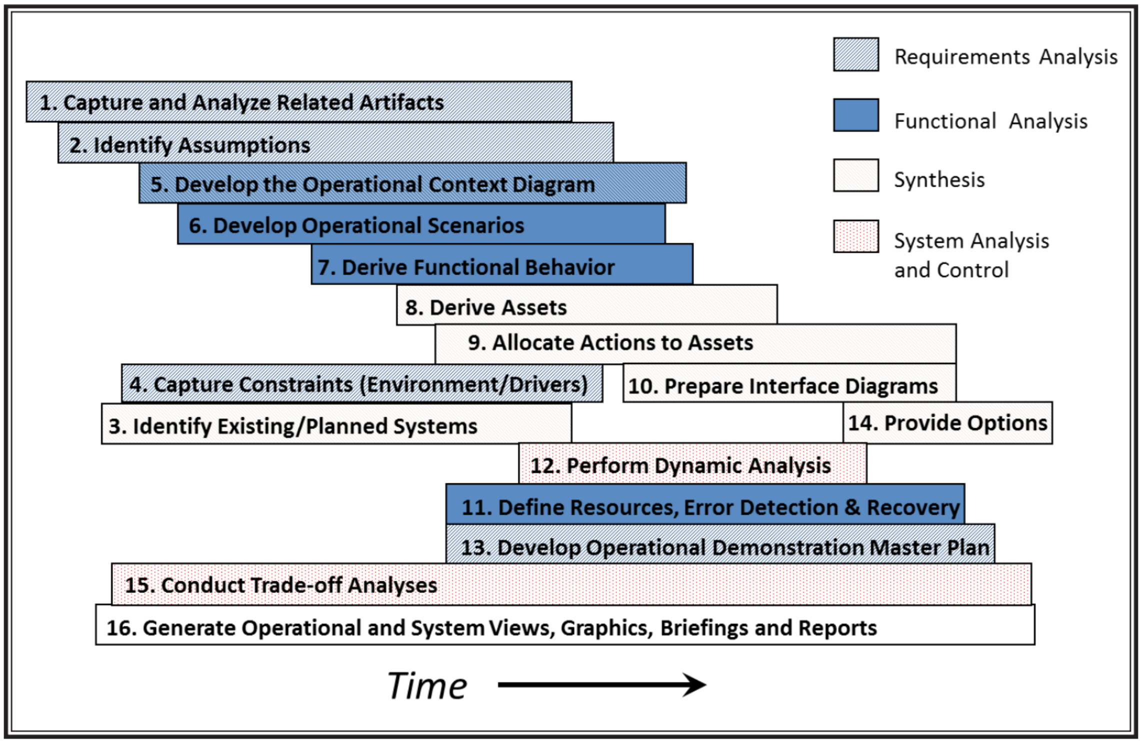

Requirements Analysis
Functional Analysis
Synthesis
System Analysis and Control
1. Capture and Analyze Related Artifacts
2. Identify Assumptions
5. Develop the Operational Context Diagram
6. Develop Operational Scenarios
7. Derive Functional Behavior
8. Derive Assets
9. Allocate Actions to Assets
4. Capture Constraints (Environment/Drivers)
10. Prepare Interface Diagrams
3. Identify Existing/Planned Systems
14. Provide Options
12. Perform Dynamic Analysis
11. Define Resources, Error Detection & Recovery
13. Develop Operational Demonstration Master Plan
15. Conduct Trade-off Analyses
16. Generate Operational and System Views, Graphics, Briefings and Reports
Time

Figure 4. Middle-Out MBSE Process.
Source: Dam (2014, 89).

3. ME Capstone Process Alignment with Architectural Development / MBSE Processes

Table 3 depicts alignment between the NPS Mission Engineering Capstone development phases and MBSE processes (Van Bossuyt et al. 2019; Dam 2014). Alignment with the DOD development architecture (DOD CIO n.d.) is also provided to support the synchronized development of architectural products.

Table 3. NPS Mission Engineering Capstone project alignment with MBSE Processes. Adapted from DOD CIO (n.d.), Van Bossuyt et al. (2019) and Dam (2014).

NPS ME Capstone Phases	MBSE for ME Activity	DOD Developmental Architecture Step	Middle-out MBSE Process
SoS Definition	**Requirements Definition**	**Step 1:** Determine Intended Use of Architecture	**Step 1:** Capture and Analyze Related Documents
			Step 2: Identify Assumptions.
			Step 4: Capture Constraints
			Step 5: Develop Operational Context Diagram
	Architecture Definition	**Step 2:** Determine Scope of Architecture	**Step 3:** Identify Existing and Planned Systems
			Step 5: Develop Operational Context Diagram
		Step 3: Determine Data Required to Support Architecture Development	**Step 6:** Develop Operational Scenarios.
			Step 7: Derive Functional Behavior
SoS Modeling	**Baseline Modeling**	**Step 3:** Determine Data Required to Support Architecture Development.	**Step 8:** Derive System Elements
		Step 4: Collect, Organize, Correlate, and Store Architectural Data.	**Step 9:** Allocate Functions to System Elements
			Step 10: Prepare Interface Diagrams
	Experimental Design	**Step 5:** Conduct Analyses in Support of Architecture Objectives.	**Step 11:** Define Resources, Error Detection, and Recovery Processes
	Simulation Modeling		**Step 13:** Develop Test Plans
SoS Analysis	**Model Analysis**	**Step 5:** Conduct Analyses in Support of Architecture Objectives.	**Step 12:** Perform Dynamic Analyses **Step 14:** Provide Options **Step 15:** Conduct Trade-off Analyses
	Dynamic Decision Support		

NPS ME Capstone Phases	MBSE for ME Activity	DOD Developmental Architecture Step	Middle-out MBSE Process
	Reporting & Documentation	**Step 6:** Document Results in Accordance with Decision-Maker Needs.	**Step 16:** Generate Views, Briefings, and Reports.

E. SUMMARY OF CHAPTERS

Chapter II focuses on defining the SoS architecture for analysis and determining the effective need concerning the challenges presented. The statement of need, the analysis of the current capabilities, and the stakeholder analysis enables a clear scope for the problem statement. The information gathered in the analysis supports the determining of the necessary capability requirements, operational tasks, system requirements, mission/system performance measures, and the supporting architecture, with focused emphasis on cyber-attack resilience, reliability, and their impact on C-UAS effectiveness and energy needs. Chapter II sets the direction for the operational analysis conducted in Chapter III.

Chapter III focuses on operational analysis of the C-UAS mission context. This analysis defines a conceptual idea for the C-UAS capability and determines the feasibility for operational mission success. An operational vignette for C-UAS Combat Patrol was developed using the C-UAS CONOPS. The mission definition summary was developed to describe both the entering conditions and boundaries, such as the operational environment and the commander's desired intent. Next, the operational architecture was developed to describe the tasks, information exchanges, operational elements, and other entities required to accomplish the mission. Lastly, a value systems design was conducted to establish performance and mission effectiveness metrics that represent stakeholder priorities. These products provided the necessary functionality to begin the development of the resource architecture explored in Chapter IV.

Chapter IV addresses the derived system context and functional requirements to develop the baseline SoS architecture. This includes analyzing the scope of the system and linking together the operational and systems architecture models by depicting how resources are structured and their interactions to realize the logical architecture. The chapter also details a high-level functional analysis of the system. These analyses facilitated the development of a generalized physical architecture. The previously identified MOPs from Chapter III were mapped to the identified systems functions. Finally, technical performance measures were captured for the system performers identified in the operational scenario to be simulated. These performance characteristics help aid in the development of the design of experiments outlined in Chapter V.

Chapter V conducts an architecture assessment of the architecture of Chapter IV. A modeling architecture was constructed to reference all model elements of the C-UAS mission characterization to include system performance characteristics, threat sUAS performance characteristics, environmental conditions, and capability metrics. The chapter continues with a high-level operational analysis to provide an initial assessment of the required system behavior identified in Chapter III. An experimental design strategy was developed to ensure appropriate examination of the system performance characteristics established in Chapter IV within the mission context. The experimental design strategy presented is intended primarily to validate the feasibility of the DROSERA Analysis Tool in emulating the behaviors and exhibiting performance measures that are traceable to the C-UAS mission architecture model.

Chapter VI concludes the report with analysis of the model simulations and provides a synopsis of the research efforts captured in the Capstone report. Additionally, the chapter addresses the results of the research questions and proposes follow-on work to expand upon the research.

II. PROBLEM DEFINITION

The Office of the Secretary of Defense acknowledges that the technology and the proliferation of small unmanned aerial systems (sUAS) continues to advance at a pace that challenges the Department of Defense's (DOD) ability to respond effectively within current paradigms (Department of Defense [DOD] 2020). Existing applications of C-UAS when compared to this growth highlights a significantly disproportionate relationship where many C-UAS infrastructures offer not only inadequate defense, but in many instances hinder operations (Theissen 2022, 66). At present, there exists a prioritization of identifying novel and innovative approaches to managing this sUAS threat. However, as a perfect C-UAS system does not exist, a combination of these must be used for adequate coverage. Even further, there currently lacks an identification, concentration, and assessment of the effects chains of these individual systems regarding joint operations. This lack of understanding of what systems are available and how they could be best applied together to certain assets and situations has subsequently inhibited appropriate deployment, integration, and usage of C-UAS.

The anticipated threats to the Joint Services and the Department of Homeland Security (DHS) from sUAS attacks are varied and include some of the following:

- airport takeoffs and landings
- civilians within protected perimeters
- surface ships and submarines stationed in-port or in littoral waters
- dismounted infantry and Light Armored Vehicles
- first responders
- command and control centers
- critical infrastructure

As identified in studies on C-UAS capabilities for battalion-and-below operations (Division on Engineering and Physical Sciences [DEPS] 2018),

> Developing effective countermeasures to highly modified and customized sUASs is a difficult challenge. Effectively countering sUASs requires the

> rapid detection, identification, and neutralization of threat sUASs. Detection and identification are exceedingly difficult because sUASs are compact, can fly at low altitude, and can have highly irregular flight paths that can range in speed from zero (hover) to close to 54 mph. Additionally, sUASs can take advantage of the significant amount of background clutter close to the ground (e.g., birds and trees) affecting many variables, such as line of sight (LOS) and signal propagation. (DEPS 2018, 9)

Greater challenges are presented to C-UAS systems once the threat is detected and identified. For neutralization, the DOD has been developing capabilities to defeat UAS, but these are primarily focused on platforms larger than the hobby-sized aircraft within sUAS. Of these solutions, there are those that are classified as kinetic or are energy responses. Kinetic counters, involving shooting down high-speed and dynamic, low fliers with common point-defense weapon systems, e.g., close-in weapon system (CIWS) and counter rocket, artillery, and mortar (CRAM), or even the usage of small arms, are extremely difficult due to the agility, small size, and even unpredictability of sUAS. Energy counters include equipment such as DroneDefender (Dedrone n.d) and generally involve denial, interruption, or spoofing[1] of communications with navigation controller, i.e., sUAS operator, GCS, or Global Positioning System (GPS). Further, this area also includes usages of electromagnetic effects or lasers. While effective in addressing many of C-UAS challenges, usage of energy counters predominately requires a significant amount of energy to effectively operate.

In response to this concern, an alternative approach is to utilize a networked squadron of UAVs designed for aerial interdiction to counter adversarial sUAS. This architectural and strategic C-UAS approach leverages high-performance with minimal SWaP requirements to create less expensive, but more capable and scalable C-UAS devices to augment existing capabilities (DEPS 2018). Experiments have shown that it is possible for these networked UAVs to deliver an aerial cyber-attack against multiple UAVs using Wi-Fi communication protocols with minimal effect on the host device, drastically

[1] Spoofing is the effort of posing with a false identity in order to gain information or access to something. In the context of UAS, it is the practice of imitating the message signature within the communications of UAS to commandeer the UAV.

contrasting power requirements, as well as presenting minimal interruption to operationally adjacent systems.

A successful outcome of this capstone project can shape design and operation recommendations for C-UAS research, development, test, and evaluation (RDT&E) as well as overall integration based on energy requirements, and explore cyber-attacks as a low energy, high impact alternative to existing C-UAS systems.

A. NEEDS ANALYSIS - CURRENT CAPABILITY ASSESSMENT

This capstone report will focus on UASs that are assigned to classification groups 1, 2, and 3 (Table 1) and shall be referred to as sUAS. A review of sUAS and C-UAS technologies, standard practices, and overall outline is needed to inform and have an understanding concerning their operations process. These technologies will form the basis for C-UAS capability taxonomy and operational conceptualization.

1. sUAS Capability Assessment

We must analyze the classification of sUAS to better understand the methods of attacking sUAS. To help identify sUAS technologies and correlate these technologies to future sUAS capabilities, a decomposition of sUAS capabilities is summarized below (DEPS 2018).

a. Types of sUAS

sUASs come in a variety of configurations, but can generally be considered one of the following,

- **Fixed Wing:** generates lift using the vehicle's forward airspeed and the upward force caused by the shape of its wings. Normally, one or more propellers provide thrust for forward motion. Forward motion is needed to maintain lift; thus, fixed wing sUAS cannot hover. Usage of fixed wings within the platform however offer significant improvements towards platform energy conservation, thus improving overall operational time and range. Overall, these platforms primarily have 4 degrees of freedom (DOF), which can be seen in Figure 5.

- **Rotary Wing:** a multi-rotor platform that generates lift and navigates by use of its vertically oriented propellers. Motion is generated by providing a difference in power to corresponding rotors or by tilting the rotors, providing 6 DOF. Rotary-wing sUAS normally have four to eight rotors. Similar to a helicopter, a rotary-wing sUAS can hover.
- **Hybrid:** exhibits a combination of mobility and transition functions such as takeoff / landing as a rotary-wing sUAS with in-flight operation like a fixed wing, commonly referred to as a vertical take-off and land (VTOL). Alternately, it may even transition back and forth between a sUAS and other UxS platform configurations, such as an unmanned ground vehicle (UGV) or unmanned surface vehicle (USV). Many of these platforms are designed to exhibit beneficial capabilities from their joined systems. In particular, the VTOL demonstrates the capability of six DOF, but also as increased flight time and distance from the integration of both a rotary and fixed-wing designs. (DEPS 2018, 10–11)

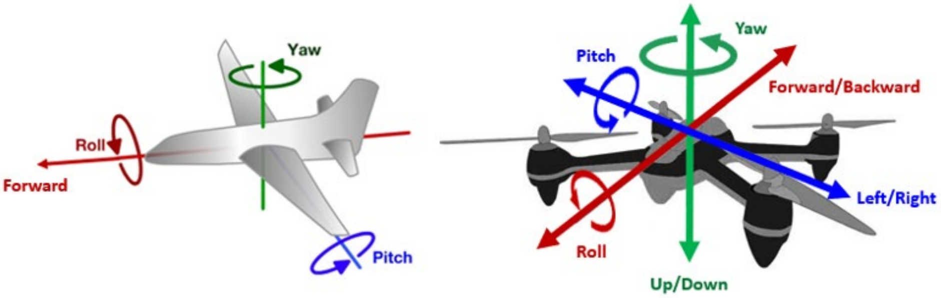


Figure 5. Fixed-Wing and Quadcopter Platform Degrees of Freedom

b. *Modes of sUAS Utilization*

Concerning the methodologies in which sUAS operates, there are a variety of techniques. Whether it is concerning the operative characteristic of a single platform or how multiples platforms coordinated interactions between one another and receive instruction, each possibility hosts important restrictions and attributes. The majority can be outlined as follows (DEPS 2018),

1. Single UAS: will have various levels of autonomy, including:

- **Wired or wireless, LOS, remote control:** An operator controls all operations of the sUAS, and the operator must have a clear LOS with the sUAS to understand its three-dimensional location and orientation while controlling the movements of the sUAS.
- **Wireless, non-LOS, remote control:** An operator controls all operations of the sUAS; however, a direct LOS is not necessary to understand its three-dimensional location and orientation while controlling its movements. Onboard sensors generate digital information (e.g., video, text, and graphical information) to enable the operator to understand the location of the sUAS with respect to its surroundings and the operator while the operator controls the movement of the sUAS.
- **Semi-autonomous:** The sUAS can perform extremely limited control activities to enhance the ability of the operator to perform other tasks. For example, it may automatically go into a hover when the operator stops inputting commands to observe video from the sUAS, or the sUAS may automatically avoid obstacles while being flown by the operator. However, the sUAS can perform very few tasks on its own without accompanying operator input. The operator often uses a communications link.
- **Nearly full autonomy:** The sUAS can perform many automated tasks, such as automatic flight control (including obstacle avoidance), engine control (for complex flight dynamics and hovering), target recognition, and target tracking. However, the automated tasks are still activated or deactivated by the operator, and, if activated, will function without the

specific knowledge of or control by the operator. An operator may direct the actions of individual or multiple sUASs in a supervisory role, especially in the execution of missions.

- **Fully autonomous:** Individual or large numbers of sUASs that require no human intervention to perform tasks, especially complex tasks such as planning and executing missions, navigating without GPS, avoiding obstacles, etc. The operator will assign missions, occasionally supervise the execution of missions, and be part of a manned-unmanned team.
- **Operator-Enabled, coordinated sUASs:** Two or more operators of single sUASs coordinate their efforts before and/or during a mission to accomplish mission tasks. The level of autonomy will most likely be used by remote-controlled or semi-autonomous sUASs.
- **Software-Enabled, coordinated sUASs:** One operator will control two or more sUASs to accomplish a mission. However, these sUASs will operate independently of each other, and the operator will control each of them individually either by pre-programming or by controlling them during flight. If a change in mission requires dynamic reprogramming or coordination during flight, this will significantly task the cognitive abilities of the operator, thus reducing the number of sUASs being controlled. The level of autonomy will most likely be wireless, non-LOS, remote controlled, semi-autonomous, or nearly fully autonomous sUASs.
- **Swarm of sUASs:** A swarm is a larger number (15 or more) of sUASs all following the same simple rules to achieve a goal. The key to a swarm is that the entire group appears to act as a single unit, but the individual sUASs act as distributed, local controllers. The individual sUASs behave like a collective organism, sharing one distributed brain for decision-making and adapting to each other, like swarms in nature. The level of autonomy will most likely be nearly fully autonomous sUASs. (DEPS 2018, 11–12)

c. *sUAS Payloads*

When assessing a UAVs capability and consequently its threat, grading is partially reliant on what the UAV may have as a payload. Payloads for UAVs consist of:

- **Non-kinetic:** Command and Control (C2) disrupters, cyber-attack.
- **ISR:** Signals Intelligence, cameras, thermal imaging.
- **Kinetic, unconventional:** Projectiles, small bombs.
- **Unconventional:** Chemical, Biological, Radiological, Nuclear, and high yield Explosives (CRBNE) weapons.
- **Targeting:** Sensors, communications links.

2. C-UAS Capability Assessment

Counter-UAS, as defined by Chamola (2021), refers to the process of prevention of potential UAV attacks by means such as capturing the UAV or jamming its communication channel to disrupt its flight pattern, possibly bring it to a halt on the ground. The various anti-UAV techniques are summarized below (Jackson et al. 2008, Castrillo et al. 2022; Kang et al. 2020; Chamola et al. 2021).

a. *Deterrence*

- UAV Operational Regulations: Enforcement of regulations that constrain frequency bandwidth, purpose, and performance of sUAS used in recreational and commercial applications. This would also include licensing requirements, such as the Federal Aviation Administration (FAA) Part 107.
- UAS Origination Regulations: The outlining and enforcement of limiting the operations of, as well as overall accessibility to UAV platforms and components and UAS equipment, such as radio controllers or flight control software, by considering country of origin concerning manufacturing and development. (Jackson et al. 2008, 94–96)

b. *Intelligence Preparation of the Operational Environment (IPOE)*

Characterization of a battlespace allows for an awareness of all aspects supporting a commander's decision-making process. The IPOE determines adversary intent and identifies networks, centers of gravity, and vulnerabilities. Employment of Intelligence, Surveillance, and Reconnaissance (ISR) is the primary capability employed for maintaining continuous overall awareness (JCS 2017).

ISR Function:

Referred to as "Support to Force Protection," the purpose of ISR is to continuously monitor the operational environment to characterize an adversary's capability, disposition, intent, and willingness to act. (JCS 2017, III 1–4)

c. *Monitoring*

The section below captures the response chain and methods of monitoring of UAVs.

1. Monitoring Operations:

- **Detection:** Sensing the presence of a UAV.
- **Identification:** Verifying and analyzing of the UAV and its properties.
- **Localization:** Tracking the position of the UAV.
- **Origination:** Tracking the location of deployment and possible operator for an UAV.

2. Monitoring Methods:

- **Radar:** Leveraging energy and properties of radio waves.
- **LiDAR:** Leveraging electromagnetic energy at the optical and infrared wavelengths.
- **Radio Frequency (RF) Analyzers:** Intercepting RF waves emitted from the UAV.

- **Video Surveillance:** Placing cameras and thermal imaging strategically in order to perform computer vision.
- **Audio Surveillance:** Utilizing machine learning to correlate audio signature of UAV moving parts with contacts of interest.
- **LOS:** Sighting a target physically by personnel (Kang et al. 2020, 168688–168691).

d. Command and Control (C2)

C2 provides communications links, data fusion, and decision aids that enable integration of available sensors, sensors, effects, and warning systems to launch rapid defense against sUAS (Granåsen 2019).

- **Decision Making:** Analyzing the situation, planning, and simulating the plans to assess the possible outcome of them.
- **Resilient Information Infrastructure:** Using communications technology that can persist, adapt, or transform in the face of attack or a changing environment.
- **Direction and Coordination:** Providing clear guidance on leadership and coordinating structures, authorization, and pre-planned responses.
- **Situational Awareness:** Perception of critical factors in the environment, understanding the meaning of these factors, and predicting what may happen in the near future. (Granåsen 2019, 17)

e. Neutralization

Neutralization is activated by the command-and-control capabilities to respond to the threat posed by the detected malicious sUASs. Stages and methods regarding neutralization are as follows:

Neutralization operations:

- **Warning:** Assuming a technique to communicate with the operator is available and the threat level is low, warning is the preferred neutralization strategy if it assessed that the UAV is engaging in non-nefarious misuse or unintended use of restricted airspace.

- **Control:** Involves the use of more sophisticated and high-end techniques and devices to control the UAV; rendering it inert, commandeering it to land safely, or triggering a built-in 'return-to-home' sequence.
- **Disruption:** Utilizing non-kinetic effects to interrupt the operation of the UAV.
- **Disablement:** The use of kinetic and non-kinetic means to cause the UAV to malfunction.
- **Destruction:** Physically neutralizing UAVs using weapons effects. Destruction is typically the last resort for neutralizing UAV; first, due to the risk to personnel from triggered explosions and falling debris, and second, because it hampers the ability to locate and capture the UAV operators. (Kang et al. 2020, 168687–168688)

Neutralization methods:

- **Electronic:** Use of electromagnetic waves to interrupt, disable or destroy a UAV.
- **RF Jamming:** Disturb, lower the quality of, or interrupt communications between the UAV and its respective control station.
- **Global Navigation Satellite System Jamming:** Utilization of RF Jamming techniques to interfere with the navigation signal received by the UAV required for navigation.
- **Spoofing:** Generating a plausible fake signal with enough strength to trick the UAV receiver into believing it is the legitimate signal.
- **Protocol-based attacks and replay attacks:** Use of cyber-attacks to exploit the vulnerabilities present in protocols used in communications networks used by sUAS. Another notable protocol-based attack is a replay attack, in which the neutralizing device intercepts the sUAS

communications by ‘eavesdropping,’ then delays or resends messages intended to control the UAV without alerting the network or the operator.

- **Electromagnetic Pulse (EMP):** devices that use high-power microwaves (HPM) to generate an EMP to disrupt or damage electronic devices
- **High Power Lasers:** systems that provide a near immediate response by burning or vaporizing threats.
- **Kinetic-mechanical:** Use of mechanical means to make contact between the neutralizer and the UAV.
- **Projectile Based:** Use of projectiles capable of destroying malicious UAS.
- **Collisions:** The targeting and engagement of a UAV in order to collide with and destroy the UAV
- **Nets:** Used to trap and immobilize UAVs
- **Birds of Prey:** Similar to military working dog (K9) units, the usage of falconry has begun training eagles and other birds of prey to neutralize targets. (Chamola et al. 2021, 12–16; Kang et al., 17–26))

B. STAKEHOLDER ANALYSIS

Team DROSERA identified primary stakeholders during the background research phase of this project. These stakeholders were then categorized into the groups outlined in Table 4.

Table 4. Stakeholder Categories

Warfare Analyst	Defines and assesses mission effectiveness
Systems Engineer	Determines solutions for specific systems
Requirements Office	Link between the using commands and the systems/ developing commands
Warfighter	Executes the mission

Stakeholder analysis helps to identify relationships between different stakeholders and map the stakeholders to the issues they care about. Having capstone project objectives mapped in this way aids in the prioritization of tasks and the crafting of products to reflect a specific viewpoint. After the project statement of need was finalized, the stakeholder categories were associated with the stakeholder needs via a Use Case Diagram (Figure 6). A summary of stakeholder needs and priorities is outlined in Table 5.

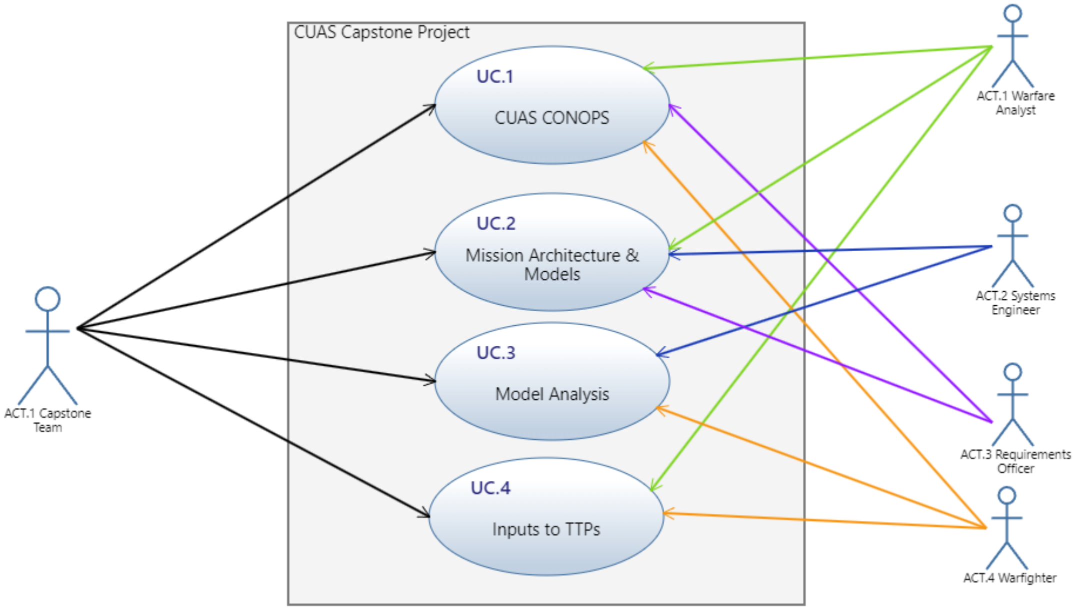


Figure 6. C-UAS Capstone Project Use Case Diagram

Table 5. Stakeholder Analysis Summary

Stakeholder	Role(s)	Need Description	Potential Impact
Deputy Assistant Secretary of the Navy, Operational Energy (DASN-OE).	Requirements Officer	Maintain a set of testable warfighting functional tasks and standards that define the C-UAS capability required for mission success	Significant
Joint Counter-Small UAS Office (JCO)	Warfighter	Establish joint solutions with a common architecture to address current and future emerging small UAS threats. Coordinate development of joint operational concepts and joint doctrine for C-UAS.	Moderate
Tactical Operators	Warfighter	Operate C-UAS systems and utilize the additional force protection capability provided	Low
NPS Department of Systems Engineering	Warfare Analyst Systems Engineer	Describe what must be done in the context of the larger C-UAS battle problem to enable performance measurement, gap determination, and concept exploration	Significant
Naval Research Partners	Warfare Analyst	Improved relevance and usefulness of the research; collaborative models and cost sharing	Moderate
NPS C-UAS Researchers	Systems Engineer	A set of testable C-UAS warfighting functions that can be further decomposed into technical functions and allocated to systems that form the basis of the mission analysis performance metrics.	Significant

C. STATEMENT OF NEED

This capstone provides a structure in which to recommend C-UAS architecture layering, configuration, Research, Development, Test and Evaluation (RDT&E), and deployment within an operational setting as well as a framework for evaluating current and future research projects that investigate energy requirements for existing C-UAS and proposed cyber-attack C-UAS methods. Specific stakeholder needs in this regard are as follows:

- C-UAS Concept of Operations (CONOPS) will provide a collective understanding of how current and new capabilities can solve these emerging problems and will aid in the development of operational and system level requirements.
- C-UAS Mission Architectures will organize alternative approaches to achieving mission objectives through interactions between operational environment, threat, operational activities/tasks, and capabilities/ systems.
- Architecture Analysis will simulate the end-to-end mission; utilizing alternative approaches to obtain and document results to draw conclusions on the suitability of selected systems in satisfying mission metrics. The priority of this topic is the investigation of resilience and reliability issues and their impact on C-UAS effectiveness, and energy needs.
- Highlight of any findings from the analysis that would inform the development of Joint C-UAS Tactics, Techniques, and Procedures (TTPs). The priority of this topic is the overall improved interoperability and command and control across the effects chain.

D. CONOPS – C-UAS OPERATIONAL SCENARIOS

The CONOPS is described in detail in Appendix A, but a summary of the operational context is provided here to define the primary phases of C-UAS effects chain, identify the primary performers, and introduce the capability functions required to satisfy the effects chain. As depicted in Figure 7, there are two tiers of operational environments that C-UAS operational concept will need to address: defense of a *stationary asset* such as a base or airport that contains one or more operational Centers of Gravity (COG) from an adversary's point of view, and a *moving asset* that consists of a less than battalion size troop deployment with possible critical assets tasked to conduct patrol in support of mission objectives. For the stationary asset, the primary C-UAS challenge is providing defense over a wide area, and for the moving asset the primary C-UAS challenge is having limited capabilities to defend against attack. In both operational environments, the C-UAS operational concept will employ defense-in-depth (DiD) strategies to leverage multiple layers of defense in a dynamic threat landscape.

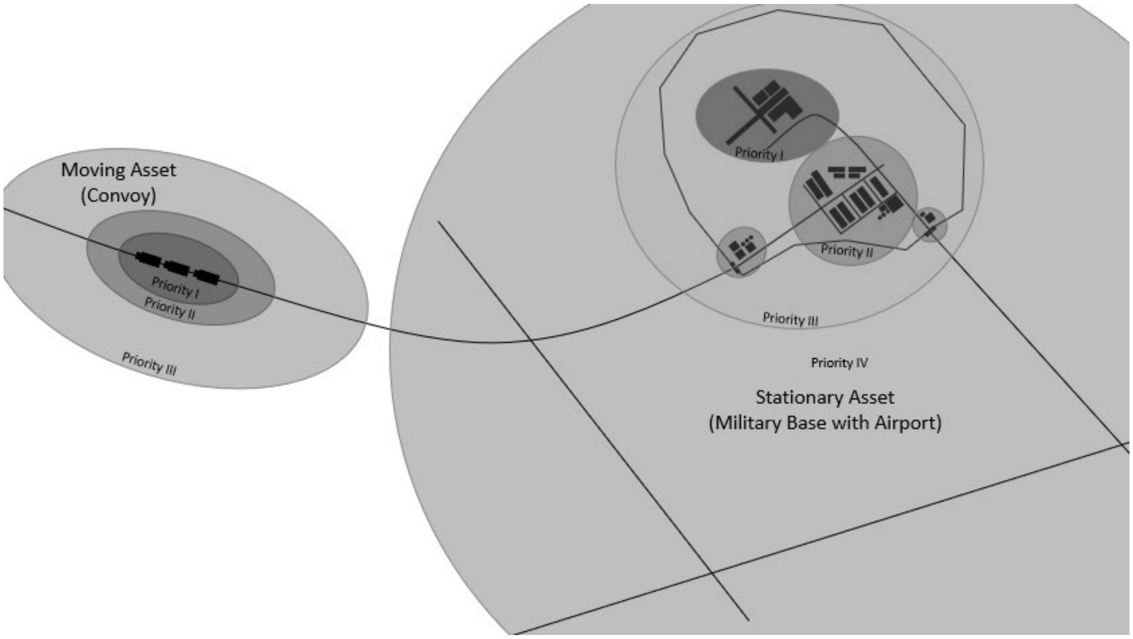


Figure 7. C-UAS Operational Environments

For each operational scenario captured in the CONOPS, the sUAS threat will attempt to close on the high value assets (Priority I) undetected from one or more axes. The goal of the C-UAS integrated system will be to thwart this attempt at far standoff distances from the high value assets (Priority IV or higher). It is useful to refer to Figure 8, which summarizes system suitability priorities as the sUAS threat progresses through the C-UAS defensive measures.

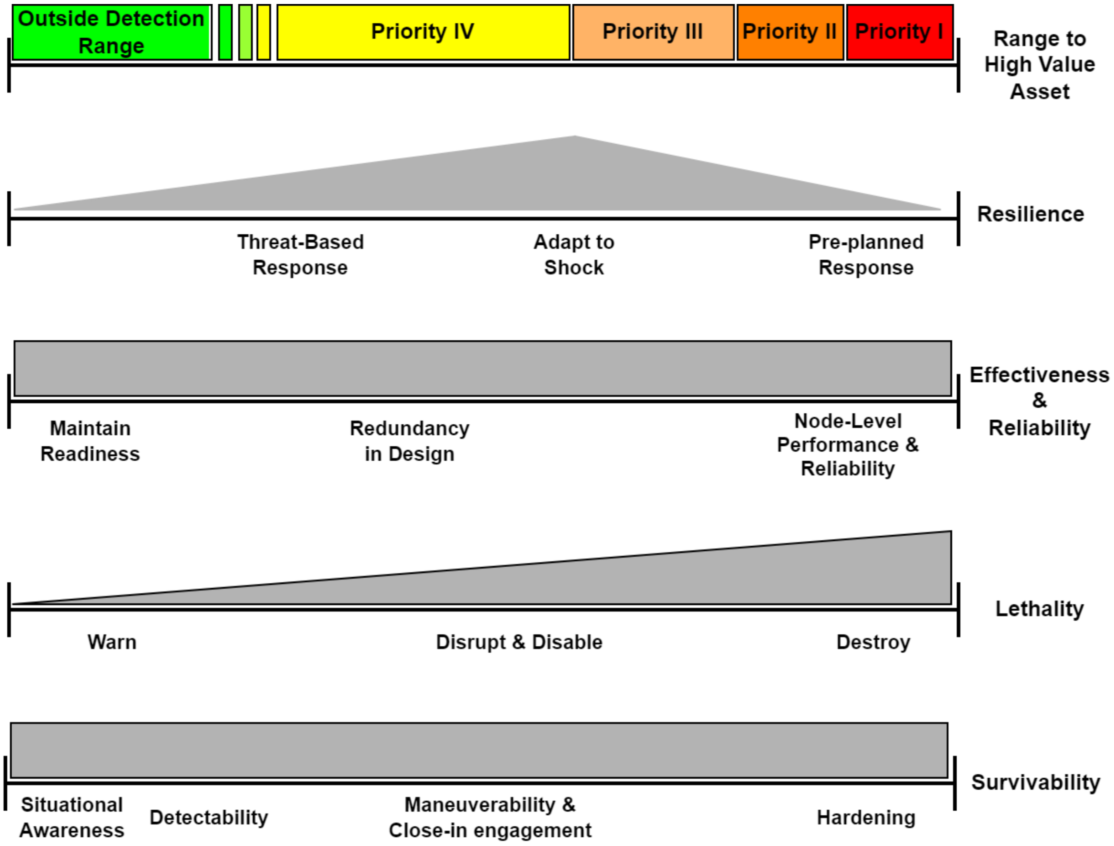


Figure 8. C-UAS Defense Profile and System Suitability Considerations

E. RESEARCH QUESTIONS

As previously mentioned in section C of this chapter, two of the major deliverables for this project include mission architectures and architecture analysis of mission engineering threads within the mission architecture. As described in the DOD Mission Engineering (ME) Guide (DD ENG 2020, 17), ME analysis evaluates missions by examining the interaction between the operational environment, threat, activities/tasks, and capabilities/systems used in current (today) or future missions. The scenario provides the overall context to the ME analysis and can be derived from the Operations Concepts. The mission scenario and vignette should be carefully selected and refined to match the needs of the problem statement to ensure the analysis focuses on the questions and concerns of interest. Figure 9 (DD ENG 2020, 15) shows the interdependencies among the mission definition, scenario, vignette, and mission metrics.

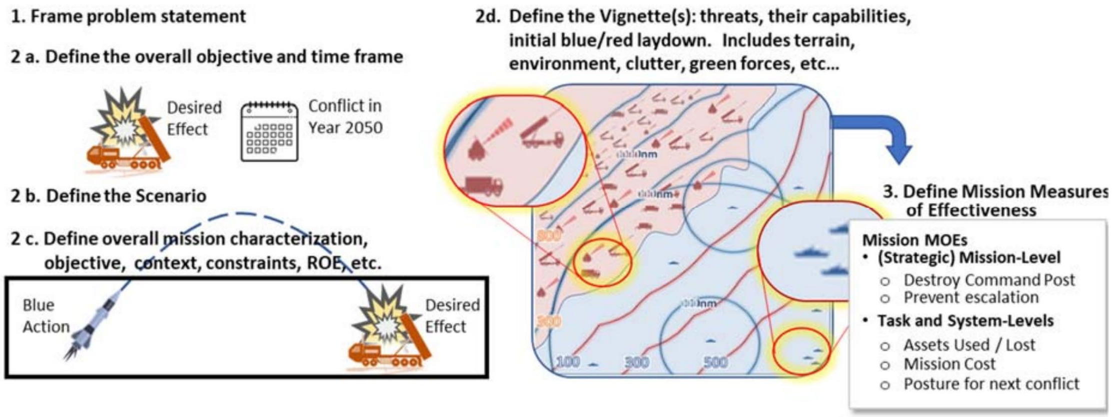

1. Frame problem statement
2 a. Define the overall objective and time frame
Desired Effect
Conflict in Year 2050
2 b. Define the Scenario
2 c. Define overall mission characterization, objective, context, constraints, ROE, etc.
Blue Action
Desired Effect
2d. Define the Vignette(s): threats, their capabilities, initial blue/red laydown. Includes terrain, environment, clutter, green forces, etc...
100
300
500
300
300
3. Define Mission Measures of Effectiveness
Mission MOEs
• (Strategic) Mission-Level
o Destroy Command Post
o Prevent escalation
• Task and System-Levels
o Assets Used / Lost
o Mission Cost
o Posture for next conflict

Figure 9. Mission Engineering Definition Elements. Source: DD ENG (2020).

DOD Mission Engineering (ME) Guide also asserts that:

> Metrics are measures of quantitative assessment commonly used for assessing, comparing, and tracking performance of the mission or system. Measurable outputs help commanders determine what is or is not working and lend insights into how to better accomplish the mission (2020).

Team DROSERA needs to identify a well-established set of metrics that can be used to evaluate the completeness and efficacy of the components of mission-enabling activities. The mission metrics represent the criteria that will be used to evaluate each of the alternative approaches in conducting the mission. The analysis in this project relies on two broad categories of measures: Measures of Effectiveness (MOE) to indicate a measurable attribute and target value for success within the overall mission; and Measures of Performance (MOP) to indicate performance characteristics of individual systems used to carry out the mission.

Team DROSERA has concluded that answering the following questions will result in project success:

Q1: What are the performance measures of the mission?

Q2: Which technology or capabilities are to be evaluated?

Q3: What are the mission capability gaps?

Q4: What is the optimal force mix for maximizing mission effectiveness and energy efficiency with reliability and resilience as the variables?

Q5: What models are required to conduct the analysis?

Q6: What models are already accessible? Do the required models already exist?

F. REQUIREMENTS ANALYSIS

C-UAS capability requirements will continue to be refined as part of the requirements definition phase of the project. Figure 10 depicts traceability between high-level C-UAS capability areas and C-UAS system functional areas.

After conducting rigorous academic research, Team DROSERA was unable to identify an Initial Capabilities Document for C-UAS, which would quantify the needed requirements and gaps associated with this capability. Thus, the team will develop capability requirements-based C-UAS Capability Assessment documented in Chapter II, Section A. C-UAS capability requirements form the basis for the C-UAS capability taxonomy. Next, the Universal Naval Task List (Chief of Naval Operations 2007) will be leveraged to identify operational activities that best align with the C-UAS capability taxonomy. We can then decompose these operational activities to provide the generalized system functions based on existing and planned C-UAS technologies. These system functions represent the type of system desired without specifying a particular system. Lastly, the system resource requirements can be defined. The focus of this project is system assessment as opposed to system design; therefore, system requirements definition is considered to be beyond the scope of this project.

It is important to note that operational tasks must be performed in accordance standards based on mission effectiveness requirements (JCS 1995). A standard consists of two parameters: a *measure* and a *criterion*. Measures provide a basis for describing various levels of performance and criterion defines acceptable levels of task performance (JCS 1995, 28–29). The DROSERA project will strive to identify define task measures that align with C-UAS mission effectiveness that can be assessed objectively. It is assessed that establishing criterion for these measures require significant stakeholder involvement and are deemed outside the scope of this project.

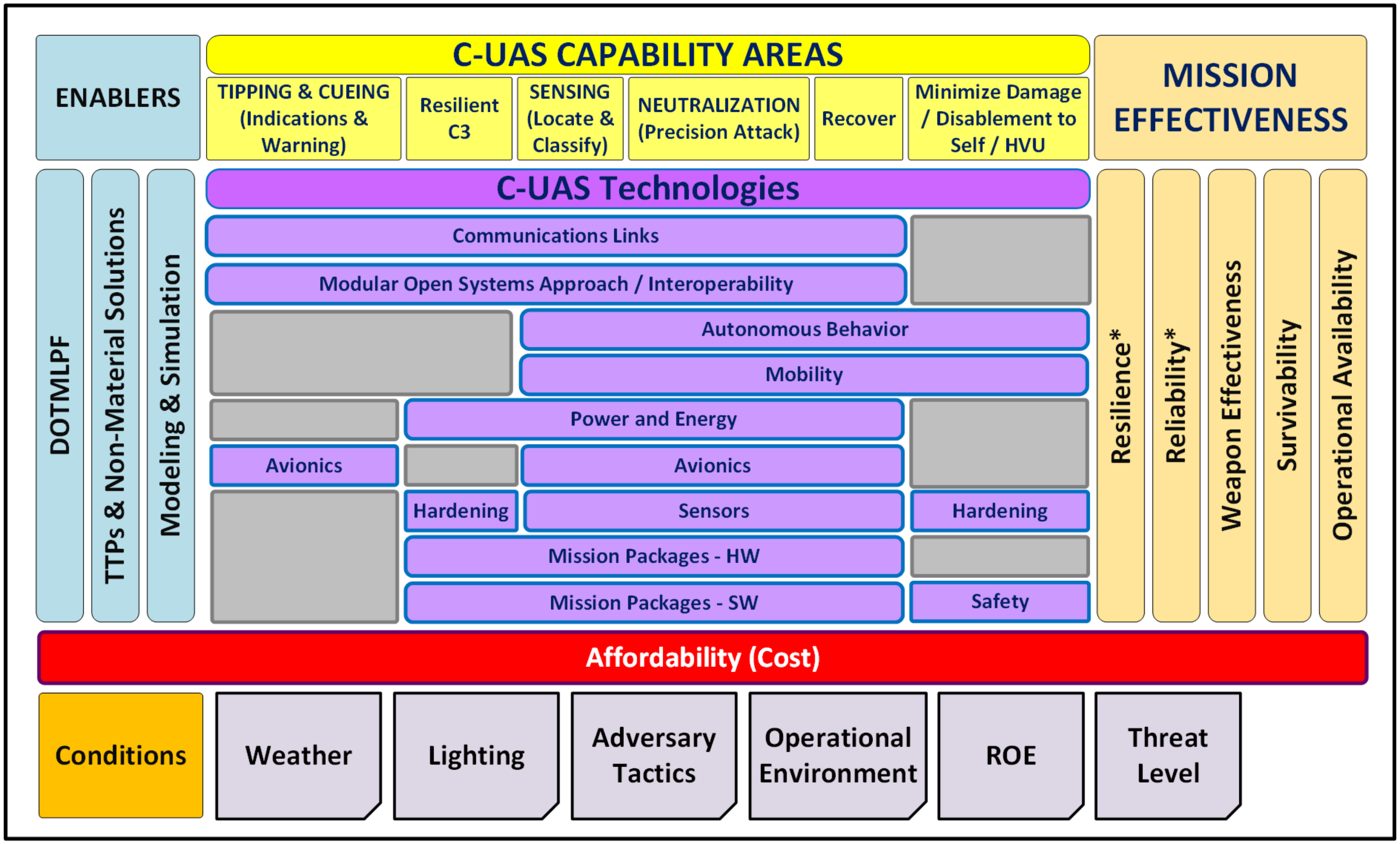


Figure 10. C-UAS Capability Framework

G. PROJECT SCOPE

As detailed in section C of this chapter, the project scope of this capstone is to develop a C-UAS CONOPS and a mission architecture that can model and simulate operational scenarios that emulate scenarios emphasized in the CONOPS. The mission models within the architecture must be capable of characterizing the behavior of a wide range of roles, platforms, and systems required to provide capability through the accomplishment of mission tasks. Analysis of these scenarios should draw conclusions about the suitability of the selected systems with specific focus on cyber-attack resilience, reliability and their impact on C-UAS effectiveness and energy needs. Furthermore, any findings from operational analysis that seem beneficial to countering hostile drone attacks will be highlighted and recommended for consideration in future TTP development. The analysis will utilize the skillsets of five NPS students with emphasis on application of information and tools provided by the NPS MSSE curriculum. The audience for this capstone includes DASN - Operational Energy, Joint Warfighters, NPS and various Naval research commands.

1. Project Limitations

The following constraints restrict the scope of the project:

- Stakeholder analysis is limited to NPS staff and advisors, review of DOD, Joint, and Naval doctrine, and research from the NPS or other publicly searchable databases.
- The period of performance for this capstone is limited to the NPS SE 320X (Engineering System Conceptualization, Implementation, & Operation) course timeline.
- Scenarios identified in the C-UAS CONOPS will be implemented and analyzed as needed to demonstrate proof of concept, identify impacts on mission effectiveness and system performance, and provide recommendations on system configurations and TTP development.
- Available documentation provided by NPS staff and advisors is limited to an unclassified level.

- Software is limited to NPS provided software for architecture development, modeling, and statistical analysis.
- Test capabilities are limited to utilizing known unclassified C-UAS capabilities.

2. Project Assumptions

The following assumptions apply to the project:

- System modeling is sufficient analysis of the system architecture.
- Assumptions and constraints made about the scenario that set the initial conditions and mission context (e.g., operational, task activities, resources, Order of Battle (OOB)) or about the performance characterization of the technologies, systems, or capabilities within the analysis will be identified in the mission architecture Summary and Overview information view (AV-1).
- This project will leverage the modeling efforts of NPS C-UAS researchers and other naval research partners if opportunities permit.
- Architecture for the resulting system of systems will be scalable to fit the theater mission as needed.

H. SUMMARY OF CHAPTER II

The purpose of this chapter is to define the SoS architecture for analysis and determining the effective need. The statement of need, the analysis of the current capabilities, and the stakeholder analysis enabled a clear scope for the problem statement. The information gathered in the analysis supports the determining of the necessary capability requirements, operational tasks, system requirements, mission/system performance measures, and the supporting architecture, with focused emphasis on cyber-attack resilience, reliability and their impact on C-UAS effectiveness and energy needs.

III. OPERATIONAL ANALYSIS

This chapter, Operational Analysis, focuses on the development of operational scenarios and vignettes to define the System of Systems (SoS) concept, normal and abnormal operating conditions, and required system capabilities for this project. Operational analysis is the first of many steps in developing an effective and accurate SoS architecture. The appropriate definition of operational architecture provides a description of the tasks, information exchanges, operational elements, and other entities required to accomplish the mission. This allows for the development of a resource architecture, which serves to implement the operational architecture and satisfy the mission goals.

A. CONCEPT OF OPERATIONS

The C-UAS CONOPS was developed to describe the characteristics of a proposed C-UAS SoS from the perspective of entities developing and implementing C-UAS technologies, as well as adjacent end users. It will provide a collective understanding of how current and new capabilities can solve concerns pertaining to the emerging sUAS threat, especially regarding such topics as asymmetric warfare and defense-in-depth. Further information regarding the C-UAS CONOPS and associated topics are included in Appendix A.

B. MISSION DEFINITON AND CHARACTERIZATION

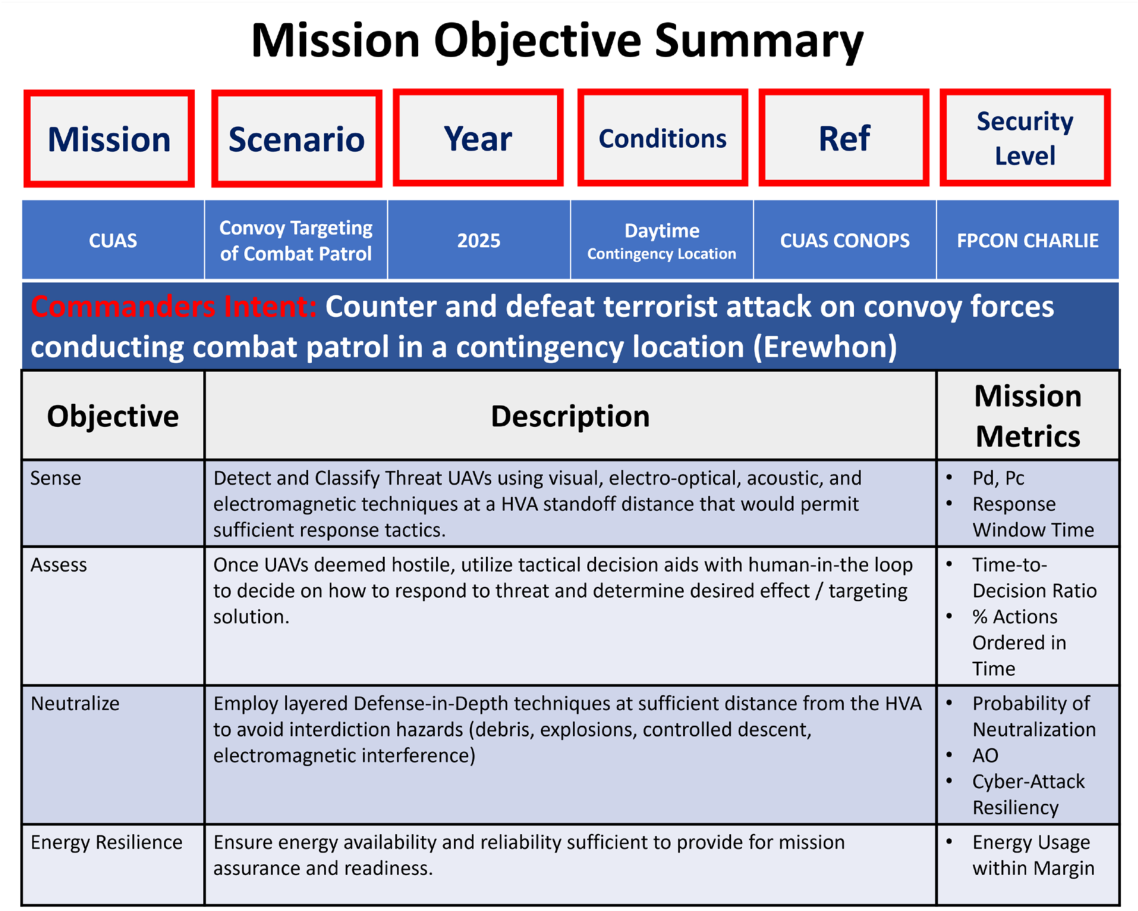
1. Capture and Analyze Commander's Intent

The mission definition and characterization provide the appropriate operational mission context and assumptions to be used as the input of the analysis of the problem to be investigated. Whereas the problem statement describes what we want to investigate, the mission definition and characterization describe both the entering conditions and boundaries such as the operational environment and the commander's desired intent or objectives for a particular mission (DD-ENG 2020, 6–11).

a. *Mission Definition Summary*

The mission definition summary forms the crux of the architecture executive summary and is outlined in Table 6. This table serves as an outline of the information and special considerations that may be necessary to scope the analysis or study.

Table 6. Mission Definition Summary.
Source: C-UAS for Convoy Targeting of Combat Patrol.



Mission Objective Summary

Mission	Scenario	Year	Conditions	Ref	Security Level
CUAS	Convoy Targeting of Combat Patrol	2025	Daytime Contingency Location	CUAS CONOPS	FPCON CHARLIE

Commanders Intent: Counter and defeat terrorist attack on convoy forces conducting combat patrol in a contingency location (Erewhon)

Objective	Description	Mission Metrics
Sense	Detect and Classify Threat UAVs using visual, electro-optical, acoustic, and electromagnetic techniques at a HVA standoff distance that would permit sufficient response tactics.	• Pd, Pc • Response Window Time
Assess	Once UAVs deemed hostile, utilize tactical decision aids with human-in-the loop to decide on how to respond to threat and determine desired effect / targeting solution.	• Time-to-Decision Ratio • % Actions Ordered in Time
Neutralize	Employ layered Defense-in-Depth techniques at sufficient distance from the HVA to avoid interdiction hazards (debris, explosions, controlled descent, electromagnetic interference)	• Probability of Neutralization • AO • Cyber-Attack Resiliency
Energy Resilience	Ensure energy availability and reliability sufficient to provide for mission assurance and readiness.	• Energy Usage within Margin

b. *Force Laydown*

The force laydown includes blue capabilities and red threats within the operational environment for the mission scenario and is captured in Figure 11. It is worthwhile to note that while this mission definitions utilizes a land-based combat patrol as the operational center of gravity, the C-UAS mission definition could easily be applied to an operational scenario involving maritime forces. Figure 12 depicts blue forces operating in a maritime environment that could be engaged by sUAS threats afloat or ashore.

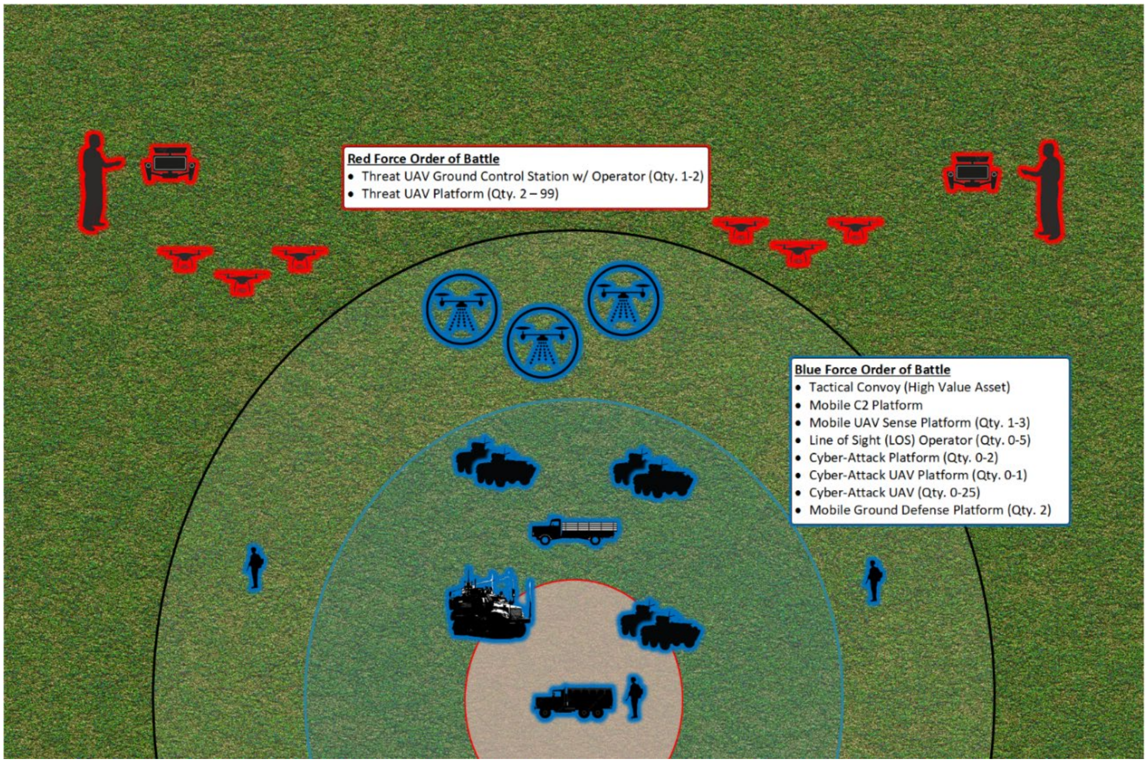

Red Force Order of Battle
• Threat UAV Ground Control Station w/ Operator (Qty. 1-2)
• Threat UAV Platform (Qty. 2 – 99)
Blue Force Order of Battle
• Tactical Convoy (High Value Asset)
• Mobile C2 Platform
• Mobile UAV Sense Platform (Qty. 1-3)
• Line of Sight (LOS) Operator (Qty. 0-5)
• Cyber-Attack Platform (Qty. 0-2)
• Cyber-Attack UAV Platform (Qty. 0-1)
• Cyber-Attack UAV (Qty. 0-25)
• Mobile Ground Defense Platform (Qty. 2)

Figure 11. C-UAS for Convoy Targeting of Combat Patrol Force Laydown

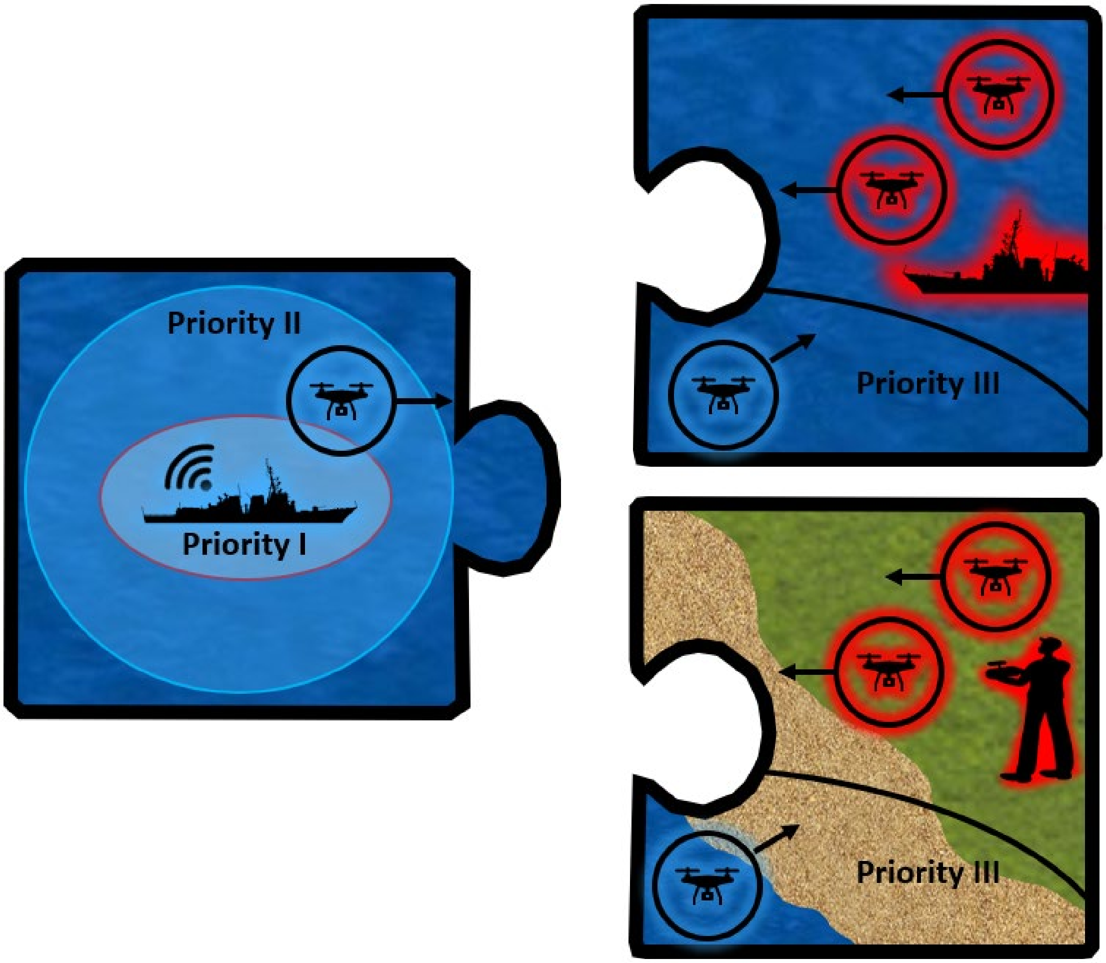


Figure 12. C-UAS for Maritime Operations Force Laydown

c. *Assumptions and Constraints*

The assumed or derived environmental conditions and resource or force limitations are stressors to the context of the mission or of specific interest by stakeholders. Assumptions reflect what is believed to be true about the problem domain and help to set boundaries on the mission analysis context. Constraints add complexity to the solution domain but represent things we know to be true that will have to be accounted for when conducting sensitivity (what-if) analysis. For the purpose of this mission definition, the following assumptions and constraints are given:

Assumptions:

1. Blue/red force strength is not reinforced during a scenario
2. Blue forces will have unlimited resources needed to sustain engagements
3. Environmental conditions will not vary over the course of a scenario
4. Outside of C-UAS Mission, blue forces will maintain mission superiority and be unchallenged in all warfare areas.

Constraints, Environment Specific:

- location of asset(s)
- type of asset(s)

Constraints, C-UAS Specific:

- number of deployed C-UAS system(s)
- location of C-UAS system(s)
- individual generic capability type of C-UAS system
- individual performance characteristics of C-UAS system

Constraints, sUAS Specific:

- number of sUAS squad(s) for red forces
- location of sUAS squad(s) for red forces
- number of individual threat sUAS deployed at specific squad location(s)
- individual sUAS squad mission capability
- individual sUAS mission goal

C. DEVELOP OPERATIONAL ARCHITECTURE

The Operational Architecture provides a description of the tasks, operational elements, and information flows required to accomplish or support a warfighting function. The DOD CIO recommends the usage of Operational Viewpoints (OV) to re-use the capabilities defined in Capability Viewpoints subsequently putting them in the context of an operation or scenario (DOD CIO n.d., Operational Viewpoint). The use of these operational models enhances stakeholder engagement to tie user requirements to strategic-level capability needs, identify the specific items to be delivered by the capability and provide a basis for test scenarios linked to user requirements. All OVs described in this section are contained in the C-UAS Mission Model Innoslate and archived as supplemental information.

1. C-UAS Meta Model

The C-UAS Meta Model defines the high-level data constructs of critical interest to the C-UAS enterprise architecture (EA) from which architectural descriptions are created in non-technical terms, so individuals at all levels can understand the data elements and relationships of the architectural description. It conforms with the DoDAF Meta Model construct but utilizes elements and relationships as defined in the Life cycle Modeling Language (LML) specification (Life Cycle Modeling Language [LML] 2015). The primary purpose of the C-UAS Meta Model is to:

a. ***Establish and define the constrained vocabulary for description and discourse about C-UAS model.***

b. ***Specify the semantics (i.e., understanding) and format for data exchange between architecture development and analysis tools within and across architectural descriptions.***

The C-UAS Meta Model is depicted in Figure 13.

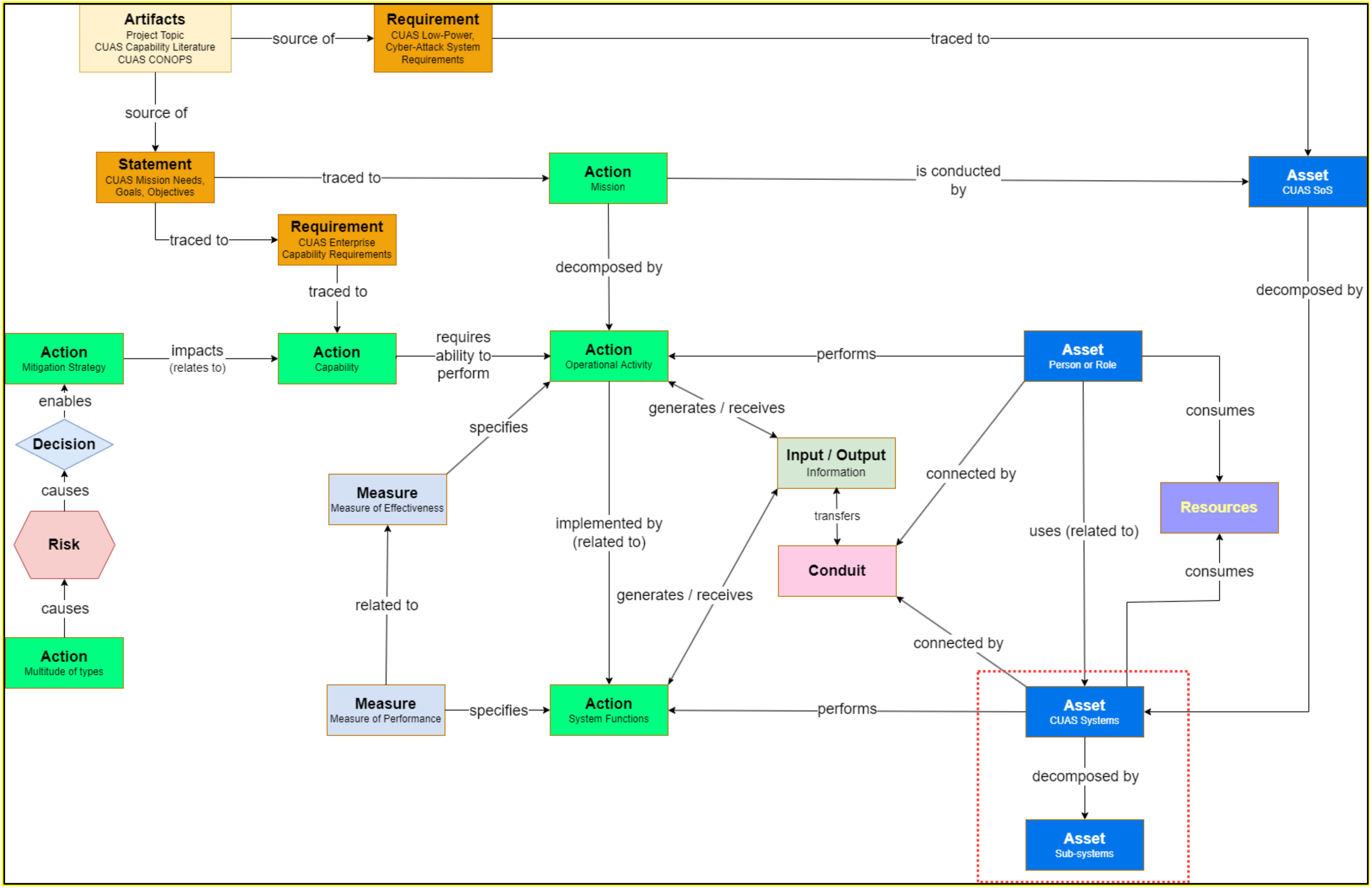


Figure 13. C-UAS Meta Model

2. Capability Taxonomy

Figure 14 captures the C-UAS capability taxonomy (CV-2). The model presents a hierarchy of capabilities summarized in the previous chapter (C-UAS Capability Assessment).

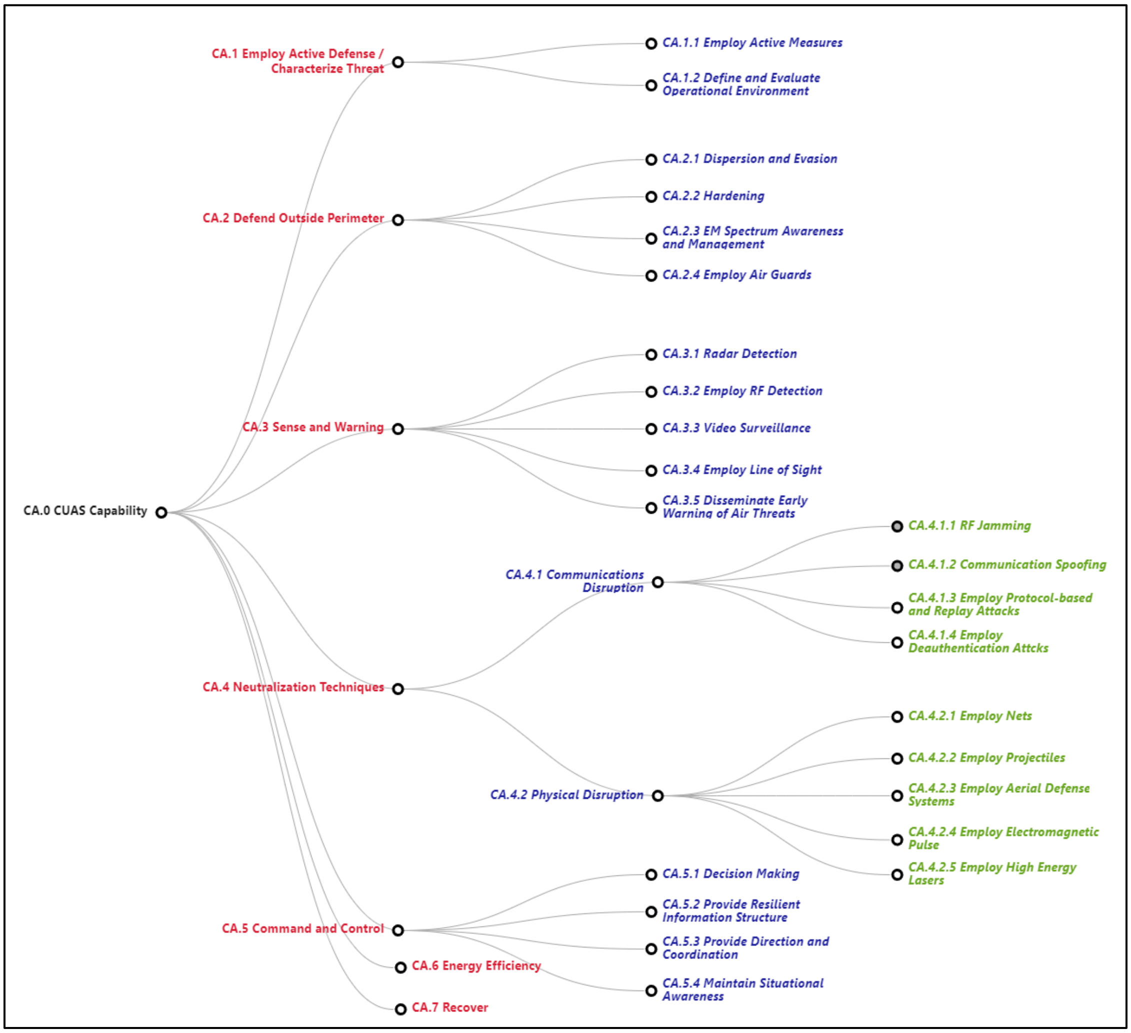

CA.0 CUAS Capability
CA.1 Employ Active Defense / Characterize Threat
CA.1.1 Employ Active Measures
CA.1.2 Define and Evaluate Operational Environment
CA.2 Defend Outside Perimeter
CA.2.1 Dispersion and Evasion
CA.2.2 Hardening
CA.2.3 EM Spectrum Awareness and Management
CA.2.4 Employ Air Guards
CA.3 Sense and Warning
CA.3.1 Radar Detection
CA.3.2 Employ RF Detection
CA.3.3 Video Surveillance
CA.3.4 Employ Line of Sight
CA.3.5 Disseminate Early Warning of Air Threats
CA.4 Neutralization Techniques
CA.4.1 Communications Disruption
CA.4.1.1 RF Jamming
CA.4.1.2 Communication Spoofing
CA.4.1.3 Employ Protocol-based and Replay Attacks
CA.4.1.4 Employ Deauthentication Attcks
CA.4.2 Physical Disruption
CA.4.2.1 Employ Nets
CA.4.2.2 Employ Projectiles
CA.4.2.3 Employ Aerial Defense Systems
CA.4.2.4 Employ Electromagnetic Pulse
CA.4.2.5 Employ High Energy Lasers
CA.5 Command and Control
CA.5.1 Decision Making
CA.5.2 Provide Resilient Information Structure
CA.5.3 Provide Direction and Coordination
CA.5.4 Maintain Situational Awareness
CA.6 Energy Efficiency
CA.7 Recover

Figure 14. C-UAS Capability Taxonomy (CV-2)

3. Operational Context Diagram (Logical)

Although the Operational Concept Diagram for C-UAS Combat Patrol mission was introduced in the C-UAS CONOPS, a logical OV-1 is required to instantiate conduits between the operational performers in the C-UAS mission context. This is shown in Figure 15.

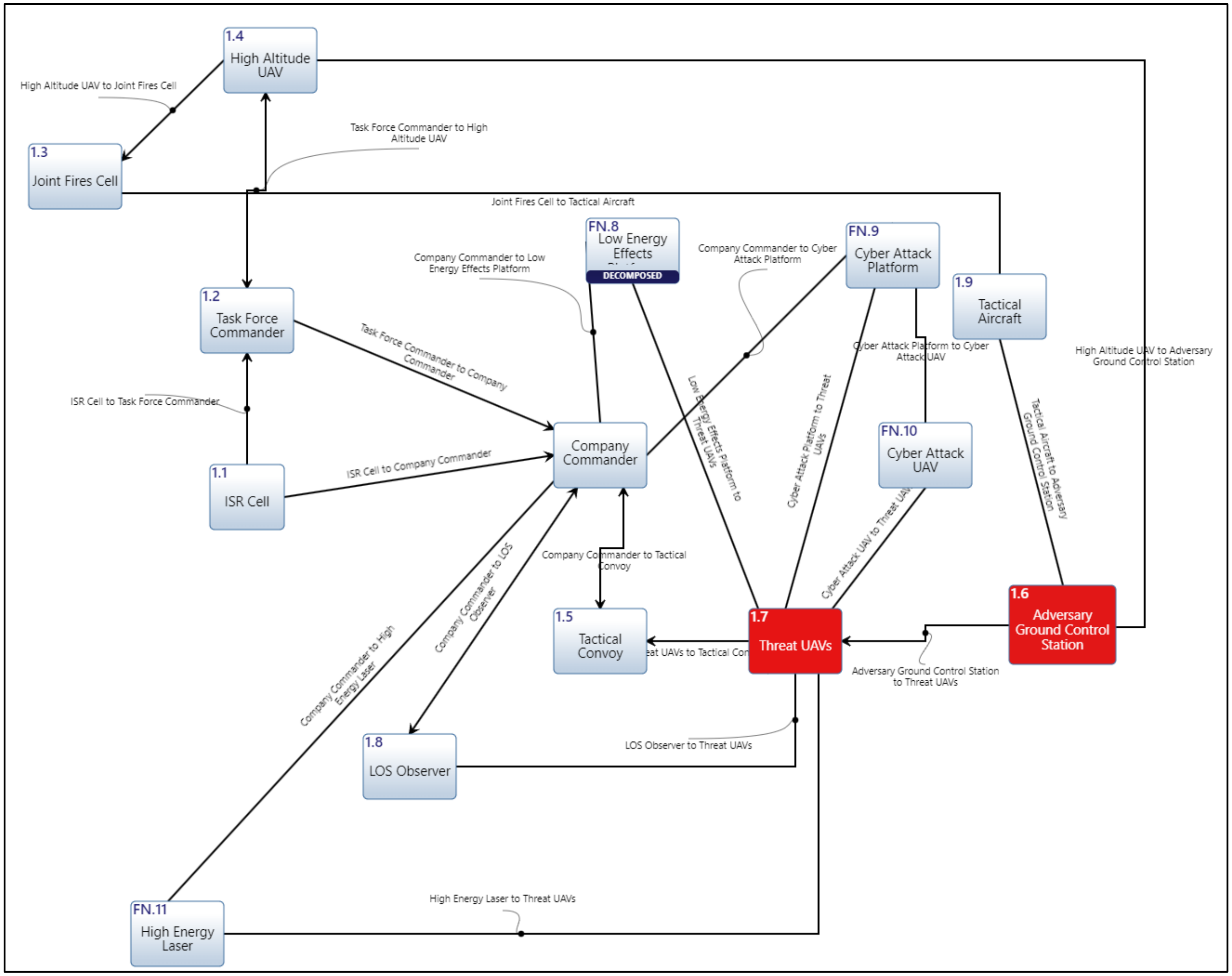

1.4
High Altitude UAV
High Altitude UAV to Joint Fires Cell
1.3
Joint Fires Cell
Task Force Commander to High Altitude UAV
Joint Fires Cell to Tactical Aircraft
FN.8
Low Energy Effects
DECOMPOSED
Company Commander to Low Energy Effects Platform
Company Commander to Cyber Attack Platform
FN.9
Cyber Attack Platform
1.9
Tactical Aircraft
1.2
Task Force Commander
Task Force Commander to Company Commander
Cyber Attack Platform to Cyber Attack UAV
High Altitude UAV to Adversary Ground Control Station
Low Energy Effects Platform to Threat UAVs
Cyber Attack Platform to Threat UAVs
Tactical Aircraft to Adversary Ground Control Station
ISR Cell to Task Force Commander
Company Commander
FN.10
Cyber Attack UAV
1.1
ISR Cell
ISR Cell to Company Commander
Cyber Attack UAV to Threat UAVs
Company Commander to Tactical Convoy
Company Commander to LOS Observer
1.6
Adversary Ground Control Station
1.5
Tactical Convoy
eat UAVs to Tactical Con
1.7
Threat UAVs
Adversary Ground Control Station to Threat UAVs
Company Commander to High Energy Laser
1.8
LOS Observer
LOS Observer to Threat UAVs
High Energy Laser to Threat UAVs
FN.11
High Energy Laser

Figure 15. C-UAS Operational Context Diagram (Logical)

4. Functional Behavior

In this step, we apply system engineering techniques to transform the mission scenario into an integrated functional behavior model. First, the Universal Naval Task List (UNTL) was imported as a library to identify operational activities suitable for achieving C-UAS capabilities. The UNTL contains a hierarchical listing of the tasks that can be performed by a naval force, describes the environment that can affect the performance of a given task, and provides measures of performance that can be applied by a commander to set a standard of expected performance (Chief of Naval Operations [CNO] 2007, 1–1). Next, the UNTL was reviewed for applicability to the C-UAS mission context. Candidates that met these criteria were copied and converted into C-UAS Operational Activities.

Now, with the developed mission specific tasks a description of mission functional behavior is required. This will be constructed and written to address all levels and outline what is required for the C-UAS SoS. The DoDAF Event-Trace Description (OV-6c) is the preferred means of moving from the initial operational concept (OV-1) to the next level of detail (DOD CIO n.d.; Event-Trace Description). It is a behavioral model that enables the tracing of actions in the mission scenario and provides the best format for stakeholder engagement and concurrence. Each step in the event sequence captures information transferred between two performers in the scenario, with the generation and receipt of this information achieved with the accomplishment of a task (operational activity). The Event-Trace Description for the C-UAS Combat Patrol Mission is depicted in Figure 16 (partial).

For the next process, each information element instantiated in the OV-6c was mapped to (*transferred by* relationship) an Operational Exchange between two operational performers in the logical OV-1, including the allocation of generating and receiving operational activities for each performer. The result of this mapping is the Operational Resource Flow Description (OV-2) and Matrix (OV-3), shown in Figure 17 and Table 7 (partial) respectively.

Following this, the Operational Activity Diagram (OV-5b) was constructed (Figure 18). The OV-5b focuses on the flow of the tasks (activities) executed by the individual operational performer, rather than the interactions between each performer. This viewpoint is useful as a system development input (DOD CIO n.d.; Operational Activity Diagram).

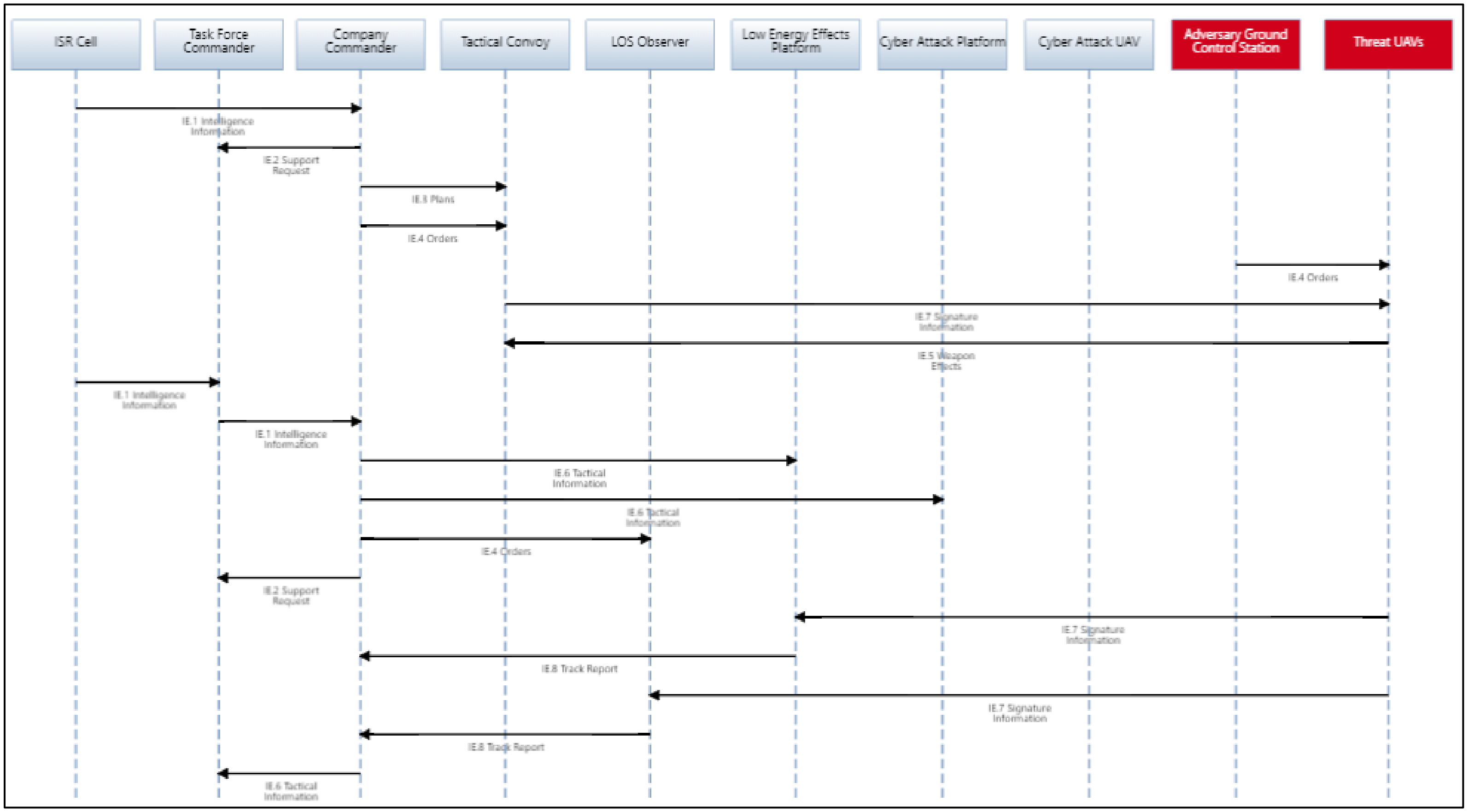

ISR Cell
Task Force Commander
Company Commander
Tactical Convoy
LOS Observer
Low Energy Effects Platform
Cyber Attack Platform
Cyber Attack UAV
Adversary Ground Control Station
Threat UAVs
IE.1 Intelligence Information
IE.2 Support Request
IE.3 Plans
IE.4 Orders
IE.4 Orders
IE.7 Signature Information
IE.5 Weapon Effects
IE.1 Intelligence Information
IE.1 Intelligence Information
IE.6 Tactical Information
IE.6 Tactical Information
IE.4 Orders
IE.2 Support Request
IE.7 Signature Information
IE.8 Track Report
IE.7 Signature Information
IE.8 Track Report
IE.6 Tactical Information

Figure 16. C-UAS Combat Patrol Event-Trace Description (Part 1)

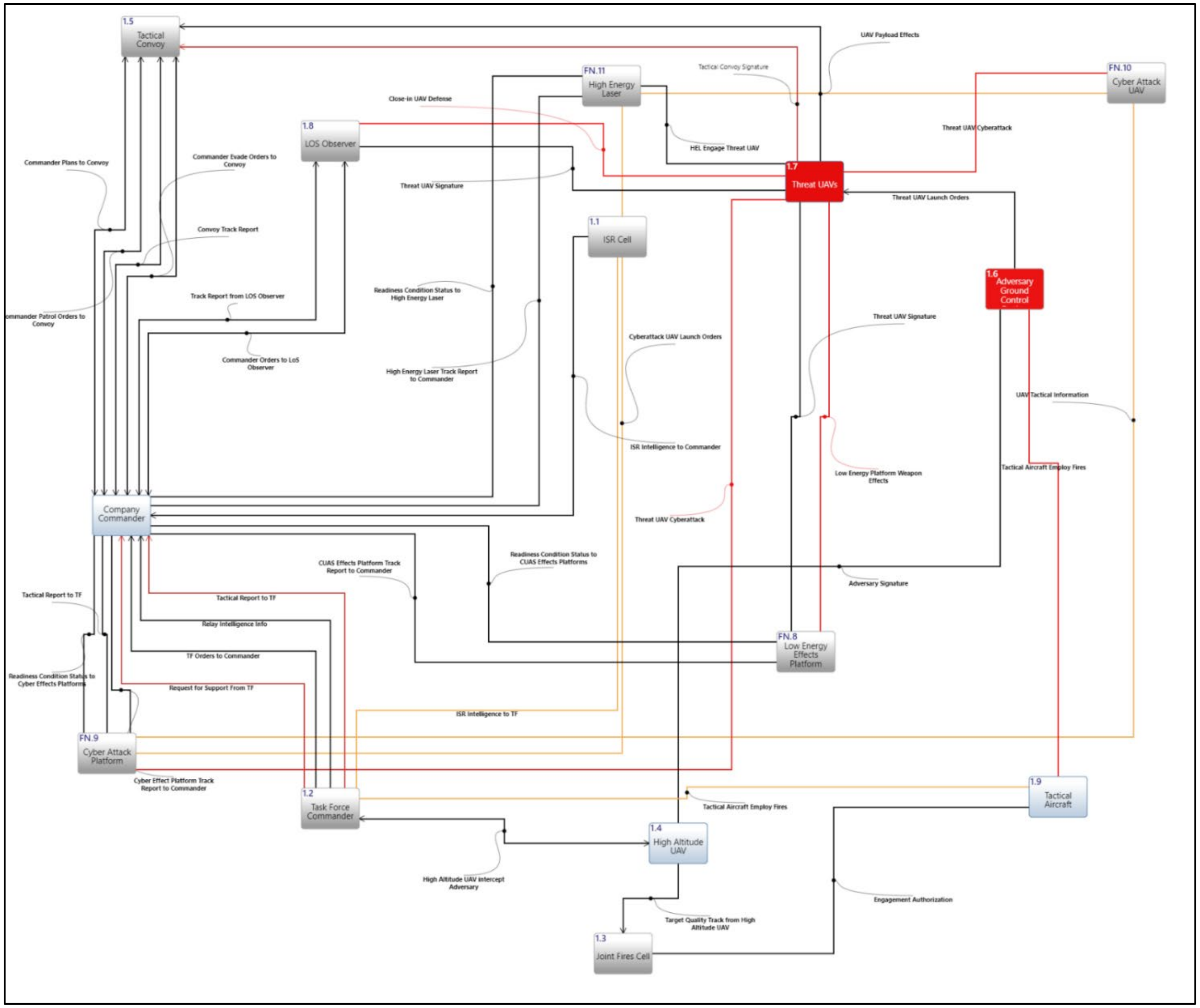

1.5
Tactical Convoy
FN.11
High Energy Laser
FN.10
Cyber Attack UAV
1.8
LOS Observer
1.7
Threat UAVs
1.1
ISR Cell
1.6
Adversary Ground Control
Company Commander
FN.8
Low Energy Effects Platform
FN.9
Cyber Attack Platform
1.2
Task Force Commander
1.9
Tactical Aircraft
1.4
High Altitude UAV
1.3
Joint Fires Cell
UAV Payload Effects
Tactical Convoy Signature
Close-in UAV Defense
Threat UAV Cyberattack
HEL Engage Threat UAV
Commander Plans to Convoy
Commander Evade Orders to Convoy
Threat UAV Signature
Threat UAV Launch Orders
Convoy Track Report
Track Report from LOS Observer
ommander Patrol Orders to Convoy
Readiness Condition Status to High Energy Laser
Commander Orders to LoS Observer
High Energy Laser Track Report to Commander
Threat UAV Signature
Cyberattack UAV Launch Orders
UAV Tactical Information
ISR Intelligence to Commander
Low Energy Platform Weapon Effects
Tactical Aircraft Employ Fires
Threat UAV Cyberattack
Readiness Condition Status to CUAS Effects Platforms
CUAS Effects Platform Track Report to Commander
Adversary Signature
Tactical Report to TF
Tactical Report to TF
Relay Intelligence Info
TF Orders to Commander
Readiness Condition Status to Cyber Effects Platforms
Request for Support From TF
ISR Intelligence to TF
Cyber Effect Platform Track Report to Commander
Tactical Aircraft Employ Fires
High Altitude UAV intercept Adversary
Engagement Authorization
Target Quality Track from High Altitude UAV

Figure 17. C-UAS Combat Patrol Operational Resource Flow Diagram (OV-2)

Table 7. C-UAS Combat Patrol Operational Resource Flow Matrix (OV-3) (Excerpt)

Source Entity Attributes	Transfers				Generated by		Performed by		Received by		Performed by	
Entity	Number	Name	Size	Units	Number	Name	Number	Name	Number	Name	Number	Name
OE1 - ISR Cell to Task Force Commander		ISR Intelligence to TF	0		A.11	Provide Updated Intelligence	1.1	ISR Cell	A.12	Relay Updated Intelligence	1.2	Task Force Commander
OE10 - High Energy Laser to Threat UAVs		HEL Engage Threat UAV	0		A.23	Conduct HEL Electronic Attack	FN.11	High Energy Laser	A.10	Close Blue Forces	1.7	Threat UAVs
OE11 - Adversary Ground Control Station to Threat UAVs		Threat UAV Launch Orders	0		A.9	Launch UAVs	1.6	Adversary Ground Control Station	A.10	Close Blue Forces	1.7	Threat UAVs
OE12 - Company Commander to LOS Observer		Commander Orders to LoS Observer	0		A.17	Orders to LOS Observer		Company Commander	A.19	Conduct Foot Patrol	1.8	LOS Observer
		Track Report from LOS Observer	0		A.32	Transmit LOS Observer Track Report	1.8	LOS Observer	A.34	Acknowledge Track Report		Company Commander
OE13 - LOS Observer to Threat UAVs		Close-in UAV Defense	0		A.33	Neutralize with handheld Drone Defense	1.8	LOS Observer	A.10	Close Blue Forces	1.7	Threat UAVs
		Threat UAV Signature	0		A.10	Close Blue Forces	1.7	Threat UAVs	A.22	Detect UAVs	1.8	LOS Observer
					▨	▨	▨	▨	▨		FN.8	Low Energy Effects Platform
OE14 - Task Force Commander to High Altitude UAV		High Altitude UAV intercept Adversary	0		A.X	Direct Forces - Operational	1.2	Task Force Commander	A.27	Conduct Wide Area Surveillance and Close-In Air Support	1.4	High Altitude UAV

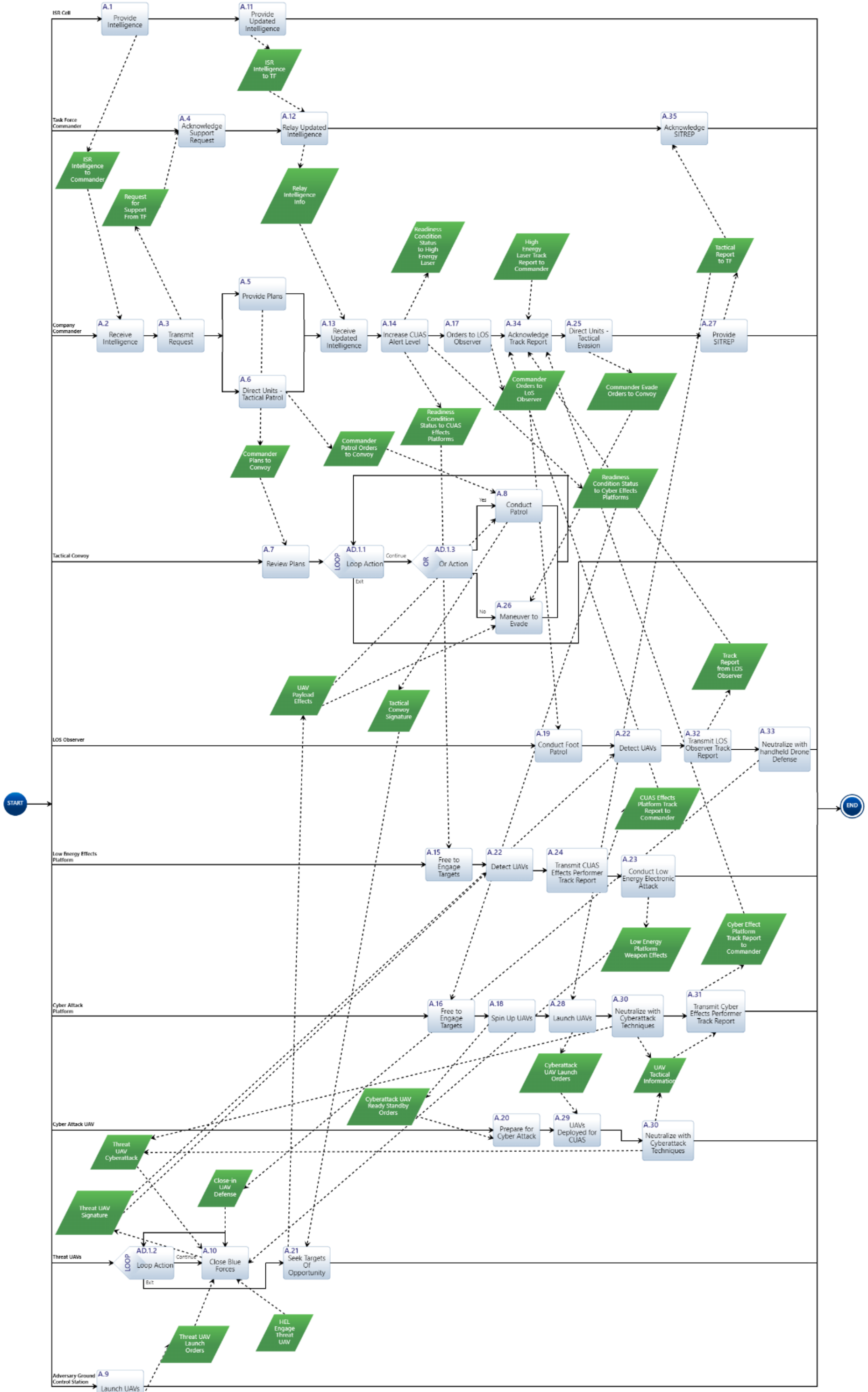

ISR Cell
A.1 Provide Intelligence
A.11 Provide Updated Intelligence
ISR Intelligence to TF
Task Force Commander
A.4 Acknowledge Support Request
A.12 Relay Updated Intelligence
A.35 Acknowledge SITREP
ISR Intelligence to Commander
Request for Support From TF
Relay Intelligence Info
Readiness Condition Status to High Energy Laser
High Energy Laser Track Report to Commander
Tactical Report to TF
Company Commander
A.2 Receive Intelligence
A.3 Transmit Request
A.5 Provide Plans
A.6 Direct Units - Tactical Patrol
A.13 Receive Updated Intelligence
A.14 Increase CUAS Alert Level
A.17 Orders to LOS Observer
A.34 Acknowledge Track Report
A.25 Direct Units - Tactical Evasion
A.27 Provide SITREP
Commander Orders to LoS Observer
Commander Evade Orders to Convoy
Readiness Condition Status to CUAS Effects Platforms
Commander Patrol Orders to Convoy
Commander Plans to Convoy
Readiness Condition Status to Cyber Effects Platforms
A.8 Conduct Patrol
Yes
Tactical Convoy
A.7 Review Plans
AD.1.1 LOOP Loop Action
Continue
Exit
AD.1.3 OR Or Action
No
A.26 Maneuver to Evade
Track Report from LOS Observer
UAV Payload Effects
Tactical Convoy Signature
LOS Observer
A.19 Conduct Foot Patrol
A.22 Detect UAVs
A.32 Transmit LOS Observer Track Report
A.33 Neutralize with handheld Drone Defense
START
END
CUAS Effects Platform Track Report to Commander
Low Energy Effects Platform
A.15 Free to Engage Targets
A.22 Detect UAVs
A.24 Transmit CUAS Effects Performer Track Report
A.23 Conduct Low Energy Electronic Attack
Low Energy Platform Weapon Effects
Cyber Effect Platform Track Report to Commander
Cyber Attack Platform
A.16 Free to Engage Targets
A.18 Spin Up UAVs
A.28 Launch UAVs
A.30 Neutralize with Cyberattack Techniques
A.31 Transmit Cyber Effects Performer Track Report
Cyberattack UAV Launch Orders
UAV Tactical Information
Cyberattack UAV Ready Standby Orders
Cyber Attack UAV
A.20 Prepare for Cyber Attack
A.29 UAVs Deployed for CUAS
A.30 Neutralize with Cyberattack Techniques
Threat UAV Cyberattack
Close-in UAV Defense
Threat UAV Signature
Threat UAVs
AD.1.2 LOOP Loop Action
Continue
Exit
A.10 Close Blue Forces
A.21 Seek Targets Of Opportunity
Threat UAV Launch Orders
HEL Engage Threat UAV
Adversary Ground Control Station
A.9 Launch UAVs

Figure 18. C-UAS Combat Patrol Operational Activity Model (OV-5b)

The Activity Decomposition Tree (OV-5a) shows activities depicted in a tree structure and is typically used to provide a navigation aid for the scope of tasks executed by an operational performer (DOD CIO n.d.; Operational Activity Decomposition Tree). Activity Decomposition Trees for the Company Commander and Low Energy Effects Platform are depicted in Figure 20 and Figure 20 respectively.

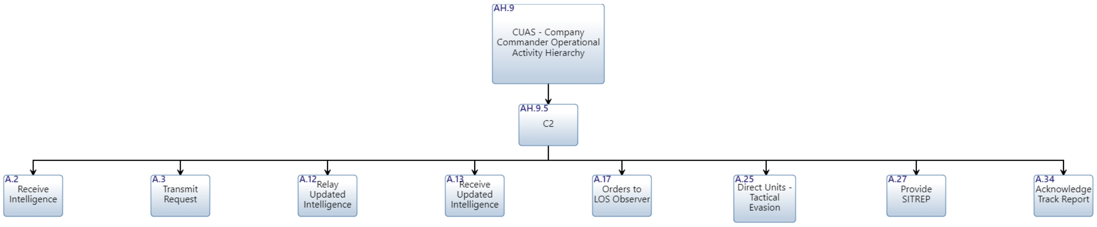

AH.9
CUAS - Company Commander Operational Activity Hierarchy
AH.9.5
C2
A.2
Receive Intelligence
A.3
Transmit Request
A.12
Relay Updated Intelligence
A.13
Receive Updated Intelligence
A.17
Orders to LOS Observer
A.25
Direct Units - Tactical Evasion
A.27
Provide SITREP
A.34
Acknowledge Track Report

Figure 19. C-UAS Company Commander Operational Activity Hierarchy

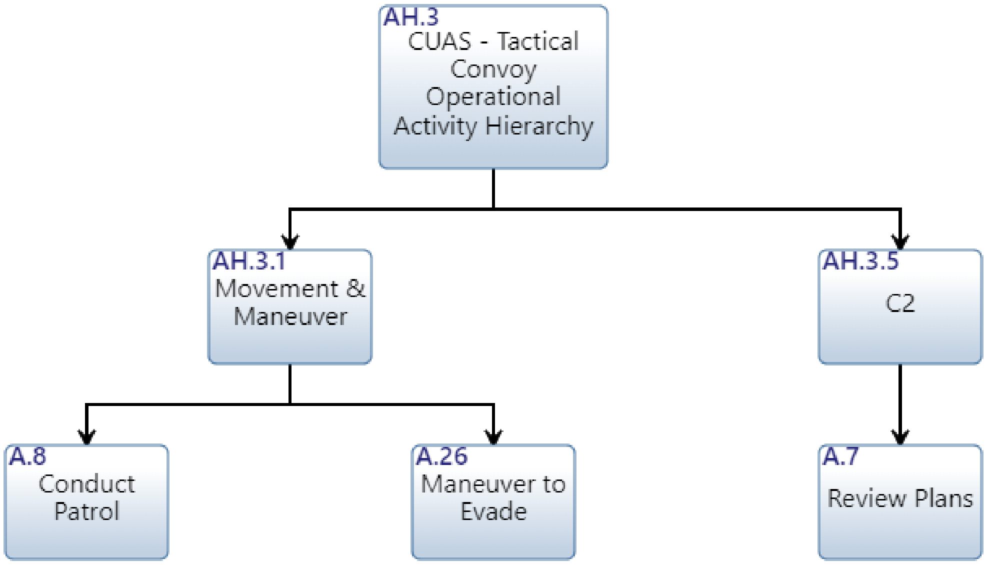
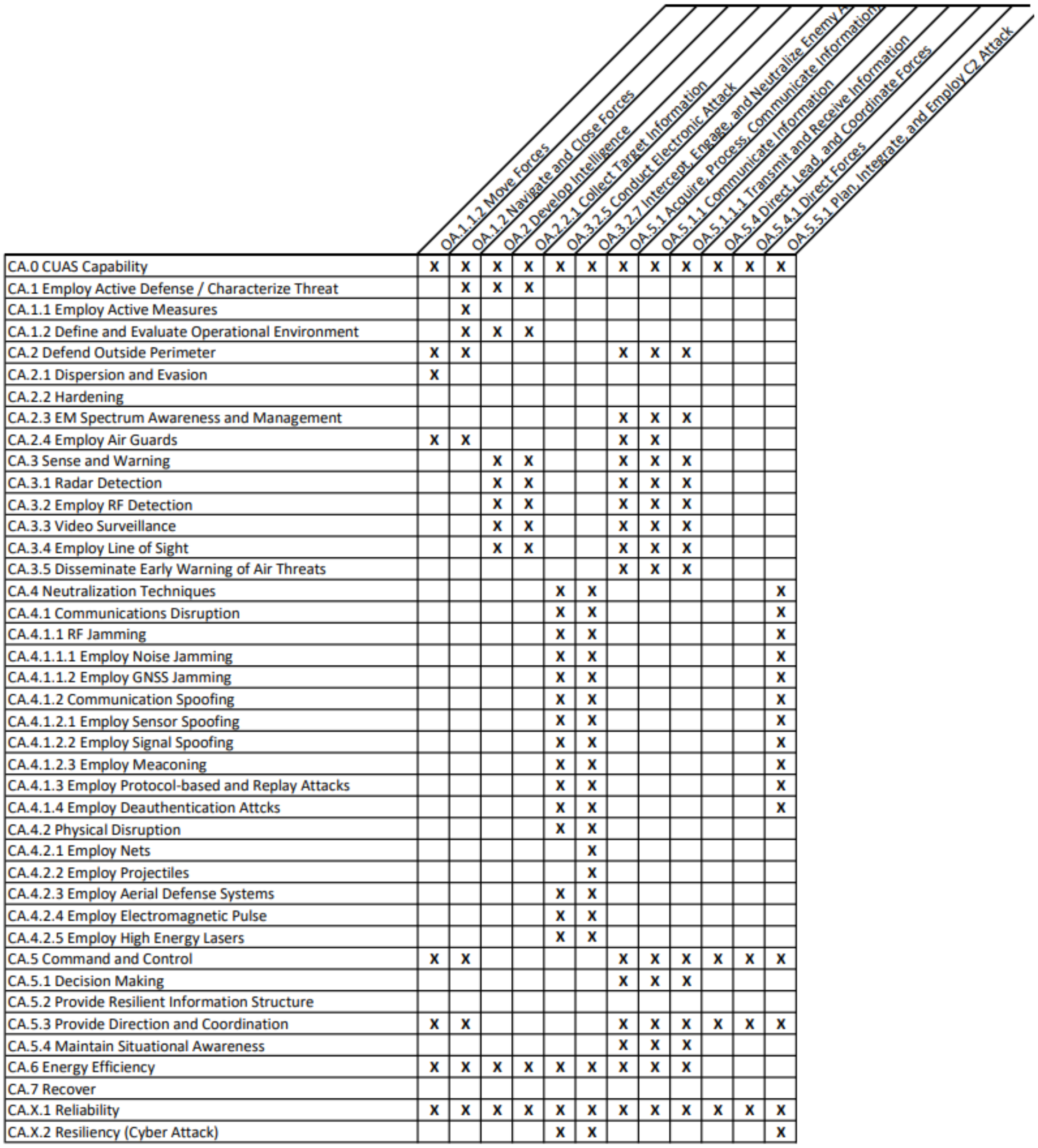


Figure 20. C-UAS Tactical Convoy Operational Activity Hierarchy

The activities described in the OV-5a are mapped to corresponding C-UAS Combat Patrol capabilities in the Capability to Operational Activities Mapping (CV-6). A cursory audit of the CV-6 (Figure 21) shows that the allocated operational tasks are sufficient achieve the capabilities desired for C-UAS Combat Control mission scenario.



	OA.1.1.2 Move Forces	OA.1.2 Navigate and Close Forces	OA.2 Develop Intelligence	OA.2.2.1 Collect Target Information	OA.3.2.5 Conduct Electronic Attack	OA.3.2.7 Intercept, Engage, and Neutralize Enemy A	OA.5.1 Acquire, Process, Communicate Information,	OA.5.1.1 Communicate Information	OA.5.1.1.1 Transmit and Receive Information	OA.5.4 Direct, Lead, and Coordinate Forces	OA.5.4.1 Direct Forces	OA.5.5.1 Plan, Integrate, and Employ C2 Attack
CA.0 CUAS Capability	X	X	X	X	X	X	X	X	X	X	X	X
CA.1 Employ Active Defense / Characterize Threat		X	X	X								
CA.1.1 Employ Active Measures		X										
CA.1.2 Define and Evaluate Operational Environment		X	X	X								
CA.2 Defend Outside Perimeter	X	X					X	X	X			
CA.2.1 Dispersion and Evasion	X											
CA.2.2 Hardening												
CA.2.3 EM Spectrum Awareness and Management							X	X	X			
CA.2.4 Employ Air Guards	X	X					X	X				
CA.3 Sense and Warning			X	X			X	X	X			
CA.3.1 Radar Detection			X	X			X	X	X			
CA.3.2 Employ RF Detection			X	X			X	X	X			
CA.3.3 Video Surveillance			X	X			X	X	X			
CA.3.4 Employ Line of Sight			X	X			X	X	X			
CA.3.5 Disseminate Early Warning of Air Threats							X	X	X			
CA.4 Neutralization Techniques					X	X						X
CA.4.1 Communications Disruption					X	X						X
CA.4.1.1 RF Jamming					X	X						X
CA.4.1.1.1 Employ Noise Jamming					X	X						X
CA.4.1.1.2 Employ GNSS Jamming					X	X						X
CA.4.1.2 Communication Spoofing					X	X						X
CA.4.1.2.1 Employ Sensor Spoofing					X	X						X
CA.4.1.2.2 Employ Signal Spoofing					X	X						X
CA.4.1.2.3 Employ Meaconing					X	X						X
CA.4.1.3 Employ Protocol-based and Replay Attacks					X	X						X
CA.4.1.4 Employ Deauthentication Attcks					X	X						X
CA.4.2 Physical Disruption					X	X						
CA.4.2.1 Employ Nets						X						
CA.4.2.2 Employ Projectiles						X						
CA.4.2.3 Employ Aerial Defense Systems					X	X						
CA.4.2.4 Employ Electromagnetic Pulse					X	X						
CA.4.2.5 Employ High Energy Lasers					X	X						
CA.5 Command and Control	X	X					X	X	X	X	X	X
CA.5.1 Decision Making							X	X	X			
CA.5.2 Provide Resilient Information Structure												
CA.5.3 Provide Direction and Coordination	X	X					X	X	X	X	X	X
CA.5.4 Maintain Situational Awareness							X	X	X			
CA.6 Energy Efficiency	X	X	X	X	X	X	X	X	X			
CA.7 Recover												
CA.X.1 Reliability	X	X	X	X	X	X	X	X	X	X	X	X
CA.X.2 Resiliency (Cyber Attack)					X	X						X

Figure 21. C-UAS Combat Patrol Capability to Operational Activities Mapping (CV-6)

D. VALUE SYSTEM DESIGN

Value systems design involves the establishment of system metrics related to the performance, effectiveness, cost, and other such quantitative factors required to meet customer expectations (Blanchard and Fabrycky 2011, 32). These quantitative factors are known as technical measures and are used to provide the stakeholders insight into progress in the definition and development of the technical solution and the associated risks and issues (Roedler and Jones 2005, 9). The types of technical measures relevant to this project are appropriately defined in Roedler (Roedler and Jones 2005) and summarized below.

> **Measures of Effectiveness (MOEs)** focus on the SoS capability to achieve mission or operational objectives within the intended operational environment. MOEs represent the acquirer's most important evaluation and acceptance criteria against which the quality of the solution is assessed. They are solution independent but are specific properties that any alternative technical solution must exhibit to be acceptable to the acquirer. MOEs represent overall or task-level operational success criteria such as mission performance, safety, operational availability, etc. When a specific solution is applied and evaluated (in a specific environment and under specific conditions), an MOE will indicate "how well a task was performed."
>
> **Measures of Performance (MOPs)** measure attributes considered as important to ensure the system has the capability to achieve operational objectives. MOPs are used to assess whether the system meets design or performance requirements that are necessary to satisfy the MOEs. They address an aspect of system performance and capability and are expressed in terms of distinctly quantifiable performance features such as speed, payload, range, or frequency. When a specific solution is applied and evaluated, an MOP will indicate "what was performed."
>
> **Key Performance Parameters (KPPs)** are a critical subset of the MOPs representing those capabilities and characteristics so significant that failure to meet the threshold value of performance can be a cause for the concept selected to be reevaluated or the project to be reassessed or terminated.
>
> **Technical Performance Measures (TPMs)** focus on the critical technical performance parameters of the specific architectural elements of the system. TPMs are derived from or provide insight for the MOPs. TPMs are used to assess design progress, compliance, and technical risk, with examples including range, accuracy, weight, size, power output, timing, and the product quality characteristics related to critical operational requirements. (Roedler and Jones 2005, 9–11)

C-UAS MOEs and MOPs will be characterized in this chapter. C-UAS system characteristics and associated TPMs will be characterized in Chapter IV. KPPs will not be specifically identified within the scope of this project.

1. Measures Context

Before defining MOEs, it is helpful to apply terminology to aspects of the C-UAS Combat Deployment operational environment (refer to Figure 22). Assuming that the Threat UAV is launched and commences intercept of the Force outside of detectable range of C-UAS sensors, the Detection Point (DP) represents the range ring corresponding to the distance of the sensor on the Low Energy Effects (*Sense*) platform with the furthest detectable range for the Threat UAV. After initial detection of a possible Threat UAV, confirmation of the Threat UAV is established if a second sensor or an identification friend or foe (IFF) challenge goes unanswered. The range ring corresponding to this confirmation is defined as the Assessment Point (AP). Any UAVs detected at a time after which AP is established will be engaged as hostile. It is desired that neutralization of threat be maximized in the Engagement Standoff Range region with operational performers capable of electronic neutralization (*Cyber-attack Platform* / *Cyber-Attack UAV*) employed. Threat UAVs that evade electronic neutralization and breach the Close-In Engagement region will be designated as leakers. This breach point is defined as the Electronic Neutralization Point Limit. Leakers that enter the Close-In Engagement region shall be engaged by operational performers capable of employing kinetic-mechanical effects (*UAV Mobile Ground Defense Platform* / *High Energy Laser*). Leakers that evade kinetic-mechanical neutralization effects and breach the Protect the Force region have reached the Kinetic Neutralization Point Limit. Leakers in this region shall be engaged using RF Jamming techniques and projectile weapons employed by the high value asset and embarked personnel. If the leaker is successful in employing effects against the high value asset, then the Overall Neutralization Point Limit is reached.

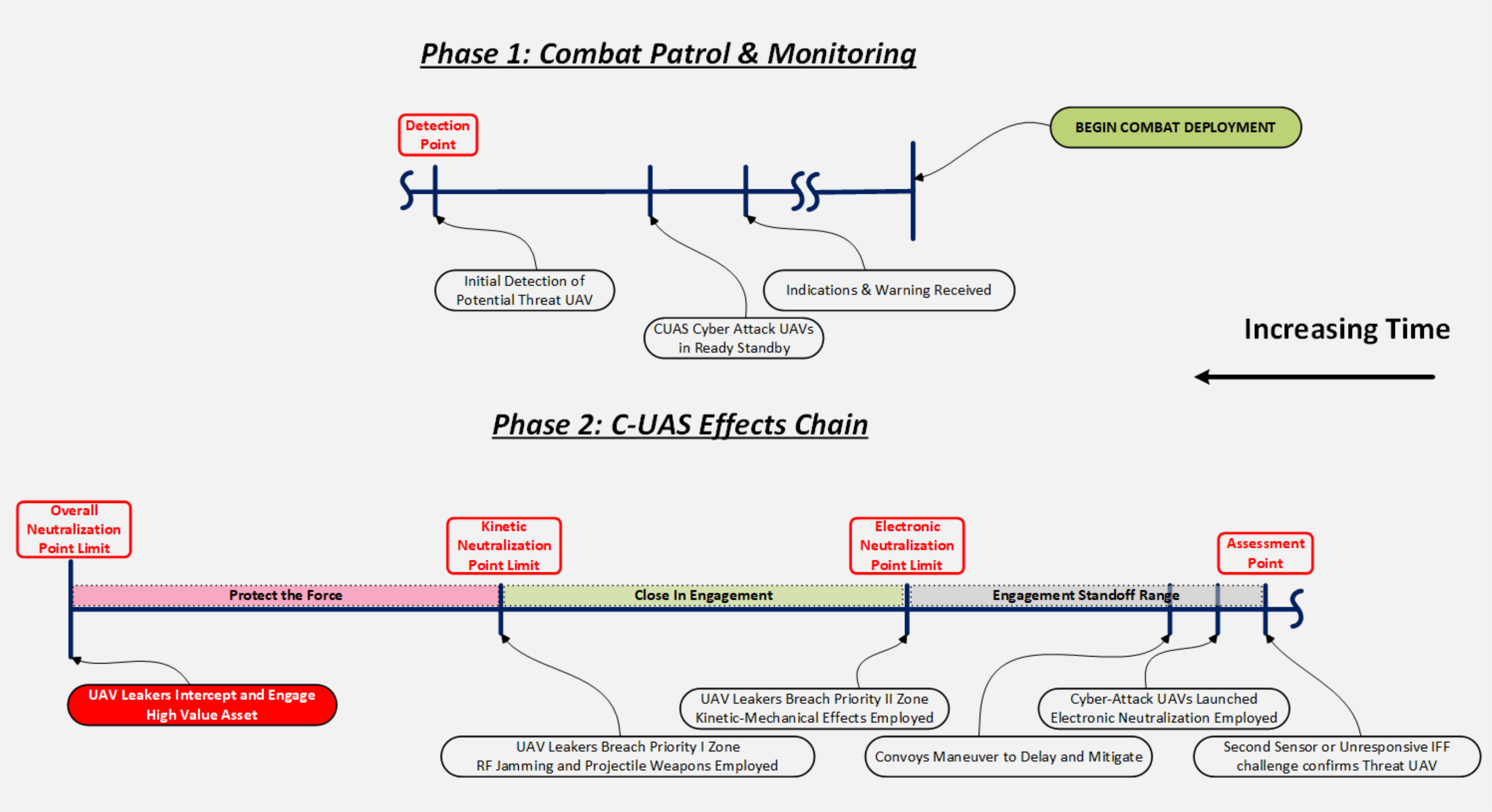

Phase 1: Combat Patrol & Monitoring
Detection Point
BEGIN COMBAT DEPLOYMENT
Initial Detection of Potential Threat UAV
CUAS Cyber Attack UAVs in Ready Standby
Indications & Warning Received
Increasing Time
Phase 2: C-UAS Effects Chain
Overall Neutralization Point Limit
Kinetic Neutralization Point Limit
Electronic Neutralization Point Limit
Assessment Point
Protect the Force
Close In Engagement
Engagement Standoff Range
UAV Leakers Intercept and Engage High Value Asset
UAV Leakers Breach Priority I Zone RF Jamming and Projectile Weapons Employed
UAV Leakers Breach Priority II Zone Kinetic-Mechanical Effects Employed
Convoys Maneuver to Delay and Mitigate
Cyber-Attack UAVs Launched Electronic Neutralization Employed
Second Sensor or Unresponsive IFF challenge confirms Threat UAV

Figure 22. C-UAS Combat Deployment Operational Timeline

2. C-UAS Measures of Effectiveness

a. C-UAS Sense Performance Metrics and Definitions

The metrics supporting C-UAS *Sense* are derived from two primary sources (Kouhestani, Woo and Birch 2017; Tan, Van Bossuyt, and Hale 2021). An illustration of C-UAS performance metrics is depicted in Figure 23 (Kouhestani, Woo and Birch 2017, 4):. The MOE for C-UAS *Sense* is given by ***Probability of Sense*** (PS), which is a product of performance metrics Probability of Detection (PD), Probability of Classification (PC), and Probability of Transmission (PT) (Kouhestani, Woo and Birch 2017, 5):

$$P_S = P_D P_C P_T \tag{1}$$

Performance metric definitions supporting C-UAS *Sense* are provided in Table 8. This project will assume that the C-UAS SoS will have perfect communications capability ($P_T = 1$), therefore, performance metrics supporting PT will not be defined here.

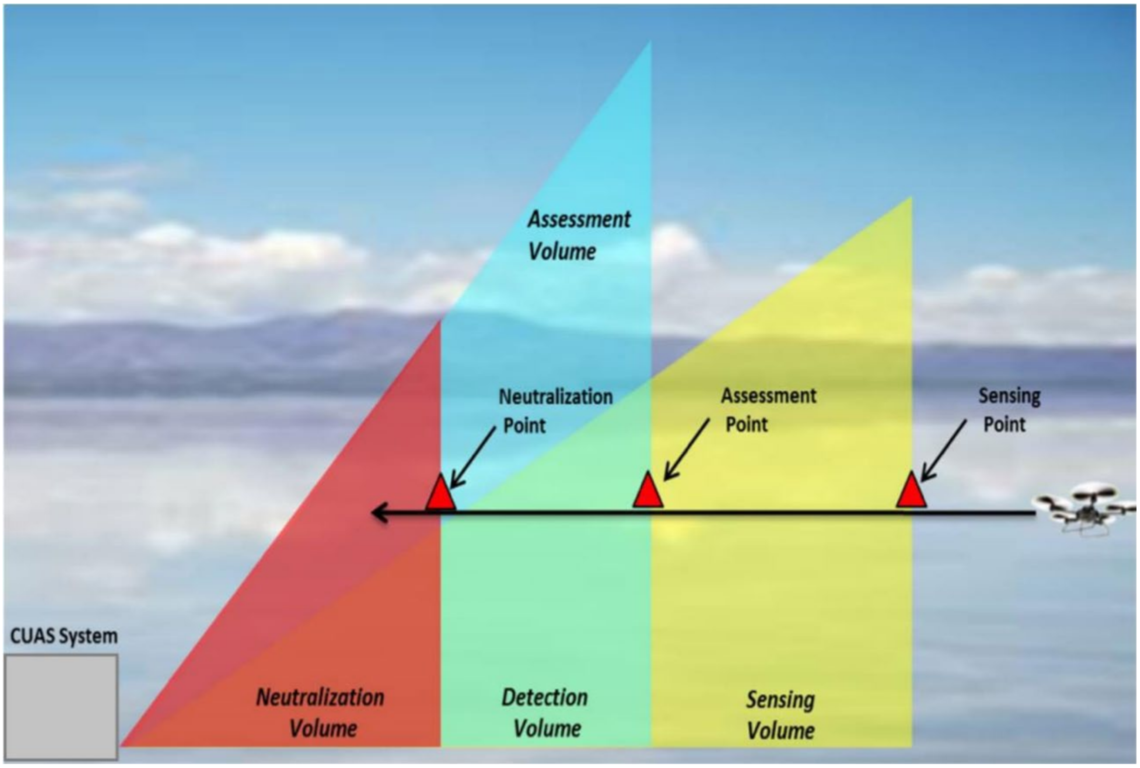


Figure 23. Illustration of C-UAS Performance Metrics.
Source: Kouhestani et al. (2017).

Table 8. Performance Metrics and Definitions of C-UAS Sense. Adapted from Kouhestani (2017).

Performance Metric	**Type**	**Definition**
		Detection Effectiveness
Note: Detection is identical to Sense as defined in Kouhestani (2017, 3)		
Probability of Detection (P_D)	MOE	The probability associated with the capability of the sensor to detect the presence of a sUAS.
Sensing Point (SP)	MOP	The location at which the UAS is sensed by the C-UAS SoS. The SP is characterized by coordinates referenced from the C-UAS Sensor (Low Energy Effects performer) location.
Sensing Volume (SV)	MOP	A three-dimensional (3D) plot of the SP coordinates from the test set that creates a volume during which the sensor can be expected to initiate an alarm caused by the presence of the sUAS stimulus.
		Classification Effectiveness
Note: Classification is identical to Assessment as defined in Kouhestani (2017, pg. 4)		
Probability of Classification (P_C)	MOE	The probability associated with the C-UAS's capability to determine whether the alarm was caused by a UAS or some other stimulus such as a friendly asset, weather, or wildlife.
Classification Point (CP)	MOP	The location at which accurate classification of sUAS threat occurs. The AP is characterized by coordinates referenced from a sensor location.
Classification Time (CT)	MOP	The time required to make an accurate classification of the cause of the detection. The CT is measured from the sensing time (ST) to the time an accurate classification is made.
Classification Volume (CV)	MOP	A 3D plot of the CP coordinates from the test set that creates a volume at which accurate classification of the cause of the alarm can be expected.
		Track Effectiveness
Probability of Track (P_{Tk})	MOE	The probability of accurate track of sUAS's geolocation. The lesser track drop will increase the C-UAS accuracy of acquiring UAS position.
Tracking Drops (TD)	MOP	The number of times that the designated C-UAS sensor fails to maintain consecutive positional information during the C-UAS operational timeline.
Tracking Accuracy (TA)	MOP	The measured distance between the C-UAS tracking points and the actual sUAS position. This value is determined by subtracting the coordinates supplied by the C-UAS and the coordinates from the sUAS GPS tracker.
		Transmission Effectiveness

Table 8 (continued)

Probability of Transmission (P_T)	MOE	The probability of successful data transferring over a period of time to a response team and/or interceptor subsystem.

b. C-UAS Assess Performance Metrics and Definitions

The metrics supporting C-UAS *Assess* are derived from Bornman (Bornman 1993). Specifically, C-UAS *Assess* metrics will characterize the ability of a C2 system, equipped with data fusion and tactical decision aid capabilities and with a human in-the-loop, to decide how to respond to threat and determine the desired effect/targeting solution. The DROSERA project has selected ***Time to Decision Ratio*** and ***Percent Actions Initiated by Time Ordered*** as its key C-UAS *Assess* metrics. ***Time to decision ratio*** (t_dr) is the proportion of time from receipt of the sUAS threat classification criteria to the time of execution action that is devoted to the commander's decision. Input data are the time of receiving the threat classification criteria (t_r), time order is given (t_o), and the time the neutralization order is executed (t_e) (Bornman 1993, 42):

$$t_dr = \frac{t_o - t_r}{t_e - t_r} \qquad (2)$$

Percent actions initiated by time ordered ($\%_I$) is the percentage of all actions initiated in response to orders that are initiated within the time specified by the order. For this project, this measure will be an indication of how many neutralization assets were able to successfully execute the order given (Bornman 1993, 42). Input data are the number of assets for which the execution order was intended (n_o) and number of assets, which successfully executed the order (n_e). Performance metric definitions supporting C-UAS *Assess* are provided in Table 9.

$$\%_I = \frac{n_e}{n_o} \qquad (3)$$

Table 9. Performance Metrics and Definitions of C-UAS Assess. Adapted from Bornman (1993).

Performance Metric	**Type**	**Definition**
C2 Decision Effectiveness		
Time to Decision Ratio definition (t_{dr})	MOE	The proportion of time from receipt of the sUAS threat classification to the time of execution action that is devoted to the commander's decision.
Assessment Time (AT)	MOP	The time required to confirm an appropriately classified sUAS as a threat and provide a recommendation for neutralizing effect. AT is measured from the classification time (CT) to the time a recommendation for neutralization is made.
Decision Time (DT)	MOP	Decision time captures the human and organizational factors involved in the final decision to neutralize a sUAS threat. DT is measured from the time a recommendation is made available by the C2 system (AT) to the time the order is promulgated to C-UAS performer.
Execution Time (ET)	MOP	The time it takes a C-UAS performer to execute a neutralization order. ET is measured from the time a neutralization order is promulgated (DT) to the time the order is assessed to be complied with.
C2 Execution Effectiveness		
Percent Actions Initiated on Time ($\%_I$)	MOE	The percentage of all actions initiated in response to orders that are initiated within the time specified by the order.
Execution Status	MOP	Reports and tracks whether the received order was executed or complied with.

c. C-UAS Neutralize Performance Metrics and Definition

Once again referencing Kouhestani and Tan (Kouhestani, Woo, and Birch 2017; Tan, Van Bossuyt, and Hale 2021), C-UAS *Neutralization* is defined as the capability to direct UAS drones away from the high value asset or stop its progress towards the high value asset. The key effectiveness measure is ***Probability of Neutralization*** (P_N) and is evaluated using metrics based on probability, location, and time. In general, the relationship between P_N and its related metrics is given in Equation 4 (Tan, Van Bossuyt, and Hale 2021, 11–12) and Table 10 (Kouhestani, Woo, and Birch 2017, 4–5) respectively.

$$P_N = P_H P_{K/D} P_R \tag{4}$$

Table 10. Performance Metrics and Definitions of C-UAS Neutralize. Adapted from Kouhestani (2017).

Performance Metric	Type	Definition
Probability of Neutralization (P_N)	MOE	The probability associated with the capability of the C-UAS system to direct the UAS away from a security interest or to stop its forward progress toward a security interest.
Probability of Hit (P_H)	MOP	The probability of successful contact made by interceptor to the UAS by either projectiles or kinetic-mechanical neutralization methods. The higher the probability depicts the better effectiveness. Note: Neutralization methods that exploit the RF spectrum will maintain $P_H = 1$.
Probability of Kill/Disable ($P_{K/D}$)	MOP	The probability of successful denial or destruction of the threat sUAS after being contacted by the neutralizer. The higher probability depicts the better effectiveness.
Probability of Risk (P_R)	MOP	Represents the possibility that the neutralizing performer can be damaged due to a threat sUAS accidentally falling, exploding, or colliding with it. The probability that a threat sUAS will contribute to this event will be held at 2–6 %.
Neutralization Point (NP)	MOP	The location where the threat sUAS is effectively neutralized, meaning the sUAS is no longer under the control of the original pilot. Ideally, the UAS is being flown/controlled by the C-UAS to a specific location where the site security force can appropriately address the threat. If the C-UAS technology does not have the capability to fly the sUAS to a specific set of coordinates, the NP is where the sUAS forward progress is halted by the C-UAS and the UAS is forced to land or return home.
Neutralization Time (NT)	MOP	The time required to neutralize the UAS. The NT is measured from the time that the neutralization begins to the time the C-UAS system directs the UAS away from a security interest or to stop its forward progress toward a security interest.
Neutralization Volume (NV)	MOP	A 3D plot of the NP coordinates from the test set that creates a volume at which the neutralization of the threat sUAS initially occurs.

d. C-UAS Effectiveness Metrics and Definition

C-UAS effectiveness ($P_{(Effectiveness)}$) is given as a product of probability of sense and probability of neutralization (Equation 5) (Tan, Van Bossuyt, and Hale 2021, 11). The breakdown of the two sub-functions is explained in the previous C-UAS MOE sections. The metrics definition for C-UAS weapon effectiveness is captured in Table 11.

$$P_{(Effectiveness)} = P_S P_N \tag{5}$$

Table 11. Performance Metrics and Definitions of C-UAS Weapon Effectiveness. Adapted from Tan (2021).

Performance Metric	**Type**	**Definition**
C-UAS Weapon Effectiveness (P(Effectiveness))	MOE	A measure of mission fulfilment in the C-UAS Combat Deployment operational scenario.

e. C-UAS Resiliency (Cyber-Attack)

The International Council on Systems Engineering (INCOSE) defines resilience as: "…the ability to prepare and plan for, absorb or mitigate, recover from, or more successfully adapt to actual or potential adverse events." (INCOSE 2015, 229). Furthermore, INCOSE explains (INCOSE 2015, 229–230) that resilience is an emergent and nondeterministic property of a system. Emergent in that it cannot be determined by examining the independent elements of the system and nondeterministic because the wide variety of possible system states at the time of disruption cannot be characterized either deterministically or probabilistically.

The project will establish a resiliency metric that characterizes how well the C-UAS SoS will be able to exploit the susceptibility of the Threat UAS architecture to cyber-attack. Specifically, DROSERA C-UAS is concerned with harvesting adversary credentialing information in order to access or interfere with local adversary networks for the purpose of distorting/destroying sensor data and take-down/lock-out/hijack of threat sUAS targets.

Thus, a means to quickly evaluate the threat cyber vulnerability and recommend the most effective C-UAS cyber-attack neutralization method is the focus here.

Hartmann and Daponte (Hartmann and Steup, 2013, 8–9; Daponte, Maguire, and Roldan 2020, 34–39) provide a framework and methodology, respectively, for evaluating a cybersecurity risk rating - a numerical value that will be associated with the most likely cyber-attack and vulnerability associated with it. UAV vulnerability risk areas are categorized as follows (Daponte, Maguire, and Roldan, 2020):

> **Integrity Risk:** Involves compromising the reliability of the information utilized by the system. A reliable system requires that the information being used is correct and authentic. In a cyber-attack scenario, exploiting an integrity risk can enable replay attacks, injection attacks, and packet modification.
>
> **Confidentiality Risk:** Exposed confidentiality means that privileged information is accessible to unauthorized users. In a cyber-attack scenario, exploiting a confidentiality risk can yield sensitive information, including the identification of the threat operator.
>
> **Availability Risk:** Impacts to availability means that the timely processing and distribution of information is not available to the system/user when needed. A denial of service (DoS) attack on the communication link is the most common type of availability exploitation in a cyber-attack scenario. (Daponte, Maguire, and Roldan, 2020, 43–45)

Figure 24 (Van Bossuyt and Hale 2020) depicts a representative view of the elements that are ingested and provided by a system capable of evaluating cyber vulnerability risk. This risk rating can be used to quickly configure and employ the cyber-attack neutralization suited for the existing threat and conditions. This could also include *not* employing cyber-attack in cases that it is deemed less effective than other neutralization methods.

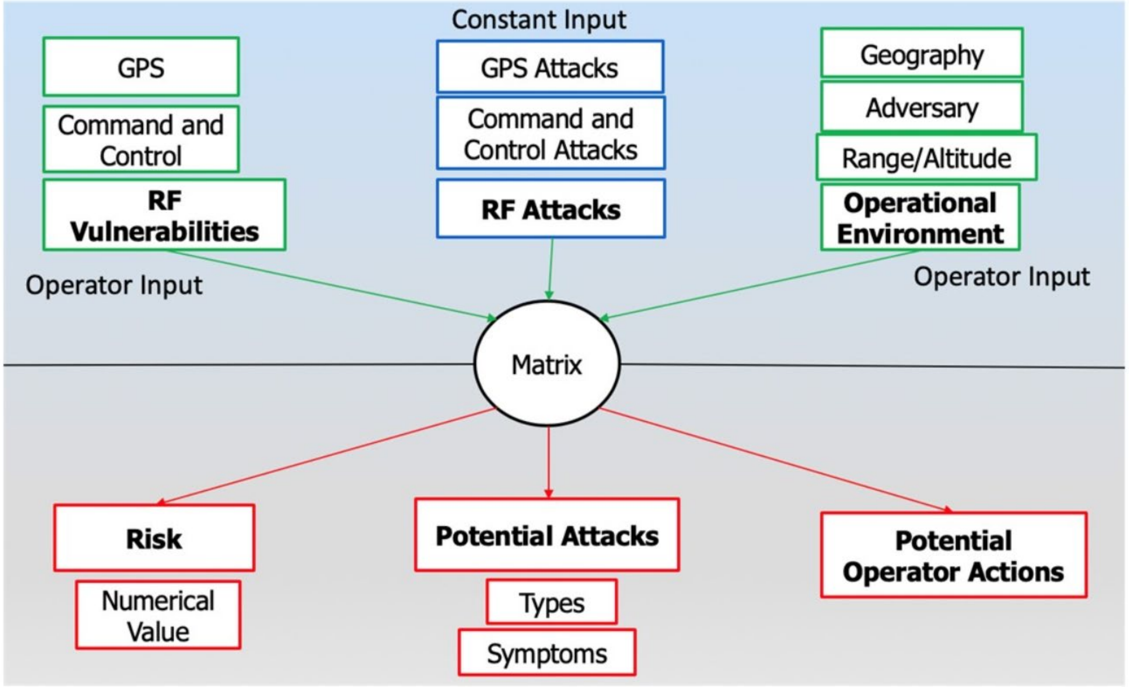


Figure 24. C-UAS Risk Decision Matrix Input/Output Diagram. Source: Van Bossuyt and Hale (2020).

The DROSERA project plans to utilize existing research (Best 2020) that contains a comprehensive assessment on the vulnerabilities of and recommended type of attack on existing and emerging UAS. This information will help to develop a risk rating matrix that could be used to assess and inform the employment of cyber-attack neutralization methods in the C-UAS Combat Deployment scenario. Table 12 captures the performance metrics and definitions for C-UAS cyber-attack *Resiliency* (Best 2020, 58–63).

Table 12. Performance Metrics and Definitions of C-UAS Resiliency (Cyber-Attack). Adapted from Best (2020).

Performance Metric	Type	Definition
Cyber-attack Risk Rating	MOE	A numerical value that is associated with the most likely of the cyber-attacks employed in a given operational scenario.
Adversary UAV Technical Capability	MOP	Represents the range of operational modes that the adversary can exhibit when executing a C2 attack against friendly forces.

Table 12 (continued)

Adversary UAV Employment	MOP	Represents the adversary UAV attack mode based on real-time input to the C-UAS SoS that the adversary is currently exhibiting.
Adversary UAV Cyber Vulnerability	MOP	A flaw or weakness in the adversary UAV, its security procedures, internal controls, or design and implementation, which could be exploited.
C-UAS Cyber-Attack Capability	MOP	Represents the range of cyber-attack neutralization methods available to C-UAS SoS in defeating the threat UAS progress.

f. C-UAS Reliability

Blanchard defines reliability as, "… the probability that a system will perform in a satisfactory manner for a given period when used under specified operating conditions." (Blanchard and Frabryky 2011, 345). Table 13 captures the performance metrics and definitions for C-UAS Resiliency.

Table 13. Performance Metrics and Definitions of C-UAS Reliability

Performance Metric	**Type**	**Definition**
C-UAS Reliability	MOE	A fractional value specifying the number of times the C-UAS can sustain mission critical function given number of trials
C-UAS mission critical failure	MOP	Indicates threshold loss of mission critical function during the course of one trial.

g. C-UAS Energy Effectiveness

Due to the inherent mobility involved, C-UAS Combat Deployment scenarios require the application of electronic effects in an energy-constrained environment. Energy efficiency is therefore a vital effectiveness measure. Although there are several more insightful energy efficiency measures that can be explored, DROSERA project will use electrical energy consumption as its effectiveness metric to support cost and capacity analysis (Equation 6). Table 14 captures the performance metrics and definitions for C-UAS Energy Effectiveness.

$$\text{Energy Consumption} = (Power)(Time) \tag{6}$$

Table 14. Performance Metrics and Definitions of C-UAS Energy Effectiveness

Performance Metric	Type	Definition
C-UAS Energy Effectiveness	MOE	Electrical Energy Consumed by all C-UAS performers during the Combat Deployment scenario.
C-UAS System Employment	MOP	Captures measures of system activities (time energized, speed) that correspond to power usage during C-UAS scenario
C-UAS System power usage	MOP	Electrical energy consumed by a single C-UAS system during the Combat Deployment scenario.

E. SUMMARY OF CHAPTER III

This chapter covered the operational analysis of the C-UAS mission context. This analysis defined a conceptual idea for the C-UAS capability and determined the feasibility for operational mission success. An operational vignette for C-UAS Combat Patrol was developed using the C-UAS CONOPS. The mission definition summary was developed to describe both the entering conditions and boundaries such as the operational environment and the commander's desired intent. Next, the operational architecture was developed to provide a description of the tasks, operational elements, and information flows required to accomplish or support a warfighting function. Lastly, value systems design was conducted to establish performance and mission effectiveness metrics that represent stakeholder priorities. These products provided the necessary functionality to begin the development of the resource architecture. The next chapter discusses the derived system context and functional requirements to develop the baseline System of Systems architecture.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESOURCE ARCHITECTURE

> A System of Systems (SoS) is a set or arrangement of systems that results when independent, and task-oriented systems are integrated into a larger systems construct, that delivers unique capabilities and functions in support of missions that cannot be achieved by individual systems alone.
>
> — Vaneman (2016, 1)

In a traditional Systems Engineering approach, the focus is the development of a single system designed to meet stakeholder needs. The resource architecture for this project relies on a System of Systems (SoS) architecture. The advantages of SoS architecture are alignment with a mission context featuring joint interoperability, dynamic reconfiguration of the architecture as needs change, and the use of a service-oriented architecture approach as the key enabler.

DoDAF was utilized for the SoS architecture development. Several DoDAF views were generated to represent the proposed system of systems identified by the capstone team. The architecture development methodology followed a hierarchal approach. As discussed in Chapter II, the SE process for our capstone will not follow all the steps of the Vee process, therefore not every DoDAF viewpoint was developed for this capstone. The main DoDAF views constructed in support of the overall architecture development were limited to the All, Capability, Operations, and System Viewpoints.

A. SYSTEM CONTEXT ANALYSIS

The system context is beneficial as it helps to provide a high-level functional view of the intended system. It can help to provide an early understanding of the system to be built by identifying the different ways the end users will rely on it. The system context helps to define the overall capabilities of the system by exploring the expectations that the end users have of the system. The system context diagram can provide a description of the overall architecture environment to include interactions with external systems or other architectures.

Understanding the system context also aids in defining the details and boundaries of the system to be designed and can help with the visualization of the flows of information between the system and other external components around it. This aids with the evaluation of the systems boundaries for the controlled inputs and outputs. Performing system context analysis is a key step early in the design process as it can help to reduce risks to the system under design. The layered architecture for a hypothetical C-UAS (Figure 25) found in Gopal (Gopal 2020, 7) served as a suitable initial system context diagram, as it includes generalized resources for all of the C-UAS effects performers identified in the C-UAS Combat Patrol OV-1 (Figure 15). The proposed SoS architecture was to remain solution agnostic so its construction could use a modular approach where any system considered for integration would be based on the perceived stakeholder need. This generalized resource architecture is used only as a starting point of system construction.

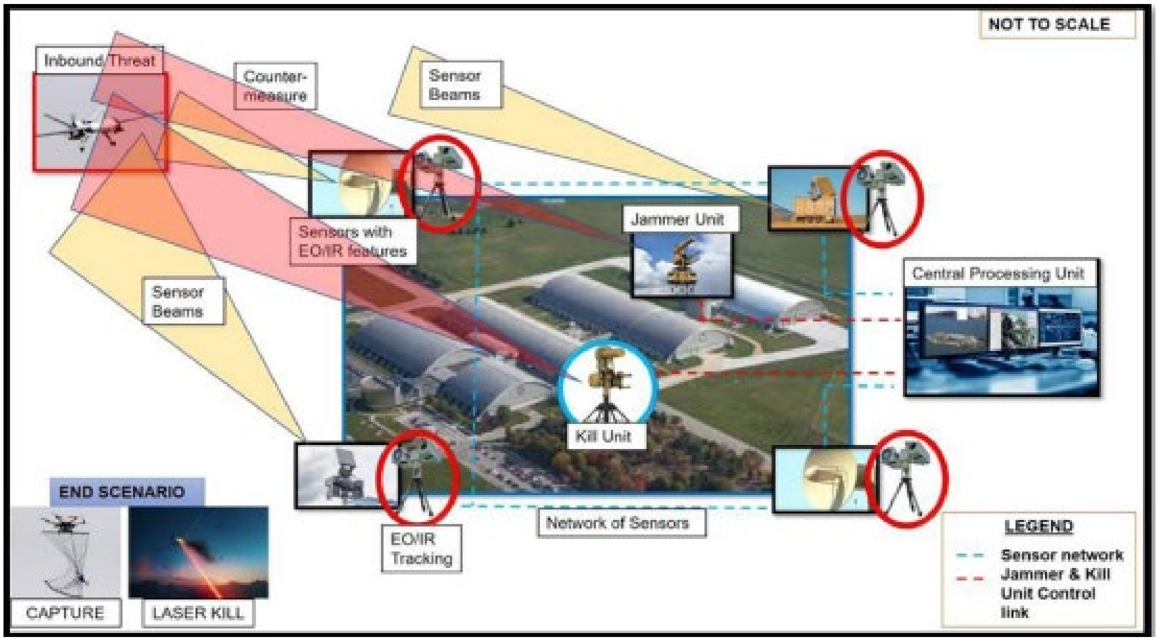


Figure 25. General Counter Unmanned Aerial System- Layered Architecture. Source: Gopal (2020).

B. C-UAS GENERALIZED RESOURCE PERFORMERS

There exists a variety of C-UAS solutions that are commercially available for purchase that can vary in their configuration. C-UAS systems can be obtained as separate systems or as system effects package that, when integrated, compose the overall C-UAS SoS. The selection of a specific C-UAS solution depends on many capability requirement factors, such as reliability, security level required, time to detect requirements, and defeat tactics (e.g., RF jamming, cyber-attack, high-energy laser, kinetic, etc.). Team DROSERA chose to maintain a generalized description of system solutions, by surveying many fielded and forthcoming systems and mapping those common performance characteristics to DROSERA generalized resource performer. The C-UAS SoS resource architecture modeling was therefore kept at a high level to allow for modularity and to allow for flexibility in design. This was done to support future decisions that may be made regarding chosen systems to implement in the C-UAS SoS configuration for a specific mission. The physical architecture still must support the C-UAS operational scenario priority phases of *Sense*, *Assess*, and *Neutralize*.

The DROSERA project has defined the generalized resource performers necessary to provide functionality to the C-UAS effects chain operational scenario priorities of *Sense*, *Assess*, and *Neutralize* (Figure 39). Specifically, this involves three unique resource performers: a Sensor system, C2 system, and an Interceptor system. The Sensor system provides the C-UAS *Sense* functions. The C2 system provides the C-UAS *Assess* functions. The Interceptor system provides the C-UAS *Neutralize* functions.

These resource performers were modeled in Innoslate via a system hierarchy to capture potential systems to utilize to support the C-UAS mission scenario defined in Chapter III. A portion of this generic physical architecture can be seen in Figure 26. In addition to the command and control, sensors, and radar, the team added the following to make up the generic system architecture: ground control station, aerial vehicle, low energy effects platform, cyber-attack platform, cyber-attack UAV, and high-energy laser. These additional systems were defined in Chapter III as operational performers in the C-UAS mission scenario developed in support of this capstone project. Each of the systems that comprise the C-UAS SoS where further decomposed to include an additional level of detail into the sub-systems that comprise these operational performers.

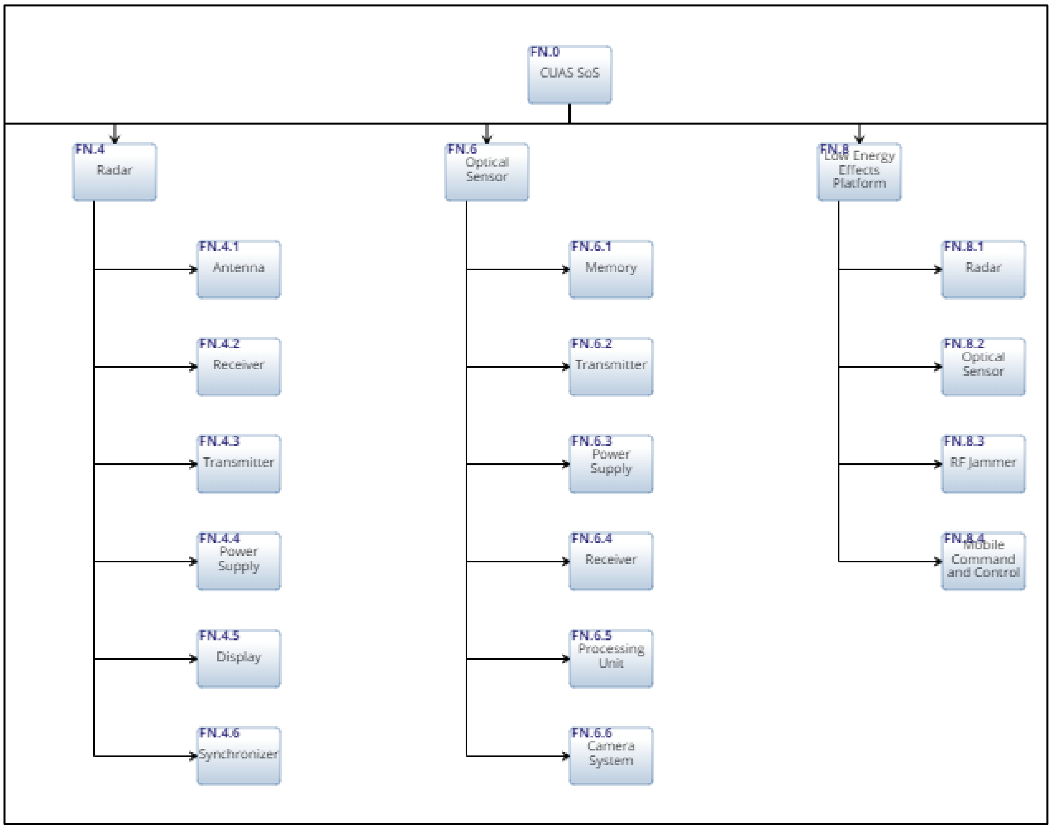


Figure 26. C-UAS Generic Physical Architecture (Excerpt)

C. FUNCTIONAL ARCHITECTURE

The next phase in the continuation of architectural development is to develop the functional architecture. Functional Analysis is “an iterative process of translating system requirements into detailed design criteria. The purpose is to develop the top-level system architecture and present an overall integrated description of the systems functional architecture” (Blanchard and Fabrycky 2011, 86). The functional analysis of the system requirements requires the identification of the design criteria that permits the system to execute its mission. This process begins with the analysis of the requirements of the system, which helps identify top-level system functions. Next, the top-level functions are further decomposed into better defined system functions. These developed functional decomposition diagrams integrate and align the functions required to form the functional baseline of the system (Blanchard and Fabrycky 2011, 104).

The DoDAF schema was utilized for the SoS architecture development. Several DoDAF views were generated to represent the proposed system of systems identified by the capstone team. The architecture development methodology followed a hierarchal approach. As discussed in Chapter II, the SE process for our capstone will not follow all the steps of the Vee process, therefore not every DoDAF product was utilized for this capstone. The main DoDAF products used in support of the overall architecture development were limited to the All, Capability, Operations, and System Viewpoints.

1. Systems Interface (SV-1) and Systems Resource Flow Descriptions (SV-2)

The Systems Viewpoint can be used to support the association of system resources to the operational requirements. The DoDAF models in the Systems Viewpoint describe system interconnections that provide support for DOD functions. The Systems Interface Description (SV-1) was the first viewpoint created in support of the functional architecture phase. "The SV-1 links together the operational and systems architecture models by depicting how resources are structured and interact to realize the logical architecture specified in an OV-2 Operational Resource Flow Description" (DOD CIO n.d., Systems Interface Description). The SV-1 can be used to show the connection of systems and what resource flows between them, to also include any human aspects of the architecture and how they interact with the systems. The C-UAS Combat Patrol SV-1 (Figure 27), aligns with the C-UAS Combat Patrol OV-2 (Figure 17), specifying the information elements passed between resource performers that implement the operational exchanges between performers in the operational context. The C-UAS Systems Resource Flow Description (SV-2) (Figure 28), details the data elements transferred between systems that convey the information elements from the C-UAS Combat Patrol Operational Resource Flow Matrix (OV-3).

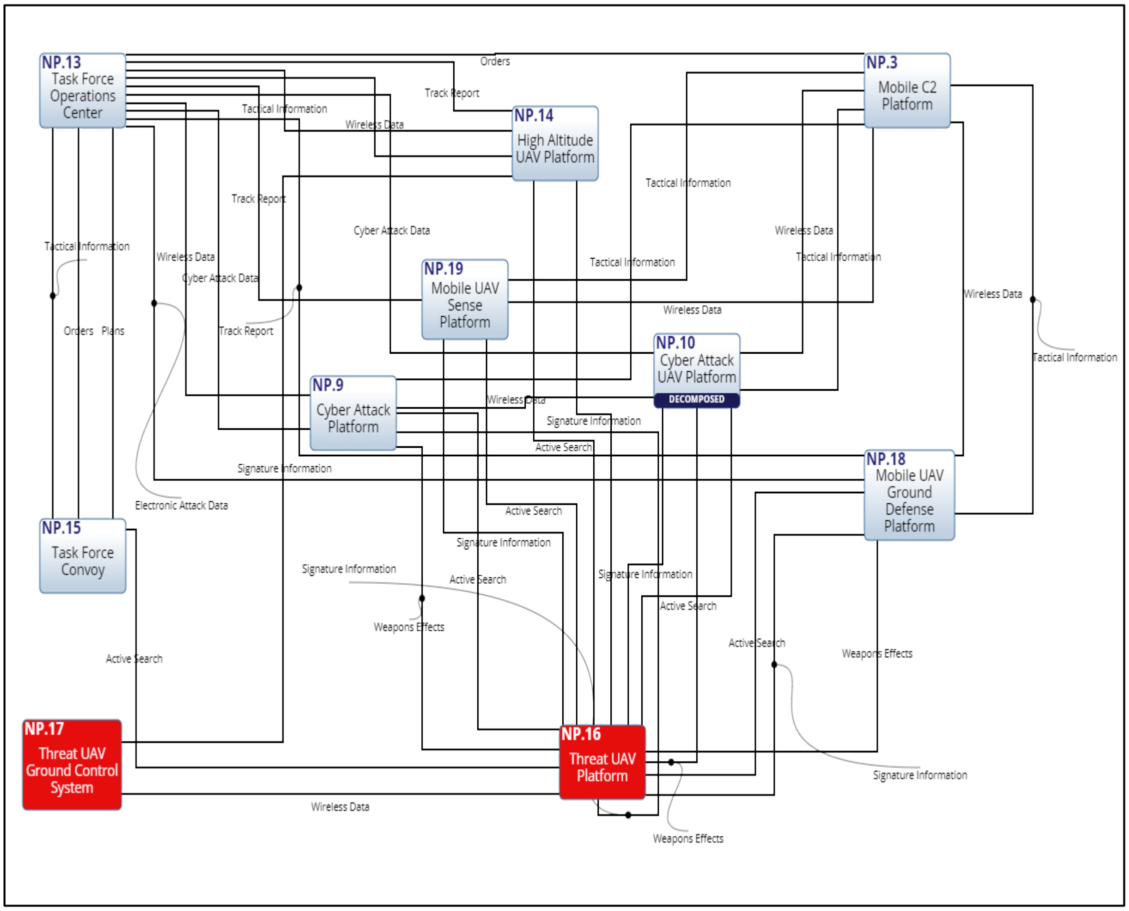


Figure 27. C-UAS Combat Patrol Systems Interface Diagram

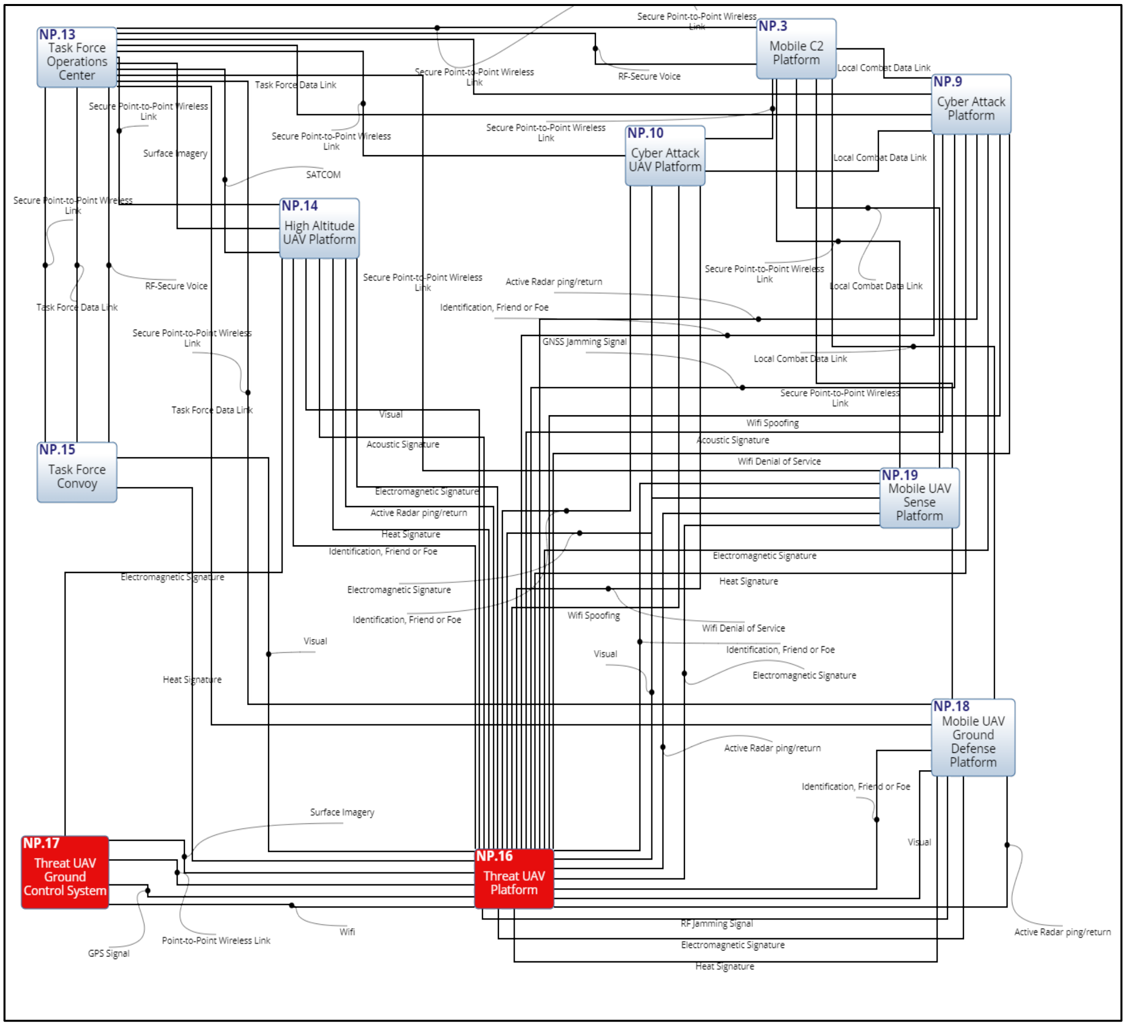

Secure Point-to-Point Wireless Link
NP.3
Mobile C2 Platform
NP.13
Task Force Operations Center
RF-Secure Voice
Local Combat Data Link
NP.9
Cyber Attack Platform
Task Force Data Link
Secure Point-to-Point Wireless Link
Secure Point-to-Point Wireless Link
Secure Point-to-Point Wireless Link
NP.10
Cyber Attack UAV Platform
Secure Point-to-Point Wireless Link
Surface Imagery
SATCOM
Local Combat Data Link
Secure Point-to-Point Wireless Link
NP.14
High Altitude UAV Platform
RF-Secure Voice
Task Force Data Link
Secure Point-to-Point Wireless Link
Active Radar ping/return
Identification, Friend or Foe
Secure Point-to-Point Wireless Link
Local Combat Data Link
GNSS Jamming Signal
Secure Point-to-Point Wireless Link
Local Combat Data Link
Secure Point-to-Point Wireless Link
Task Force Data Link
Visual
Wifi Spoofing
Acoustic Signature
Acoustic Signature
Wifi Denial of Service
NP.15
Task Force Convoy
NP.19
Mobile UAV Sense Platform
Electromagnetic Signature
Active Radar ping/return
Heat Signature
Identification, Friend or Foe
Electromagnetic Signature
Electromagnetic Signature
Heat Signature
Electromagnetic Signature
Identification, Friend or Foe
Wifi Spoofing
Wifi Denial of Service
Visual
Identification, Friend or Foe
Visual
Electromagnetic Signature
Heat Signature
NP.18
Mobile UAV Ground Defense Platform
Active Radar ping/return
Identification, Friend or Foe
Surface Imagery
Visual
NP.17
Threat UAV Ground Control System
NP.16
Threat UAV Platform
GPS Signal
Point-to-Point Wireless Link
Wifi
RF Jamming Signal
Active Radar ping/return
Electromagnetic Signature
Heat Signature

Figure 28. C-UAS Combat Patrol Systems Resource Flow Description

2. Systems Functionality Description (SV-4)

The Systems Functionality Description (SV-4) serves to specify the functionality of resources in the system architecture (DOD CIO n.d., Systems Functionality Description). Project DROSERA constructed SV-4 viewpoints in a functional hierarchy format to shows decomposition of functions suitable for product line architecture. The five system functionality descriptions depicted in Figure 29 through Figure 33 capture the high-level C-UAS Combat Patrol system functions that implement the *Sense*, *Assess*, and *Neutralize* operational tasks.

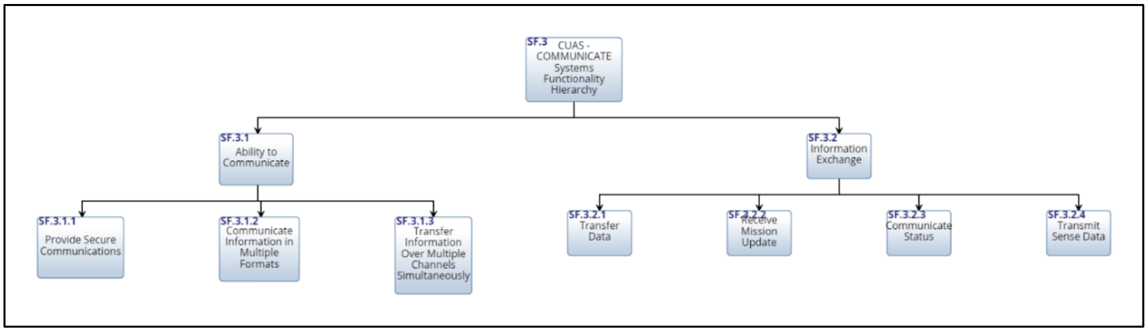

SF.3 CUAS - COMMUNICATE Systems Functionality Hierarchy
SF.3.1 Ability to Communicate
SF.3.2 Information Exchange
SF.3.1.1 Provide Secure Communications
SF.3.1.2 Communicate Information in Multiple Formats
SF.3.1.3 Transfer Information Over Multiple Channels Simultaneously
SF.3.2.1 Transfer Data
SF.3.2.2 Receive Mission Update
SF.3.2.3 Communicate Status
SF.3.2.4 Transmit Sense Data

Figure 29. C-UAS Communicate Systems Functionality Description

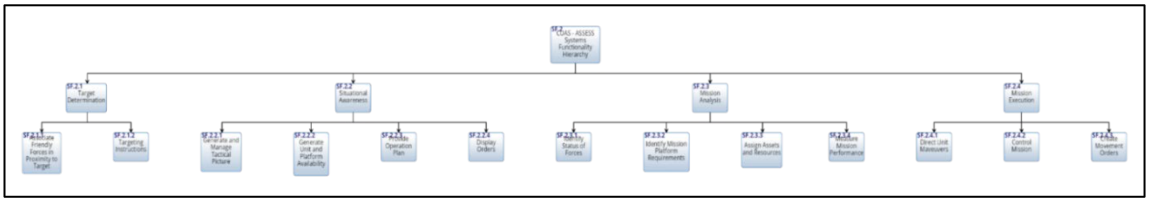

SF.2 CUAS - ASSESS Systems Functionality Hierarchy
SF.2.1 Target Determination
SF.2.2 Situational Awareness
SF.2.3 Mission Analysis
SF.2.4 Mission Execution
SF.2.1.1 Associate Friendly Forces in Proximity to Target
SF.2.1.2 Targeting Instructions
SF.2.2.1 Generate and Manage Tactical Picture
SF.2.2.2 Generate Unit and Platform Availability
SF.2.2.3 Provide Operation Plan
SF.2.2.4 Display Orders
SF.2.3.1 Identify Status of Forces
SF.2.3.2 Identify Mission Platform Requirements
SF.2.3.3 Assign Assets and Resources
SF.2.3.4 Measure Mission Performance
SF.2.4.1 Direct Unit Maneuvers
SF.2.4.2 Control Mission
SF.2.4.3 Create Movement Orders

Figure 30. C-UAS Assess Systems Functionality Description

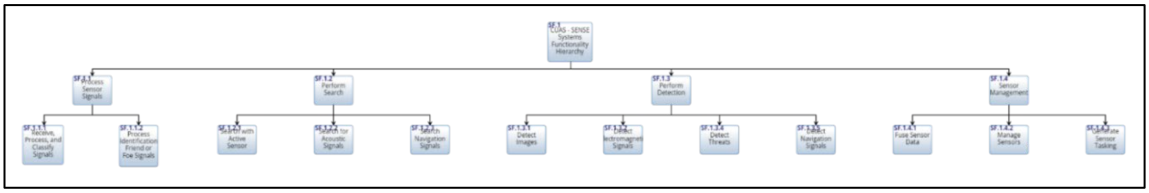

SF.1 CUAS - SENSE Systems Functionality Hierarchy
SF.1.1 Process Sensor Signals
SF.1.2 Perform Search
SF.1.3 Perform Detection
SF.1.4 Sensor Management
SF.1.1.1 Receive, Process, and Classify Signals
SF.1.1.2 Process Identification Friend or Foe Signals
SF.1.2.1 Search with Active Sensor
SF.1.2.2 Search for Acoustic Signals
SF.1.2.3 Search Navigation Signals
SF.1.3.1 Detect Images
SF.1.3.2 Detect lectromagneti Signals
SF.1.3.4 Detect Threats
SF.1.3.5 Detect Navigation Signals
SF.1.4.1 Fuse Sensor Data
SF.1.4.2 Manage Sensors
SF.1.4.3 Generate Sensor Tasking

Figure 31. C-UAS Sense Systems Functionality Description

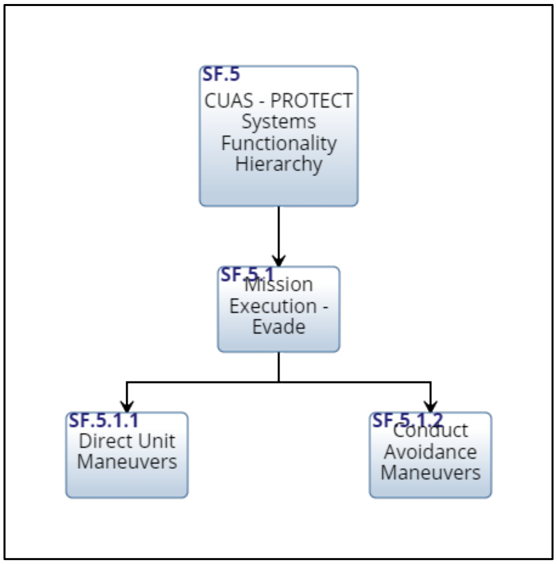

SF.5
CUAS - PROTECT Systems Functionality Hierarchy
SF.5.1
Mission Execution - Evade
SF.5.1.1
Direct Unit Maneuvers
SF.5.1.2
Conduct Avoidance Maneuvers

Figure 32. C-UAS Protect Systems Functionality Description

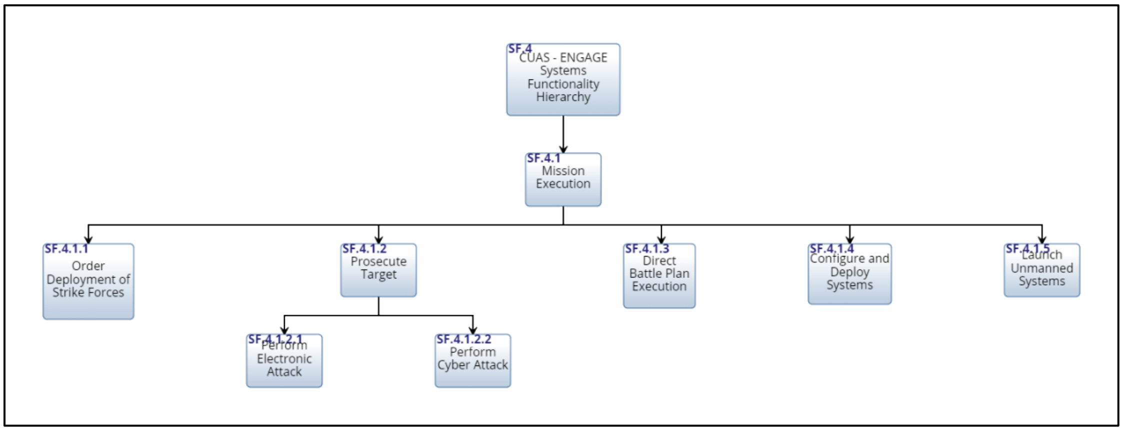
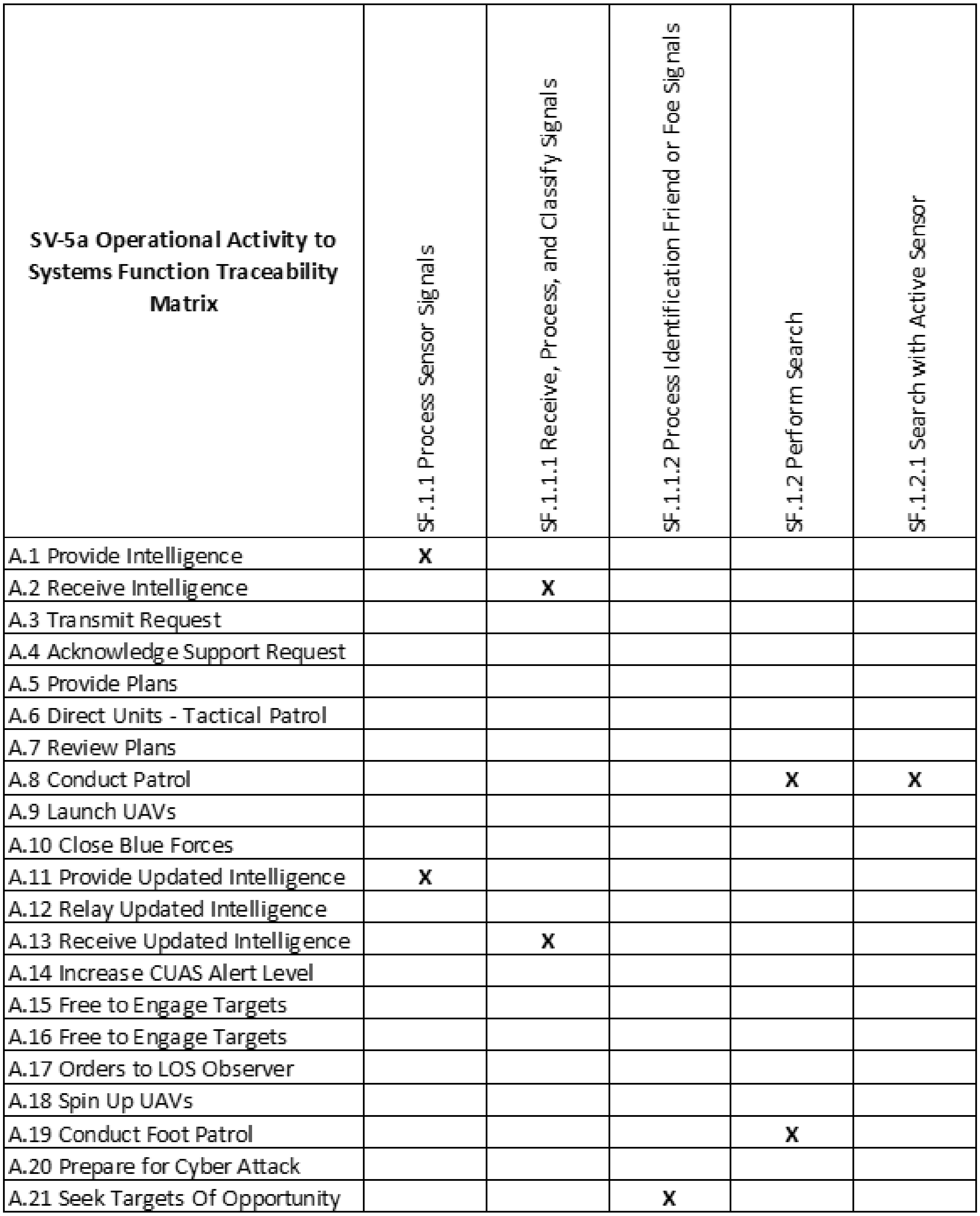

SF.4
CUAS - ENGAGE Systems Functionality Hierarchy
SF.4.1
Mission Execution
SF.4.1.1
Order Deployment of Strike Forces
SF.4.1.2
Prosecute Target
SF.4.1.2.1
Perform Electronic Attack
SF.4.1.2.2
Perform Cyber Attack
SF.4.1.3
Direct Battle Plan Execution
SF.4.1.4
Configure and Deploy Systems
SF.4.1.5
Launch Unmanned Systems

Figure 33. C-UAS Engage Systems Functionality Description

3. Operational Activity to Systems Function Traceability Matrix (SV-5a)

The Operational Activity to Systems Function Traceability Matrix (SV-5a) "is a specification of the relationships between the set of operational activities applicable to an Architectural Description and the set of system functions applicable to that Architectural Description" (DOD CIO n.d). The SV-5a was constructed to illustrate the traceability between the C-UAS Combat Patrol operational activities and system functions (0). Operational Activities are organized in the column headers and system functions are located in the row headers. The intersection of functionality provided for an operational task is indicated by the (*X*) symbol. Assessment of the C-UAS SV-5a should leave the user satisfied that there is a resource performer function identified for every C-UAS Combat Patrol task that must be performed. This assessment of results from the model helps to prevent activities from potentially being overlooked and ensuring any unnecessary redundancies did not creep into the project.

Table 15. Operational Activity to Systems Function Traceability Matrix (OV-5a) (excerpt)



SV-5a Operational Activity to Systems Function Traceability Matrix	SF.1.1 Process Sensor Signals	SF.1.1.1 Receive, Process, and Classify Signals	SF.1.1.2 Process Identification Friend or Foe Signals	SF.1.2 Perform Search	SF.1.2.1 Search with Active Sensor
A.1 Provide Intelligence	X				
A.2 Receive Intelligence		X			
A.3 Transmit Request					
A.4 Acknowledge Support Request					
A.5 Provide Plans					
A.6 Direct Units - Tactical Patrol					
A.7 Review Plans					
A.8 Conduct Patrol				X	X
A.9 Launch UAVs					
A.10 Close Blue Forces					
A.11 Provide Updated Intelligence	X				
A.12 Relay Updated Intelligence					
A.13 Receive Updated Intelligence		X			
A.14 Increase CUAS Alert Level					
A.15 Free to Engage Targets					
A.16 Free to Engage Targets					
A.17 Orders to LOS Observer					
A.18 Spin Up UAVs					
A.19 Conduct Foot Patrol				X	
A.20 Prepare for Cyber Attack					
A.21 Seek Targets Of Opportunity			X		

4. Operational Activity to Systems Traceability Matrix (SV-5b)

Whereas the SV-5a links system functions to operational activities, the Operational Activity to Systems Traceability Matrix (SV-5b) shows traceability between the operational activities and the systems that implement the operational performer tasks (DOD CIO n.d., Operational Activity to Systems Traceability Matrix). The C-UAS Combat Patrol SV-5b is outlined in Table 16.

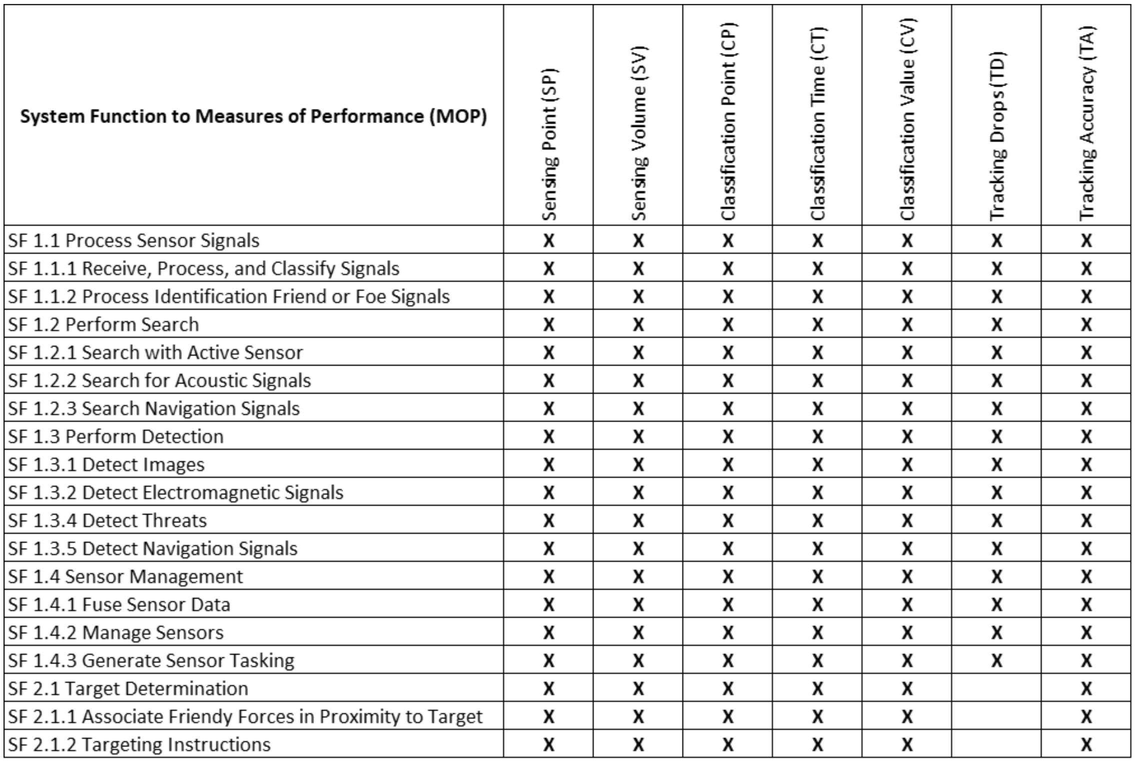
Table 16. C-UAS Operational Activity to Systems Traceability Matrix

SV-5b Operational Activity to Systems Traceability Matrix	1.1 ISR Cell	1.2 Task Force Commander	1.5 Tactical Convoy	1.8 LOS Observer	FN.4 Radar	FN.8 Low Energy Effects Platform	FN.9 Cyber Attack Platform	FN.10 Cyber Attack UAV	Company Commander
OA.1.1.2 Move Forces		X							
OA.1.2 Navigate and Close Forces		X							
OA.2 Develop Intelligence	X								
OA.2.2.1 Collect Target Information					X				
OA.3.2.5 Conduct Electronic Attack						X	X	X	
OA.3.2.7 Intercept, Engage, and Neutralize Enemy Aircraft and Missile Targets (DCA)				X		X	X	X	
OA.5.1 Acquire, Process, Communicate Information, and Maintain Status		X							X
OA.5.1.1 Communicate Information		X							X
OA.5.1.1.1 Transmit and Receive Information	X		X		X				
OA.5.4 Direct, Lead, and Coordinate Forces		X							X
OA.5.4.1 Direct Forces		X							
OA.5.5.1 Plan, Integrate, and Employ C2 Attack									X

5. C-UAS System Functions to Measures of Performance (SV-7)

Team DROSERA's goal is to ensure that the C-UAS SoS can exhibit the performance measures identified in Chapter III. To support that goal, it was necessary to map the MOPs to system functions. Table 17 was generated to perform this assessment with the system functions identified previously in this chapter along the vertical axis and the MOPs identified in Chapter III along the horizontal axis. A cursory audit of the table demonstrates that the identified system functions are sufficient to support an assessment of the defined measures of performance.

Table 17. Mapping of System Function to MOPs (excerpt)



System Function to Measures of Performance (MOP)	Sensing Point (SP)	Sensing Volume (SV)	Classification Point (CP)	Classification Time (CT)	Classification Value (CV)	Tracking Drops (TD)	Tracking Accuracy (TA)
SF 1.1 Process Sensor Signals	X	X	X	X	X	X	X
SF 1.1.1 Receive, Process, and Classify Signals	X	X	X	X	X	X	X
SF 1.1.2 Process Identification Friend or Foe Signals	X	X	X	X	X	X	X
SF 1.2 Perform Search	X	X	X	X	X	X	X
SF 1.2.1 Search with Active Sensor	X	X	X	X	X	X	X
SF 1.2.2 Search for Acoustic Signals	X	X	X	X	X	X	X
SF 1.2.3 Search Navigation Signals	X	X	X	X	X	X	X
SF 1.3 Perform Detection	X	X	X	X	X	X	X
SF 1.3.1 Detect Images	X	X	X	X	X	X	X
SF 1.3.2 Detect Electromagnetic Signals	X	X	X	X	X	X	X
SF 1.3.4 Detect Threats	X	X	X	X	X	X	X
SF 1.3.5 Detect Navigation Signals	X	X	X	X	X	X	X
SF 1.4 Sensor Management	X	X	X	X	X	X	X
SF 1.4.1 Fuse Sensor Data	X	X	X	X	X	X	X
SF 1.4.2 Manage Sensors	X	X	X	X	X	X	X
SF 1.4.3 Generate Sensor Tasking	X	X	X	X	X	X	X
SF 2.1 Target Determination	X	X	X	X	X		X
SF 2.1.1 Associate Friendy Forces in Proximity to Target	X	X	X	X	X		X
SF 2.1.2 Targeting Instructions	X	X	X	X	X		X

D. C-UAS SYSTEM CHARACTERISTICS

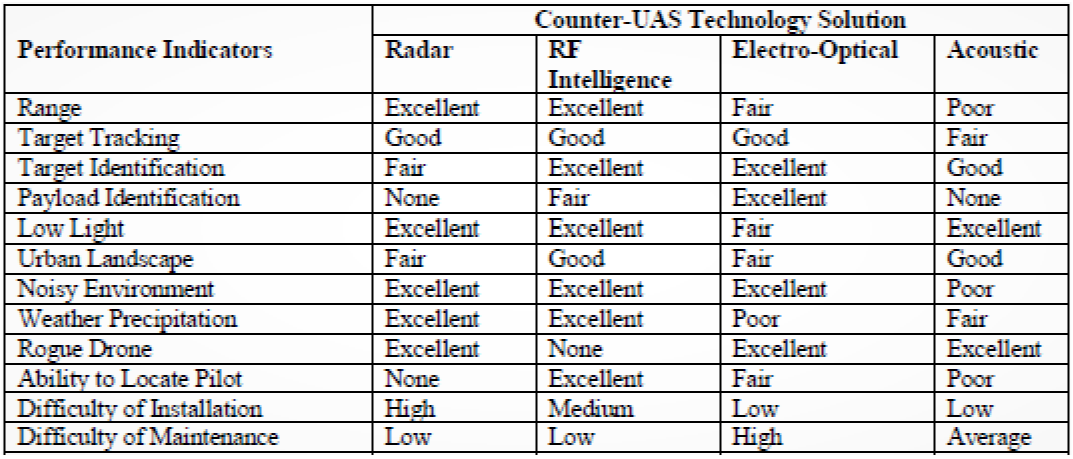
This section will summarize the different technologies that may be utilized in an effective C-UAS SoS. The DROSERA team reviewed commercially available open-source technical data to assist in applying quantitative values to the identified system functions of *Sense*, *Assess*, and *Neutralize*, where available. The *Sense* system function can be performed via either a radar system or an electro optical sensor. Additionally, the electro optical sensor can also support the C2 platform with *Assess* system function. Finally, for the *Neutralize* system function, the team has allocated that role to the cyber-attack UAV, cyber-attack platform, low energy effects platform, and high energy laser.

1. C-UAS Sense Technologies

Team DROSERA performed a literature review of C-UAS technologies available from commercial vendors. The purpose of this review was to review initial information collected detailing the existing technologies, manufacturers, and available products to assist in performing the tasks of detection, tracking, and identification of sUAS. The information presented in this report was collected via readily available information such as internet publications, professional literature, and original equipment manufacturer (OEM) technical brochures. The intent of this section is not to serve as an all-encompassing review of available technologies but rather a preliminary literature synthesis of currently available C-UAS technologies. The literature information gathered through this process was used to perform an initial selection of commercially available C-UAS products and did not take into consideration availability in the U.S. market.

As previously discussed, the capstone team did not find one singular C-UAS product that utilizes a single type of sensing technology capable of addressing all of the previously mentioned challenges in detecting, tracking, and identifying sUAS. Table 18 was developed by researchers at the University of Massachusetts Amherst to provide a summary of the strengths and limitations of C-UAS technologies based on their performance criteria (Plotnikov 2019, 13). This summary supports the assertion that there is no single most effective C-UAS technology present; however, it can help to guide when designing a C-UAS SoS solution.

Table 18. C-UAS Technology Performance Indicators. Source: Plotnikov (2019).



Performance Indicators	**Counter-UAS Technology Solution**			
	Radar	**RF Intelligence**	**Electro-Optical**	**Acoustic**
Range	Excellent	Excellent	Fair	Poor
Target Tracking	Good	Good	Good	Fair
Target Identification	Fair	Excellent	Excellent	Good
Payload Identification	None	Fair	Excellent	None
Low Light	Excellent	Excellent	Fair	Excellent
Urban Landscape	Fair	Good	Fair	Good
Noisy Environment	Excellent	Excellent	Excellent	Poor
Weather Precipitation	Excellent	Excellent	Poor	Fair
Rogue Drone	Excellent	None	Excellent	Excellent
Ability to Locate Pilot	None	Excellent	Fair	Poor
Difficulty of Installation	High	Medium	Low	Low
Difficulty of Maintenance	Low	Low	High	Average

As Table 18 indicates, there are many different technologies available and in use to detect, track, identify, and counter sUASs. Each technology has different physical operating principles. As identified in Chapter III, section III.D.2.a, the primary parameters related to system performance include the detection, tracking, and identification ranges. In the context to the C-UAS Combat Patrol scenario, these measures have a direct impact on the amount of time that ground forces have to respond and apply effective countermeasures. A graphical depiction the different ranges of detection for a radar-based system, an electro-optical system, and acoustic detectors can be found in Figure 34 (Plotnikov 2019, 9). The horizontal axis depicts the distance from the incoming drone to the defined protected area.

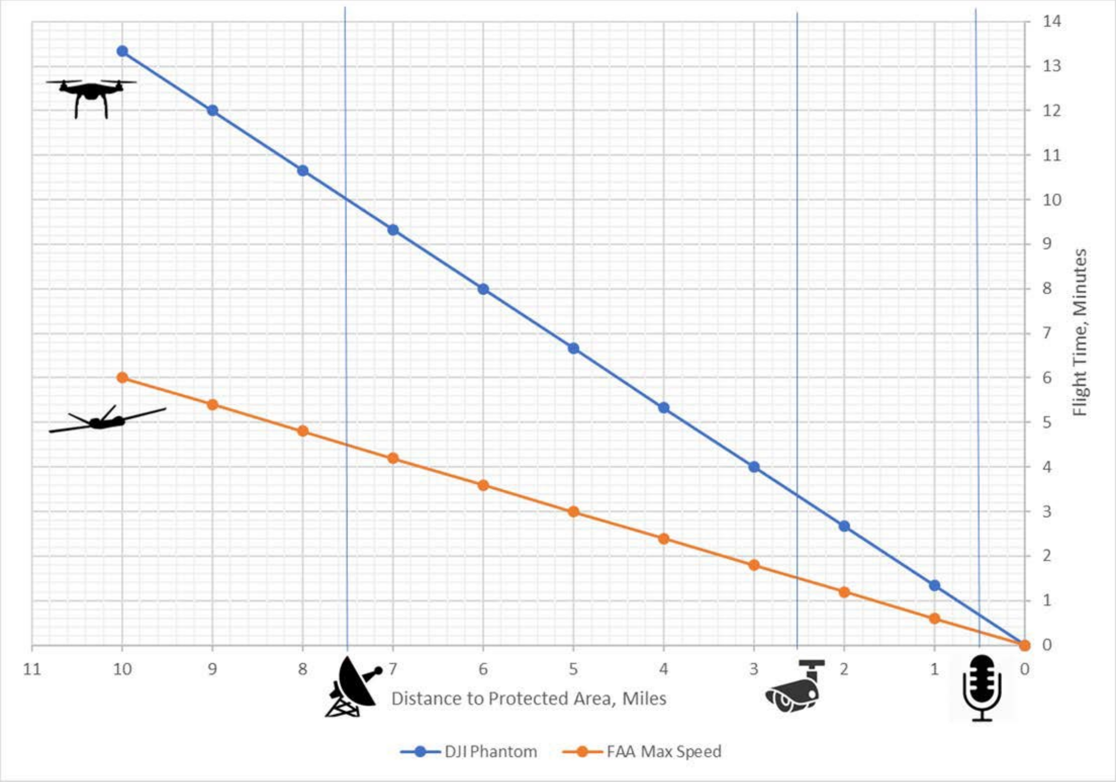


Figure 34. Typical Detection Ranges of Various C-UAS technologies vs. UAS Flight Time. Source Plotnikov (2019).

A review of Figure 34 indicates a typical detection range for a radar-based system is 7.5 miles, an electro-optical based system is 2.5 miles, and an acoustic detector is approximately 0.5 miles. The ranges for UAS detection are shown on the horizontal axis with a corresponding system icon depicting each systems respective detection range. The vertical axis depicts the travel time the UAS will take to enter into the protected area. The longer the detection range, the longer period of time before the adversarial UAS will enter into the protected area. The lines inclining from the axis origin represent the two different types of UAS approaching the protected area. The blue line is representative of a quadcopter of the DJI Phantom class type drone. This sUAS has an approximate cross section of 0.25 to 0.3 square meters and can travel at a maximum speed of 45 mph. The orange line depicts a fixed-wing type drone that can travel at a maximum speed of 100 mph and has a similar reflective surface as the DJI Phantom class.

It should be noted that the ranges depicted in the graph are under ideal conditions and do not take into consideration land topography, obstructions, weather, etc. (Plotnikov 2019, 8). As depicted, the radar system has the greater detection range when compared to the electro-optical sensor and an acoustic sensor. The RF system ranges are not depicted in this graph because the typical range can vary drastically between systems and are dependent on the transmitters power output, radio frequency and the communication link between the sUAS and its associated ground controller. An additional reason for not depicting RF system ranges is in relation to the variability in antenna and amplifier type that are utilized in the given RF C-UAS system. According to Plotnikov: "…the detection range of the stationary system from the same manufacturer with a complex array of directional antennae and a high sensitivity amplifier can increase the detection range to up to 10 times as far." (Plotnikov 2019, 9).

2. C-UAS Assess Technologies

The detection and identification of sUAS can be difficult based on the fact that that these systems are typically low-flying and small objects. This presents an added level of difficulty to the detection, which can then decrease the timeline of response. The timeline between the initial detection of the sUAS and the identification that it is going to pose an immediate and real threat can be very short. This highlights the importance of the decision-making process being performed in a relatively quick order. The C-UAS system chosen to perform the initial detection is the first critical piece to help increase the time decision makers have on what, if any, threat may be present. These C-UAS systems need to be flexible enough to support the detection and ultimate neutralization of unmanned systems that come in a variety of sizes and shapes. There also are requirements for detection systems that have a direct impact on the assessment and decision-making process. Key C-UAS detection requirements include the ability to reliably detect and limit false positives, the ability to classify and identify, the ability to determine intent, the ability to distribute information to the human decision maker, the ability to integrate into a larger system, and the ability to perform the actions in a timely manner (Dominicus 2022, 8).

As mentioned previously, there does not currently exist a single sensor system that can fulfill all of these requirements in all possible scenarios against all different types of sUAS. Therefore, the SoS approach is still the desired C-UAS approach to support the detection of the sUAS across the different energy spectrum, then cue the sensors and mitigation measures to intervene and destroy the sUAS before it can complete its intended mission set. Ultimately, the assessment function of a C-UAS system comes down to supplying timely and accurate data to the decision maker on how to address a potential incoming threat. As identified in Dominicus:

> Other C-UAS systems now being used employ an active radar for initial detection and an electro-optical (EO) sensor for further investigation and identification of the contact. In present systems, the radar has an operator who hands over the radar contact to the operator of the EO system. Decision-making on intervention can be performed by these two operators or is delegated to a higher echelon (Dominicus 2022, 2).

Deploying a system with multiple sensors is important in ensuring reliable detection and allows for an accurate assessment to be made. This transfer of information is necessary to reduce the number of false positive and to enable a reliable assessment and identification on the sUAS of interest (Dominicus 2022, 15). The sensor data that is shared from each source is then relayed to the human operator to make the assessment decision on how to respond to the potential threat. The sensor data of the surrounding environment is collected from one or more sensors which is then shared with the C2 system. The C2 system executes a detection algorithm based on the sensor data provided. The reliability of the sensor data should be as high as possible as the C2 system will then perform its threat analysis to then determine a mitigation strategy and select the appropriate neutralization tactic to employ. This collected sensor data is how the C2 system will establish whether the sUAS is a threat or not and then must decide the appropriate tracking and mitigation mode to employ (Castrillo et al. 2022).

While this process is human-in-the-loop dependent, the future of detection, assessment and decision-making will rely on the ability to combine these various sensors into an overall C-UAS SoS and to automate the process. This will apply the concept of sensor fusion where the integration of these systems can be combined with existing C2 infrastructure and help to reduce the manpower requirements to operate the system. This process of sensor fusion can also help reduce the amount of time needed to decide on intervention and may allow the assessment and decision process to be fully automated (Dominicus 2022, 2). Current C-UAS systems can provide the operator with a two-dimensional topographical view along with alerts provided to draw the operator's attention to newly identified potential threats. The implementation of sensor fusion can provide a more sophisticated display and prioritized list of threats that are updated in real time as the situation unfolds. Dominicus expands further on the decision support this next generation SoS approach can provide:

> True decision support would also incorporate available effectors and advise on what effector to use on what target, taking into consideration what the desired effect is on that specific target. …Second generation decision support systems should migrate from having humans-in-the-loop towards having humans-on-the-loop. …The focus on the development of decision support systems should be to match available effectors with targets, minimize the risk of erroneous (proposed) decision, shortening timeliness and reducing manpower requirements (Dominicus 2022, 15).

A research study was conducted to explore if the accuracy of real-time drone detection for C-UAS systems can be improved upon. This was conducted by training three existing object detection models utilizing different images of drones to develop the drone detector further (Cetin 2021, 1871). Once the training of the models was completed, the researchers then tested the detection algorithms by providing them with previously unseen images of drones. The overall score for each detection system was deduced based on the comparison between true positives, true negatives, false positives, and the false negatives (Cetin 2021, 1883). The research demonstrated that when using brand new drone images simulated from the internet, the EfficientNet-B0 model has an accuracy rate of detection of 95%. Conversely, the same model was tested with simulated images containing no drones and showed an accuracy of 80%. This research demonstrates promising results that drones can be accurately detected using a real time object detection algorithm to speed the detection process (Cetin 2021, 1886). Providing accurate and timely detection of adversarial drones is one critical process of the C-UAS kill chain by providing other C-

UAS systems the necessary data to make a well informed decision on whether to deploy neutralization effects against the identified drone.

3. C-UAS Neutralize Technologies

The third system function in the C-UAS effects chain is the neutralize action. This function can be performed by a various number of different platforms dependent on the needs of the C-UAS system architecture. The sensing systems provide their gathered data and transmit their observations to the C2 system. The C2 system then either aids or autonomously performs the decision making based on the detection / identification / classification data received from the sensing platform to then decide what mitigation system should be employed to counter the identified adversarial UAV. If supported by the C-UAS system architecture, the C2 system can employ several neutralization systems simultaneously to cooperatively address the adversarial UAV. Figure 35 provides a visual description of the UAS mitigation process.

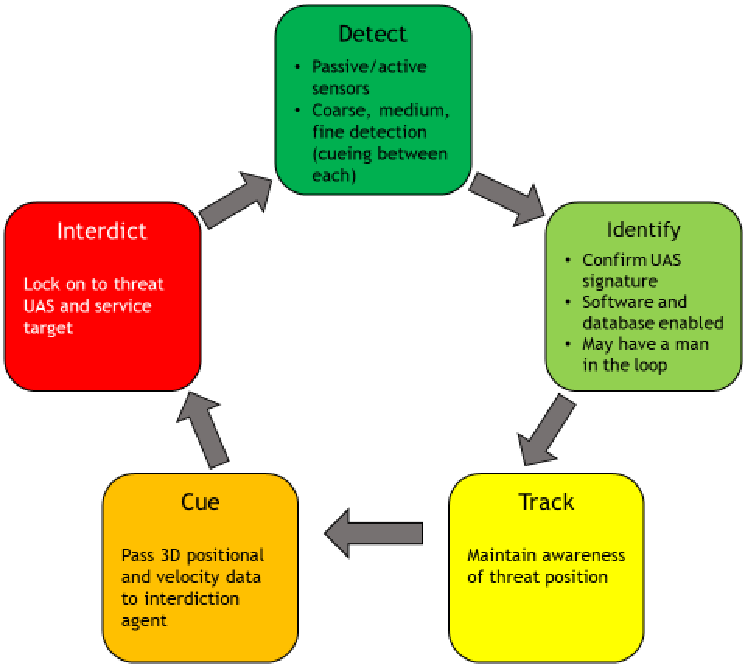

Detect
• Passive/active sensors
• Coarse, medium, fine detection (cueing between each)
Identify
• Confirm UAS signature
• Software and database enabled
• May have a man in the loop
Track
Maintain awareness of threat position
Cue
Pass 3D positional and velocity data to interdiction agent
Interdict
Lock on to threat UAS and service target

Figure 35. UAS Mitigation Process.
Source: Cline (2020).

Neutralization methods fall into the two main categories of kinetic effects and non-kinetic effects. Non-kinetic effects are those employed where there is no direct and physical contact between the adversarial system and the mitigator. These non-physical mitigation methods can include high-powered electromagnetics, lasers, and several cyber-attack methods previously discussed in Chapter II. Examples of the kinetic neutralization effects can include the usage of projectiles or potential usage of collision UAVs with the sole purpose of detecting and tracking to crash into and destroy an adversarial UAV (Kang et al. 2020).

There is not a neutralization system that is 100 percent effective and each previously mentioned method has its respective drawbacks. A drone that is physically destroyed via kinetic means would pose a threat by falling out of the sky with some potential force behind it. These destructive effects, no matter the precautions employed, will generate falling debris from the drone and should be considered a last line of defense (Tewes 2017). There is also the need for the system performing the kinetic interdiction to be extremely precise to ensure it can hit is intended target to minimize the potential effects to an innocent bystander. The UAV is often a fast-moving target that can also be flying an unpredictable path.

On the non-kinetic side, jamming can also interfere with communications that are from a legitimate link that is within the area of employment resulting in an interference that was unintentional. There is also the instance that RF jamming could have no effect against the adversarial sUAS if it is operating without an active RF link and a limited range of effectiveness of a few hundred meters (Michel 2019, 9). With the desire to thwart potential jamming or spoofing, commercial industry has been active in developing drones that can operate in a GPS-denied environment or additionally programmed to evade certain jamming frequencies or switch frequencies during flight to avoid interdiction. One additional real-world threat is the lack of information available for deployed systems and their effectiveness. Michel outlined this issue in their report:

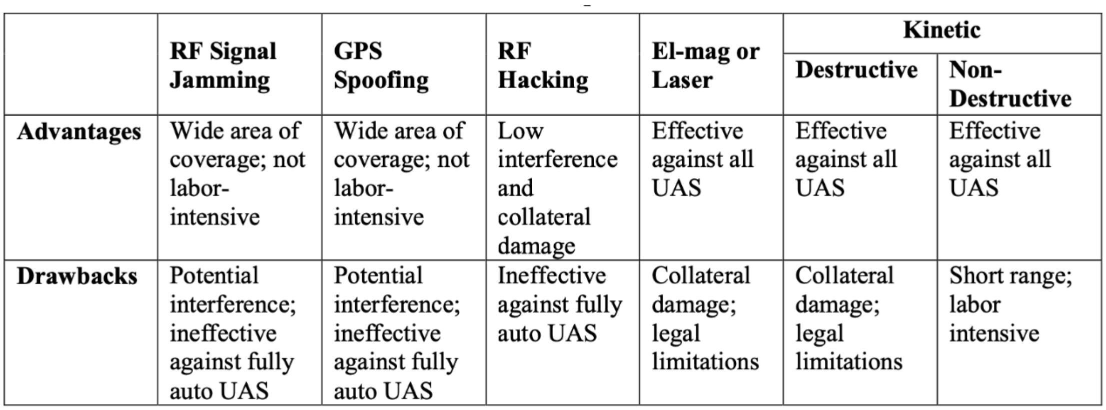
> Not a single C-UAS manufacturer approached in the preparation of this report would provide details about their product’s performance in real-world use. This information vacuum makes it difficult for would-be C-UAS owners to know what actually works and what doesn’t, anticipate potential

> issues, and select a system that is best suited to their needs (Michel 2019, 11).

The employment of electronic neutralization methods has also been utilized as an effective C-UAS line of defense. Lasers as a C-UAS interdiction method have demonstrated promise as one such non-kinetic method. UAS are susceptible to attack by a laser system as they require much less energy to thwart. A laser with as little has two kilowatts of energy has been demonstrated to successfully take down a consumer drone (Tewes 2017). Laser interdiction also holds a distinct advantage over kinetic effects in that the cost per engagement is lower along with a lower risk of unintentional consequences or collateral damage to nearby systems.

Cyber-attack via either jamming or spoofing constitutes the more common electronic neutralization techniques employed. When attacking a UAS susceptible to jamming, the jammed system could potentially respond by landing where it is currently located, execute a return to home, or it could descend out of the sky to the ground or fly with no positive control in a random direction. It is also possible to jam the remote system that is controlling the drone. Similarly, when performing GNSS jamming, the GPS receiver of the jammed drone can cause the drone to drift and instigate control difficulties (Castrillo et al. 2022). Often it is desired to employ both RF and GNSS jamming so each can compensate for the others weakness. For example, GNSS jamming is ineffective when a drone is equipped with a remote-control link, and conversely RF jamming is ineffective when a drone is not equipped with a remote link. Table 19 contains a summary highlighting some of the advantages and drawbacks of the different C-UAS neutralization methods that may be employed.

Table 19. C-UAS Interdiction Methods: Advantages and Drawbacks. Source: Plotnikov (2019).



	RF Signal Jamming	GPS Spoofing	RF Hacking	El-mag or Laser	Kinetic	
					Destructive	Non-Destructive
Advantages	Wide area of coverage; not labor-intensive	Wide area of coverage; not labor-intensive	Low interference and collateral damage	Effective against all UAS	Effective against all UAS	Effective against all UAS
Drawbacks	Potential interference; ineffective against fully auto UAS	Potential interference; ineffective against fully auto UAS	Ineffective against fully auto UAS	Collateral damage; legal limitations	Collateral damage; legal limitations	Short range; labor intensive

4. C-UAS Resource Architecture Technical Performance Measures

The system performers identified in the systems architecture in support of the C-UAS mission scenario included a cyber-attack UAV, cyber-attack platform, radar, optical sensor, low energy effects platform, and a high energy laser. A literature review was conducted by Team DROSERA to investigate commercially available C-UAS technologies that could be evaluated in support of C-UAS SoS Modeling. The intended generalized SoS approach for the C-UAS mission scenario required the team to investigate commercially available C-UAS technologies and to capture any available technical performance measures for each system. The technical performance measures captured in this section represent the range of values that the DROSERA project will utilize for system measures exhibited by each respective C-UAS system type.

a. Cyber-Attack UAV

Not all systems under consideration are currently commercially available. One such example is the cyber-attack UAV. This system is based on the previous thesis work presented by Lee (Lee 2022). The cyber-attack UAV is comprised of a Skydio2+, a Raspberry Pi 4 Model B+, and a Wi-Fi Antenna. The cyber-attack UAV parameters are outlined in Table 20.

Table 20. Cyber Attack UAV Performance Measures. Adapted from Lee (2022).

Cyber Attack UAV Parameters	
Maximum Detection Range:	250 meters
Time to Detect and Classify target:	Lognormal distribution (Mean = 4.92s, Std = 2s)
Time to Neutralized Target:	Lognormal distribution (Mean = 9.83s, Std = 2s)
Probability of Success for Detect & Attack Actions for 1x UAS:	0.8
Power Consumption to Detect 1x Adversary Drone:	1.54 Watt
Power Consumption to Attack 1x Adversary Drone:	1.59 Watt

b. Cyber-Attack Platform

A representative C-UAS system to fulfill the cyber-attack platform role in the mission scenario that is capable of performing both detection and mitigation of an adversarial sUAS is the EAGLE108 manufactured by Phantom Technologies (Figure 36). There are several additional commercial systems available that perform RF signal detection and RF jamming along with sUAS detection with the EAGLE 108 serving as a viable representative for many of these systems. The EAGLE 108 is also an ideal candidate for use in this project because the technical data is readily available. This system is capable of consistent detection and tracking with a detection and mitigation range of 1000 meters. The EAGLE108 has an RF jamming capability to neutralize the adversary drones by jamming the sUASs downlink signal. The system operates at Wi-Fi signal bands of 2.4GHz and 5.8GHz with an output transmission power of 375W. The estimated time from drone detection to mitigation is 15 seconds (Lee 2022).

Figure 36. Tactical Drone Jammer Model EAGLE 108.
Source: Phantom Technologies (2022).

c. Radar

When it comes to detecting aircraft, a Radar system does hold advantages over other sensors in terms of the effects of weather, night and day operational capability, and the ability to measure velocity and range simultaneously. The challenge arises with sUAS in that their radar cross sections (RCS) are very small and they fly at lower speeds and altitudes compared to larger aircraft. A traditional radar system is designed to detect medium and large size aircraft (RCS larger than 1m^2). This can pose a challenge when the goal is to detect UAVs. There are several types of available radar that are designed specifically for the detection, tracking and classification of drones that can be classified into two categories: active detection and passive detection radars. The main disadvantage of active detection radars is the necessity for a specialized transmitter to be designed which can be difficult to deploy. The main disadvantage to passive radar is to receive a higher detection accuracy, there is a large effort in the post-processing of data and the possibility of having multiple receivers to deploy (Besada 2022).

For this project, the team identified one commercially available active radar and one passive radar system. The commercially available active radar system identified is the ART Midrange 3D. The radar is designed for the purpose of detecting, tracking, and classifying sUAS, specifically micro quadcopters and micro fixed-wing UAVs. The main specifications were obtained from Besada (2022) and are detailed in Table 21.

Table 21. ART Midrange 3D Active Radar Specifications. Adapted from Besada (2022).

Specification	Value
Frequency Band	Ku-band
Bandwidth	1 GHz
Elevation Control	+/- 5 degrees
Instrumental Detection Range	5000 m
Coverage Area	78 km^2
Azimuth Coverage	360 degrees
Scan Rate	60 rpm
Range Resolution	1 m - 0.2 m
Range Accuracy	0.25 m - 0.05 m
Communications	TCP/IP over Ethernet
Protocol	XML-based on NMEA0183

The passive radar system evaluated for the capstone project is the Doruk UAV Detection radar. The radar was designed specifically for detecting low altitude target moving over land or sea. The radar is capable of performing detection and classification to include angle, range, RCS, radial velocity, heading, width of Doppler Frequency Spectrum, and large tracking over a map of the targets (Doruk 2022). The main specifications are detailed in Table 22.

Table 22. Doruk Passive Radar Specifications. Adapted from Doruk (2022).

Specification	Value
Frequency band	X-Band
Detection Probability	80%
Detection Range	6 km
Detection Velocity	0.2 - 100 m/s
Elevation beamwidth	20◦
Azimuth accuracy	≤1◦ (RMS)
Azimuth resolution	≤2◦
Azimuth coverage	360◦
Range accuracy	≤5 m
Range resolution	≤15 m
Velocity accuracy	≤0.2 m/s
Scanning rate	90 ◦/s
Target Tracks	>200, Track While Scan
Clutter suppression	≥45 dB

d. Optical Sensor

The main purpose for an optical sensor as part of the proposed C-UAS SoS is for image processing and threat sUAS classification. The camera and video can be utilized to capture images of the approaching UAVs and use that information to estimate the UAVs position. As part of the optical sensor, there is often a software or online recognition system that can perform the initial identification of approaching 3D objects. One experiment conducted utilized neural networks to identify the appearance of UAVs. The results of that experimentation were summarized in Besada and included below:

> The authors developed a system that is capable of detecting, recognizing, and tracking a UAV using a single camera automatically. For that purpose, a single Pan–Tilt–Zoom (PTZ) camera detects flying objects and obtains their tracks; once a track is identified as a UAV, it locks the PTZ control system to capture the detailed image of the target region. Afterward, the images can be classified into the UAV and interference classes (such as birds) by a convolution neural network classifier trained with an image dataset. The identification accuracy of track and image reaches 99.50% and 99.89%, respectively. This system could be applied in a complex environment where many birds and UAVs appear simultaneously. (Besada 2022)

While the additional performance specifications for the PTZ camera used in the experiment were not specified, there exist several commercially available cameras that can perform the video and image capture similarly. For this project, Team DROSERA chose to utilize Triton PT-Series HD Camera from FLIR Enterprise. The PTZ optical sensor has a very high range and can be integrated into the C-UAS SoS for video and image capture. The technical specifications were found are outlined below in Table 23.

Table 23. Triton PT-Series HD Camera Specifications. Adapted from Besada (2022).

Specification	Value
Range	2–4 km (depending on visibility conditions)
Min Illumination/light sensitivity (color)	0.01 lux
Max video resolution	1920 × 1080
Focal length	4.3–129 mm
Field of view (min-max)	21◦ × 28◦ W 1.5◦ × 2◦ N
Lens field of vie (min-max)	2.3◦–63.7◦
Pan range	360◦
Pan velocity	0.1 to 60◦/s
Tilt range	−90◦ to +90◦
Tilt velocity	0.1 to 30◦/s
Optical zoom	120
Digital zoom	22

e. Low Energy Effects Platform

Team DROSERA is defining the Low Energy Effects platform as a generalization of potential C-UAS systems that would perform in the engage, or neutralization portion of the C-UAS effects chain. These systems would include the previously identified cyber-attack platform and cyber-attack UAV along with a handheld RF jammer and a mobile ground attack system. The Dronebuster Block 3B (Figure 37) is advertised as the only handheld electronic attack defeat solution approved for use by DOD. The system is a compact and lightweight C-UAS system that can be deployed to defeat COTS drone threats. The system is also able to covert from a fixed site jammer into a man-portable jammer for dismounted troop use in combat-fluid C-UAS situations. The system is battery operated but can also support external DC-power for continuous operation. When operating on battery power, the Dronebuster has a battery endurance of 45+ minutes of jamming and 10+ hours of detection. For GNSS frequency jamming, directional emissions are utilized to minimize inadvertent GNSS disruption of civilian GNSS frequencies (Flexforce 2021).

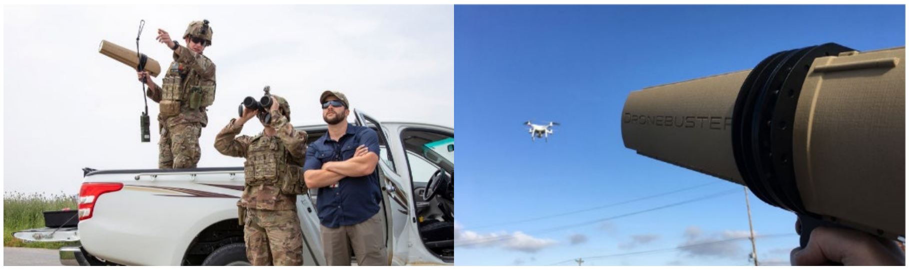


Figure 37. Dronebuster Block 3B Handheld RF Jammer.
Source: Flexforce (2021).

For the literature review conducted by Team DROSERA on potential commercially available mobile attack platforms, the team identified the FLIR LVSS C-UAS Mobile Surveillance with Air Domain Awareness (ADA) and Counter UAS Capabilities platform. The platform, displayed in Figure 38, is a rapidly deployable and relocatable surveillance solution to support large areas with UAS detection capabilities. The platform can perform both threat detection and non-kinetic RF countermeasures which provide full C-UAS kill chain support. This platform was also chosen as all of the sensors and effectors as implemented are at a high technology readiness level (TRL) and can be configured to meet specific user requirements. The system utilizes a 3D Radar, EO/IR Camera, and both RF detection and mitigation sensors. The threats can be simultaneously displayed and detected with supporting position and elevation for the radar tracks (Teledyne, 2021). Table 24 represents a summary of FLIR LVSS C-UAS ADA system performance measures.

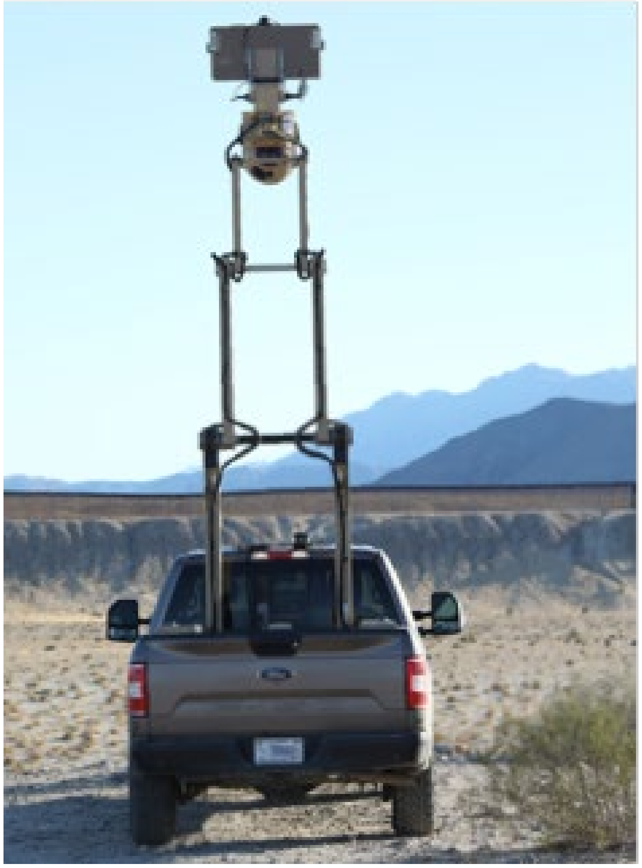


Figure 38. FLIR LVSS ADA C-UAS Mobile Attack Platform.
Source: Teledyne (2021).

Table 24. FLIR LVSS ADA C-UAS Mobile Attack Platform Specifications.
Adapted from Teledyne (2021).

Specification	Value
Weight	Approx 7700 lbs
Radar	R20SS-3D Long Range Ground Surveillance
Camera	TacFLIR-380 HD
Simultaneous tracking	>500 targets
RF sensor	Standard RF Sensor Kit: 2.4 GHz / 5.8 GHz / Wi-Fi; Extended Frequency Kit: 433 / 868 / 915 MHz / 1.2 GHz / Wi-Fi

Table 24 (continued)

Detection range	Up to 3km horizontal, 457m vertical
Defeat range	Up to 1.5 km horizontal, 457m vertical
RF power output	Up to 30 Watts

f. *High Energy Laser*

The Elector Optics Systems Holdings Limited (EOS) Directed Energy (DE) system utilizes a high-powered laser as its kinetic defense against adversary UAS systems (Figure 39). The DE system was developed as an additional element of the manufacturers Titanis UAS defense system and is designed to disable Groups 1, 2, and 3 UAS systems. The system itself, along with the laser, is also complimented with a radar system, and infrared threat detection, and target acquisition and beam locking. The system is also capable of continuous operation if hooked up to an external electrical power source. The advantage of this system is it can complement other potential kinetic effects C-UAS systems, such as guns or cannons, with the advantage of minimization of collateral damage from potential rounds flying past their intended target (EOS 2022). The laser has demonstrated successful disablement of Group 1 drones at a rate of 20 drones per minute at ranges of above 1,000 meters. Other kinetic weapons can each neutralize 5–6 drones per minute which could be challenged by a swarm capability, which can readily be 20 drones per minute. Table 25 represents a summary of EOS Directed Energy System performance measures.

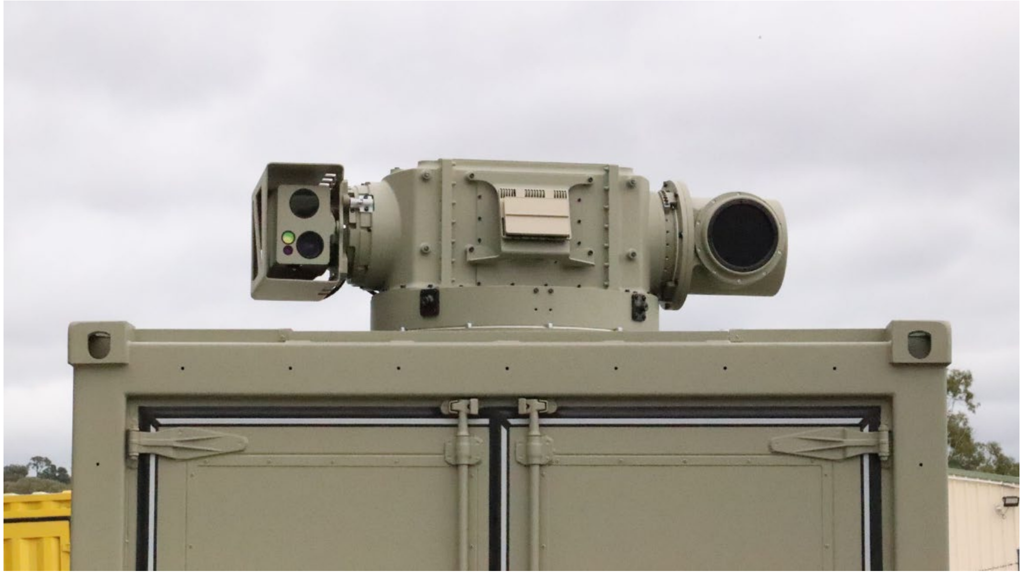


Figure 39. EOS Directed Energy System. Source: EOS (2022).

Table 25. EOS Directed Energy System Titanis Specifications. Adapted from EOS (2022).

Specification	**Value**
Laser Power	25 kW, 35 kW, or 50 kW
Laser Beam Elevation	+90° to −10°
Laser Beam Stability	0.1 mrad
Engagement Target Lock	500 msec
Target Neutralization (Group 1)	1.3 sec (35 kW)
Target Neutralization (Group 2)	4.4 sec (35 kW)
Engagement Range	200 m to 3 km (typical)
Sensor Detection Range	>12,000 m
Sensor Recognition Range	>5,600 m
Sensor Identification Range	>4,700 m

E. SUMMARY OF CHAPTER IV

This chapter discussed the derived system context and functional requirements to develop the baseline System of Systems architecture. This included analyzing the scope of the system and connecting operational and systems architecture models by illustrating how resources are structured and interact to realize the architecture. The chapter also detailed a high-level functional analysis of the system. These analyses facilitated the development of a generalized physical architecture. This architecture focuses on the system functions derived by the functional analysis for mission success. The previously identified MOPs from Chapter III were mapped to the identified systems functions. Finally, technical performance measures were captured for the system performers identified in the operational scenario to be simulated. These performance characteristics will help aid in the development of the design of experiments to be outlined in the next chapter.

V. ARCHITECTURE ASSESSMENT

As a result of asymmetric warfare, the application of an effective C-UAS solution is a concern for all warfighters and it is thus important to accurately capture the operational environment, element behavior, and effectiveness of these systems. These systems, however, cannot be isolated when determining their success as aside from the intended influence they impose on UAS threats, they additionally affect both other C-UAS, as well as non-C-UAS infrastructure, in a variety of significant manners. This is especially true as it is beneficial to deploy these capabilities with a defense in depth distribution in mind, layering several C-UAS infrastructures alongside each other bolstering strengths and mitigating weaknesses across systems, complicating the individual C-UAS system within its position of an overarching system of systems that must work cohesively.

The ME analysis approach adopted by this project is informed by the DOD ME Guide (DD-ENG 2020, 17–24). ME analysis evaluates missions by examining the interaction between the operational environment, threat, activities, and systems used in present or future missions. The mission architecture represents the detailed structure of the conduct of the mission and is detailed in III. Operational Analysis. The DROSERA project will evaluate C-UAS vignettes through simulation analysis. Specifically, ME assessment will construct and represent data that is traceable to system performance measures identified in Resource Architecture and model the mission definition such that it executes the previously identified event chain, demonstrating the end-to-end mission, and answering the fundamental questions of the problem statement, which are set forth by the C-UAS capability MOEs.

With the challenge of evaluating a growing number of sUAS, C-UAS systems, and other participants within a setting, a modeling and simulation (M&S) environment is needed. This project developed the DROSERA analysis tool as its C-UAS M&S environment. The DROSERA analysis tool relies on agent-based modeling (ABM), a method of representing complex systems of autonomous objects and simulating the outcomes of these objects' behaviors and interactions through the enactment of rule-based or programmatic decisions that result in an array of potential outcomes (Nicholls, Amelung, and Student 2017, 3). Monte Carlo methods will be applied to the ABM scenarios to generate non-deterministic behaviors associated with the operational scenario. While a variety of techniques and simulation tools were evaluated, team DROSERA selected AnyLogic Personal Learning Edition (AnyLogic North America n.d.) as the modelling software for developing the DROSERA analysis tool. This application was chosen as it supports ABM, contains easy-to-use libraries and manuals, and is free-to-use for educational purposes.

It is a desired objective that the DROSERA Analysis Tool be continuously improved to the extent that it could be validated for use as a constructive simulation tool suitable for C-UAS *Concept Exploration* and *Evaluation and Design and Development* within the Defense acquisition process. A validated DROSERA Analysis Tool would offer a low-cost M&S solution, enabling high reusability and repeatability while providing scope and risk reduction for the Virtual/Live testing that will be required later in the acquisition life cycle. Test scenarios can be built in this constructive environment in direct accordance with what the system would see if it were to undergo a live testing environment.

A. MODELING ARCHITECTURE

The DROSERA analysis tool aims to capture the mutual relationships of systems and the dynamic nature of these environments that will help illustrate mission effectiveness, asset preparedness, and projected resource requirements of capability deployment. To determine system effectiveness within this complex space, it is practical to model all possible C-UAS capabilities deployed, the environment in which they are being deployed, and interactions between not only other C-UAS systems, but also UAS threats. More specific to the goals of this project, the results of the DROSERA analysis tool will shape design and operation recommendations for C-UxS based on energy requirements, and explore cyber-attacks as a low energy, high impact alternative or addition to existing C-UxS systems, providing a defense in depth capability.

In order to capture and exhibit the innumerable permutations of behaviors that can be expressed within the C-UAS operational scenario, a modeling architecture is required. The C-UAS Modeling Architecture (Figure 40) references all model elements of the C-

UAS mission characterization to include system performance characteristics, threat sUAS performance characteristics, environmental conditions, and capability metrics. Multiple instances of the model elements can be constructed to conform to the performers required in the mission scenario, with scenario-based logic applied analytically and programmatically to each element for autonomous behavior. The modeling architecture also specifies the projected trial outcomes associated with each performer, traceable to system performance metrics. The modeling architecture assumes an ABM is employed the computational model for simulating the actions but is specified to be tool-agnostic.

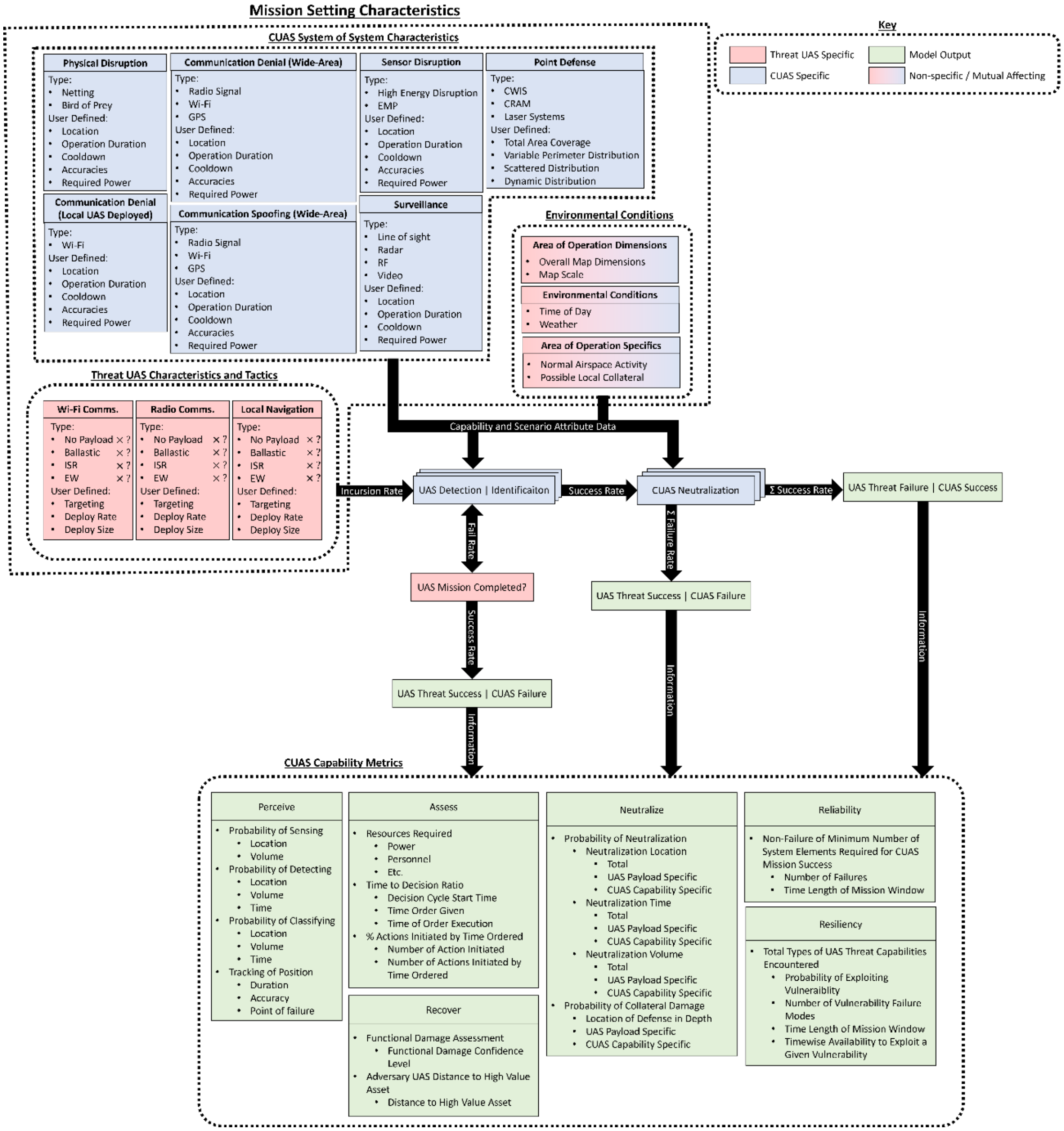


Figure 40. C-UAS Modeling and Simulation Architecture

B. OPERATIONAL ENVIRONMENT MODELING

The operational environment specifies detailed aspects of the mission scenario and vignette(s) of interest that contain the geographic area, conflict, threat laydown, red and blue forces, Order of Battle (OOB) and the overall rules of engagement (DD-ENG 2020, 17–24). Operational environment aspects that are currently implemented in the DROSERA analysis tool are summarized below.

1. Area of Operation Dimensions

Providing a medium in which to place UAV threats, C-UAS capabilities, and priority assets, this represents the area for which the C-UAS scenario activities will be conducted.

Overall Map Dimensions: Within the DROSERA analysis tool, the virtual environment is currently a fixed two-dimensional (2d) grid space consisting of 100 by 100-pixel squares to fit within the default window size of the application, which is 1200 by 600-pixels. As a default, the map is representative of a 1200 by 600-meter operational area.

Map Scale: Modifiable at program design time, but not adjustable at runtime. At current, it is necessary to maintain the 2:1 dimensional ratio to maintain symmetry and appropriate visual representation within the simulation.

2. Red/Blue Force Laydown

Agents representing the scenario forces, referred to as red force for the attacking threat and blue force as the defending party, are specified after launching, but prior to beginning the simulation where they are assigned by the user to an initial location point when spawned.

- **Threat sUAS drones:** Placement of spawn locations is referenced to a pre-user defined deployment site, which is represented by a scalable circle whose location is specified through x-y coordinates within the operational area. The Deployment Location element defines the area in which UAVs may deploy from within the simulation environment. With the ability to place multiple of the referenced deployment locations throughout the simulation with their own specifically defined number of UAVs to be launched, the ability to provide complex interaction becomes possible. The desired quantity of UAVs to be generated from this site is distributed uniformly within the deployment site to provide a form of randomness. Figure 41 details the AnyLogic deployment logic for the launching of threat UAVs within a given Deployment Location. The first initial stages "delay" and "resize" represent initializing phases in which user-defined characteristics are assigned to variables within the appropriate agent of a sUAS threat population. The following state, *AwaitingPlay* exists to maintain the agent until the simulation begins. Once the user has set their vignette and indicated for the simulation to commence, all threats enter their final stage of "Deploy," where they execute their prescribed tasks.

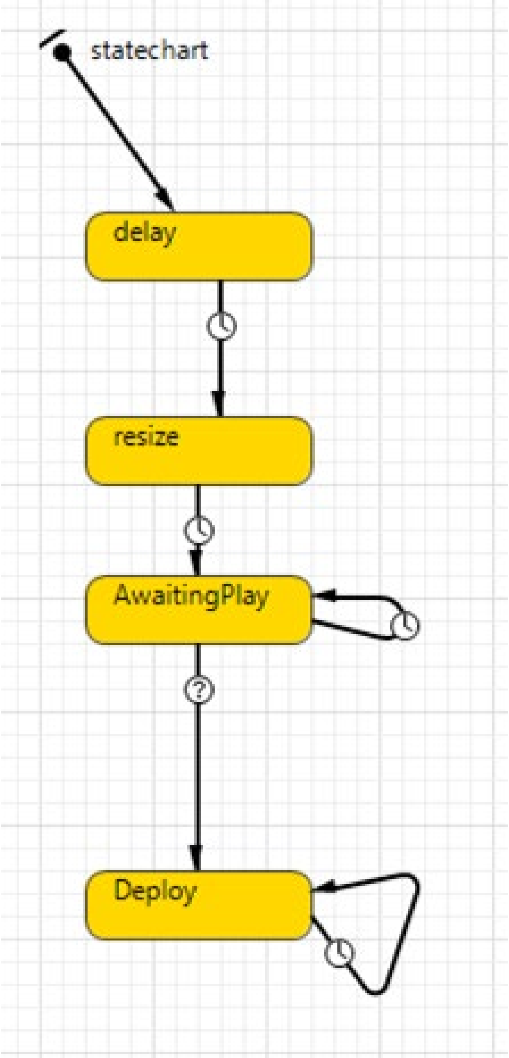


Figure 41. Threat sUAS Deployment Site State-Based Behavior

- **C-UAS platforms:** The placement of C-UAS platform locations is referenced to a pre-user defined deployment site, specified by x-y coordinates within the operational area. While C-UAS infrastructure also has definable dimensions regarding its area, it differs from UAV deployment locations in that there are two definable area dimensions that correlate to x-y coordinate placement. For C-UAS infrastructure, these spaces include regions in which threats may be detected and the capability employed, referred to as detection space and defensive space respectively. Various examples of C-UAS platforms being used within the operational scenario to provide area coverage are depicted in Figure 42 through Figure 44 These capture a generalized deployment of most variations C-UAS capabilities, presented as: a large operational area defended by a single capability, a collection of capabilities to secure a perimeter, a collection of capabilities to defend a large operational area, and a collection of capabilities with a corresponding sequence of patrols to secure an operational area. Subsequently, the DROSERA analysis tool attempts to mirror this deployment strategy through its present C-UAS capabilities.

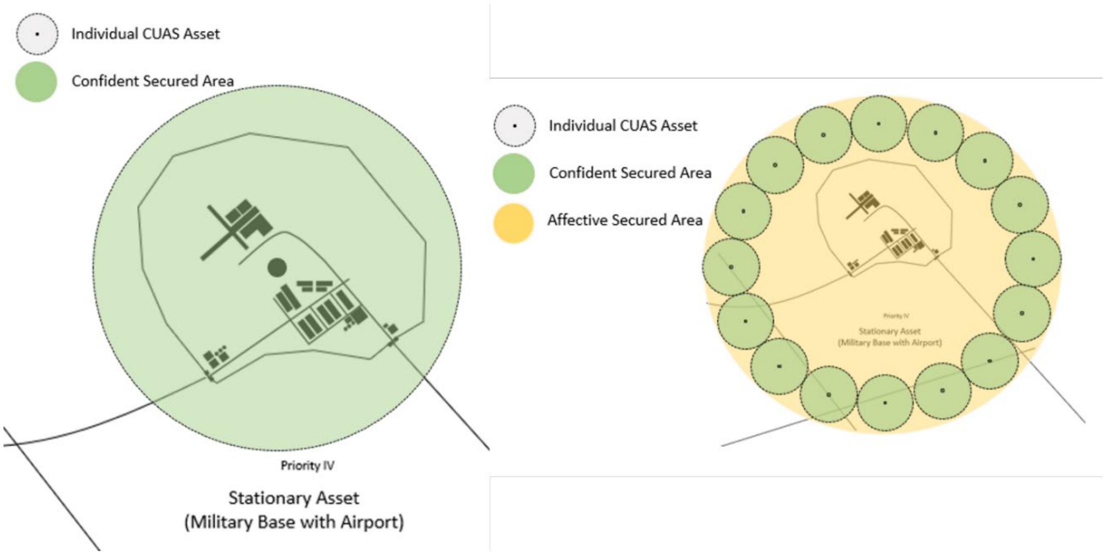


Figure 42. C-UAS Force Laydown: Total Area Coverage vs. Perimeter Distributed Coverage

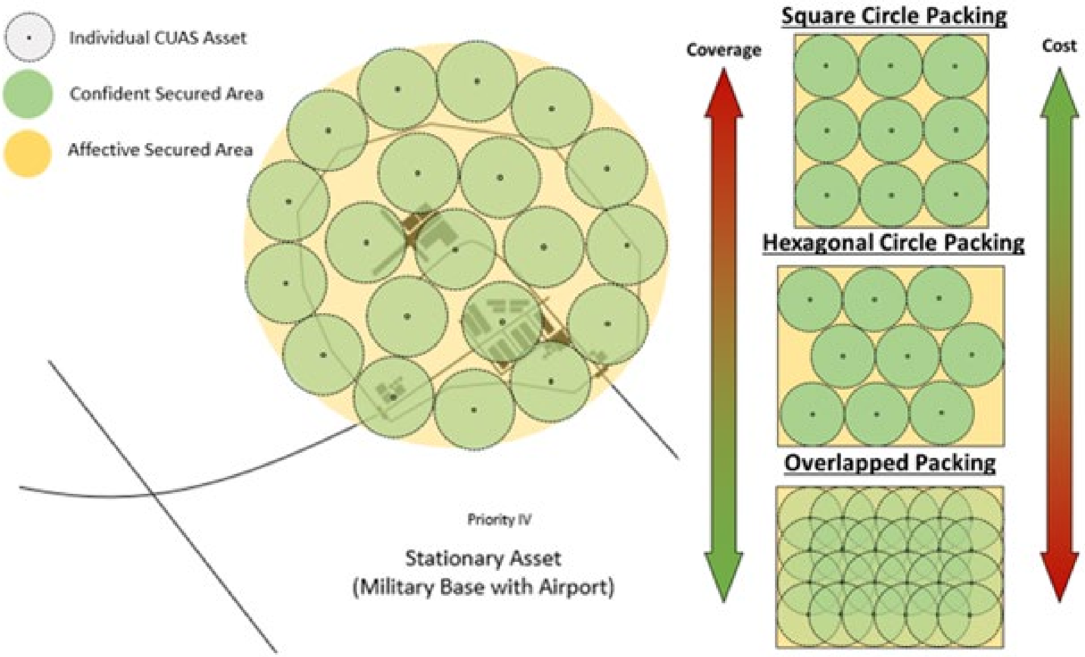


Figure 43. C-UAS Force Laydown: Scattered Distributed Coverage

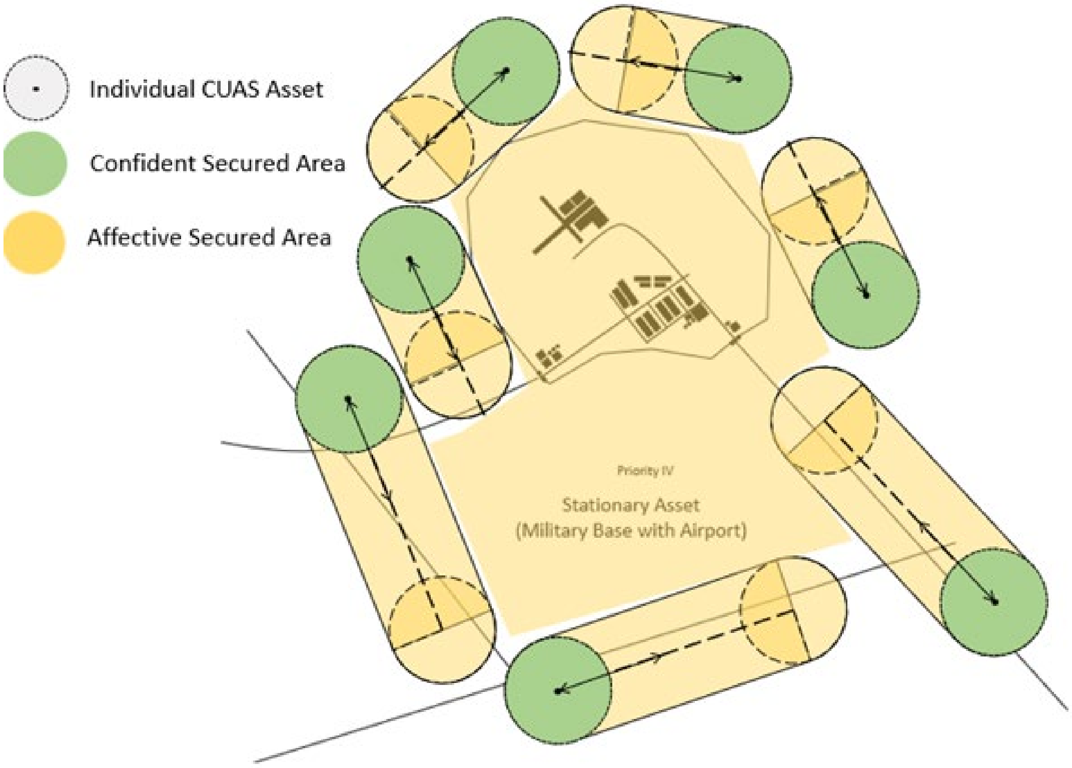


Figure 44. Dynamic Distributed Coverage

C. MISSION ELEMENT MODELING

A mission element is a combination of platform, system, and possible subsystem(s) that provide functional performance using specific technical characteristics to perform a specific task (DD-ENG 2020, 37). It is important to accurately model individual elements within the simulation to exhibit performance measures as defined by the resource architecture and the emulated behaviors as defined by the mission architecture. System characteristics and employment techniques that are currently implemented in the DROSERA analysis tool are summarized below.

1. Threat sUAS

Within the DROSERA Analysis Tool, the Threat sUAS consists of two primary agents, the previously outlined deployment location, as well as the individual UAV agent. The Individual UAV Agent element represents the exhibited performance and behavior of a single threat UAV within the simulation space.

a. Employment Techniques

Command and Control: For the simulation, two generic representations of how the UAV receives its navigational information have been selected being Radio Communications (RC) and localized autonomy.

1. **Radio Communications (RC):** In actuality, many of the current UAVs employed in asymmetric warfare require some variety of consistent communication connection with an operator and even in many cases line of sight with the operator. When these get interrupted, the majority of UAV by default will enter a lost connection protocol and it is customary to either remain in place until communications are restored, land at their current location, or return to the launch location of the platform. Having a C-UAS capability that affects this connection effectively renders the UAV threat neutralized, aside from adherence to EOD protocol.
2. **Autonomy:** Unlike RC, autonomy does not require communications with an operator. It is common for current autonomy platforms to rely on GNSS out of simplicity and convenience, which is a communications path that can be exploited. Improved autonomy can conduct a mission using companion computing[2] and entirely localized sensors, such as optical flow and object recognition, to complete tasks with devastating accuracy. The only truly effective way to eliminate a fully autonomous UAV is with physical disruption, such as a point-defense system or high-power electronic countermeasures.

- **Threat UAV Behavior:** The UAVs behavior addresses the factors of how it will perform its intended mission. The first attribute this includes is how an agent's target is chosen. Currently, this is captured through either the nearest possible target, or the nearest high value target. The

[2] Companion Computing: A localized device, generally a microcomputer, that is used to expand processing and control capabilities through communication of a platforms on-board autopilot.

second item that determines platform behavior is the payload contained within the UAV. At present, the only payload-derived behavior available is an Explosive Ordnance payload. As defined within its state diagram and programmatically, this will have the UAV navigate by the shortest path to the target where it will detonate upon reaching its destination. Figure 45 depicts the AnyLogic state machine describing the threat UAV behavior.

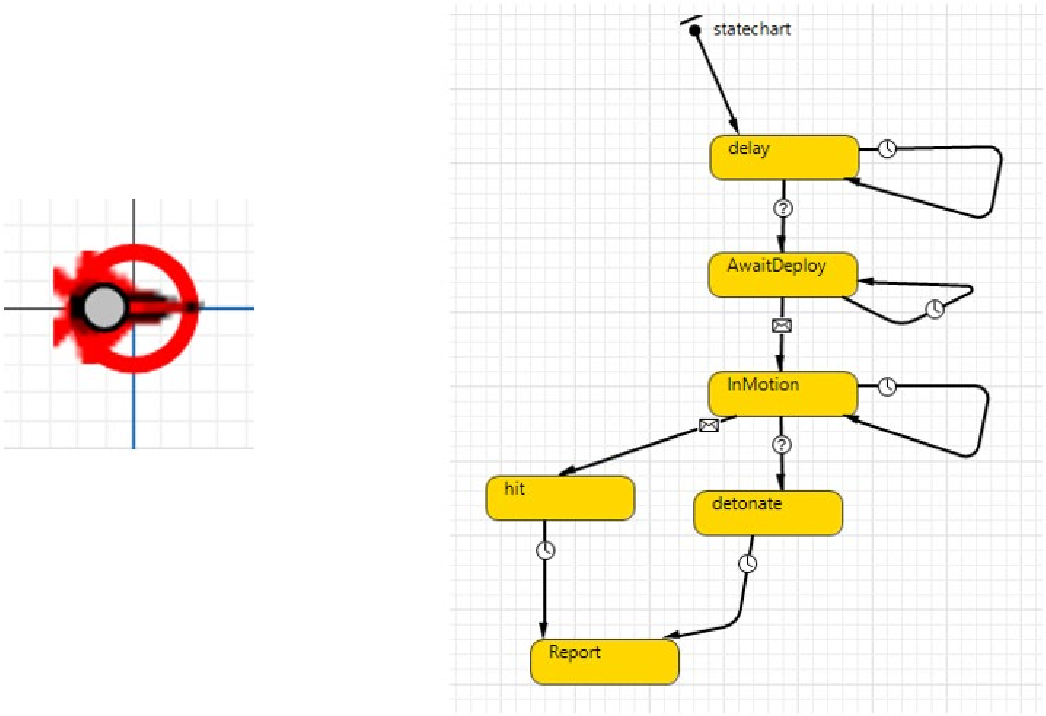


Figure 45. Threat UAV Visualization and State-Based Behavior

b. Characteristics

- **Payload:** There are a variety of payloads that red forces may employ to further complicate a scenario, such as explosive ordnance, electronic warfare, surveillance, and others. Only a single payload option is currently implemented, the previously outlined Explosive Ordnance.

- **Operational Attitude:** This characteristic represents the amount of force presence and aggression strategy that the threat is exhibiting to accomplish objectives.
- **Deployment Size:** Total number of UAVs launched from a deployment site.
- **Deployment Rate:** Frequency of amount of UAS deployed given a user-defined measurement of time.

2. C-UAS System of Systems

The DROSERA analysis tool was designed to incorporate the C-UAS effects chain Sense, Assess, and Neutralize phases. Within the tool, as previously remarked with the UAV threats section, the user must characterize their C-UAS infrastructure individually to match the scenario, platform, and capabilities they wish to evaluate. Similarly, C-UAS infrastructure also has definable dimensions regarding its area. However, as opposed to the UAV deployment areas, the space for C-UAS infrastructure includes location in which threats may be detected and neutralized. Additionally, across all C-UAS infrastructure there are common attributes. This includes tracked attributes such as the required power for operation, which is a summation of power consumption for when the capability is in use. Pertaining specifically to the aforementioned detection and defensive spaces are the two notable associated probability percentages assigned by the user to indicate the capabilities accuracy or likelihood to detect in addition to neutralization of their target.

a. C-UAS Sense

With the goal of simplicity and expedited development in mind, the Sense and Assess capabilities were combined within the model to demonstrate a systems capability of identifying a threat. They are represented visually by a further expanded dotted circle centered on the C-UAS platform. Once a UAV threat has been identified, it is assumed that communication between C-UAS Sense platforms is established and thus removes the need for other capabilities to detect that individual threat. Most methods of detection have been generalized for these items for convenience to the user as most systems have multiple forms of threat identifiers

- **Wide Area Sensing:** Wide area sensing is provided in the simulation tool to emulate C-UAS systems to include early warning systems, radio frequency spectrum identifiers, and even model the passive perception of highly trafficked areas by personnel who could report a threat. Once a threat is reported, all C-UAS platforms are assumed to effectively track the threat and will attempt to neutralize the system if it is within effective range. Notably, Wide Area Sensing C-UAS platforms only possess a detection layer when it is deployed and subsequently only contributes to the detection phase of the events chain. This in turn promotes a further cohesive and complex defense in depth representation. Figure 46 depicts a Wide Area Sensing platform's model visualization and behavioral description. Inspection of **Error! Reference source not found.** demonstrates that all C-UAS performers that exhibit neutralization capabilities can detect all threat UAVs within the Wide Area Sensing performance parameters set by the user.

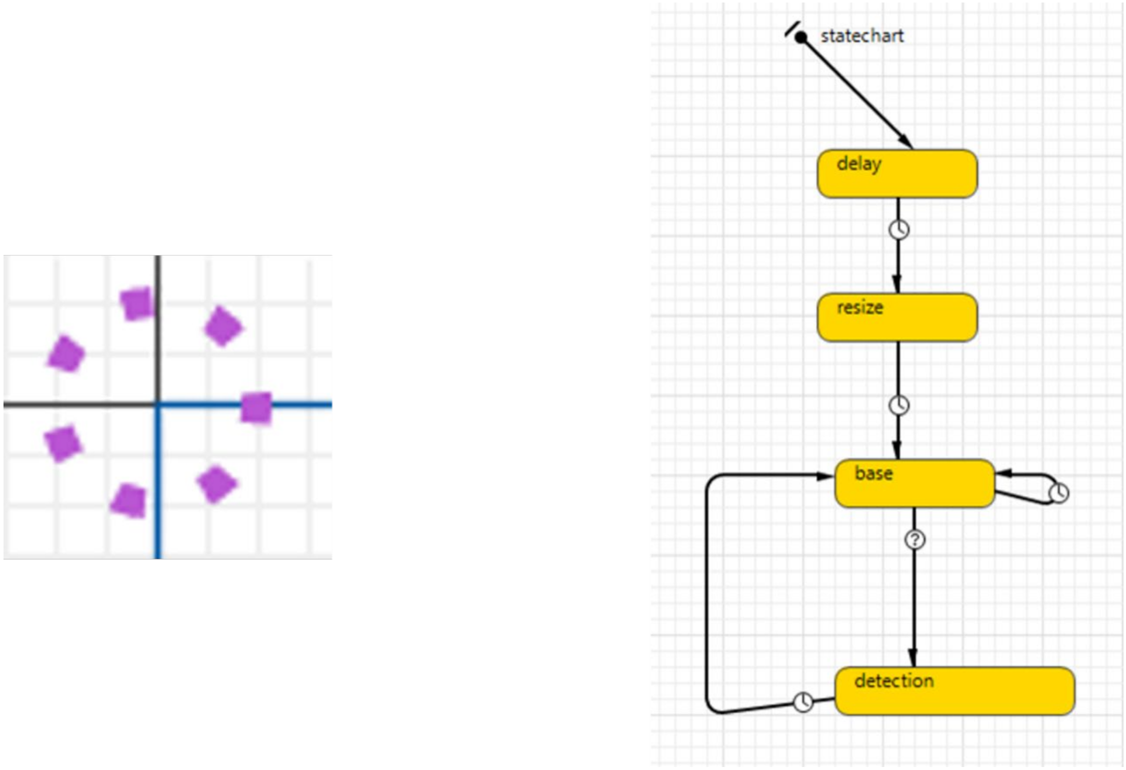
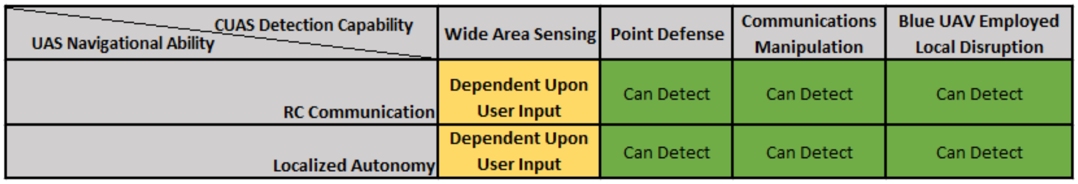


Figure 46. Wide Area Sensing: Visualization and State-Based Behavior

Table 26. Wide Area Sensing Capability Matrix

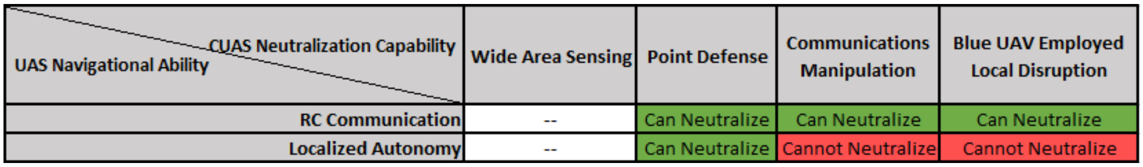


CUAS Detection Capability UAS Navigational Ability	Wide Area Sensing	Point Defense	Communications Manipulation	Blue UAV Employed Local Disruption
RC Communication	Dependent Upon User Input	Can Detect	Can Detect	Can Detect
Localized Autonomy	Dependent Upon User Input	Can Detect	Can Detect	Can Detect

b. C-UAS Neutralize

For C-UAS Neutralization, capabilities are generalized and categorized based upon behavior and intended outcome. Neutralization capabilities are denoted by an area with a solid color ring centered on the C-UAS platform. Currently, there are three Neutralization capabilities implemented in the analysis tool: Point Defense, Communications Manipulation, and Blue UAV Employed Local Disruption. The user must choose from this collection what best applies to the capability they wish to model. **Error! Reference source not found.** summarizes the C-UAS performers capable of neutralizing UAVs exhibiting specified navigational abilities.

Table 27. C-UAS Neutralize Capability Matrix



CUAS Neutralization Capability UAS Navigational Ability	Wide Area Sensing	Point Defense	Communications Manipulation	Blue UAV Employed Local Disruption
RC Communication	--	Can Neutralize	Can Neutralize	Can Neutralize
Localized Autonomy	--	Can Neutralize	Cannot Neutralize	Cannot Neutralize

- **Point Defense:** Point defense systems are characterized in this simulation tool as platforms that affect an individual agent given an interaction, more specifically neutralization. This category includes systems such as high energy lasers, netguns, and close-in weapon systems (CIWS), to name a few. Point defense systems have an additional unique user-defined attribute being the total number of attempts of pacification before entering a cooldown state. During this state, the agents wait for a user-defined amount of time before attempting to reengage. Figure 47 depicts a Point Defense platform’s model visualization and behavioral description.

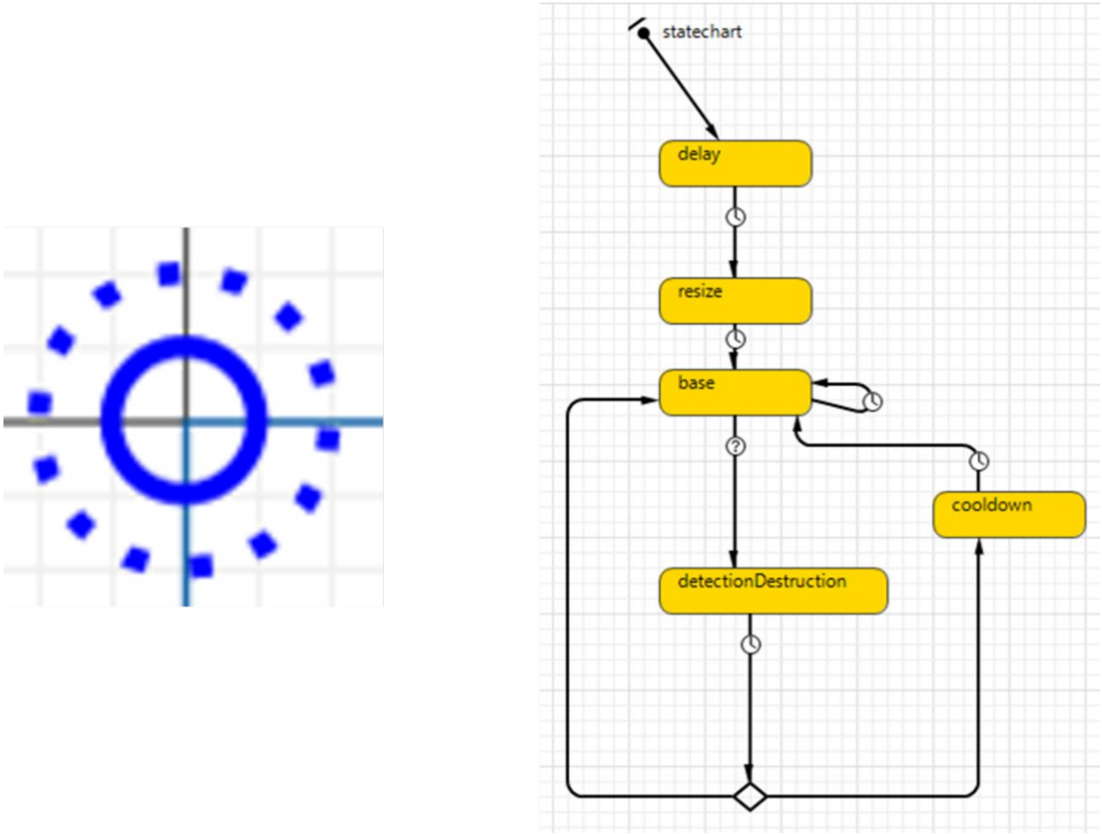


Figure 47. Point Defense: Visualization and State-Based Behavior

- **Communications Manipulation:** Communication manipulations, such as command spoofing and jamming, is one of the possible C-UAS neutralization techniques that implement electronic countermeasures. The activation of these capabilities within their neutralization region affects all present UAVs in the area, so long as they are not autonomously operated. Figure 48 depicts a Communications Manipulation platform's model visualization and behavioral description.

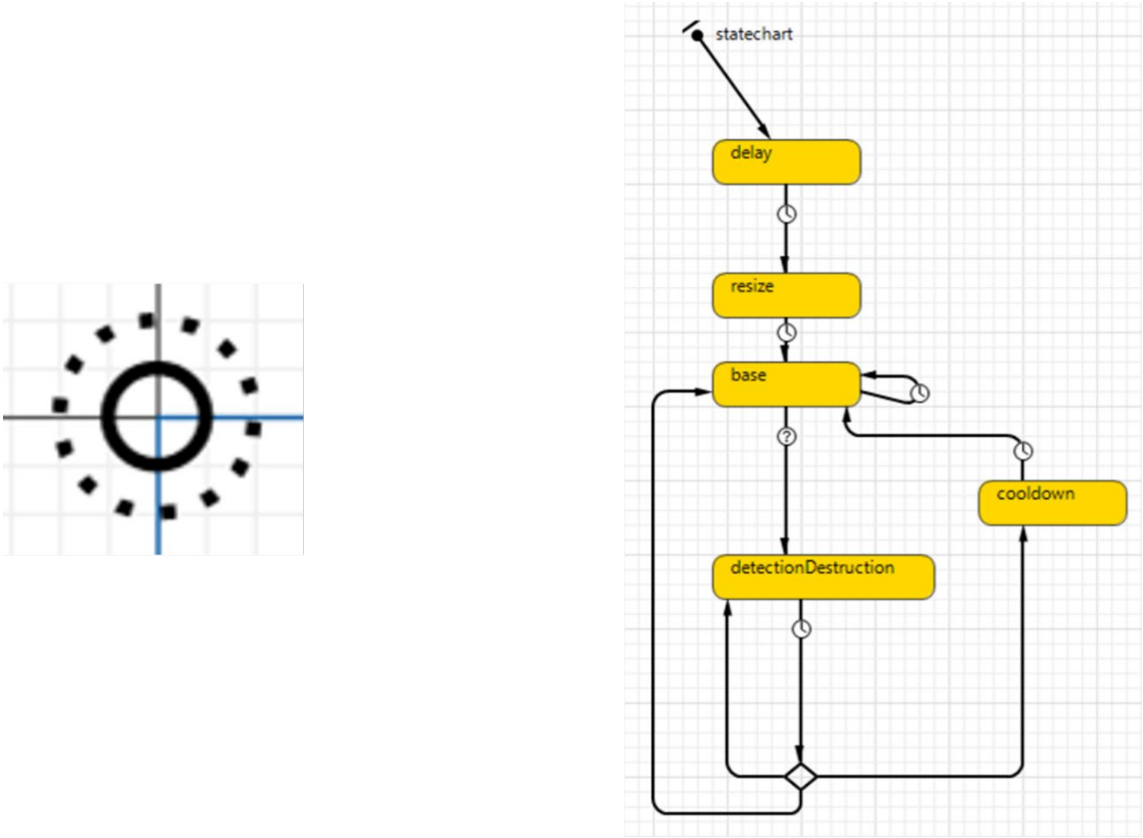


Figure 48. Communications Manipulation: Visualization and State-Based Behavior

- **Blue UAV Employed Local Disruption:** The usage of UAV-employed neutralization techniques within C-UAS SoS is a unique and specific test case of interest with the desired goal to analyze its influence and performance within the effects chain, possible scenarios, and overall C-UAS implementation. More specifically, this will be used to report on the effectiveness of a low-power, non-collaterally disruptive communication denial approach. The capability of Blue UAV Employed Local Disruption consists of two joint agents. The first of these is a deployment site for the UAV. This consists of an agent that represents the deployment site and detection region that searches for a threat to identify and another agent that represents the blue UAV independently. Characteristics for the deployment and detection site are similar to that of the wide area sensing capability, but also includes a triggering messaging system to launch the Blue UAV. Once the blue UAV is launched it tracks the location of its target with the goal of intercepting. Upon arrival, the blue UAV employs a similar effect as the communications manipulation capability where several UAVs are affected by its influence. Figure 49 depicts a Blue UAV platform's model visualization and behavioral description.

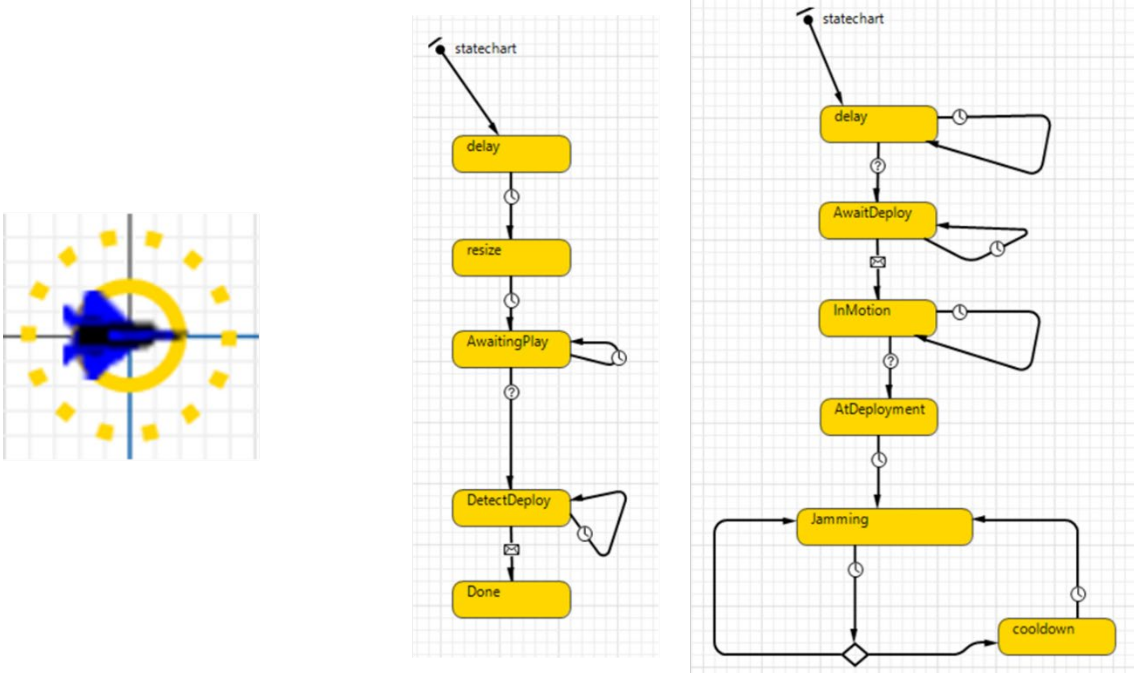


Figure 49. Blue UAV Employed Local Disruption: Visualization and State-Based Behavior

c. *Priority Locations*

For the operational scenario's simulation, the overall goal for all agents revolves around priority locations. For UAV threats, their objective is to conduct their defining mission characterization outlined by the user upon the priority location. In contrast, C-UAS infrastructure is tasked with defending the priority locations through neutralization of the UAV threats. There are two generic notable location classifications implemented in the simulation tool: high priority and low priority (Figure 50). The two priority classes have been defined to demonstrate possible UAV red teaming strategies, such as distractions to waste defensive resources and assets. This contributes to more realistic scenarios and subsequently a better estimation of overall mission effectiveness. Regarding the design of these elements from a programmatic perspective, they are relatively simple, consisting of only the standard location definition. From this, agents within the simulation are able to access the location of each notable location within the simulation space and calculate which location is closest.

Figure 50. Priority Locations Visualization

D. C-UAS CAPABILITY METRICS

In order to thoroughly understand the interactions and results of a simulation given a complex environment, metrics within the simulation execution must be appropriately tracked. The DROSERA Analysis Tool is capable of computing and storing the following measures of performance in support of follow-on C-UAS mission effectiveness analysis:

C-UAS Sense (w/ embedded Assess)

1. How many UAVs were detected or not detected?
2. What is the average time until detection?
3. How many threat UAVs were deployed?
4. How many threat UAVs of what types were deployed?

5. What is the average time between detection and neutralization?[3]

C-UAS Neutralize

1. How many C-UAS capabilities were deployed?
2. How many C-UAS of what types were deployed?
3. How many threat UAVs were neutralized?
4. How many of what type of threat UAVs were neutralized?

C-UAS Reliability

1. How many UAVs passed within threat proximity of (Indicator for potential C-UAS platform failure) the C-C-UAS Sense/Neutralize platforms?[3]

C-UAS Energy Effectiveness

1. What is the overall power consumed in sustaining a C-UAS platform from the time that it is energized in response to a threat until the end of its use in the operational scenario?
2. What is the total power consumption of the C-UAS SoS for the entire operational scenario?

C-UAS Mission Effectiveness

1. How close did the threat UAV get to Priority Location(s)?
2. What are the times corresponding to first threat UAV breaching the Close-In Engagement region, the Protect the Force Region, and the Priority Location respectively?[3]
3. What is the overall time of simulation?[4]

[3] Planned but not currently implemented in the DROSERA Analysis Tool. Actual measures were not captured in the Simulation Modeling phase. But the functionality may be included as a stretch goal for this project or targeted for future work.

[4] Time from first threat UAV detection to operational environment void of any threat UAV population.

E. TRACEABILITY TO C-UAS MEASURES OF EFFECTIVENESS

A traceability matrix mapping the DROSERA Analysis Tool mission architecture capability measures to C-UAS capability mission effectiveness and performance measures is summarized in Appendix C. Upon review of the traceability matrix, it is evident that the DROSERA Analysis Tool provides behavioral output that maps to nearly all C-UAS mission effectiveness and performance measures.

F. DROSERA ANALYSIS TOOL USER INTERFACE

The DROSERA Analysis Tool provides a user interface (UI) that enables the user to configure and control the operational environment and model elements to be simulated within the C-UAS scenario. Additional information on the features and usage of the DROSERA Analysis Tool UI can be found in Appendix B.

G. EXPERIMENTAL DESIGN

After the elements supporting the creation of a detailed ABM representing the C-UAS operational scenario were constructed, an experimental design strategy was developed to ensure appropriate examination of the system performance characteristics within the mission context. It is important to remember that the resource architecture developed in this project represent *generalized* system elements attributed with performance measures commensurate with existing and projected C-UAS systems. Furthermore, the experimental design strategy presented in forthcoming paragraphs is intended primarily to validate the feasibility of the DROSERA Analysis Tool in emulating the behaviors and exhibiting performance measures that are traceable to the C-UAS mission architecture model. As such, the observed outcomes and interactions that result from the experimental design and model analysis should not be used to make recommendations for system configurations. While it is assessed that the DROSERA Analysis tool is robust enough to provide analysis results suitable for enabling decisions on C-UAS design areas to focus on, it is recommended that follow-on efforts be initiated to expand on the vignettes explored in this project.

1. Activity Sequence

The activity sequence for the modeled operational scenario, including constraints, is summarized below.

1. Company commander alerted to sUAS threat via intelligence sources. Cyber-Attack Platforms placed in operational standby.[5]

2. Threat sUAS UAV detected by C-UAS Sense platform.[6]

3. Threat sUAS classified by secondary C-UAS sensor.[6]

4. Classification information ingested by C2 platform and cyber-attack recommendation provided to Company Commander. Assessment made by Company Commander to engage threat and assigns cyber-attack neutralizers.[6]

5. UAV Cyber-attack platforms employ the cyber-attack technique in the Stand-off region as directed by the Company Commander. Threat UAV leakers are reported to the C2 platform for handover to the UAV Ground Attack Platform.

6. UAV Ground Attack Platform detects and engages leakers in the Close-in Engagement region using Kinetic-Mechanical Neutralization Techniques. Leakers are reported to the C2 Platform for handover to the Tactical Convoy.

7. Tactical Convoy perform self-defense tactics such as RF Jamming and Projectile weapons to defeat remaining leakers.[7]

An operational scenario ends when there are no confirmed targets that remain in the simulation. Each threat UAV is limited to a single sortie per scenario, and egress

[5] Not simulated.

[6] C-UAS Sense and Assess model functionality is currently aggregated, so the simulation emulating classification-to-engage activity sequences is currently implemented as one behavioral description.

[7] A maneuver to delay tactic by a tactical convoy would increase the probability of success in a C-UAS operational scenario; however, this behavior is not currently implemented, therefore not addressed in the activity sequence.

activities are not modeled. The scenarios are performed once per day in the midst of a campaign. Monte Carlo analysis shall be performed by running a minimum of 50 iterations of each operational scenario.

2. C-UAS Operational Architectural Variants (Vignettes)

Several mission architecture variants are under consideration as summarized in Table 28. Each architecture variant represents a unique vignette of the C-UAS Combat Patrol scenario that varies the C-UAS capability configuration and Threat sUAS packages employed in each scenario.

Table 28. C-UAS Operational Architecture Variants

Architecture Variant	**C-UAS Configuration**	**Threat sUAS Package**
1	Baseline	Baseline
2	Baseline	Complex
3	Cyber-attack	Baseline
4	Cyber-attack	Complex
5	Defense-in-depth	Baseline
6	Defense-in-depth	Complex

a. C-UAS Configurations

All C-UAS Configurations maintain the same system performance characteristics and identical C-UAS Sense platforms (Wide Are Sensing Capability) in the Engagement Standoff Range region but vary in the types of Neutralization Systems employed. C-UAS capability configurations are summarized in Table 29 with the C-UAS platform performance parameters to be applied highlighted in yellow. A simplified graphical description of the architectural variants to be assessed is depicted in Figure 51

- **Baseline:** The C-UAS baseline configuration leverages a single traditional C-UAS neutralization method (Point Defense) and forgoes the usage of Blue UAV employed Local Disruption (UAV Local Cyber Attack).
- **Cyber-attack:** The C-UAS Cyber-attack configuration relies exclusively on the use of Blue UAV employed Local Disruption (UAV Local Cyber Attack) as its neutralization technique.
- **Defense-in-depth:** The C-UAS Defense-in-depth configuration combines a combination of all implemented C-UAS capabilities, including Cyber-attack configurations, within the DROSERA analysis tool to provide a more comprehensive measure of threat sUAS defense.

b. Threat sUAS Configurations

There are two threat sUAS configurations constructed for experimental design. They are defined below with configurations summarized in Table 30 with the sUAS performance parameters to be applied highlighted in yellow.

- **Baseline:** The threat sUAS baseline configuration employs a simplified UAV threat package. It consists of two sUAS Deployment Locations that launch UAVs from two threat axes exhibiting the Radio Communications C2 attribute.
- **Complex:** The threat sUAS complex configuration exhibits higher levels of system performance as compared to the sUAS baseline configure, a greater volume of UAVs employed, and exhibits two different C2 attributes (Radio Communications, Autonomous).

Table 29. C-UAS System Performance Characteristics

Point Defense			
Detection Accuracy	**Defensive Accuracy**	**Detection Range (radius)**	**Defensive Range (radius)**
Fair, 50%	Fair, 50%	Fair, +10 *m*	Fair, 50 *m*
Good, 75%	Good, 75%	Good, +20 *m*	Good, 100 *m*
Better, 90%	Better, 90%	Better, +50 *m*	Better, 150 *m*
Point Defense (continued)			
Attempts Before Cooldown	**Cooldown Time**	**Operational Power (Total Consumed)**	
Fair, 3	Fair, 10 *s*	Fair, 10–30 *kW*	
Good, 6	Good, 5 *s*	Good, 1–6 *kW*	
Better, 10	Better, 2 *s*	Better, 0.1-0.6 *kW*	
Communication Denial			
Detection & Defensive Range (radius)	**Duration**	**Operational Power (Total Consumed)**	
Fair, 50 *m*	Fair, 2 *s*	Fair, 2–3 *kW*	
Good, 85 *m*	Good, 5 *s*	Good, 1–2 *kW*	
Better, 125 *m*	Better, 10 *s*	Better, < 1 *kW*	
UAV Local Cyber Attack			
Detection Accuracy	**Detection & Defensive Range (radius)**	**Platform Speed**	**Operational Power (Total Consumed)**
Fair, 50%	Fair, 15 *m*	Fair, 10–20 *m/s*	Fair, 80–150 *W*
Good, 75%	Good, 30 *m*	Good, 20–30 *m/s*	Good, 30–60 *W*
Better, 90%	Better, 50 *m*	Better, 40–50 *m/s*	Better, 2–10 *W*
Wide Area Sensing			
Detection Accuracy	**Detection Range (radius)**	**Detection Method**	
Fair, 50%	Fair, 100 *m*	Visual ID	
Good, 75%	Good, 200 *m*	Spectrum ID	
Better, 90%	Better, 300 *m*		

Table 30. Threat sUAS Performance Characteristics

sUAS Threat: Baseline

# UAVs Deployed	Wave Size (% of forces)	Deployment Rate (Wave delay)	Speed
Low, 1–3	Low, 10–25%	Low, 10–20 *s*	Low, 10–20 *m/s*
Med, 4–10	Med, 30–60%	Med, 2–5 *s*	Med, 20–30 *m/s*
High, 11–20	High, 75–100%	High, 0 *s*	High, 40–50 *m/s*

sUAS Threat: Baseline (continued)

Navigation Method	Deployment Radius	Distance From Target	
RC	Low, 10 - 30 *m*	Low, 100–300 *m*	
Autonomy	Med, 50 - 100 *m*	Med, 300–600 *m*	
	High, 150 - 200 *m*	High, 600–900 *m*	

sUAS Threat: Complex

# UAVs Deployed	Wave Size (% of forces)	Deployment Rate (Wave delay)	Speed
Low, 1–3	Low, 10–25%	Low, 10–20 *s*	Low, 10–20 *m/s*
Med, 4–10	Med, 30–60%	Med, 2–5 *s*	Med, 20–30 *m/s*
High, 11–20	High, 75–100%	High, 0 *s*	High, 40–50 *m/s*

sUAS Threat: Complex (continued)

Navigation Method	Deployment Radius	Distance From Target	
RC	Low, 10 - 30 *m*	Low, 100–300 *m*	
Autonomy	Med, 50 - 100 *m*	Med, 300–600 *m*	
	High, 150 - 200 *m*	High, 600–900 *m*	

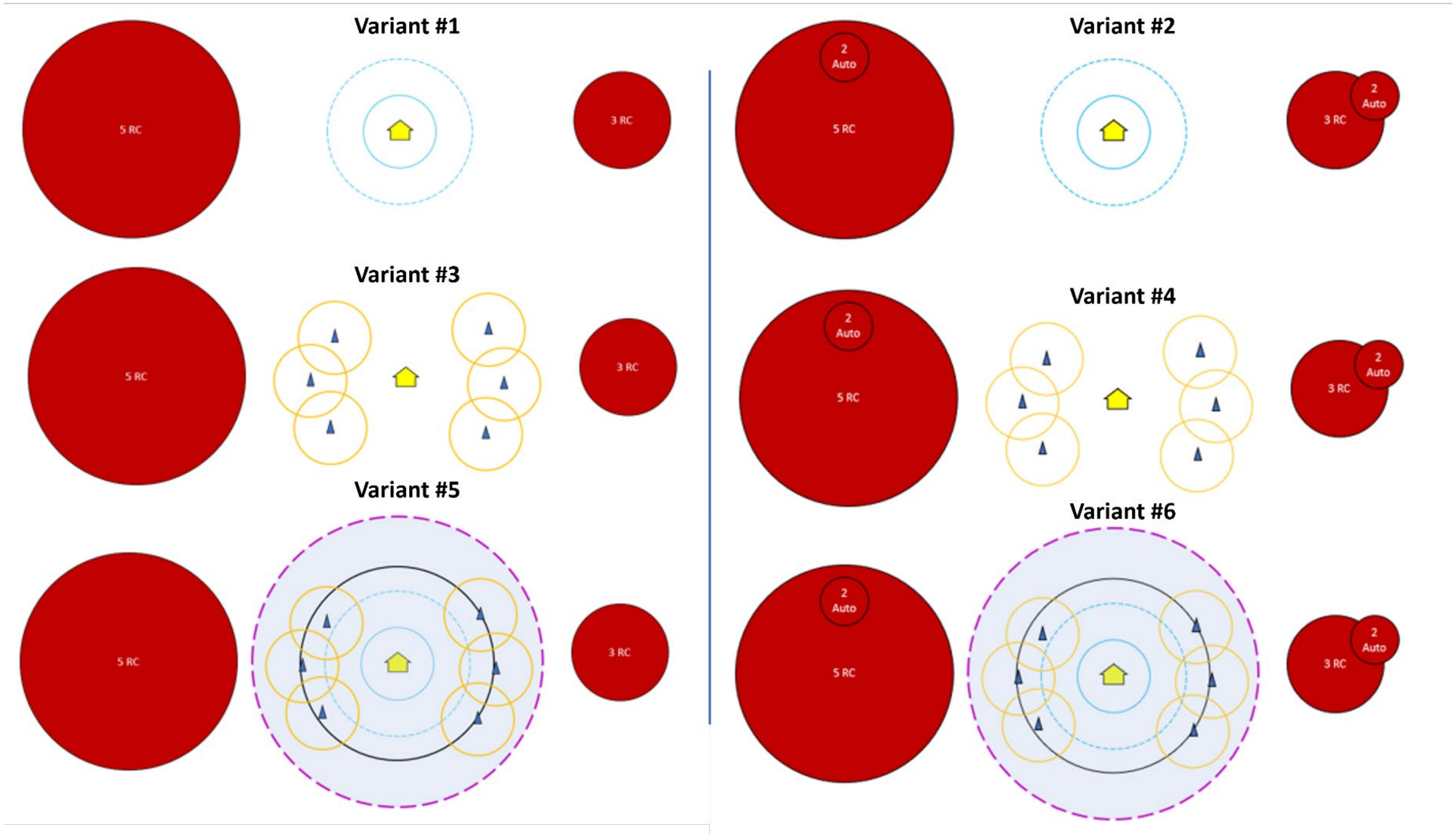


Figure 51. Architecture Variant Configuration Summary

H. SIMULATION AND RESULTS

Monte Carlo analysis was performed running 100 iterations of the C-UAS Combat Deployment Operational Scenario. Simulation results were tabulated and available as a supplemental file. Model analysis is detailed in Chapter VI.

I. SUMMARY OF CHAPTER V

This chapter details the architecture assessment for the C-UAS Mission Architecture. A modeling architecture was constructed to reference all model elements of the C-UAS mission characterization to include system performance characteristics, threat sUAS performance characteristics, environmental conditions, and capability metrics. The DROSERA Analysis Tool was developed as its C-UAS M&S environment, with the objective of emulating all behaviors and performance characteristics needed to evaluate C-UAS mission effectiveness. Next, an experimental design strategy was developed to ensure appropriate examination of the system performance characteristics within the mission context. The experimental design strategy presented is intended primarily to validate the feasibility of the DROSERA Analysis Tool in emulating the behaviors and exhibiting performance measures that are traceable to the C-UAS mission architecture model. The simulations runs corresponding to six architecture variants were executed, with results tabulated in a separate appendix. The following chapter utilizes these results in a conclusion addressing the research questions and discussing a recommendation for follow-on work.

VI. CONCLUSIONS

The increased proliferation of sUAS by adversarial countries requires the employment of C-UAS systems that can mitigate the threat. There is a continued need to evaluate current available technologies to ensure both safety and security by employing systems that can detect, track, identify, and interdict, when necessary, with adversarial sUAS. To meet these demands and maintain security of critical assets, there must be an investment in the most capable technologies to provide the warfighter the decisive advantage necessary to maintain control.

A. MODEL ANALYSIS

1. Measures of Effectiveness

It will be helpful to provide formulas (defined in terms of model simulation variables) for the MOEs analyzed in this section.

- **MOE #1: Probability of Sense**

$$P_{Sense} = \frac{\text{UAVs detected}}{\text{Total UAVs} - \text{UAVs neutralized before detection}} \tag{7}$$

- **MOE #2: Assessment Time**

$$\overline{\text{Time to detect UAV}} \tag{8}$$

- **MOE #3: Probability of Neutralize**

$$P_{Neutralize} = \frac{\text{UAVs neutralized}}{\text{UAVs deployed}} \tag{9}$$

- **MOE #4: Neutralization Time**

$$\text{Simulation Time} - \overline{\text{Time to detect UAV}} \tag{10}$$

- **MOE #5: Neutralization Point**

$$\text{Closest distance without detonation OR } 0_{\text{if UAV detonation occurs}} \tag{11}$$

- **MOE #6: C-UAS Weapon Effectiveness**

$$P_{Sense} * P_{Neutralize} \tag{12}$$

- **MOE #7: Energy Effectiveness**

$$\text{Total power consumed by C-UAS platforms} \tag{13}$$

2. Statistical Analysis

Statistical summaries for all six architectural variants are outlined in Table 31. Although not indicated in the table, the sample mean for nearly all MOE results were found to be 95% confidence interval. Since there are no thresholds or objectives prescribed or required for this project, hypothesis testing is unnecessary.

Table 31. C-UAS Operational Scenario Statistical Summary

Architecture Variant	MOE 1: Probability of Sense		MOE 2: Assessment Time [s]		MOE 3: Prob. Of Neutralization		MOE 4: Neutralization Time [s]	
	μ	σ	μ	σ	μ	σ	μ	σ
Variant 1	0.890	0.104	10.22	1.05	0.806	0.137	9.547	1.83
Variant 2	0.741	0.111	9.87	1.14	0.674	0.101	10.23	2.40
Variant 3	0.962	0.113	6.03	1.30	0.984	0.049	7.29	3.01
Variant 4	0.489	0.069	5.94	1.28	0.659	0.032	12.58	2.44
Variant 5	1.000	0.000	6.43	1.48	1.000	0.000	6.50	1.56
Variant 6	0.992	0.039	6.58	0.86	0.995	0.023	9.78	1.55

Architecture Variant	MOE 5: Neutralization Point [m]		MOE 6: CUAS Weapon Effectiveness		MOE 7: Energy Effectiveness [W]	
	μ	σ	μ	σ	μ	σ
Variant 1	4.36	11.56	0.725	0.180	1082.19	196.90
Variant 2	0.00	0.00	0.504	0.127	1216.96	248.86
Variant 3	121.45	50.49	0.951	0.142	1538.58	651.70
Variant 4	0.000	0.000	0.324	0.052	3893.89	755.03

Architecture Variant	MOE 1: Probability of Sense		MOE 2: Assessment Time [s]		MOE 3: Prob. Of Neutralization		MOE 4: Neutralization Time [s]
Variant 5	133.13	25.17	1.000	0.033	2834.85	3408.05	
Variant 6	45.125	10.66	0.98	0.056	23765	4720.6	

Boxplots aid in providing a quick graphical summary of the sample data. Boxplots were created from the primary MOEs and are depicted in Figure 52 through Figure 55. Observations are as follows:

- **MOE #1:** Variants 5 and 6 yield the highest P_{Sense} measures; the shared attribute of DiD capability may be the dominant factor.
- **MOE #2:** Variants 3 and 4 yield the lowest assessment time, pointing to the shared attribute of Cyber-attack only capability as the dominant factor.
- **MOE #3:** Variants 5 and 6 yield the highest $P_{Neutralize}$ measures; again, the shared attribute of DiD is the likely dominant factor. The reader should also note that when countering radio-controlled-only UAV threats, the Cyber-attack-only capability yields comparable $P_{Neutralize}$ results.
- **MOE #4:** Variants 3 and 5 lead in this category of achieving neutralization in the shortest time. The Cyber-attack capability and the type of threat deployed (sUAS Baseline) are the common factors here.
- **MOE #5:** Variants 3 and 5 scored well in this category, attaining neutralization with the closet target coming within about 120 and 130 meters respectively to the priority location. Employment of Cyber-attack capabilities against a sUAS Baseline capability is the common factor here.
- **MOE #6:** As $P_{Effectiveness}$ is a product of P_{Sense} and $P_{Neutralize}$, it follows that variants 5 and 6 lead this category with DiD capability as the likely dominant factor.

- **MOE #7:** All variants consume comparatively similar amounts of power in the scenarios, with exception of variant 6, whose energy consumption is an order of magnitude larger. The dominant factor is the use of comms denial equipment against an autonomous (locally controlled) threat.

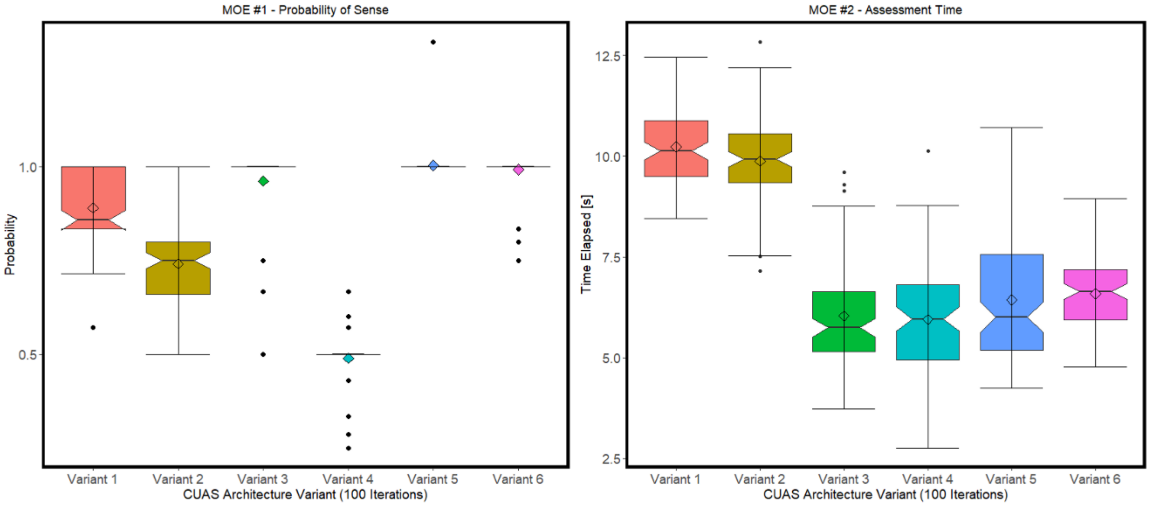


Figure 52. C-UAS Architecture Variant Boxplot (MOE #1 and MOE #2)

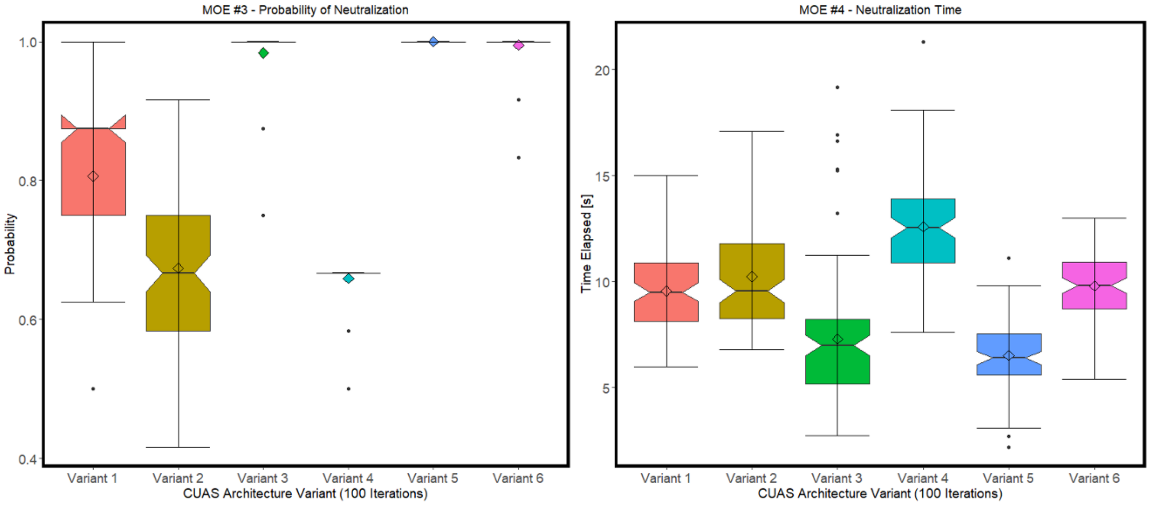


Figure 53. C-UAS Architecture Variant Boxplot (MOE #3 and MOE #4)

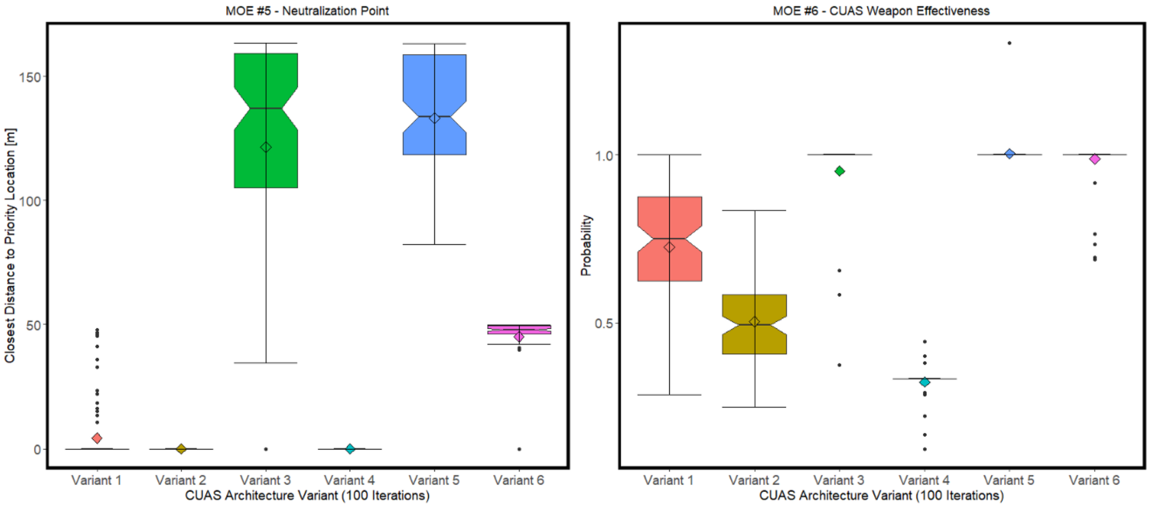


Figure 54. C-UAS Architecture Variant Boxplot (MOE #5 and MOE #6)

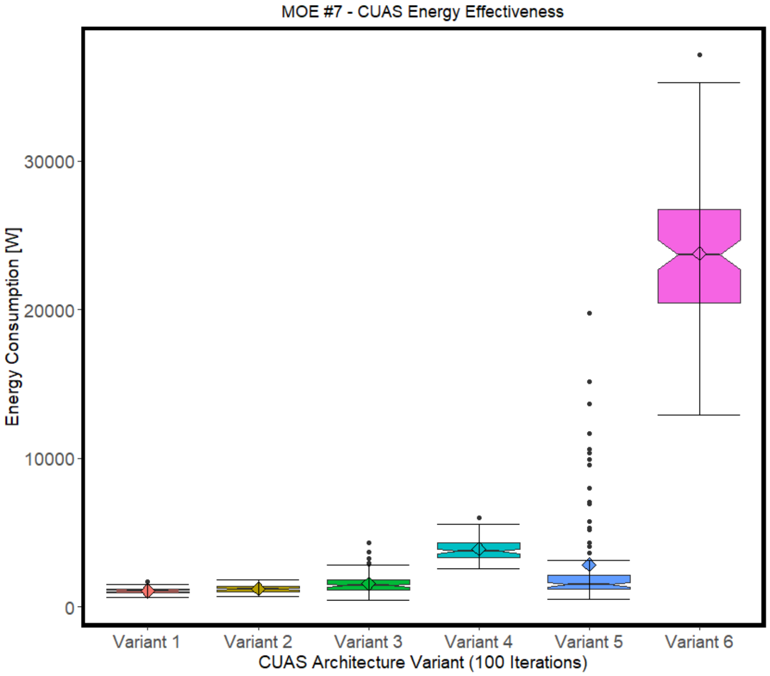


Figure 55. C-UAS Architecture Variant Boxplot (MOE #7)

3. Output Analysis – Main Effect Plots

The main effect plots in Figure 56 through Figure 62 depict the average sample means of each MOE across the configuration categories for C-UAS and threat sUAS respectively. Observations are as follows:

- **MOE #1:** C-UAS DiD capability against the sUAS Baseline configuration yield better P_{Sense} measures. This agrees with intuitive expectations and the boxplot.
- **MOE #2:** C-UAS DiD capability against the sUAS Complex configuration yields the lowest Time to Assess. This agrees with the boxplot, but the only intuitive explanation is that the autonomous UAVs in the sUAS Baseline are virtually "invisible" to the C-UAS Cyber-attack only capability, permitting the simulation to end earlier.
- **MOE #3:** C-UAS DiD capability against the sUAS Baseline configuration yields the highest $P_{Neutralize}$ measures. This agrees with the intuitive expectation that DiD would perform better against the sUAS Baseline configuration, but the boxplot reveals that C-UAS performs equally well against both sUAS threat configurations in this category.
- **MOE #4:** C-UAS DiD capability against the sUAS Baseline configuration yields the shortest Time to neutralize. This agrees with intuitive expectations and the boxplot.
- **MOE #5:** C-UAS DiD capability against the sUAS Baseline configuration yields the Neutralization points that are furthest from the priority location. This agrees with intuitive expectations and the boxplot.
- **MOE #6:** C-UAS DiD capability against the sUAS Baseline configuration yields the best $P_{Effectiveness}$ measures. The result is unsurprising given that the same combinations contributed to the top P_{Sense} and $P_{Neutralize}$ measures. This result also agrees with the boxplot.
- **MOE #7:** C-UAS Baseline capability against the sUAS Baseline configuration yields the best Energy Effectiveness measures. This agrees with intuitive expectations and the boxplot.

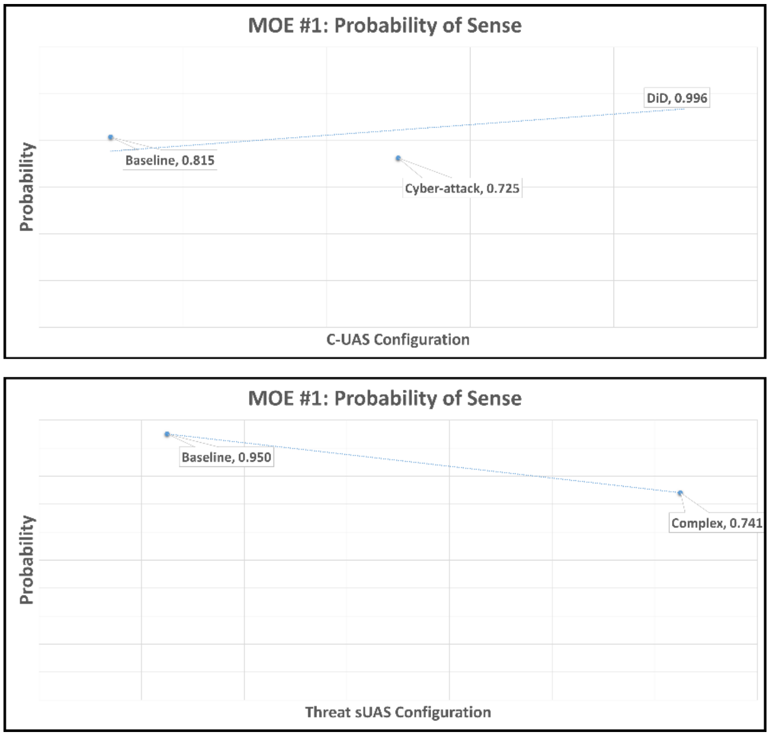


Figure 56. Main Effect Plots (MOE #1)

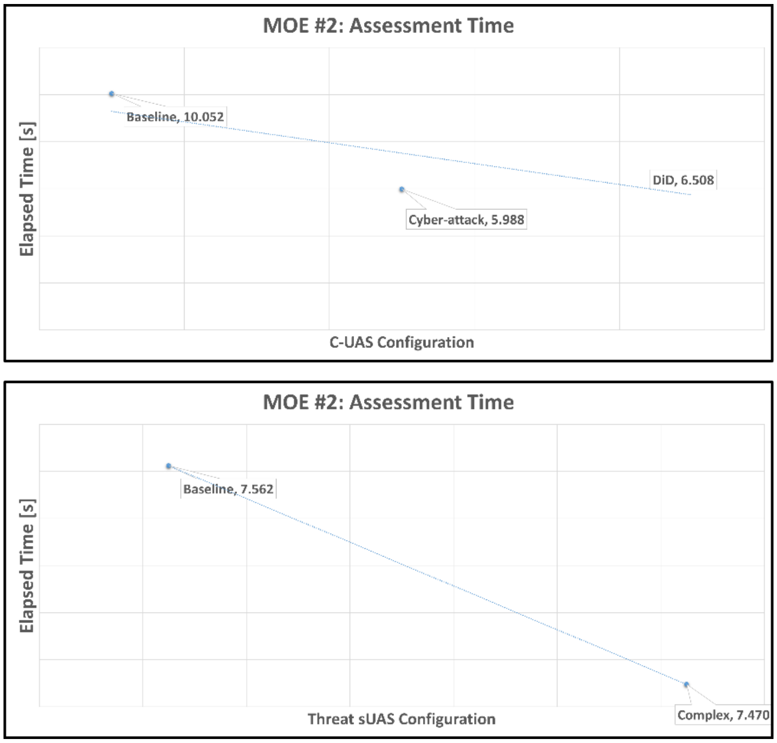


Figure 57. Main Effect Plots (MOE #2)

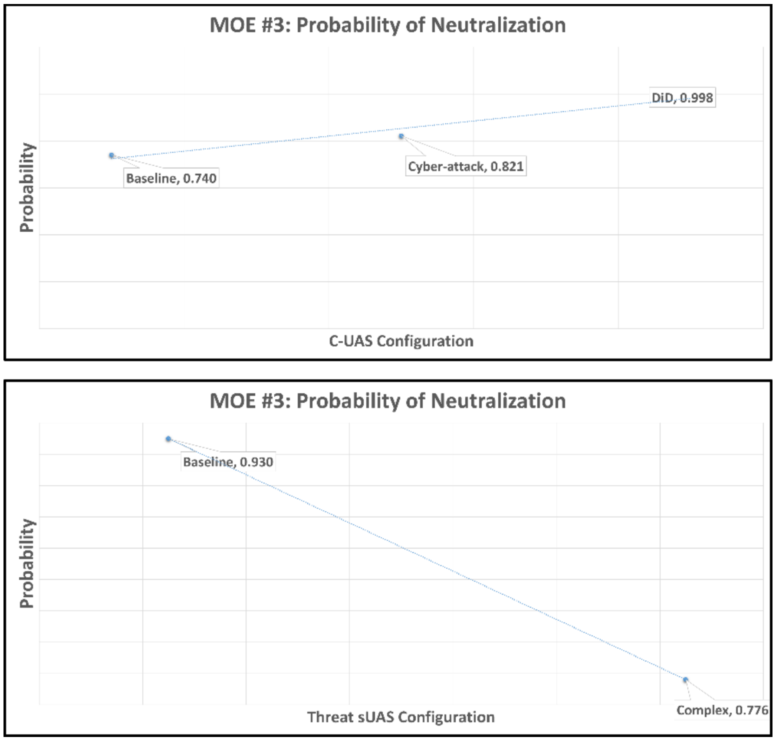


Figure 58. Main Effect Plots (MOE #3)

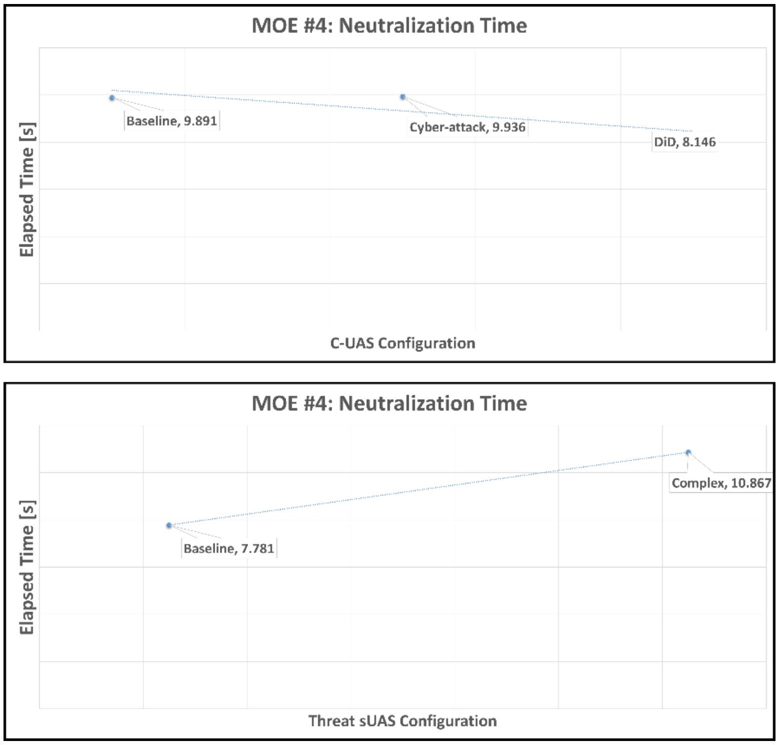


Figure 59. Main Effect Plots (MOE #4)

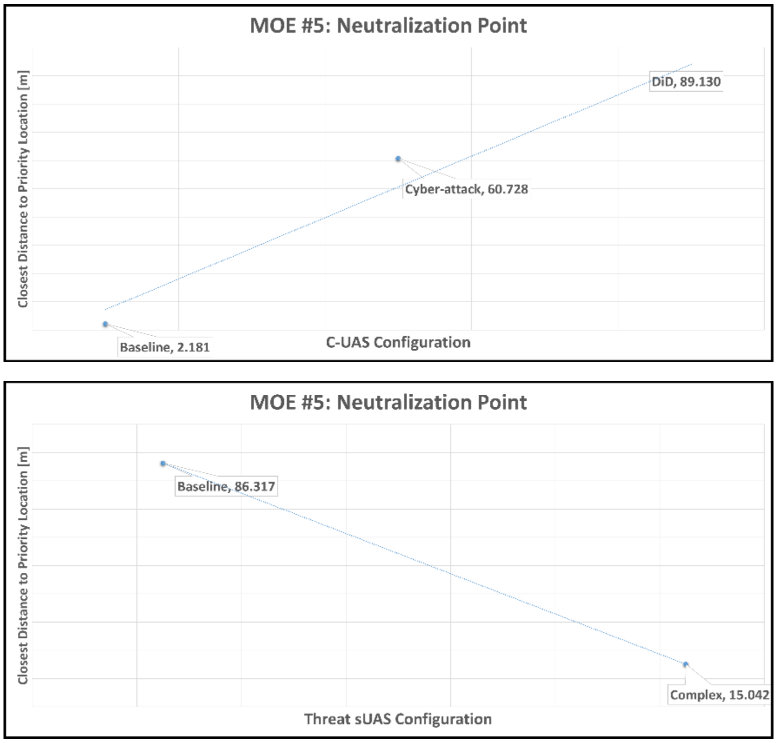


Figure 60. Main Effect Plots (MOE #5)

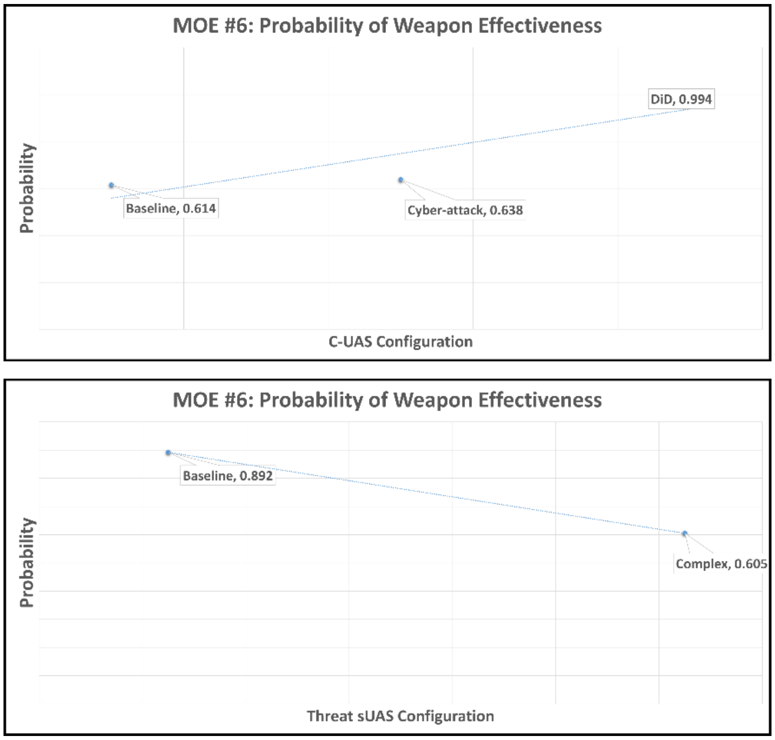


Figure 61. Main Effect Plots (MOE #6)

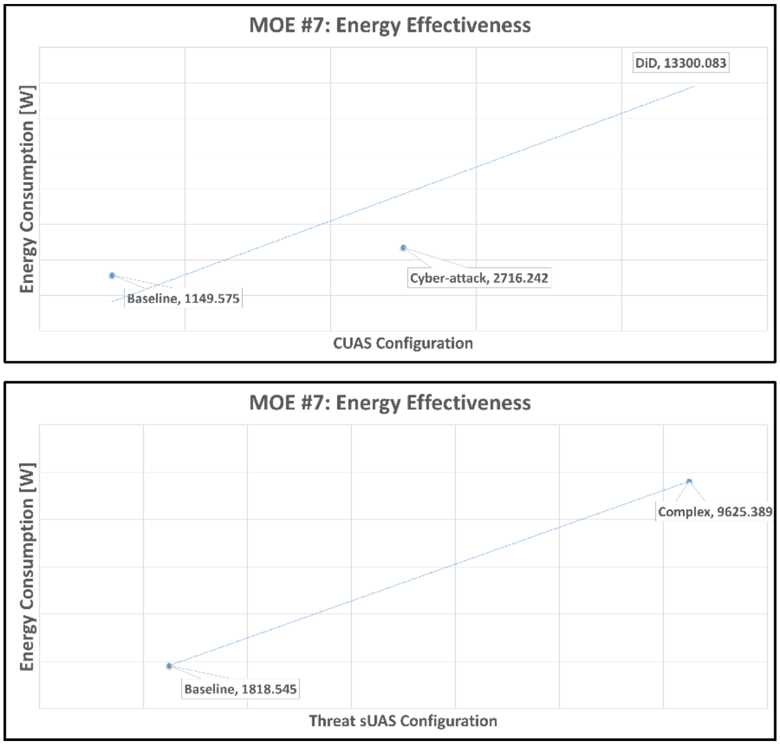


Figure 62. Main Effect Plots (MOE #7)

4. Output Analysis – Interaction Plots

Interaction plots can be used to reveal significant interactions between factors. Interaction plots for all MOEs are grouped in Figure 63 through Figure 66. Observations are as follows:

- **MOE #1:** C-UAS DiD capability yields the best P_{Sense} measures against both sUAS configuration types.
- **MOE #2:** C-UAS Cyber-attack capability yields the lowest Time to Assess against both sUAS configuration types.
- **MOE #3:** C-UAS DiD capability yields the highest $P_{Neutralize}$ measures against both sUAS configuration types.
- **MOE #4:** C-UAS DiD capability yields the shortest Time to neutralize against both sUAS configuration types.

- **MOE #5:** C-UAS Cyber-attack capability yields the Neutralization points that are furthest from the priority location against both sUAS configuration types.
- **MOE #6:** C-UAS DiD capability yields the best $P_{Effectiveness}$ measures against both sUAS configuration types.
- **MOE #7:** C-UAS Baseline capability yields the best Energy Effectiveness measures against both sUAS configuration types.

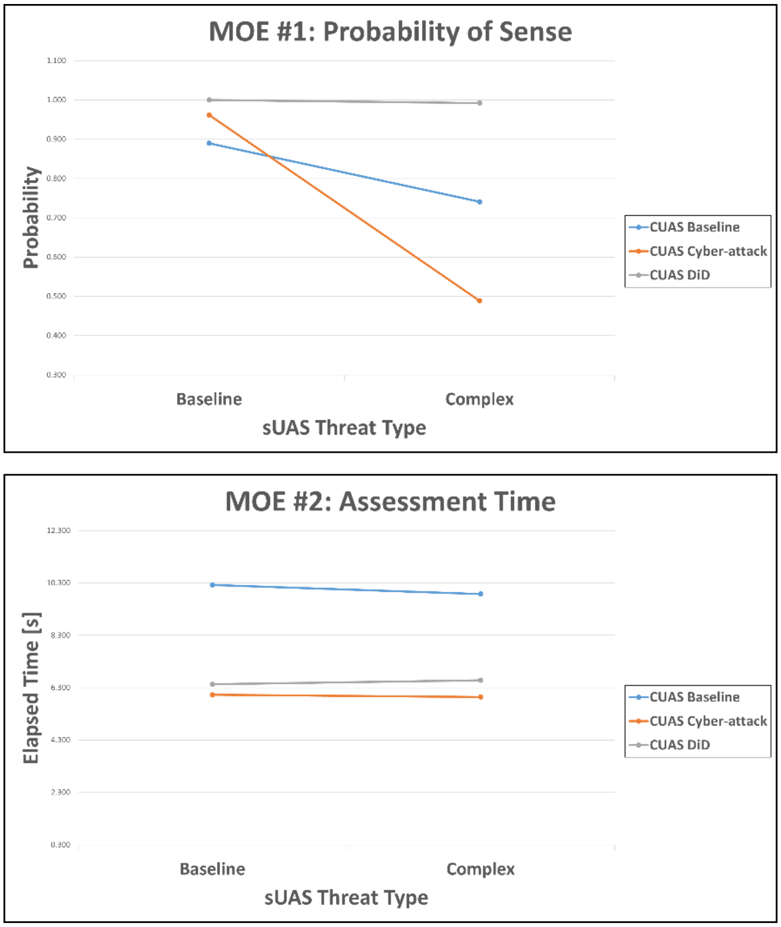


Figure 63. Interaction Plot Summary (MOE #1 and MOE #2)

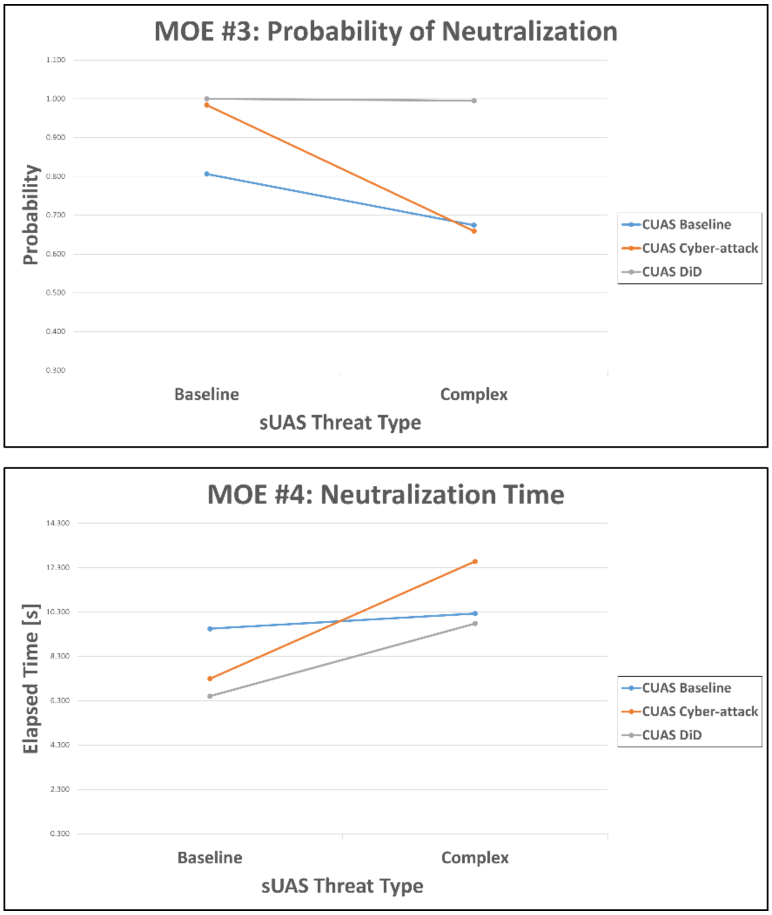


Figure 64. Interaction Plot Summary (MOE #3 and MOE #4)

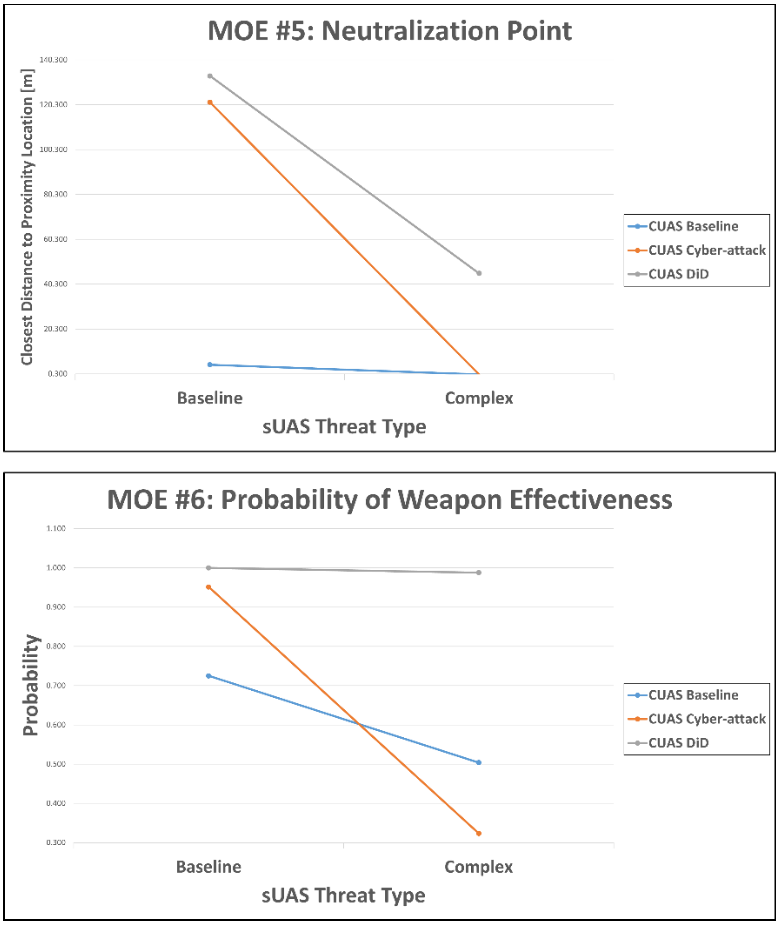


Figure 65. Interaction Plot Summary (MOE #5 and MOE #6)

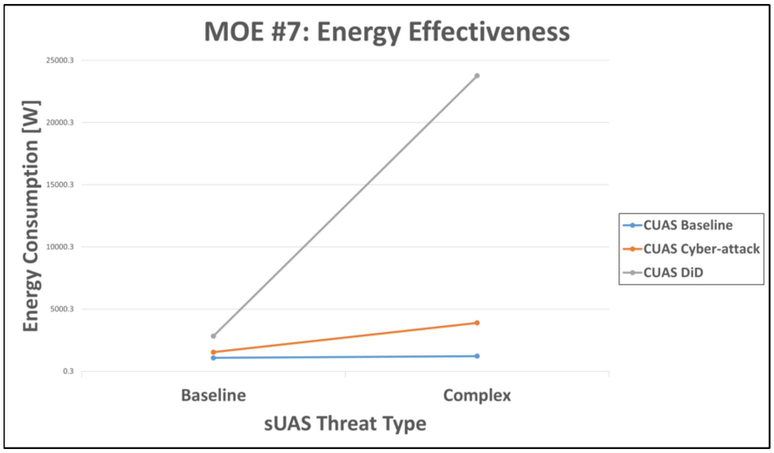


Figure 66. Interaction Plot Summary (MOE #7)

5. Qualitative Summary

The UAS Architecture scoring summary is outlined in Table 32. Two points are awarded to the C-UAS capability configuration that achieved the best measure against any one of the sUAS configuration categories. If a C-UAS capability configuration achieves best measure against both sUAS categories, then a total of three points are awarded. One point is awarded to the C-UAS configuration with the second-best measure. In addition to the MOE scores, a point category was added for cost to consider the cost benefits of opting for a system with an assessed lower total ownership cost. The result is that the C-UAS DiD configuration achieved the highest score as it performed equal or better against the other C-UAS configurations in five out of seven MOE categories. It should also be noted that the C-UAS Cyber-attack configuration is assessed to be a viable alternative to the DiD configuration; C-UAS cyber-attack achieves comparable performance with DiD for radio-controlled sUAS threats, and it offers a low-cost, mobile (not scored) solution.

Table 32. C-UAS Configuration Scoring Summary

	Baseline	**Cyber-attack**	**Defense-in-Depth**
MOE #1	1	1	3
MOE #2	0	3	2
MOE #3	1	1	3
MOE #4	1	1	3
MOE #5	0.5	1.5	3
MOE #6	1	1	3
MOE #7	3	2	0
Cost	2	3	1
Total	**9.5**	**13.5**	**18**

B. OBSERVATIONS

The research efforts captured in this report demonstrated that a Mission Engineering approach to use systems and SoS within operational mission context contributes significantly to maturing the C-UxS concept. Furthermore, the application of MBSE principles helped to promote efficiency and reuse of the mission architecture, in order to provide a reliable means of defining mission elements (operational behaviors, systems, relationships, information flow) within the constraints of the operational mission context (scenario & vignettes).

A CONOPS was developed to capture the accomplishment of commander's intent with known and planned resources. Once the specific stakeholder questions were understood and constructed into a problem statement, a mission definition and characterization was developed to provide the appropriate mission context, conditions and assumptions to be used as inputs to analysis. The mission definition was translated into a mission architecture that identified the operational performers, operational tasks, information and data flows, generalized systems, and specified performance measures. This mission architecture elements can be integrated to describe relevant systems/ capabilities executing end-to-end tasks within a mission context. Varying these systems/ capabilities and tasks to develop alternative approaches and SoS architectures (vignettes/ mission threads) helps to focus the scope to a specific problem statement. Once the sufficient conditions and data is identified, analysis can be conducted to obtain and document the results to draw conclusion suitable for answering the problem.

This project developed the DROSERA Analysis Tool as its C-UAS M&S environment. This tool aims to capture the mutual relationships of systems and the dynamic nature of these environments that will help illustrate mission effectiveness, asset preparedness, and projected resource requirements of capability deployment and is developed based on an architecture that references and emulates all model elements of the C-UAS mission characterization to include system performance characteristics, threat sUAS performance characteristics, environmental conditions, and capability metrics. The DROSERA analysis tool relies on agent-based modeling (ABM) and applies Monte Carlo methods to the ABM scenarios to generate non-deterministic behaviors associated with the operational scenario.

The DROSERA Analysis Tool performed simulations on six architecture variants that represented a unique vignette of the C-UAS Combat Patrol scenario, varied based on the C-UAS capability configuration and Threat sUAS packages employed in each scenario. Monte Carlo analysis was performed running 100 iterations of the C-UAS Combat Deployment Operational Scenario. Simulation results were tabulated and model analysis was performed. Statistical, output, and qualitative analysis of the simulation date revealed that C-UAS DiD configuration achieved the highest score based on unmatched performance across seven MOE categories, but the C-UAS Cyber-attack configuration is assessed to be a viable alternative to the DiD configuration because it offers comparable performance with DiD for radio-controlled sUAS threats, and it offers a low-cost, mobile solution.

In conclusion, the DROSERA project has successfully demonstrated, via proof of concept, that the C-UAS scenarios and vignettes implemented and analyzed were traceable to C-UAS strategic objectives, aligned with Joint tasks, and could satisfactorily identify impacts on mission effectiveness and system performance. It is recommended that the C-UAS Mission Model and the DROSERA Analysis Tool continue to be utilized and refined to support the definition and analysis of more specific research questions as pertaining to C-UxS.

C. RESEARCH QUESTIONS ANSWERED

As stated in Chapter II, the goal of this report is to develop a C-UAS CONOPS and a mission architecture that can model and simulate operational scenarios that emulate the scenarios emphasized in the CONOPS. The analysis of these scenarios can draw conclusions on the suitability of the selected systems with specific focus on cyber-attack resilience, reliability, and their impact on C-UAS effectiveness and energy needs. To support that development, there were six questions posed in Chapter II that were subsequently answered in Chapters III-VI and Appendix A.

1. What are the performance measures of the mission?

The defined performance and mission effectiveness metrics align with the identified stakeholder priorities. Section III.D.2 provides detailed descriptions on the C-UAS MOEs and MOPs for the proposed operational scenarios to support the mission architecture.

2. Which technology or capabilities are to be evaluated?

Detailed descriptions on the C-UAS capabilities of sense, assess, and neutralize that were evaluated along with potential C-UAS technologies that can support each capability were outlined in Section IV.D.

3. What are the mission capability gaps?

The proposed CONOPS focused on the sense, assess, neutralize, and energy resilience capability gaps in C-UAS systems in addressing the sUAS threat. Appendix A provides details on the C-UAS capability gaps that currently exist across the operating environment in addressing sUAS threats.

4. What is the optimal force mix for maximizing mission effectiveness and energy efficiency with reliability and resilience as the variables?

When determining the best solution, the team analyzed the simulation results against the seven following MOEs: probability of sense, assessment time, probability of neutralize, neutralization time, neutralization point, CUAS weapon effectiveness, and energy effectiveness. Supplemental information outlines the simulation results obtained from the models created in support of the projects experimental design. Section VI.A provides the analysis of the results from the simulation data.

5. What models are required to conduct the analysis?

The architecture variants represent a unique vignette of the C-UAS Combat Patrol scenario that also varies the modeled C-UAS capability configuration along with the threat sUAS packages employed in each scenario. Section V.G outlines the experimental design strategy that was developed to emulate the behaviors of the C-UAS system performers based on their respective performance measures in the C-UAS mission architecture.

6. What models are already accessible? Do the required models already exist?

The team was able to utilize available open-source technical performance data along with previously completed experimental data for platforms that were simulated in the model. Section V.G.2 outlines the C-UAS system performance characteristics and Threat sUAS performance characteristics of the agent-based model created. The models required to support this project were not in existence prior to the Team DROSERA effort.

D. RECOMMENDED FOLLOW-ON WORK – MISSION AND SYSTEM OF SYSTEMS ARCHITECTURE MODELING

The C-UAS Capability Framework developed by the DROSERA project requires a model-based environment for both mission models that realize the mission architecture (detailed structure of the conduct of the mission) and platform models that realize the SoS architecture (detailed description of the systems required to execute the mission). While Team DROSERA utilized Innoslate to construct models in the operational and resource domains needed to demonstrate the feasibility of the C-UAS operational concept and answer the research questions fundamental to C-UxS operational and energy analysis. The following topics are recommended for consideration for follow on efforts in improving the model-based environment.

1. Project Dashboard

The use of a dashboard for a system or mission model is a recommended practice in MBSE; the dashboard provides a visual representation of the important aspects of the model. For the project it is recommended that the dashboard be organized in groupings corresponding to the DoDAF Architectural Development 6-Step Process (Figure 3), containing links to the primary views prescribed by the Middle-Out MBSE Process (Figure 4).

2. Mission Engineering Threads

Every vignette evaluated within the C-UAS Operational Concept has an associated mission thread that includes the technical details of the capabilities and systems required to execute the vignette mission. Thus, each vignette realized in the model can be referred to as a Mission Engineering Thread (MET), containing an *Operational Architecture* that capture the tasks needed to provide C-UAS capabilities, which are in turn implemented by a *Capability Configuration*, representing the physical and human resources assembled to meet a capability (Object Management Group [OMG] 2022). These METs are specific instances of the C-UAS mission model and need to be packaged and defined as such. Within Innoslate, The DROSERA project intended to capture these METs as branched projects from the C-UAS mission model, with concordance of generalized entities maintained by the Innoslate tool's *Cross Projects Relationships* feature.

3. Dynamic Analytical Methods

While the DROSERA Analysis Tool serves as the primary engine of analysis and discovery for this project, it is reasonable to conclude that there are some behaviors that may be difficult to incorporate using the agent-based modeling approach. One such example includes human-in-the-loop behaviors exhibited in the C-UAS Assess phase that are difficult to emulate. The Innoslate supports execution of the mission threads with a discrete-event-simulator and comes with a complete set of application programming interfaces (APIs) that could be used to integrate with the DROSERA Analysis Tool, pushing or pulling information as needed to supplement the overall vignette simulation.

4. Architecture Framework Traceability

Since the primary stakeholders of this project either belong to or directly support DOD organizations, it is a priority that the C-UAS mission model generate views that are DoDAF-compliant. It is purported that LML utilized by Innoslate can be extended to develop entities and relationships that are aligned more closely with the DoDAF Metamodel. Extending LML to provide a more accurate description of DoDAF does not seem practical when you consider that there are modeling languages better suited to describe a DoDAF-compliant enterprise architecture with little to no customization. The Unified Architecture Framework (UAF) Enterprise Architecture (EA) provides a modeling language that allows Systems Modeling Language (SysML) implementation of models, provides an architectural framework that is a foundation for DoDAF, and maintains traceability to other architectural frameworks. Notably, there is a modeling tool available for use via the NPS CloudLab server that provides a UAF standardized solution - Magic Systems of Systems Architect (MSOSA) (Dassault Systems 2022).

It is conceivable to establish an extended architectural framework that utilizes an LML-based tool for the conceptual and logical definition of the C-UAS architecture (*Architectural Conceptualization*), while relying on a UAF-based tool for the physical definition of the SoS architecture (*Architectural Elaboration*). A graphical example of this concept is depicted in Figure 67 (OMG 2022, 4).

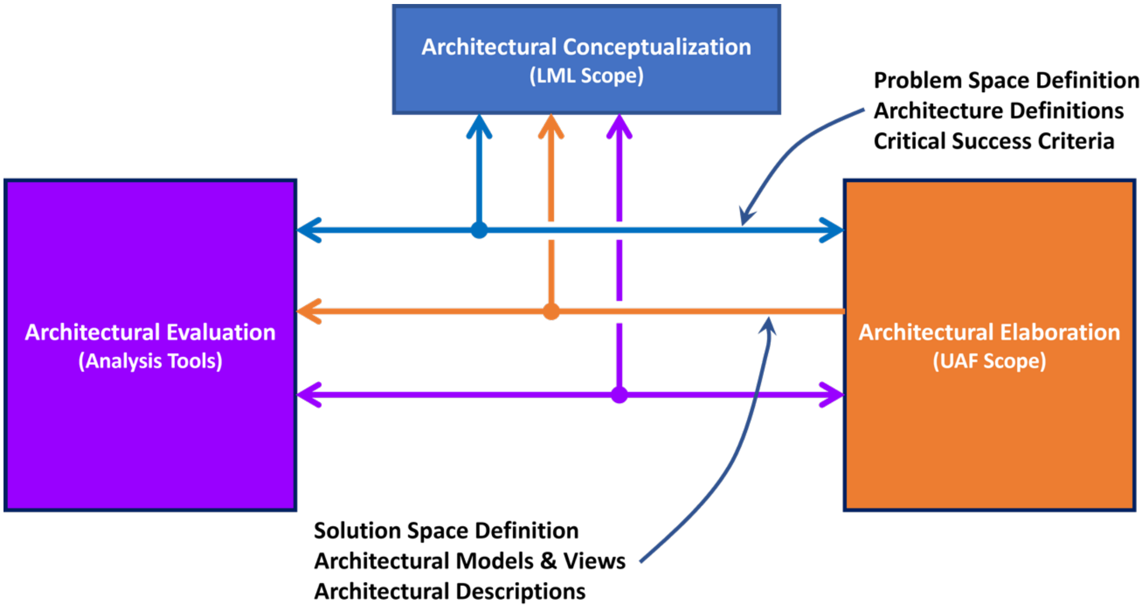

Architectural Conceptualization
(LML Scope)
Problem Space Definition
Architecture Definitions
Critical Success Criteria
Architectural Evaluation
(Analysis Tools)
Architectural Elaboration
(UAF Scope)
Solution Space Definition
Architectural Models & Views
Architectural Descriptions

Figure 67. Architecture Framework Traceability Concept. Adapted from OMG (2022).

E. RECOMMENDED FOLLOW-ON WORK – MODELING & SIMULATION

The DROSERA Analysis Tool described in this report and provided as supplemental information is the initial foundation demonstrating the key interactions and behaviors within defense in depth and asymmetric warfare concerning the relationships of C-UAS and UAS. While much has been completed and accomplished with the available time and resources concerning the creation of this capstone and its resultants, there still exist developments for further impact and achievement. The following denotes a combination of either topics that require further research or desired additions identified to continue in refining the capability framework developed by the Team DROSERA Capstone project:

1. All-Inclusive Element Properties

Spanning all placeable elements within the DROSERA Analysis Tool, to include sUAS, C-UAS, and Priority Locations, there are a variety of factors that can be developed to further enhance the applications and accuracy of this model. These additions are listed below:

Degraded Status: At current within the simulation there is no method or variable in place to track damage to a modelled element. The representation of existence and operability is binary. With the addition of a trackable "health bar" to elements within the simulation will further track effectiveness at a higher resolution and add further complexity and realism. Examples of how this may be applied and affect the DROSERA Analysis Tool are itemized as follows:

1. **sUAS –** While UAV platforms are not known for their physical robustness as they are generally sensitive and fragile, increased resolution on possible damage towards a UAV, or even with an increased scope to include all elements within UAS, could yield valuable results.
2. **C-UAS –** With the consideration of health in mind concerning C-UAS, attributes within a system can demonstrate degradation or overall destruction as a whole as it is damaged. This could yield notable results from red-teaming strategies such as overwhelming or targeted strikes.
3. **Priority Assets –** Regarding the mission goals, or priority assets, within the simulation, tracking conditions would be beneficial not only as an after-simulation result identifying successfulness of CUAS defenses, but also as a dynamic modelling element. This could affect a simulation during run-time in that as priority assets receive successful attacks by

UAS threats and sustain sufficient damage, if non-deployed or UAVs still exist, they can be re-tasked.

Route/Path Dynamics: An additional attribute to be applied across these elements, pathways would include the ability for a simulation element to move in a user-defined path. This provides further dynamics to the model pertaining to the following:

1. **sUAS –** Inherent to the UAV is the ability to move in order to reach their targeted destination to complete their outlined goal. However, through user-defined pathways, improved mission planning regarding path planning of UAV threat becomes possible. This will allow mirroring of piloting or more complex waypoint navigation ultimately improving accuracy and complexity of the DROSERA Analysis Tool
2. **C-UAS –** Apart from the cyber-attack UAVs within the simulation, all C-UAS systems were modelled as stationary; therefore, increasing the autonomy on part of the C-UAS systems would be an additional measure to implement in future research. This addition could be used to implement patrol behavior, which will be elaborated upon later in this section, among other possibilities
3. **Priority Assets –** By providing pathway and movement characteristics to priority assets it would greatly expand the possibilities of vignettes and scenarios within the simulation. In particular, this would allow for the capture of convoy or underway vessels as operational spaces, which are both significantly susceptible to asymmetric warfare.

Sensor Characterization and Definition: Currently, sensor suites associated to UAS and C-UAS have been generalized for simplicity. By further outlining, defining, and characterizing applied sensors within these elements, more realism can be achieved as these agents interact with each other and their environment.

Areas of Influence: Defensive and detection space associated with elements within this simulation have been conveniently denoted as the area of a circle. To introduce further intricacy in an attempt to better model a wider variety of capabilities more accurately, it would be better to define these spaces as a user-defined polygon. Ideally, this would be provided through the user specifying individual points within a sequence with the polygon be generated after they have finished.

Packages and Customization: As a result of the DROSERA Analysis Tool's user inputting process of defining elements within and characteristics continually evolving into a further complex and time-consuming process, it is advantageous if not entirely necessary to introduce a method in which to save and manage elements and simulations. From this, simulation time can be expedited where previous capabilities can be loaded, or entire scenarios all together.

Effects Chain Refinement: For initial simplicity, the effects chain within the simulation combines the detection and identification processes of the scenario. It would be beneficial to model these individually to increase the resolution concerning the overall effect chain of the sUAS and C-UAS relationship.

Emergent Behavior Analysis: The simulation was focused on assessing the functionality of the resource performers modeled to ensure their behaviors were yielding results that one would expect to see. The model could be refined to instead explore emergent behavior and investigate what system behaviors occur when they are interacting with one another.

2. Blue-Forces Specific Properties

To better capture realistic settings and variables pertaining to drone defense and forces, there exists a seemingly infinite range of possibilities. A few that have been identified by team DROSERA include:

- **C-UAS:** The elements of C-UAS within this simulation were designed ideally to capture capabilities within a generic form. Following this approach, an additional factor that would be desired is the ability to have responsive and adaptable capabilities that react to an event occurring in the scenario. Specific examples include the following:

1. **C-UAS Deployment** – C-UAS that is deployed to a location once a threat is detected. This introduces a unique representation of behaviors similar to security forces responding to a UAS threat. This would be valuable in characterizing and analyzing the effectiveness of a security response event chain. Use of a responsive or reactive capability as described would be paired with a new purposed ability to include individual personnel assets. These agents could identify possible drone threats through visual means, as well as possibly by using an RC spectrum analyzer. They would also be outfitted with a C-UAS capability, such as drone defender, which can neutralize an individual UAS.
2. **C-UAS Behavior Attributes** – Introducing behavior patterns for the activation of the C-UAS capabilities, this would allow the user to vary energy usage strategies in order to assess efficiency.
3. **Refined System Performance Measures** – Implementation of more accurate system performance measures from additional known deployed C-UAS systems to increase the validity of the data produced from the simulation runs. The parameters used in the models were derived from open-source documentation and higher fidelity performance measures would allow for further model validation against real world data to achieve an operationally accurate model.

Priority Assets: Priority assets in the model represents a goal for C-UAS to defend and UAS to assault. As such, they are fairly simplistic, lacking much of the complex behavior or detail characteristics and attributes as other portions of the simulation. However, by changing this, an additional dimension and further realism can be acquired.

1. **Assets with Effects –** Similar to the other elements within the DROSERA Analysis Tool, priority assets should have special attributes or behaviors associated. One possibility could be power supply assets, such as powerlines or power stations, that when damaged or destroyed will deactivate C-UAS infrastructure. Another such example is a security

station in which security response forces previously identified would be deployed from. Destruction of this asset would remove the corresponding spawn location of this capability.

2. **Collateral Assets –** Existing in reality but absent from this simulation is the representation of possible collateral damage. The inclusion of collateral assets would be one of the methods in which to introduce this important data point. This would include non-combative or civilian locations that may be present and targeted in a scenario and should be subsequently represented within the simulation where they may be affected directly or indirectly, which will be elaborated on further in this section.

3. Red-Forces Specific Properties

As the aggressing force within the simulation, accurate representation of Red-force elements is pivotal for demonstrating system effectiveness and highlighting any possible complications within a scenario. This simulation begins to scratch the surface within these complex relationships where further improvements and additions can be made, a few of which have been identified as follows:

Improved Tactics – Captured within the current version of the simulation exists rudimentary methods of mission planning and strategic capabilities concerning deployment and incursion tactics. A highly desirable improvement to this model would be the tuning and expansion of Red-Force tactics to better emulate possible threats.

Complex Swarm Behavior – Introducing complex swarm capability into the simulation for the modeled adversary UAVs would allow the agents to react to the simulation environment and provide more interesting behavior for which to assess the C-UAS capabilities. This would involve reactive behavior through forms of autonomy which have been defined by the user.

Enhanced Mission Planning – Integration of standard mission planning practices would include such items as operative keep-out zones as well as waypoint path planning which was mentioned earlier in this section.

sUAS Payloads and Behaviors – In continual attempt to better emulate a more accurate scenario is the development of further capabilities to expand upon threat toolbox. In order to construct these, logic state charts and subsequent java programming are necessary pertaining to the desired behavior

Intelligence, Surveillance, and Reconnaissance (ISR) – The goal of an ISR platform is to collect and extract information regarding a target. The platform would go to a target location, survey the environment, and then return to its initial launch or another user-denoted location.

Electronic Warfare (EW) – An EW platform within the application of the simulation is tasked to affect or interrupt CUAS abilities to detect or neutralize a UAS threat. This can be used to significantly impact a defensive environment and lead to further complex scenarios

Loitering – The goal of a Loitering platform is to provide a capability with a reactive and delayed action until a user-defined event occurs.

No-payload – Resulting from the fact that the response time needed to effectively react to a possible UAV threat is notably small, the usage of simple UAVs without payloads are effective in occupying C-UAS resources, restricting an asset's ability to appropriately defend itself, consequently improving the survival likelihood of other UAS employed.

Collateral Damage – Depending on neutralization method, when a UAV is interdicted, there is a likelihood percentage of it damaging something within the area it was neutralized such as by crashing into an asset and should be modelled within the simulation.

4. Environment Properties

Due to schedule constraints, there were no environmental or geographical conditions introduced into the simulation model. The introduction of these variables would influence sensor and radar performance measures in a variety of ways and provide potentially more realistic data. For the continued pursuit of accurate emulating the environment, below are a few examples of purposed environmental properties.

Weather: Weather within an operative environment can lead to a variety of hinderances as well as improvements to both C-UAS and UAS performance. How these systems may be affected is briefly outlined below for future integration within the simulation represented over time through the model's runtime.

1. **sUAS –** Factors such as rain, excessive heat or cold can affect the operability and spontaneous chance of failure within platforms. Additionally, high winds can affect the speed, operational range, and capability of UAVs depending on direction, where a consistent tail wind improves, and a headwind reduces flight time. Lastly, fog will reduce visibility of Visual Line of Sight (VLOS) platforms or those that use video streams for navigation.

2. **C-UAS –** Similar to UAS, extreme weather can influence the abilities of C-UAS. However, these systems tend to be more rugged as the majority do not the physical limitations of UAVs. However, extreme head and cold can still affect system operability. Further, fog will also reduce visibility systems that require VLOS or video streams for detection and neutralization.

Time of day: Time of day predominately affects visual abilities across UAS and C-UAS. These can result in UAVs having improved performance concerning avoidance of detection and neutralization, improving likelihood of survival. However, this factor mutually affects both UAS and C-UAS's ability to identify targets. Lastly, if collateral assets are introduced to the simulation, time of day would also affect the number of possible collateral agents, such as non-combative personnel or vehicles.

3D Operation Space: In order to improve agent interactions, it would be beneficial to expand the current 2D space into a 3D environment to best capture all affects presented within the complex scenario. This can introduce unique perspectives regarding VLOS limitations among other issues.

Frequency Spectrum Modelling: Absent from this model that is significant within actual operation is the reality of existing and conflicting communications. A notable complication of this reality is the interference between all elements that use or interact with communication frequencies. This is further complicated with the possible introduction of collateral effects from C-UAS infrastructure as wide area communications denial, that influences possible blue or neutral communication frequencies.

Non-Combatant UAVs: An interesting scenario could include the nearby operation of a non-combatant UAV, such as those used by civilians, that could further complicate the detection and identification event chain for the simulation. The presence of such elements would draw resources away from possible defense of priority assets.

Obstacles: The introduction of obstacles such as towers, trees, and other entities to mirror an environment adds complexity to the model in that it could conflict with the UAVs path planning or VLOS of elements.

Roads: Providing roads within a scenario can allow for such factors as increased movement speed of ground operated and deployed CUAS, as well as offer a representation of restrictions of travel for possible mobile priority or collateral assets.

5. User Interface (UI) Improvements

With the increasing additions of possible new elements, attributes, and more to an already complex simulation it would be beneficial to improve and further develop various characteristics of the UI presented within the DROSERA Analysis Tool. Involvement of a specialist concerning this, such as a human factors engineer, is recommended. Noted below is a collection of identified items aimed to improve user and simulation interactions:

Element Manipulation and Definition: As one of the most tedious procedures within the model, improvement concerning placement and definitions of capabilities are necessary. This would include such features as: a “drag and drop” method in which to place and move existing capabilities; creation of a window that displays currently active elements that can be deleted, copied, or edited; and an improved toolbox in which to access and define elements for the simulation.

User Focused Status Bars: With the enormous amount of data and interactions between agents occurring within an individual simulation it is difficult to remain perceptive of all factors. With the addition of status bars that show metrics as the simulation is running presenting variables as enemy count, power used, cool down time, the user can better avoid information overload.

Operation Space and its Manipulation: Presently the simulation's operation space is limited to a fixed area. Ideally, to capture larger and more variable environments this board needs to be extended and defined by the user. Subsequently, it is also necessary to introduce a method in which to navigate this space in such factors visually and with the ability to move focused space with zoom, panning, etc.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. CONOPS

This Concept of Operations (CONOPS) is an initial effort to provide the project stakeholders with Counter UAS (C-UAS) Operational Concept, in order to inform current and future capability developments, including operational and system requirements. This CONOPS aligns with ongoing joint efforts (DOD 2020; DHS 2019; DEPS 2018; JCS 2017; Jasper 2021).

This CONOPS focuses on the use of sUAS as a means of enabling asymmetric warfare, where the primary threat employed in most cases is by a less capable adversary. While the C-UAS operational context will capture all phases of the warfighting effects chain, the CONOPS scenarios will specifically focus on the phases of the mission that uniquely challenges the C-UAS capability (Figure 68). These focus areas are denoted as: Sense (detect, classify, locate, and track), Assess (decide how to respond to threat and determine desired effect/targeting solution), and Neutralize (engage).

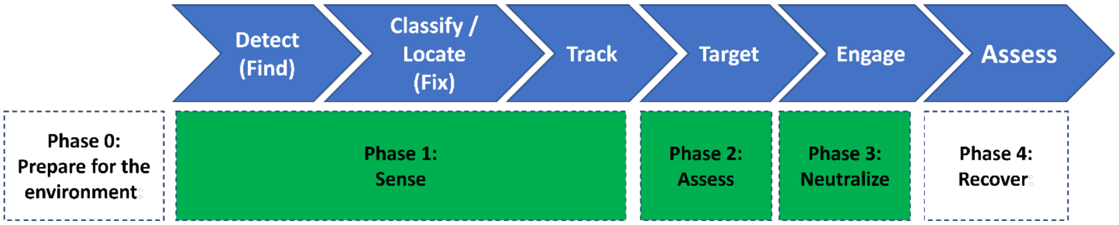


Figure 68. C-UAS Operational Scenario Priorities

The operational environments outlined within this CONOPS include the defense against sUAS threats for both a fixed installation and a small mobile asset, such as a combat team conducting patrols. The operational scenarios that can be represented in the aforementioned environments include the following threat characteristics:

- **Actors:** Ranging from ideologues acting alone or as coordinated squads to state-sponsored forces.

- **sUAS Technology:** Ranging from customized commercial equipment with standard interfaces to militarized equipment with indeterminate vulnerabilities.
- **sUAS Autonomy:** Ranging from single UAV operating with semi-autonomous ability in cooperation with line-of-sight (LOS) ground station to multiple UAVs exhibiting swarm behaviors (Giles 2016) and operation autonomously with a command, control, and communications (C3) link available to a leadership cell that is beyond LOS.

While operational concept diagrams will be included for both the installation defense and combat patrol scenarios, more detailed scenario descriptions and operational views will only be provided for the combat patrol scenario. The operational scenario for C-UAS combat patrol presents the most uncertain and complex operational environment and will allow for the application and assessment of the widest range of threats and conditions.

In summary, this CONOPS serves to:

- present the C-UAS problem
- introduce components (operational performers) anticipated for its solution
- provide the operational concept for C-UAS
- present a mission scenario narrative

A. MILITARY PROBLEM

In the Counter Small Unmanned Aircraft Systems Strategy (DOD 2020, 7), Department of Defense (DOD) asserts the following with regards to the threat of sUAS:

> The emergence of sUAS as both hazard and threat has complicated an already complex and challenging security environment. While fundamentally aircraft, sUAS exist in the gap between air defense, force protection, and airspace control across the operating environment continuum. The continued proliferation of these systems will challenge DOD's existing paradigm for how it addresses emergent technologies that may pose a threat to the force. (DOD 2020, 7)

Furthermore, the aforementioned strategy also recommends that DOD stakeholders and allies work collaboratively to achieve the following strategic objectives (Figure 69):

> (1) Enhance the Joint Force through innovation and collaboration to protect DOD personnel, assets, and facilities in the homeland, host nations, and contingency locations; (2) Develop materiel and non-materiel solutions that facilitate the safe and secure execution of DOD missions and deny adversaries the ability to impede our objectives; and (3) Build and broaden our relationships with allies and partners to protect our interests at home and abroad. As a Department we will address those objectives by focusing on three lines of effort (LOEs): Ready the Force, Defend the Force, and Build the Team. (DOD, 2020, 10–11)

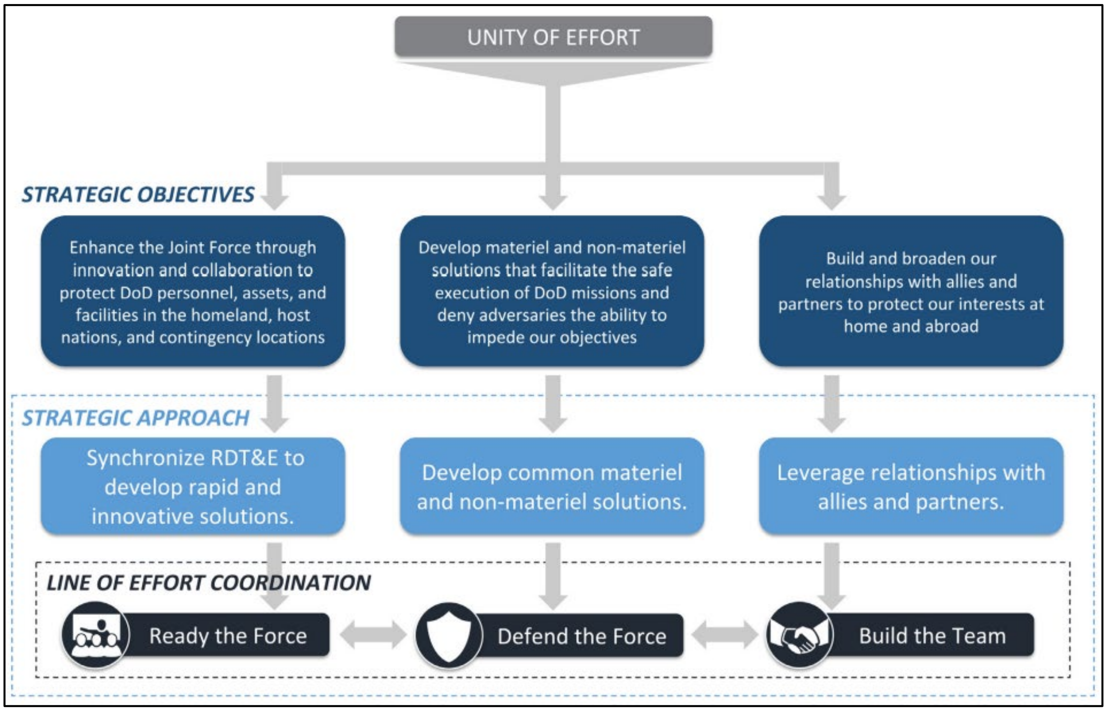

UNITY OF EFFORT
STRATEGIC OBJECTIVES
Enhance the Joint Force through innovation and collaboration to protect DoD personnel, assets, and facilities in the homeland, host nations, and contingency locations
Develop materiel and non-materiel solutions that facilitate the safe execution of DoD missions and deny adversaries the ability to impede our objectives
Build and broaden our relationships with allies and partners to protect our interests at home and abroad
STRATEGIC APPROACH
Synchronize RDT&E to develop rapid and innovative solutions.
Develop common materiel and non-materiel solutions.
Leverage relationships with allies and partners.
LINE OF EFFORT COORDINATION
Ready the Force
Defend the Force
Build the Team

Figure 69. C-UAS Unity of Effort.
Source: Department of Defense (2020).

This CONOPS will prioritize on the C-UAS *Ready the Force* LOE and seek to align current and future capability development to defeat threat sUAS. Specifically, this CONOPS will focus on the following sUAS capability gaps:

1. **Sense Capability:** sUAS are difficult to detect, classify, locate, and track.

2. **Assess Capability:** A human-in-the-loop performer must decide how to respond to the threat and determine desired effect/targeting solution.

3. **Neutralize Capability:** Mitigation systems are required to intercept and isolate/disorient/disable/destroy threat sUAS.

4. **Energy Resilience Capability:** Minimize, adapt to, and recover from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability sufficient to provide for mission assurance and readiness (Department of the Navy 2020, 2).

B. OPERATIONAL CONTEXT

A summary of the operational context is provided here to define the primary phases of C-UAS effects chains, identify the primary performers, and introduce the capability functions required to satisfy the effects chain. As depicted in Figure 70, there are two tiers of operational environments that C-UAS operational concept will need to address: defense of a *stationary asset* such as a base or airport that contains one or more operational Centers of Gravity (COG) from an adversary's point of view, and a *moving asset* that consists of a less than battalion size troop deployment with possible critical assets tasked to conduct patrol in support of mission objectives. For the stationary asset, the primary C-UAS challenge is providing defense over a wide area, and for the moving asset the primary C-UAS challenge is having limited capabilities to defend against attack. In both operational environments, the C-UAS operational concept will employ defense-in-depth (DiD) strategies to leverage multiple layers of defense in a dynamic threat landscape.

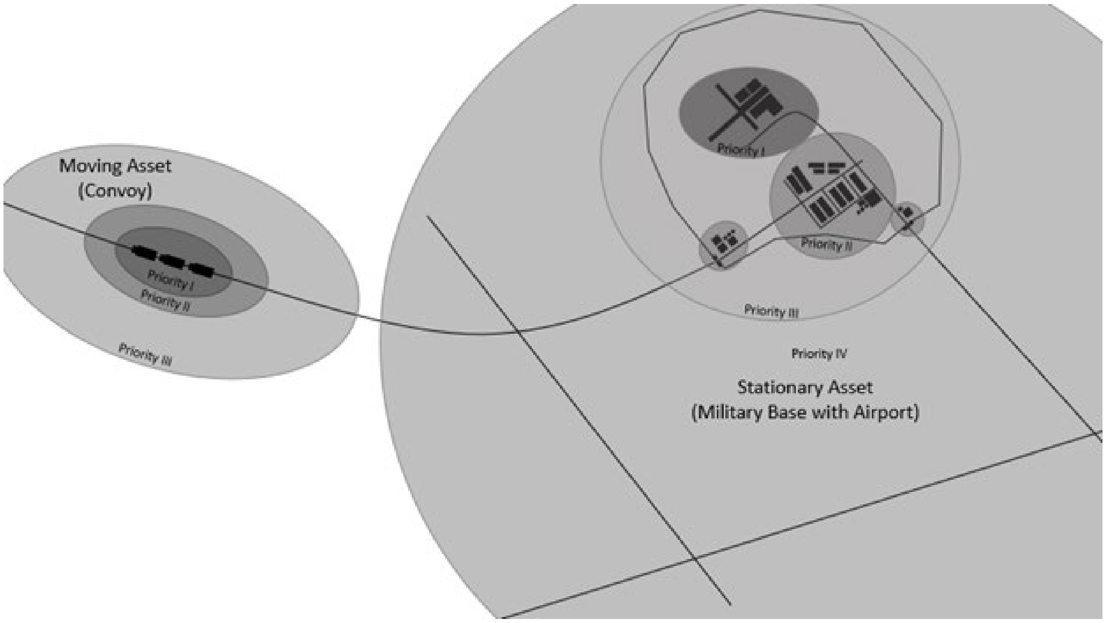


Figure 70. C-UAS Operational Environments

For each operational scenario captured in the CONOPS, the sUAS threat will attempt to close on the high value assets (Priority I) undetected from one or more axes. The goal of the C-UAS integrated system will be to thwart this attempt at far standoff distances from the high value assets (Priority IV or higher).

A scenario walkthrough will now be presented. A C-UAS effects chain to operational scenario mapping is depicted in Figure 71 for reference. The forthcoming scenarios were constructed according to guidelines presented in Army Techniques Publication, *C-UAS Techniques* and the Center for the Study of the Drone's *Counter Drone Systems* (Department of the Army [Army] 2017; Michel 2019).

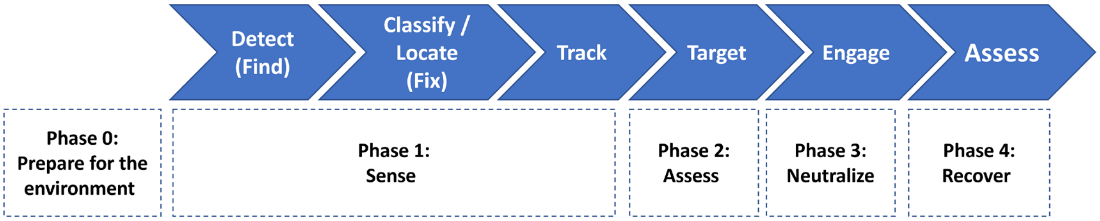


Figure 71. C-UAS Effects Chain to Operational Scenario Mapping

5. Phase 0: Prepare for the environment

This phase involves understanding the mission, threat, and other operational variables that assists the commanders and staff in developing deployment and operations plans.

> Knowing these conditions allows commanders to make the right decisions on unit and movement readiness, air and ground threat considerations, and unit training. Commanders need to know detailed, updated information and predictive intelligence about the threat disposition capabilities, and intentions.
>
> Organizations should train the force assigned air guard to perform observation and identification to improve rapid detection and reporting of sUAS. If RF sensors are available, they should be tuned to search for sUAS that meets the expected threat criteria for the current environment. Commanders should also employ TTP that will help to mitigate the possibility of friendly forces becoming lucrative targets. Practicing avoidance TTP reduces the unit's chances of detection from the enemy and becoming targets of opportunity. One such TTP may be to ensure units are trained in air threat avoidance techniques. For example, the unit could use routes with natural cover or travel at night to mask its movements. (Army 2017, 1–5)

Characteristics are:

- **Proximity to High Value Asset:** Outside Detection Range
- **Effects Chain Phase:** Not Applicable
- **Capabilities Employed:** Deterrence, IPOE
- **Operational Performers:** Intelligence Cell, C-UAS Commander, Air Guard, Sensor

6. Phase 1: Sense

Successful completion of this phase requires that a sensor detect, classify, locate, and track an adversary sUAS.

> Depending on the type of system used, a sensor that makes an initial detection, such as a wide-area search radar or an RF detector, may have to "cross-cue" to secondary sensors such as cameras or electronic identification elements to confirm that the detected object is in fact a threat sUAS, as well as determine its precise location and track its movements. Secondary sensors may also serve to provide additional information about the sUAS, which may help determine intent. For example, a camera may be able to show whether a sUAS appears to be carrying explosives. Certain electronic sensors may be able to additionally identify the location of the drone operator. Sensor data can often be stored for later use as evidence. (Michel 2019, 5)

Characteristics include:

- **Proximity to High Value Asset:** Priority IV
- **Effects Chain Phase:** Detect, Classify, Locate, and Track
- **Capabilities Employed:** Monitor, C2
- **Operational Performers:** C-UAS Commander, Air Guard, Sensor(s), C2 Cell

7. Phase 2: Assess

Based on the information from these sensors, a human operator using tactical decision aids must decide how to respond to the incoming sUAS threat.

> Depending on the threat level and time available, the Commander would select an appropriate mitigation approach. Particularly in civilian environments, where the authority to disable or destroy may not be legal, C-UAS operators often describe mitigation as a "last resort" measure. C-UAS teams may have an extremely limited window of time to make this decision. C-UAS UAV standby, launch, and intercept decisions are made during this phase. (Michel 2019, 5)

Characteristics are:

- **Proximity to High Value Asset:** Priority III – IV
- **Effects Chain Phase:** Target

- **Capabilities Employed:** C2
- **Operational Performers:** C-UAS Commander, Sensor(s), C2 Cell, UAV

8. Phase 3: Neutralize

A mitigation system is activated, and the sUAS is intercepted. Depending on the technique used, this could result in a range of effects, including the drone landing on the ground or activating a "return to home" mode (in the case of jamming or spoofing), the capture of the drone (nets), or the complete or partial destruction of the threat sUAS (lasers, projectiles, collision UAVs, high powered microwaves). (Michel 2019, 5)

Characteristics include:

- **Proximity to High Value Asset:** Priority I – IV
- **Effects Chain Phase:** Engage
- **Capabilities Employed:** C2, Neutralization
- **Operational Performers:** C-UAS Commander, C2 Cell, UAV

9. Phase 4: Recover

Depending on the circumstances, once a threat sUAS is intercepted the device may need to be isolated and retrieved. If the drone is potentially armed, an explosive ordnance disposal team may be called in to assess and, if needed, disable the device. Unarmed drones must likewise be treated with caution. If the device is damaged, its lithium-ion battery poses a risk of combustion. If the device continues to be functional, its rotors can pose a risk of injury. Those wishing to perform forensic analysis on the device may need to follow a series of steps to ensure that the integrity of the system and the potentially valuable data it carries are not compromised. (Michel 2019, 5)

Characteristics include:

- **Proximity to High Value Asset:** Priority I – 1V
- **Effects Chain Phase:** Assess
- **Capabilities Employed:** C2, Neutralization
- **Operational Performers:** C-UAS Commander, C2 Cell, UAV

C. OPERATIONAL PERFORMERS

The following operational roles are key to constructing a C-UAS mission scenario:

- **Threat UAV:** Primary impetus for power projection within the Threat effects chain. A low, slow flier that is difficult to detect, classify, and intercept due to its size and proliferation. Its task is to navigate and close friendly forces in order to gather intelligence, relay targeting information, or employ weapon effects.
- **Adversary Ground Control Station:** This typically includes the Human-Machine Interface and processing for the control, video and data links to the *Threat UAV*.
- **High Value Asset (HVA):** A resource or system that is so critical that a loss or degraded capability to it would significantly jeopardize the success of the primary mission or create a national security risk. The *HVA* is the primary target of the *Threat UAV*.
- **Company Commander:** Primarily accountable for ensuring the *HVA* is defended against the *Threat UAV*. The majority of **Assess** capability functions are accomplished by this performer, who requires a capable *C2 platform* that is interoperable with local combat and joint networks.
- **Low Energy Effects Platform:** Utilizes energy resilient systems to provide Sense and Neutralize capabilities to the C-UAS solution.
- **Sense Platform:** A specialized type of *Low Energy Effects Platform* that continuously monitors downrange and along threat axes to detect and provide early indicators of sUAS activity. Assets include RF, Electro-Optical, and human-in-the-loop Line of Sight systems.
- **Cyber-attack Platform:** A specialized type of *Low Energy Effects Platform* capable of employing cyber-attack techniques to exploit the *Threat UAV* dependency on wireless networks in order to neutralize the navigation and C2 functions of the treat effects chain.

- **Cyber-attack UAV:** Friendly force fliers equipped with payloads that can provide a force multiplier and employ Cyber-attack techniques in proximity of the *Threat UAV*.
- **Mobile Ground Effects Platform:** A platform capable of employing a mechanical-kinetic neutralization techniques at or near the surface of the *Threat UAV* in an attempt to destroy or disable.
- **Task Force (TF) Commander:** Executes a mission that has a definite and limited objective. The *Company Commander* interacts with the *TF Commander* to provide status and request support from C-UAS performers outside of the *Company Commander* tactical control.

D. OPERATIONAL CONCEPT DIAGRAM

The interaction of the C-UAS performers within the operational environments is captured in Figure 72 and Figure 73 respectively.

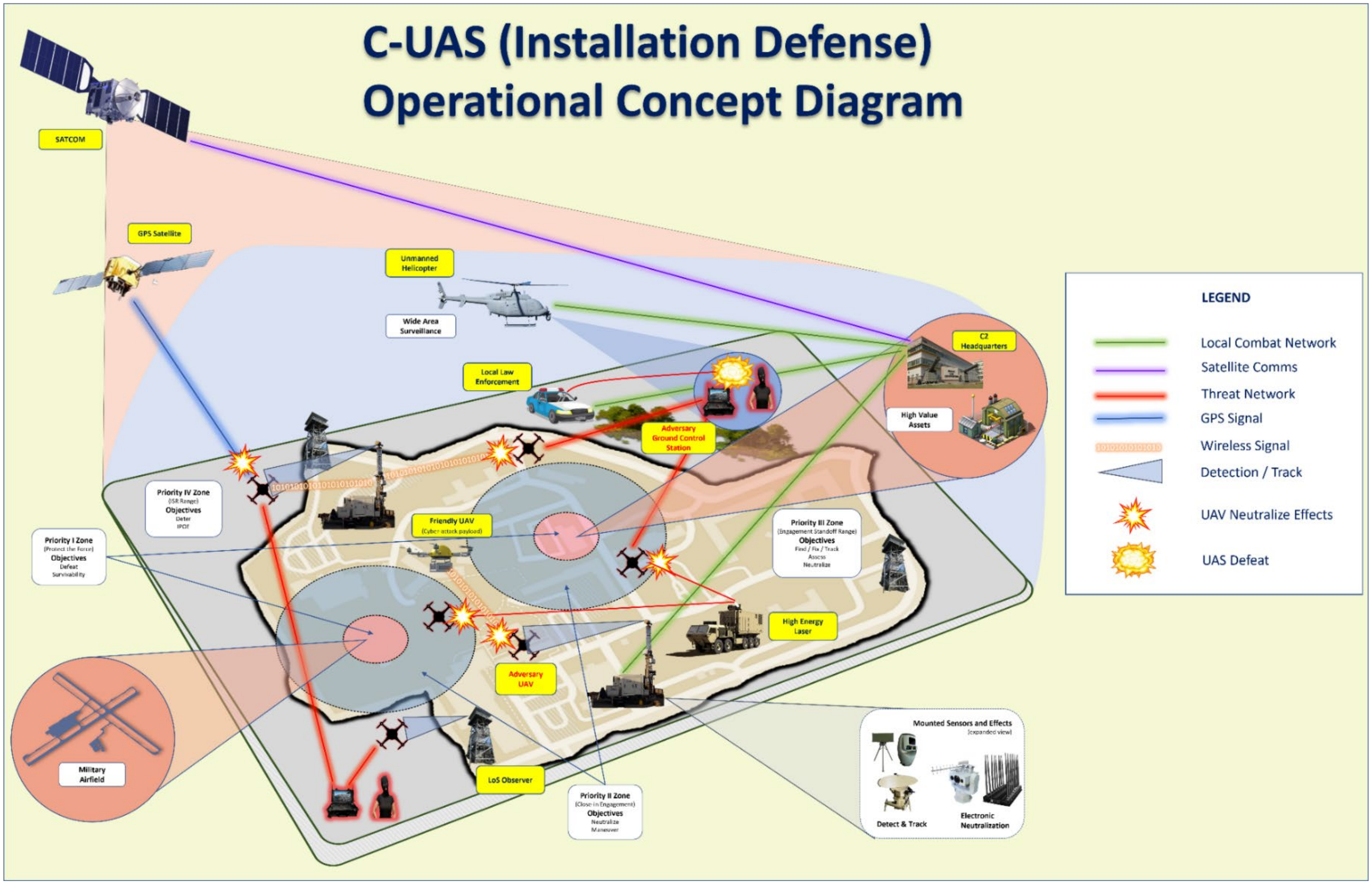


Figure 72. C-UAS Operational Concept Diagram (Installation Defense)

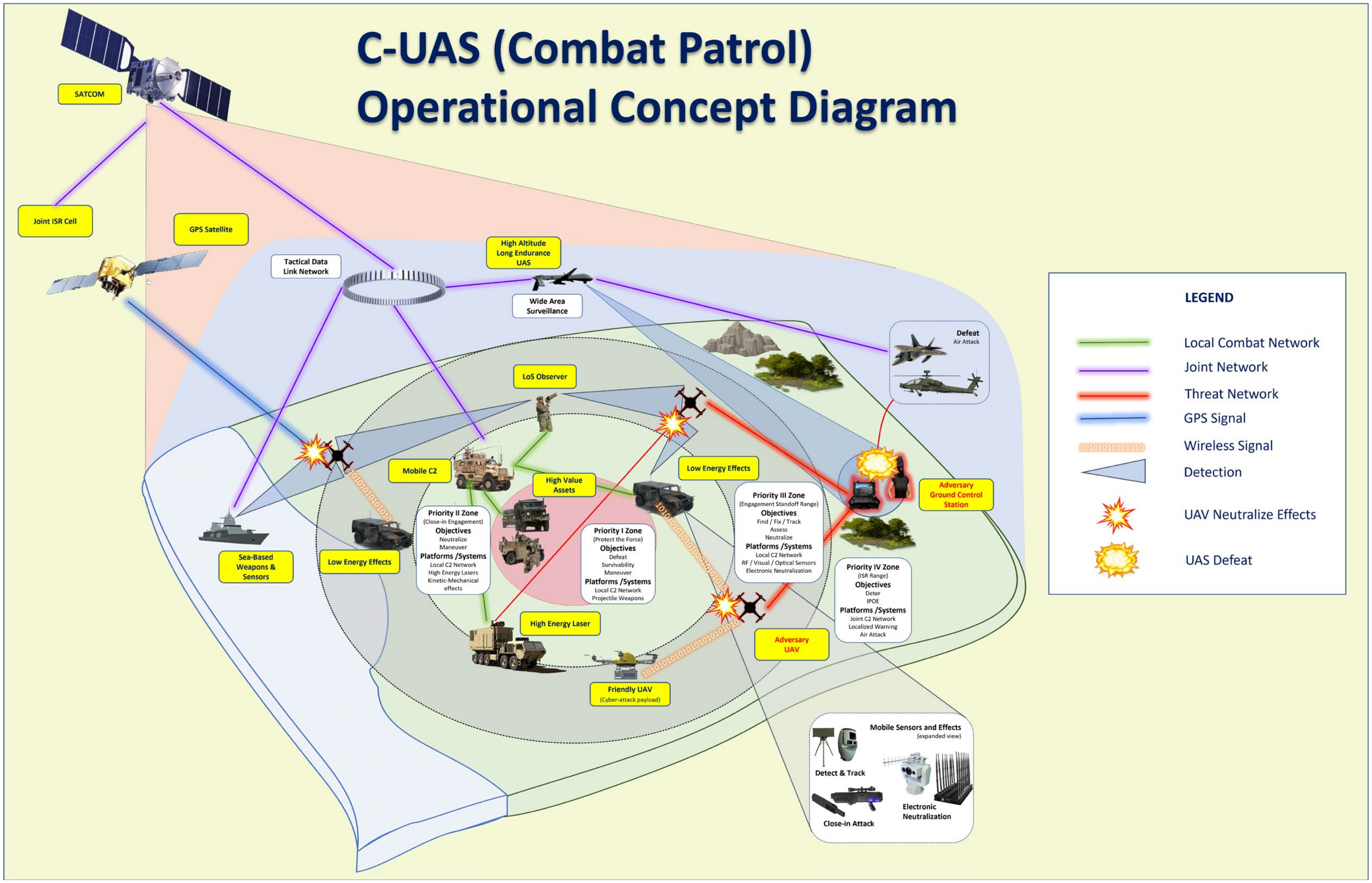


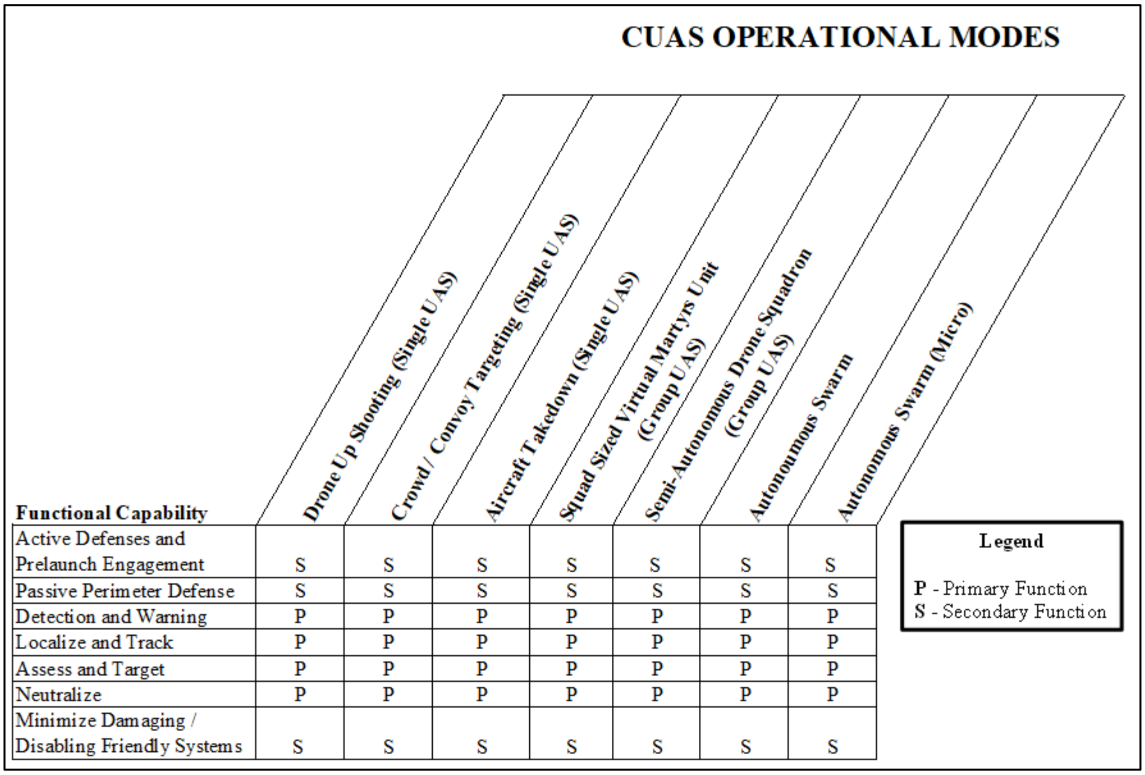
Figure 73. Operational Concept Diagram (Combat Deployment)

E. MISSION SCENARIOS AND VIGNETTES

Scenarios describe the role of the asset or system, and how it will interact with external entities in various operational modes. The C-UAS scenarios presented will help to bind together different capabilities, showing how the capabilities are related. They can also provide detailed and validated information which can be used for analysis and modeling tasks later in the project.

The C-UAS operational support modes are outlined in Table 33, shown mapped to the C-UAS functional capabilities. These modes represent the different threat categories that C-UAS system of systems may be subjected to for a given operational environment.

Table 33. C-UAS Operational Support Modes



CUAS OPERATIONAL MODES

Functional Capability	Drone Up Shooting (Single UAS)	Crowd / Convoy Targeting (Single UAS)	Aircraft Takedown (Single UAS)	Squad Sized Virtual Martyrs Unit (Group UAS)	Semi-Autonomous Drone Squadron (Group UAS)	Autonoumous Swarm	Autonomous Swarm (Micro)
Active Defenses and Prelaunch Engagement	S	S	S	S	S	S	S
Passive Perimeter Defense	S	S	S	S	S	S	S
Detection and Warning	P	P	P	P	P	P	P
Localize and Track	P	P	P	P	P	P	P
Assess and Target	P	P	P	P	P	P	P
Neutralize	P	P	P	P	P	P	P
Minimize Damaging / Disabling Friendly Systems	S	S	S	S	S	S	S

Legend

P - Primary Function
S - Secondary Function

1. Mission Scenario – Convoy Targeting by Single UAS

A representative narrative that depicts the employment of C-UAS effects against a single UAS threat in a Combat Patrol scenario is summarized below.

- **0800:** In preparation of the upcoming security patrol to disrupt the insurgency in the Erehwon (Wikipedia 2022) Province, the platoon receives an intelligence brief on the commander's intent, environmental conditions, and known threats in the region. While the whereabouts of potential insurgents are unknown, intelligence collection reports with high confidence that the insurgents have the ability to equip commercially available drones with plastic explosives that can be detonated remotely or explode on impact. Current drones are known to have operating ranges up to 5 miles from the operator but can also be programmed to operate semi-autonomously. Wide area surveillance was requested for various intervals of the security patrol and joint fires support was included in the air tasking plan.
- **1000:** Security patrol underway enroute to the Erehwon province, approximately 30 miles away from the patrol headquarters. The company commander decides to support her troop patrol of 1 mobile C2 unit and 4 armored tank squads with a wedged C-UAS defense consisting of 4 human observers, 2 mobile units mounted with UAS detect/track/neutralize equipment, and a battery of cyber-attack UAVs. Each combat team would have one member equipped with a personal drone defender for point defense.
- **1135:** Patrol headquarters relays an intelligence report based on updated collections that assesses a credible UAS threat along the patrol route. The company commander relays the alert to the company elements, dispatches the human observers to conduct patrol on foot, reduces the speed of the vehicles to avoid separation of patrol members, and directs the cyber-attack UAVs to be placed in ready stand-by mode.

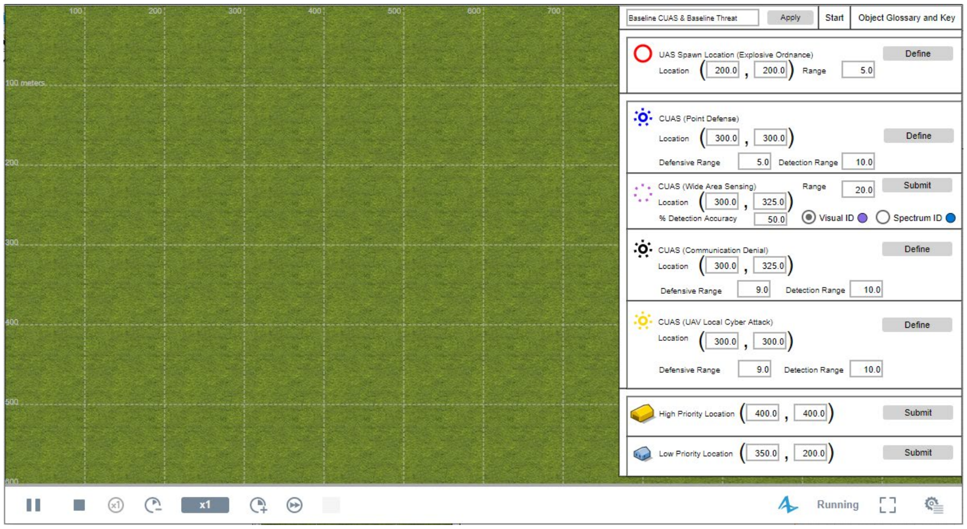
Additionally, the Company Commander requests joint air assets surveil the area as resources permit.

- **1200:** Human observers pickup RF signal emission corresponding to commercial drones, detection sensors corroborate this. Company Commander directs launch of cyber-attack UAVs. The presence of identification friend or foe (IFF) signals are undetected, and commander declares incoming targets as hostiles. Company Commander maneuvers the troop patrol tanks and C2 to open distance between C-UAS mobile units and evade attack.
- **1205:** Threat UAVs detected via radar and visually. Three radar contacts are held, while the optical sensors identify approximately 8 UAVs in 3 distinct clusters. Radar contacts are 5–6 miles out, closing on the forces at a speed of 45 mph. Clusters are engaged with rapid microwave pulses. Many of the UAVs are disabled, but 3 leakers penetrate the close-in attack region.
- **1210:** Friendly UAVs engage with remaining threat UAVs and employ cyber-attack techniques to disorient and disable the devices.
- **1215:** Two (2) threat UAVs are disabled by the friendly UAVs, with one leaker penetrating into the *Protect the Force* region. Human personnel employ handheld drone jammers to disable the remaining target.
- **1230:** All threat UAVs are confirmed disabled, but not destroyed. Blast perimeters established until explosive ordinance disposal arrives on scene to render the UAVs inert.
- **1245:** High-Altitude, long endurance UAS has located the ground control station of the threat UAVs and relayed targeting info to the Joint Fires Cell. Air to ground fires initiated on hostile ground control station.
- **1400:** Proceed on security patrol.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DROSERA ANALYSIS TOOL USER INTERFACE

The DROSERA Analysis Tool provides a user interface (UI) that enables the user to configure and control the operational environment and model elements to be simulated within the C-UAS scenario. Figure 74 depicts the default UI for the DROSERA analysis tool. This consists of three major components: the native simulation control-bar from AnyLogic, the operational map, and the simulation specific toolbar. The native simulation control bar launches by default when using an AnyLogic simulation, which gives the ability to pause, as well as increase the speed of the simulation. The operational map, as previously outlined earlier in this section, is the location in which the simulation elements are to be placed.


Baseline CUAS & Baseline Threat

UAS Spawn Location (Explosive Ordnance) Location (200.0, 200.0) Range 5.0

CUAS (Point Defense) Location (300.0, 300.0) Defensive Range 5.0 Detection Range 10.0

CUAS (Wide Area Sensing) Range 20.0 Location (300.0, 325.0) % Detection Accuracy 50.0 ● Visual ID ○ Spectrum ID

CUAS (Communication Denial) Location (300.0, 325.0) Defensive Range 9.0 Detection Range 10.0

CUAS (UAV Local Cyber Attack) Location (300.0, 300.0) Defensive Range 9.0 Detection Range 10.0

High Priority Location (400.0, 400.0)

Low Priority Location (350.0, 200.0)

Figure 74. DROSERA Analysis Tool Simulation UI Overview

Simulation Specific Toolbar:

The simulation specific toolbar, Figure 75, rests at the top right corner of the simulation's UI and serves as the container for the main control interface for the simulation. This component further consists of three additional elements. The first of these items, which is visible in Figure 76, is the pre-constructed vignette drop-down list. Using this, the user can generate a collection of scenarios that are ready to be simulated after selecting

"Apply." Continuing to the right of this component is the "Start" button. This indicates for the program to begin execution of the simulation.

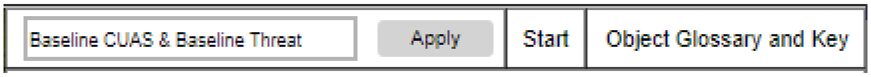

Baseline CUAS & Baseline Threat

Figure 75. DROSERA Analysis Tool Simulation Toolbar

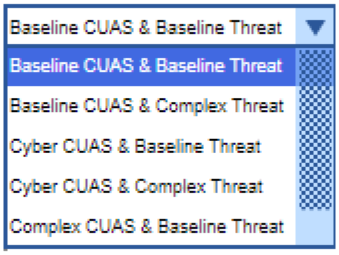
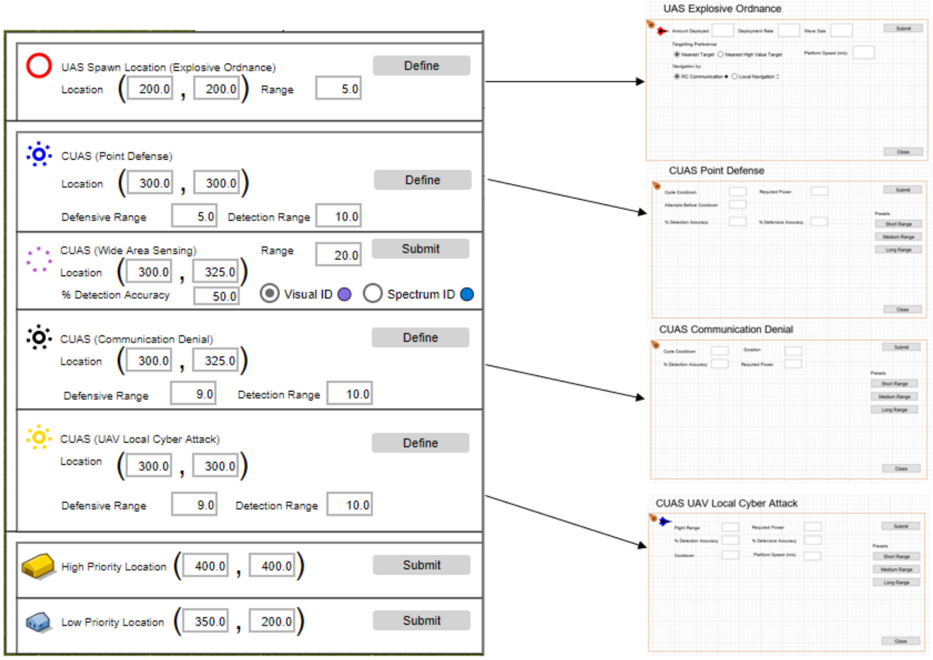

Baseline CUAS & Baseline Threat
Baseline CUAS & Baseline Threat
Baseline CUAS & Complex Threat
Cyber CUAS & Baseline Threat
Cyber CUAS & Complex Threat
Complex CUAS & Baseline Threat

Figure 76. DROSERA Analysis Tool Preset Vignettes

Object Glossary:

The Object Glossary is the primary interface for user input and is used as a tool tray in which to build a scenario. As provided in Figure 77, the Object Glossary consists of a collection of input boxes, radio buttons, and a variety of other elements in which to classify capability, threat, or priority location assets. Even further, a collection of these elements have additional definition windows in which to characterize their abilities.


UAS Spawn Location (Explosive Ordnance) Location (200.0 , 200.0) Range 5.0

CUAS (Point Defense) Location (300.0 , 300.0) Defensive Range 5.0 Detection Range 10.0

CUAS (Wide Area Sensing) Location (300.0 , 325.0) % Detection Accuracy 50.0 Range 20.0 ◉ Visual ID ○ Spectrum ID

CUAS (Communication Denial) Location (300.0 , 325.0) Defensive Range 9.0 Detection Range 10.0

CUAS (UAV Local Cyber Attack) Location (300.0 , 300.0) Defensive Range 9.0 Detection Range 10.0

High Priority Location (400.0 , 400.0)

Low Priority Location (350.0 , 200.0)

Figure 77. DROSERA Analysis Tool Object Glossary

Monte Carlo:

To introduce Monte Carlo methods within this simulation, the user must indicate the “ParameterVariation” selection before running the AnyLogic simulation (Figure 78). This will run the simulation given a pre-outlined scenario at design-time, allowing for large numbers of simulations to be run consecutively conveniently. This will yield a significantly improved understanding of the scenario with the corresponding data outputting to an excel file.

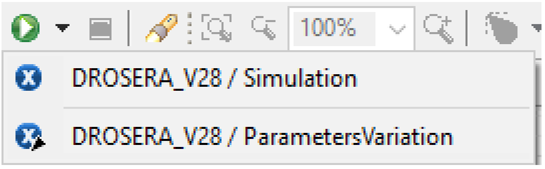


Figure 78. DROSERA Analysis Tool Simulation Run Options

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. C-UAS MEASURES TRACEABILITY MATRIX

A DROSERA Analysis Tool M&S capability metrics to C-UAS mission effectiveness and performance measures traceability chart is outlined in Table 34. Applicable notes are defined below.

X: Applicable behavior is implemented in DROSERA Analysis Tool and performance measure is exhibited in or can be computed from exhibited measures.

1: Applicable behavior is partially implemented in DROSERA Analysis Tool.

2: Applicable behavior is not exhibited in DROSERA Analysis Tool.

⬜ No traceability present between M&S tool capability metric and C-UAS performance metric.

Table 34. C-UAS M&S Tool Capability Metrics to C-UAS Mission Effectiveness & Performance Measures Traceability

	MEA.0 CUAS Weapon Effectiveness (MOE)	MEA.1 Probability of Sense (MOE)	MEA.1a Probability of Detection (MOE)	MEA.1a.1 Sensing Point (SP) (MOP)	MEA.1a.2 Sensing Volume (SV) (MOP)	MEA.1b Probability of Classification (MOE)	MEA.1b.1 Classification Point (CP) (MOP)	MEA.1b.2 Classification Time (CT) (MOP)	MEA.1b.3 Classification Volume (CV) (MOP)	MEA.1c Probability of Track (MOE)	MEA.1c.1 Tracking Drops (TD) (MOP)	MEA.1c.2 Tracking Accuracy (TA) (MOP)	MEA.1d Probability of Transmission (MOE)	MEA.2 Time to Decision Ratio (MOE)	MEA.2.1 Assessment Time (AT) (MOP)	MEA.2.2 Decision Time (DT) (MOP)	MEA.2.3 Execution Time (ET) (MOP)	MEA.3 Percent Actions Initiated on Time (MOE)	MEA.3.1 Execution Status (MOP)	MEA.4 Probability of Neutralization (MOE)	MEA.4a Probability of Hit (MOE)	MEA.4b Probability of Kill/Disable (MOE)	MEA.4c Probability of Risk (MOE)	MEA.4.1 Neutralization Point (NP) (MOP)	MEA.4.2 Neutralization Time (NT) (MOP)	MEA.4.3 Neutralization Volume (NV) (MOP)	MEA.5 Cyber-Attack Risk Rating (MOE)	MEA.5.1 Adversary UAV Technical Capability	MEA.5.2 Adversary UAV Employment (MOP)	MEA.5.3 Adversary UAV Cyber Vulnerability	MEA.5.4 CUAS Cyber-Attack Capability (MOP)	MEA.6 CUAS Reliability (MOE)	MEA.6.1 CUAS Mission Critical Failure (MOP)	MEA.7 CUAS Energy Effectiveness (MOE)	MEA.7.1 CUAS System Employment (MOP)	MEA.7.2 CUAS System Power Usage (MOP)
CCM.1 Perceive Probability of Sensing	1	1																																		
CCM.1.1 Sensing Location				2																																
CCM.1.2 Sensing Volume					2																															
CCM.2 Perceive Probability of Detecting			X																																	
CCM.2.1 Detecting Location				X																																
CCM.2.2 Detecting Volume					X																															
CCM.2.3 Detecting Time				X																																
CCM.3 Perceive Probability of Classifying						2																														
CCM.3.1 Classifying Location							2																													
CCM.3.2 Classifying Volume									2																											
CCM.3.3 Classifying Time								2																												
CCM.4 Perceive Tracking of Position										1																										
CCM.4.1 Tracking Duration											2	2																								
CCM.4.2 Tracking Accuracy												2																								
CCM.4.3 Tracking Point of Failure											2																									
CCM.5 Assess Resources Required																																		X		
CCM.5.1 Resources Power																																			X	X
CCM.5.2 Resources Personnel																																			2	
CCM.5.3 Resources Etc.																																			2	
CCM.6 Assess Time to Decision Ratio														X																						
CCM.6.1 Decision Cycle Start Time															X																					

CCM.6.2 Time Order Given																X																				
CCM.6.3 Time of Order Execution																	X																			
CCM.7 Assess % Actions Initiated by Time Ordered																		2																		
CCM.7.1 Number of Actions Initiated																		2	2																	
CCM.7.2 Number of Actions Initiated by Time Ordered																			2																	
CCM.8 Recover Functional Damage Assessment																															X					
CCM.8.1 Function Damage Confidence Level																																X				
CCM.9 Recover Adversary UAS Distance to High Value Asset																																				
CCM.10 Neutralize Probability of Neutralization	X																			X							X							X		
CCM.10.1 Neutralization Location																					X	2	2													
CCM.10.1.1 Total																								X					X							
CCM.10.1.2 UAS Payload Specific																								X				X		X						
CCM.10.1.3 CUAS Capability Specific																								X							X				X	X
CM.10.2 Neutralize Time																					X	2	2													
CCM.10.2.1 Total																									X				X							
CCM.10.2.2 UAS Payload Specific																									X			X								
CCM.10.2.3 CUAS Capability Specific																									X						X				X	X
CCM.10.3 Neutralization Volume																					X	2	2													
CCM.10.3.1 Total																										X			X							
CCM.10.3.2 UAS Payload Specific																										X		X								
CCM.10.3.3 CUAS Capability Specific																										X					X				X	X
CCM.11 Neutralize Probability of Collateral Damage (2)																																				
CCM.11.1 Location of Defense in Depth (2)																																				
CCM.11.2 UAS Payload Specific (2)																																				
CCM.11.3 CUAS Capability Specific (2)																																				
CCM.12 Reliability Non-Failure of Minimum Number of System Elements Required for CUAS Mission Success														X						X												X				
CCM.12.1 Number of Failures																					X	X											X			
CCM.12.2 Time Length of Mission Window															X																		X			
CCM.13 Resiliency Total Types of UAS Threat Capabilities Encountered	X													X						X							X							X		
CCM.13.1 Probability of Exploiting Vulnerability																					X	X						X		X	X				X	
CCM.13.2 Number of Vulnerability Failure Modes																												X		X	X				X	
CCM.13.3 Time Length of Mission Window															X																					
CCM.13.4 Timewise Availability to Exploit a Given Vulnerability															X																					

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AnyLogic North America. n.d. "AnyLogic Personal Learning Edition." Accessed October 21, 2022. https://www.anylogic.com/s/download-free-simulation-software-for-education/.

Beery, Paul, and Eugene Paulo. 2019. "Application of Model-Based Systems Engineering Concepts to Support Mission Engineering." *Systems (Basel)* 7 (3): 44–. https://doi.org/10.3390/systems7030044.

Besada, J.A., Campaña, I., Carramiñana, D., Bergesio, L., and de Miguel, G. 2021. "Review and Simulation of Counter-UAS Sensors for Unmanned Traffic Management." *Sensors* 2022, 22, 189. https://doi.org/10.3390/s22010189.

Best, Katharina Ley. 2020. *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks and Analysis Tools*. Santa Monica, California: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2972/RAND_RR2972.pdf.

Blanchard, Benjamin S., and W. J. Fabrycky. *Systems Engineering and Analysis*. 5th ed. Upper Saddle River, NJ: Pearson, 2011.

Bornman, Louis. 1993. *Command and Control Measures of Effectiveness Handbook*. Fort Leavenworth, KS: TRADOC Analysis Command - Study and Analysis Center. https://apps.dtic.mil/sti/pdfs/ADA459359.pdf.

Buede, Dennis M., and William D. Miller. 2016. *The Engineering Design of Systems: Models and Methods*. 3rd ed. New York: Wiley.

Castrillo, Vittorio Ugo, Angelo Manco, Domenico Pascarella, and Gabriella Gigante. 2022. "A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones." *Drones (Basel)* 6 (3): 65–. https://doi.org/10.3390/drones6030065.

Cetin, E. 2021. "Improving Real-Time Drone Detection for Counter-Drone Systems." *The Aeronautical Journal* 125, no. 1292 (October 2021): 1871–1896. https://doi.org/10.1017/aer.2021.43.

Chamola, Pavan Kotesh, Aayush Agarwal, Naren, Navneet Gupta, and Mohsen Guizani. 2021. "A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques." *Ad Hoc Networks* (111) (February): Article 102324. https://doi.org/10.1016/j.adhoc.2020.102324.

Chief of Naval Operations. 2007. *Universal Naval Task List (UNTL)*. OPNAVINST 3500.38B. Washington, D.C.: Chief of Naval Operations

Cline, Travis, 2020. “Mitigation Drone Attacks for Large, High-Density Events” PhD dissertation, Purdue University 2020. https://www.researchgate.net/publication/348133407.

Crawley, E., Cameron, B., and Selva, D. 2015. *Systems Architecture: Strategy and Product Development for Complex Systems*; Pearson Education: London, UK, 2015. 17.

Dam, Steven. 2014. *DOD Architecture Framework 2.02 – A Guide to Applying Systems Engineering to Develop Integrated, Executable Architectures.* Manassas, VA: SPEC Innovations. https://specinnovations.com/download-dodaf-2-0/.

Daponte, Aaron M., Gregory A. Maguire, and Calvin J. Roldan. 2020. “Unmanned Aerial System Risk Management Decision Matrix.” Master’s thesis, Naval Postgraduate School. https://nps.primo.exlibrisgroup.com/permalink/01NPS_INST/kn4t3i/alma991005672078103791.

Dassault Systems. 2022. “Magic Systems of Systems Architect.” November 3, 2022. www.3ds.com/products-services/catia/products/catia-magic/magic-systems-of-systems-architect/.

Dedrone. n.d. “DroneDefender® Smart Counter S-UAS Device.” Accessed full date. October 16, 2022. https://www.dedrone.com/products/mitigation.

Department of the Army. 2017. *C-UAS Techniques*. ATP 3-01.81. Washington, DC: Department of the Army. https://irp.fas.org/doddir/army/atp3-01-81.pdf.

Department of Defense. 2020. *Counter-Small, Unmanned Aircraft Systems Strategy*. Washington, D.C.: U.S. Department of Defense. https://permanent.fdlp.gov/gpo150130/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf.

Department of Defense Chief Information Officer. n.d. “DOD Architecture Framework Version 2.02.” Accessed October 16, 2022. https://dodcio.defense.gov/Library/DOD-Architecture-Framework/.

Department of Homeland Security and National Urban Security Technology Laboratory. 2020. *Counter-Unmanned Aircraft Systems Technology Guide*. (2019) U.S. Department of Homeland Security.

Department of the Navy. 2020. *DON Installation Energy Resilience Strategy*. Washington, DC: Department of the Navy. https://www.secnav.navy.mil/eie/Documents/DON-Installation-Energy-Resilience-Strategy.pdf.

Division on Engineering and Physical Sciences. 2018. *Counter-Unmanned Aircraft System (C-UAS) Capability for Battalion-And-Below Operations: Abbreviated Version of a Restricted Report*. Washington, D.C.: National Academies Press. https://nap.nationalacademies.org/catalog/24747/counter-unmanned-aircraft-system-cuas-capability-for-battalion-and-below-operations.

Dominicus, Jacco. 2021. "New Generation of Counter UAS Systems to Defeat of Low Slow and Small (LSS) Air Threats." Paper presented at *North Atlantic Treaty Organization Science and Technology Organization Collaboration Support Office Systems, Concepts & Integration Panel: Drone Detectability: Modelling the Relevant Signature, Virtual, April 28, 2021.* https://doi.org/10.14339/STO-MP-MSG-SET-183.

EOS Defense Systems USA Inc. 2022. "Directed Energy UAS Defense," Accessed October 15, 2022. https://www.eosdsusa.com/defense-systems/.

Flex Force. 2021. "Dronebuster Block 3B," 2021, https://flexforce.us/dronebuster/.

Giles, Katy. 2016. A Framework for Integrating the Development of Swarm Unmanned Aerial System (UAS) Doctrine and Design. Monterey, California: Naval Postgraduate School. http://hdl.handle.net/10945/61857.

Gold, Robert. 2016. "Mission Engineering*."* In *Proceedings of the 19th Annual NDIA Systems Engineering Conference*. https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2016/systems/18950_RobertGold.pdf.

Gopal, Vivek. 2020. "Developing an Effective Anti-Drone System for India's Armed Forces." ORF Issue Brief No. 370, June 2020, Observer Research Foundation.

Granåsen, Magdalena. 2019. "Exploring C2 Capability and Effectiveness in Challenging Situations: Interorganizational Crisis Management, Military Operations and Cyber Defence." https://doi.org/10.3384/lic.diva-156151.

Hale, Britta, and Douglas Van Bossuyt. 2022. *Operational C-UxS Energy Optimization through Cybersecurity Strategy*. White Paper. Monterey, CA: Naval Postgraduate School.

Hartmann, Kim, and Christoph Steup. 2013. "The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment." In 2013 5th International Conference on Cyber Conflict (CYCON 2013), 1–23. IEEE.

IEEE Architecture Working Group. 2000. *IEEE Recommended Practice for Architectural Description of Software-Intensive Systems*, IEEE Std 1471–2000, IEEE, 2000.

INCOSE. 2015. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, version 4.0. Hoboken, NJ, USA: John Wiley and Sons, Inc.

Jackson, Brian A, David R Frelinger, Michael J Lostumbo, and Robert W Button. 2008. *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*. Santa Monica: RAND Corporation. https://doi.org/10.7249/mg626dtra.

Jasper, Mila. 2021. "DOD's Plan to Counter Small Drones Hinges on Interoperability." *Nextgov.com (Online)*. February 2, 2021. https://libproxy.nps.edu/login?url=https://www.proquest.com/magazines/dods-plan-counter-small-drones-hinges-on/docview/2485782477/se-2?accountid=12702.

Joint Chiefs of Staff. 1995. *Joint Mission Essential Task List (JMETL) Development Handbook*. 1995. Washington, D.C.: Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/training/JMETLbook.pdf?ver=2017-12-29-171303-350.

Joint Chiefs of Staff. 2017. Countering Air and Missile Threats. JP 3-01. Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff. 2021. *Joint Air Operations*.JP 3-30. Washington, D.C.: Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf.

Kang, Honggu, Jingon Joung, Jinyoung Kim, Joonhyuk Kang, and Yong Soo Cho. 2020. "Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems." IEEE Access 8: 168671–710. https://doi.org/10.1109/ACCESS.2020.3023473.

Kouhestani, C, B Woo, and G Birch. 2017. *"Counter Unmanned Aerial System Testing and Evaluation Methodology."* In , 10184:1018408–1018408–7. SPIE. https://doi.org/10.1117/12.2262538.

Life cycle Modeling Language Steering Committee. 2015. "Life cycle Modeling Language (LML) Specification, Version 1.1," December 1, 2015, www.lifecyclemodeling.org.

Lee, C.H., Thiessen, C., Van Bossuyt, D.L., and Hale, B. 2022. *A Systems Analysis of Energy Usage and Effectiveness of a Counter-Unmanned Aerial System Using a Cyber-Attack Approach.* Drones 2022, *6*, 198. https://doi.org/10.3390/drones6080198.

Long, D., and Scott, Z. 2011. *A Primer for Model-Based Systems Engineering (2nd Edition)*. [Blacksburg, VA]: Vitech Corporation.

Michel, Arthur Holland. *Drones At Home*, 2017. https://doi.org/10.1093/acrefore/9780190264079.013.127.

Nicholls, Sarah, Bas Amelung, and Jillian Student. 2017. "Agent-Based Modeling: A Powerful Tool for Tourism Researchers." *In Journal of Travel Research*, 56(1), 3–15. https://doi-org.libproxy.nps.edu/10.1177/0047287515620490.

Object Management Group. 2022. *Enterprise Architecture Guide for UAF*. Appendix C, Version 1.2. Milford, MA. https://www.omg.org/spec/UAF/1.2.

Office of the Deputy Director for Engineering. 2020. Department of Defense Mission Engineering Guide. Washington, DC: Office of the Under Secretary of Defense for Research and Engineering. https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf.

Phantom Technologies. 2022. "Eagle 108 Drone Jammer: Drone Jammer & Detector," 10 October 2022, https://phantom-technologies.com/eagle108-drone-detection-jamming-system/.

Plotnikov, Michael. 2019. *The Application of Unmanned Aerial Systems in Surface Transportation – Volume II-E: Assessment of Unmanned Aircraft System Situational Awareness Technology to Support Applications in Surface Transportation*. 19–010. https://rosap.ntl.bts.gov/view/dot/49142.

Roedler, Garry and Cheryl Jones. 2005. *Technical Measurement Guide*. INCOSE-TP-2003-020-01. San Diego, CA, USA: International Council on Systems Engineering (INCOSE). INCOSE Store.

RST. 2022. "Doruk UAV Detection Radar 2D & 3D," 10 October 2022, https://www.rstteknoloji.com.tr/project/doruk-uav-detection-radar/.

Shaffer, Greg. 2017. "Model Based Systems Engineering (MBSE) in Large Complex Systems." 2017 INCOSE Mini Conference (MS PowerPoint document). https://sdincose.org/resources/documents/.

Tan, Choon Seng, Douglas L. Van Bossuyt, and Britta Hale. 2021. "System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment." Systems (Basel) 9 (4): 79–. https://doi.org/10.3390/systems9040079.

Teledyne FLIR, "FLIR LVSS ADA C-UAS," 2021, https://www.flir.com/products/lvss-c-uas/?vertical=integrated+systems&segment=uis.

Tewes, Jacob. 2017. "Lasers, Jammers, Nets, and Eagles: Drone Defense is Still Illegal." https://ssrn.com/abstract=3304914.

Theissen, Christian, 2022. "Redesigning the Counter Unmanned Systems Architecture" Master's Thesis, Naval Postgraduate School. http://hdl.handle.net/10945/70767.

Van Bossuyt, Douglas, Paul Beery, Bryan O'Halloran, Alejandro Hernandez, and Eugene Paolo. 2019. "The Naval Postgraduate School's Department of Systems Engineering Approach to Mission Engineering Education through Capstone Projects." *Systems 7.3* (2019): 38. http://hdl.handle.net/10945/65173.

Van Bossuyt, Douglas, and Britta Hale. 2020, April. "Unmanned Aerial System Cybersecurity Risk Management Decision Matrix for Tactical Operators." Monterey, California, Naval Postgraduate School.

Vaneman, W.K., 2016, April. "The System of Systems Engineering and Integration 'Vee' Model." In *Systems Conference (SysCon)*, *2016 Annual IEEE* (pp. 1–7). http://hdl.handle.net/10945/58172.

Wikipedia. "Erewhon." Last modified October 16, 2022. https://en.wikipedia.org/w/index.php?title=Erewhon&oldid=1109727155.

Wubben, Jamie, Fabra, Francisco, Calafate, Carlos, Krzeszowski, Tomasz, Marquez-Barja, Johann, Cano, Juan-Carlos, and Manzoni, Pietro. 2019. *Accurate Landing of Unmanned Aerial Vehicles Using Ground Pattern Recognition*, 8. 1532. 10.3390/electronics8121532.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California