NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE PROJECT REPORT

DRONE DEFENSE SYSTEM ARCHITECTURE FOR U.S. NAVY STRATEGIC FACILITIES

by

David Arteche, Kenneth Chivers, Bryce Howard, Terrell Long,
Walter Merriman, Anthony Padilla, Andrew Pinto,
Stenson Smith, and Victoria Thoma

September 2017

Project Advisors: John M. Green
Mark Rhoades

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2017	**3. REPORT TYPE AND DATES COVERED** Capstone project report

4. TITLE AND SUBTITLE
DRONE DEFENSE SYSTEM ARCHITECTURE FOR U.S. NAVY STRATEGIC FACILITIES

5. FUNDING NUMBERS

6. AUTHOR(S)
David Arteche, Kenneth Chivers, Bryce Howard, Terrell Long, Walter Merriman, Anthony Padilla, Andrew Pinto, Stenson Smith, and Victoria Thoma

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. IRB number ____N/A____.

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

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Small, commercially available unmanned aerial systems (UAS) are an emergent threat to Navy continental U.S. (CONUS) military facilities. There are many counter unmanned aerial system (C-UAS) tools focused on neutralization, and many sensors in place. A system-of-systems, defense-in-depth approach to C-UAS requires a central system to connect these new and existing systems. The central system uses data fusion and threat evaluation and weapons assignment (TEWA) to properly address threats. This report follows a systems engineering process to develop a software architecture for that central system, beginning with a requirements analysis, a functional baseline, and the resulting module allocation. A series of simulations in ExtendSim derives the performance requirements by examining the overall C-UAS scenario with currently available technology. Through a sensitivity analysis, the simulation shows that effective engagement range (combination of initial target range, detection range and neutralization range) is the dominant factor driving response time. The architecture modeled in Innoslate provides a discrete event simulation for system performance expectations.

14. SUBJECT TERMS C-UAS, drone, UAS, TEWA			**15. NUMBER OF PAGES** 95
			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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

DRONE DEFENSE SYSTEM ARCHITECTURE FOR U.S. NAVY STRATEGIC FACILITIES

David Arteche, Kenneth Chivers, Bryce Howard,
Terrell Long, Walter Merriman, Anthony Padilla,
Andrew Pinto, Stenson Smith, and Victoria Thoma

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

and

MASTER OF SCIENCE IN ENGINEERING SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September 2017

Lead Editor: Victoria Thoma

Reviewed by:
John M. Green
Project Advisor

Mark Rhoades
Project Advisor

Accepted by:
Ron Giachetti, Ph.D.
Chair, Systems Engineering Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Small, commercially available unmanned aerial systems (UAS) are an emergent threat to Navy continental U.S. (CONUS) military facilities. There are many counter unmanned aerial system (C-UAS) tools focused on neutralization, and many sensors in place. A system-of-systems, defense-in-depth approach to C-UAS requires a central system to connect these new and existing systems. The central system uses data fusion and threat evaluation and weapons assignment (TEWA) to properly address threats. This report follows a systems engineering process to develop a software architecture for that central system, beginning with a requirements analysis, a functional baseline, and the resulting module allocation. A series of simulations in ExtendSim derives the performance requirements by examining the overall C-UAS scenario with currently available technology. Through a sensitivity analysis, the simulation shows that effective engagement range (combination of initial target range, detection range and neutralization range) is the dominant factor driving response time. The architecture modeled in Innoslate provides a discrete event simulation for system performance expectations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AGL	above ground level
AoA	analysis of alternatives
C-UAS	counter unmanned aerial system
CONUS	continental United States
COTS	commercial off-the-shelf
DOD	Department of Defense
DoDAF	Department of Defense Architectural Framework
DOE	design of experiments
EO/IR	electro-optical/infrared
FAA	Federal Aviation Administration
FL	flight level
GOTS	government off-the-shelf
JEON	joint emergent operational need
ICAM	integrated computer aided manufacturing
ICOM	input control output mechanism
IDEF0	ICAM definition for function modeling
IO	input/output
KSA	key system attribute
M&S	modeling and simulation
MBSE	model-based systems engineering
MOE	Measure of Effectiveness
OV	Operational View
RAM	reliability, availability, and maintainability
RF	radio frequency
SA	situational awareness
SE	systems engineering
SOP	standard operating procedures
StdV	standard view
SV	system view
SWFLANT	Strategic Weapons Facility Atlantic

SWFPAC	Strategic Weapons Facility Pacific
TE	threat evaluation
TEWA	threat evaluation weapon assignment
UAS	unmanned aerial system

EXECUTIVE SUMMARY

Small commercially available drones (Group 1 and 2 drones) and modified commercial drones (55 pounds and under) are an emergent threat to U.S. Navy Strategic CONUS facilities due to their ease of attainment and the difficulty associated with detection and neutralization. The rapid proliferation of unmanned aerial system (UAS) for intelligence gathering, nuisance activities, and aggressive action from governments and military use since the late 1990s has rapidly become a technology now easily available and modifiable from off the shelf technologies to the typical private consumer and other non-state actors.

The U.S. Navy requires a counter unmanned aerial system (C-UAS) to protect the operations, facilities, and personnel at continental United States (CONUS) military facilities. Detection and defense against UASs currently lag the rapid adoption and capability improvements of these systems. Because of the increasing capabilities of drones, a large number of drone incursions, and their impact on military operations, there is an urgent need to address drone defense.

This report addresses the command and control subsystem of a notional C-UAS that would integrate with current security systems in place at the facilities and minimize interference with sensitive operations and nearby electronics systems. This subsystem, known as Storm Shield, is designed to execute decision support and command and control at U.S. Navy Strategic CONUS facilities. Storm Shield takes the sensor input, identifies the UAS threat, performs threat evaluation and weapon assignment, and provides recommendations to decision support, which can act with or without human intervention. From a functional perspective, the eventual solution defined all necessary functions from detection to neutralization.

Decisions made by Storm Shield must happen within a limited time due to the envelope for engagement. Capabilities of UAS, sensor systems, and neutralization systems drive this requirement. Data fusion, situational awareness, risk analysis, and impact analysis support the decision-making algorithms and model.

The general operation of the Storm Shield C-UAS system involves monitoring the area around the installation to detect and address possible threats. The system will gather real-time data from sensor inputs, determine contacts, assess their threat level, predict their future path, and suggest possible weapon assignments. The system analyzes this data utilizing an internal library of information and internal modeling and simulation-based decision support architecture. The Storm Shield C-UAS architecture will provide command and control coordination from start to finish in the threat evaluation weapon assignment (TEWA) process within the kill chain.

Storm Shield requires a system network that interfaces with the CONUS military facility's IT infrastructure, sensors, and weapons systems. An independent processing capability is also required to enhance system performance and meet mission requirements. Rapid deployment of Storm Shield requires the capability to interface with existing systems.

The "Fuse Data" function will process the data from an identified threat and utilize real-time information to output physical parameters to track the current UAS threat within boundaries of the facility detection area. The "Assess Threat" function uses the tracking parameters provided by the "Fuse Data" function. This second function also uses historical data from identified threats to support tracking a current UAS of interest. This information updates the threat database for comparison against new tracks in the future. The "Assess Threat" function will output predicted UAS type and intent, projection data, and alternative decisions.

The outputs from "Assess Threat" will serve as inputs for the function "Provide Decision Support." The described controls, along with the decision support mechanism, will produce the final outputs of this system: the identified threat and assigned weapon. This output serves as feedback to the previously mentioned functions, but more important, to the neutralization system.

Two top-level mechanisms primarily perform these functions: a UAS data library consisting of existing UAS data, and a software-intensive simulator used to determine UAS type and intent, to project UAS behavior, and to provide alternative decisions.

The decision support system to take in fused data, assess the situation, and make a decision, requires three main modules: a visualization system, a situational awareness system, and a decision system.

Two models were created to represent the system. The first model was built from the component level up, based on the functional architecture of the system, using the SPEC Innovations' Innoslate web application. This dual approach allows a designer to identify, investigate, and compare design options.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The technical effort and value represented within the pages of this project required significant coordination and work behind the scenes to be successful. It is with great appreciation that we wish to take a moment to thank the people who made this possible. First, in terms of the background research into the C-UAS realm, we would like to thank Tom Moulds, Tom Ruscitti, JT Torres, Andy Macyko, and others for their help in guiding us through the work already ongoing and helping us to find a space to play in this exciting arena.

We would also like to thank the NPS facility at Patuxent River for providing space for meetings and resources for our team. Ron Carlson and Barbara Lawson were incredibly helpful in making sure we had access to the resources we needed there. And of course, our advisors, John Green and Mark Rhoades, were invaluable in providing guidance throughout the process.

Finally, we need to give a big thank you to our families for putting up with the long hours and late meetings. Taking on graduate classes with a full-time job is a big commitment and a team effort. They were always very supportive of the times we could not be home for dinner or had to spend time on the weekends working on projects or team meetings. Without their support, this project would not have been completed.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The U.S. Navy requires a counter unmanned aerial system (C-UAS) to protect the operations, facilities, and personnel at continental United States (CONUS) military facilities. The rapid proliferation of the unmanned aerial system (UAS) for intelligence gathering, nuisance activities, and aggressive action from governments and military use since the late 1990s has rapidly become a technology now easily available and modifiable from off the shelf to the typical private consumer and other non-state actors. A UAS, commonly referred to as a drone, is an aircraft piloted by remote control, onboard computers, or a combination of the two. This technology is increasingly prevalent, and UAS proliferation and capabilities are rapidly increasing. In recent years, there has been an emergence of drone development efforts in the private sector, as evidenced by the rapid increase in drone patent applications from 20 in 1995 to 1,700 in 2015 (Desjardins 2016). Additionally, there are currently 86 countries with military drone capabilities, including both armed and unarmed (Bergen et al.). The U.S. Navy needs to keep pace with the UAS proliferation, and it needs to focus on its strategic military facilities.

A. BACKGROUND

While the primary goal of the private sector is to focus on areas of economic growth, such as agriculture, construction, media, private security, and other industries; the potential for using these drones as weapons systems and surveillance are becoming more prevalent. As companies continue to invest millions of dollars to develop drone technology, the market for commercial and civilian drones is expected to increase substantially over the next ten years (Desjardins 2016). New capabilities such as motion tracking, solar power, thermal scanning, 3D mapping, facial recognition, and autopilot are just some of the features that are currently under development. As drones continue to become more sophisticated with new functions added, they will pose a greater threat to the U.S. military. It is crucial that we identify defense systems and tactics to protect against possible drone attacks now, as defending against such attacks will likely become increasingly complex in the near future.

There are five groups of UASs categorized by weight and capability. Table 1 lists the classification criteria and examples of each group. In the first 30 days of drone registration, the Federal Aviation Administration (FAA) received 300,000 applications (Rosenburg and Brown 2016). The FAA reports that there were 2.5 million drone sales in 2016, and forecasts that number to increase to seven million by 2020 (Schaufele 2015).

Table 1. UAS Group Definitions. Adapted from UAS Task Force: Airspace Integration Integrated Product Team (2011).

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

UAS incursions to restricted airspace around airports and other protected sites are on the rise. Detection and defense against UASs currently lag behind the rapid adoption and capability improvements of these drones. From January to September 2016, the FAA reported more than 1,300 sightings of UASs in unauthorized areas (FAA 2017). Small UAS detection and identification is difficult and makes it hard to take action upon many of these sightings (Whitlock 2014).

Due to the increasing capabilities of drones, a large number of drone incursions, and their impact on military operations, there is an urgent need to address drone defense.

There have been many efforts to increase the level of knowledge and capability of drone defense activities. One relevant effort is a Counter UAS (C-UAS). Counter UAS is a joint emergent operational need (JEON). Work is in progress to create a high-level architecture focusing on a framework for detection, identification, tracking, and neutralization. This effort, called C-UAS, currently has a draft Department of Defense Architectural Framework (DoDAF) model, basic modeling parameters, and a set of notional logical interfaces developed as part of their Speed to Fleet (S2F) efforts.

B. PROBLEM STATEMENT

Small commercially available drones (Group 1 and 2 drones) and modified commercial drones (55 pounds and under) are an emergent threat to U.S. Navy Strategic CONUS facilities due to their ease of attainment and the difficulty associated with detection and neutralization. An adaptable open architecture command and control system for UAS security is required. This system must integrate with current security systems in place at the facilities and minimize interference with sensitive operations and nearby electronics systems

C. SCOPE

The goal of this project was to establish the systems architecture best suited to executing decision support and command and control requirements for a counter C-UAS system designed to protect Strategic U.S. Navy facilities. The Storm Shield C-UAS architecture will provide command and control coordination from start to finish in the TEWA process within the kill chain. Figure 1 is an OV-1 that illustrates the operational concept.

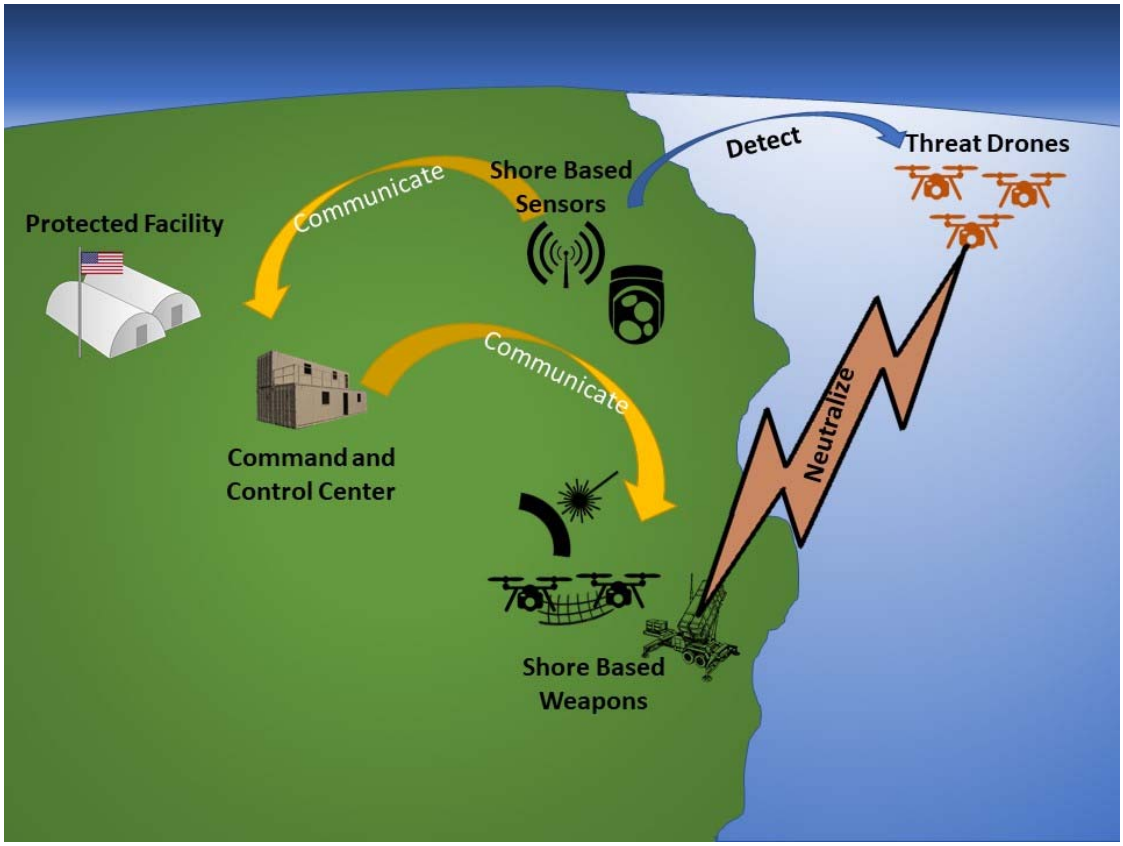

Figure 1. Storm Shield OV-1

Published capabilities and performance specifications of mature systems provided the basis for modeling and simulation parameters when available. If unavailable, M&S used estimated performance parameters. Figure 2 provides the context for the Storm Shield effort.

Figure 2. System Context Diagram

This effort focused on steps 2–4 of the Joint Targeting Cycle (kill chain) shown in Figure 3. Storm Shield takes the sensor input, identifies the UAS threat, performs threat evaluation and weapon assignment, and provides recommendations to decision support which can act with or without human intervention. Since this effort focused on defining the system architecture and not on the actual hardware, suitability requirements or target disposition (what happens immediately after target prosecution) were beyond the scope of this project. The effort included target detection and tracking (location, heading, and airspeed), threat evaluation, command, and control functionality (relaying information and gaining fire authority), and threat neutralization (assessing different modalities for effectiveness). Understanding the dynamics of the system, given the limitations of current technologies, was key to a successful outcome. Of particular concern were:

- What systems requirements are key to flow down into the system architecture?
- How is the information from data fusion and the internal decision support systems going to be communicated?
- What information is to be communicated?

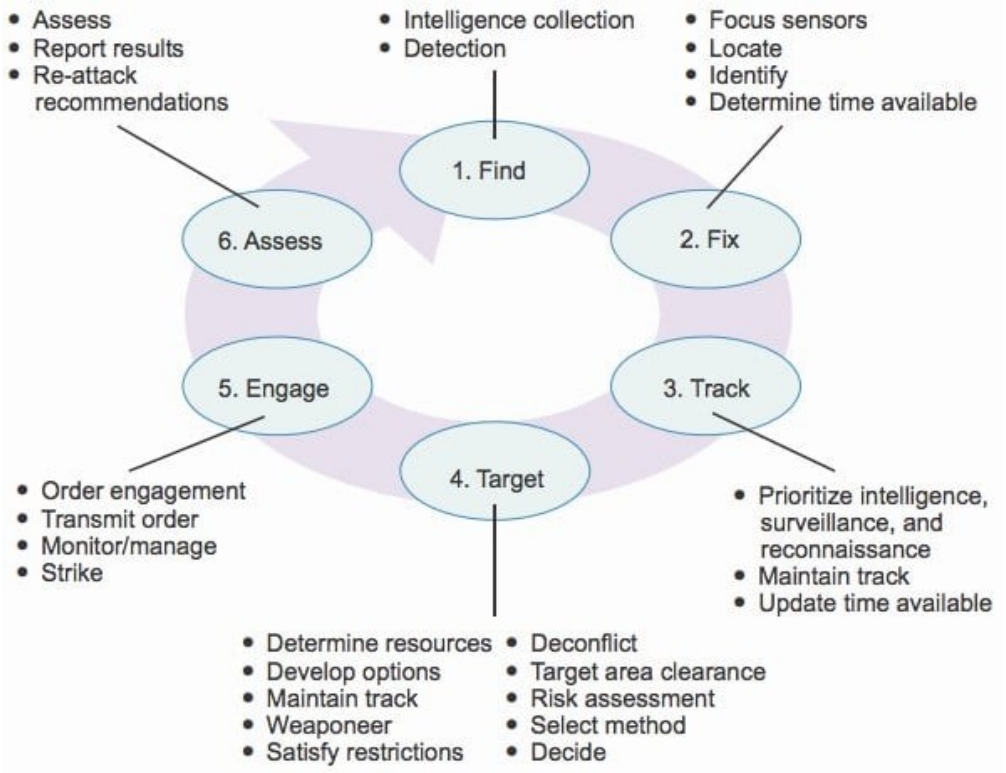

Figure 3. Joint Targeting Cycle. Source: Joint Chiefs of Staff (2013).

D. SYSTEMS ENGINEERING PROCESS

The approach selected for this project closely matches the standard approach with modifications made to accommodate the needs of the effort. Figure 4 illustrates this process. The major deviation from the standard process is the lack of DT&E and OT&E. The effort stopped with an extensive modeling and simulation effort; necessary due to the nature of the study.

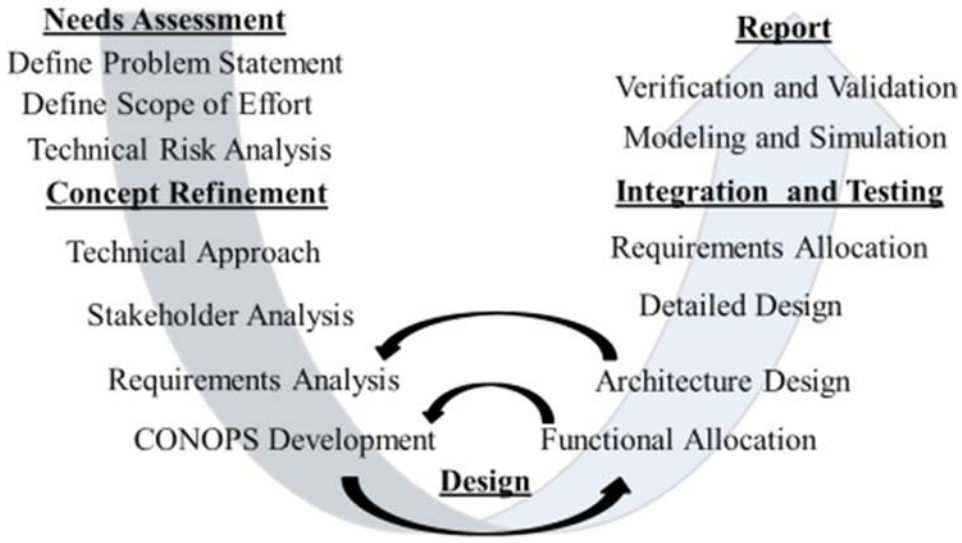

Figure 4. Systems Engineering Approach

Defining the problem statement was the crucial first step in establishing the project's purpose and direction. Finalizing the statement created several permutations and revisions. Extraordinary effort in this area was necessary, due to the novelty and obscurity of the operational need. Similarly, the scope of effort required a careful analysis of the problem space to determine the boundaries of the project.

The central effort of the project was the development of the functional architecture. The functional baseline emulated a standard TEWA model composed of three primary functions: fuse data, assess threat, and provide decision support. This project followed a spiral model of system development, with successive iterations further decomposing and refining the functional architecture. The detailed design led to a model of the system. Verification and validation reviews ensured the model accurately and effectively reflected the functional architecture.

This capstone effort was limited in scope, as described in the engineering approach section. As a result, modeling and simulation are the only means available to

test the system design. It follows then that the verification and validation of the system design would necessitate a follow-on effort. However, the models created to represent the system, which mirrors its functional architecture and performance, can be verified and validated. Verification and validation are prudent as the models are appropriate for future research and design efforts.

E. SUMMARY

Storm Shield is a C-UAS system architecture that illustrates the requirements of the TEWA process for the command and control piece of the kill chain. The system design focused on providing emergent security and C-UAS capability for strategic U.S. Navy facilities, primarily focused on Group 1 and 2 drones. The driving need for this system is the rapid proliferation of UAS technologies by state and non-state actors and the threat UAS represents to military facilities.

II. CONCEPT REFINEMENT

The goal of the system is to support the C-UAS kill chain starting with the data fusion of multiple sensor readings and threat information, moving into situational awareness and operational risk analysis, and then ending in the optimized assignment to multiple neutralization systems. The system must be capable of converting the information from external sensors into a decisive identification and neutralization of the threat. Future sections further define and explain the functional architecture of the Storm Shield system concept, focusing on the information acquired, processed, stored, and exchanged by each module within the system. Decisions made by Storm Shield must happen within a limited time due to the envelope for engagement. Capabilities of UAS, sensor systems, and neutralization systems drive this requirement. Data fusion, situational awareness, risk analysis, and impact analysis support the decision-making algorithms.

A. REQUIREMENTS ANALYSIS

Two strategic CONUS facilities are the focus of this project: Naval Submarine Base Kings Bay, shown in Figure 5, located in southeastern Georgia and Naval Submarine Base Bangor, located in Bangor Washington. These two facilities, better known as Strategic Weapons Facility Atlantic (SWFLANT) and Strategic Weapons Facility Pacific (SWFPAC), are home to sensitive operations; including the integration of strategic weapons systems into submarines (Commander, Navy Installations Command). As with any other military installation, controlled airspace above, including a buffer zone, established by FAA regulations restricting drone operation to remain outside the boundaries of military installations, is in effect.

Figure 5. Naval Submarine Base Kings Bay. Source: Webster (2001).

Neither base is part of a larger facility or grouping of facilities. The project does not detail the security posture, capabilities, and readiness of these facilities; however, it is reasonable that both SWFLANT and SWFPAC face the threat of disrupted operations due to unsanctioned UAS activity. Given the gravity of the operations that occur at these locations, it is prudent to develop the C-UAS TEWA concept within the context of their operational environment.

B. STAKEHOLDER REQUIREMENTS ANALYSIS

Parties familiar with the operational environment and security posture of the strategic facilities provided stakeholder requirements. The problem statement provided the basis for developing the requirements as detailed in Table 2. The overall requirement to protect the strategic CONUS facility from UAS Threat (requirement R.0) is broken down into three requirements: Detect Threats, Perform C-UAS TEWA, and Neutralize Threats. Storm Shield System satisfies the requirements to perform C-UAS TEWA

(requirement R.2). The requirements to Detect Threats and to Neutralize Threats are left to groups specializing in these areas and are not part of Storm Shield system. To better visualize the requirements a hierarchal view is shown in Figure 6.

Table 2. Storm Shield Stakeholder Requirements

ID	Requirement	Description
R.0	Protect Strategic CONUS Facility from UAS Threat	Prevent the UAS threat from entering a CONUS facility by executing Command and Control and decision support methods
R.1	Detect Threats	Using collected intelligence detect any possible incoming threat in the form of a UAS
R.3	Neutralize Threats	Order engagement to UAS threat and assess outcome. Report results to command and control
R.2	Perform C-UAS TEWA	
R.2.1	Execute “middle of the kill chain” TEWA	Execute “middle of the kill chain” TEWA decision support and control system for C-UAS security. The TEWA process must detect, assess, and neutralize UAS threat within facility boundaries, driven by detection range, processing time, and weapon assignment and weapon firing and time to intercept and kill percentage.)
R.2.1.1	Identify Group 1 and 2 drones	Identify the possible type of detected threats.
R.2.1.2	Track Group 1 and 2 drones	Track drones from detection through neutralization.
R.2.1.3	Support Command and Control (Decision Support)	Provide an interface for accomplishing Command and Control, situational awareness, and communication with external systems.
R.2.1.3.1	Provide Decision Interface	Provide the decision maker or algorithm with the ability to garner information from and provide commands to the system.

ID	Requirement	Description
R.2.1.3.2	Provide Situational Awareness	Take inputs from Data Fusion system and apply a model/abstraction to inform the user. Ensure the user is aware of the current state of the area of interest.
R.2.1.4	Provide Situational Analysis	Provide calculations, visualizations that aid the user in making decisions.
R.2.1.4.1	Provide Threat Capability	Provide user information from Collected Threat Info and Data Fusion to provide threat identification and capabilities information.
R.2.1.4.2	Provide Threat Intent	Uses information from Collected Threat Info and Data Fusion to provide threat identification and capabilities information.
R.2.1.4.3	Provide Weapon Assessment	Identify quantity of weapons available and suggest weapon best matched to the threat.
R.2.2	Compatible with existing counter threat and site security systems.	Must be compatible with existing systems (sensors, C&C, neutralization, and communications) at strategic facilities.
R.2.2.1	Interface with external systems	Must interface with existing external (sensors, neutralization, and command and control) systems.
R.2.2.1.1	Interface with sensor systems	Must interface with detection and tracking (external) systems. (Detection, Tracking, and Telemetry data).
R.2.2.1.2	Interface with neutralization systems	Must interface with existing neutralization (external).
R.2.2.2	Communicate with External Systems	Send information needed by external neutralization systems.
R.2.2.2.1	Communicate with External Sensors	Send tracking command and control information to external sensor systems.
R.2.2.2.2	Communication with Neutralization Systems	Send targeting and command information to external neutralization (weapon) systems.

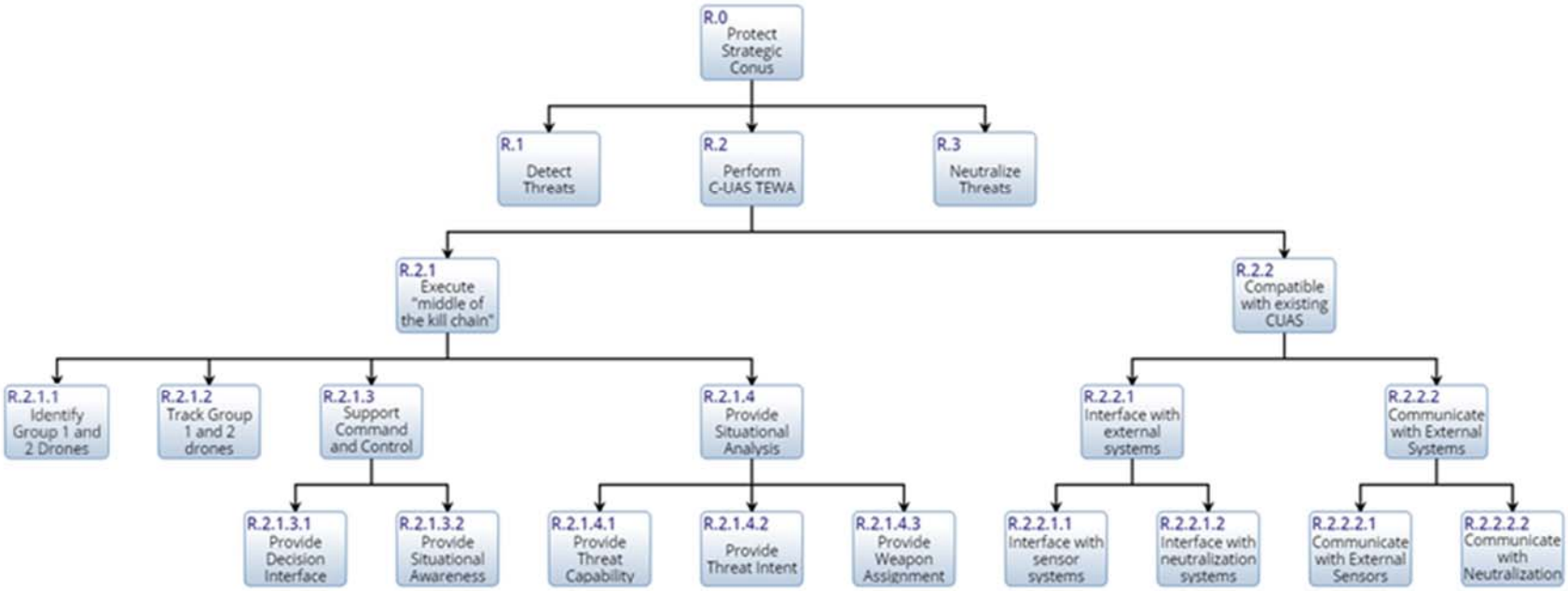

Figure 6. Storm Shield Requirements Hierarchy

C. CONCEPT OF OPERATIONS

Storm Shield is a software system architecture that is part of a larger system designed for C-UAS. The general operation of the system involves monitoring the area around the installation to detect and address possible threats. The system takes readings from sensor inputs, determine contacts, assess their threat level, predict their future path, and suggest possible weapon assignments. The system gathers sensor inputs and identified threat information in real time. The system analyzes this data utilizing an internal library of information and internal modeling and simulation-based decision support architecture. Storm Shield provides command and control coordination from start to finish in the TEWA process within the kill chain. Figure 1 is an OV-1 that illustrates the operational concept.

(1) Monitoring Sensors

Storm Shield receives data from a fleet of sensors for processing. Sensors constantly monitor the area to detect threats.

(2) Determine Contacts

The system processes and aligns sensor data. Sensor outputs provide target attributes, which could include position, size, velocity, and emission signature, to determine contacts and assess the threat.

(3) Assess the Threat

Using real-time sensor information provides information for UAS identification. Real-time sensor information combined with previously collected UAS information feeds the assessment of threat capability and intent.

(4) Predict Future Path

Known capabilities and tactics for identified entities predict possible future paths. The system tracks this information in real-time and compares against current sensor data to correct as needed.

(5) Weapon Assignment

After target identification, Storm Shield provides decision support analysis to facilitate weapon assignment to neutralize the current threat.

(6) System Interface

The system communicates the information known about the detected threats and makes recommendations for the suggested action. That could include directing sensors to gather additional readings to increase confidence in the track, the location and direction of a threat, or assigning weapons to attempt to neutralize the threat.

D. CONSTRAINTS

The C-UAS system is limited to neutralizing within the facilities boundaries and up to 400-feet altitude exclusion zone around military facilities, [Title 14 of the Code of Federal Regulations (14 CFR) § 99.7 – "Special Security Instructions"]. Technological constraints mainly stem from the capabilities and interfaces involved with the sensors, the network, and the neutralization systems. Neutralization options range from kinetic measures to cyber-attacks, depending on priority and post-event intent such as recovery and forensics. Matching legal conditions to doctrine and operational intent and system capabilities presents a large response range.

E. SYSTEM FIELDING

Storm Shield is a software system architecture independent of specific hardware. Storm Shield will require a system network that interfaces with sensors, weapons, and the IT infrastructure, to include independent processing capability. The system needs to interface with current and sensors for data collection and weapons systems and security facilities for weapon assignment. The system is intended to interface with current sensors and weapons systems to aid in rapid deployment as well as future system to allow for upgrades.

F. SUMMARY

The Storm Shield system design provides real-time C-UAS decision support concerning TEWA for strategic U.S. Navy facilities. All U.S. Navy strategic facilities fall

under FAA rules and military air control policies that allow neutralization of trespassers, especially unauthorized UAS, by any means necessary. The top-level requirements include: 1) execute the middle of the C-UAS kill chain, 2) must be compatible with existing infrastructure, and 3) implement data fusion, assess the threat, and provide decision support. Storm Shield first integrates the current CONOPS, U.S. Navy and FAA policy into a tactics doctrine and threat assessment. Then, Storm Shield evaluates known information on the type of UAS identified, possible operators, possible scenarios of concern, and the UAS capabilities. A simulation incorporates this information to provide real-time decision support concerning the best methods for neutralization and/or maintaining the security and CONOPS requirement of the facility. Both requirements analysis and functional analysis show a high level of overlap and interfacing. Human factors engineering will be a challenge as the key to Storm Shield is the user interface for command and control. Decision support includes operator control and interfaces with the information to identify, track, evaluate, and neutralize the threat.

III. PRELIMINARY DESIGN

This section describes the allocation and decomposition of system functions. The process ensured that each lower level allocation satisfied the relevant higher level requirement. Reference the appendix for a full view of Integration Definition for Functional Modeling (IDEF0) diagrams.

Existing frameworks and academic research provided the foundation for the functional allocation of Storm Shield. The resulting generic functional architecture for TEWA relied upon two main concepts: data fusion and situational awareness (SA). The general process is to transform data from multiple sources into information through data fusion. The result is SA through the creation of an understandable model of the threat(s) relative to the area to be protected. (Van Vuuren and Roux 2007). The resulting SA can then be used to make decisions.

In this generic TEWA process, various levels of data fusion and situational awareness exist. The Joint Directors of Laboratories Data Fusion Model (Steinberg 1999) of Figure 7 was used as a guide to organize data fusion into different levels of complexity and usefulness.

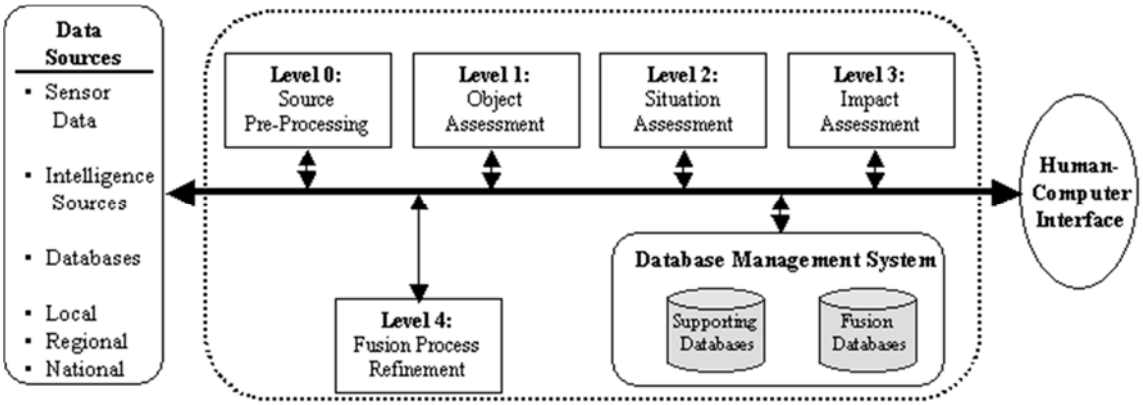

Figure 7. Generic Data Fusion Process

The Endsley model of Situational Awareness (Endlsey 1995), included in Figure 8, provided the definitions for the different levels of Situational Awareness. Table 3 describes the JDL Data Fusion Models and indicates its relationship to the Endsley model levels of situation awareness.

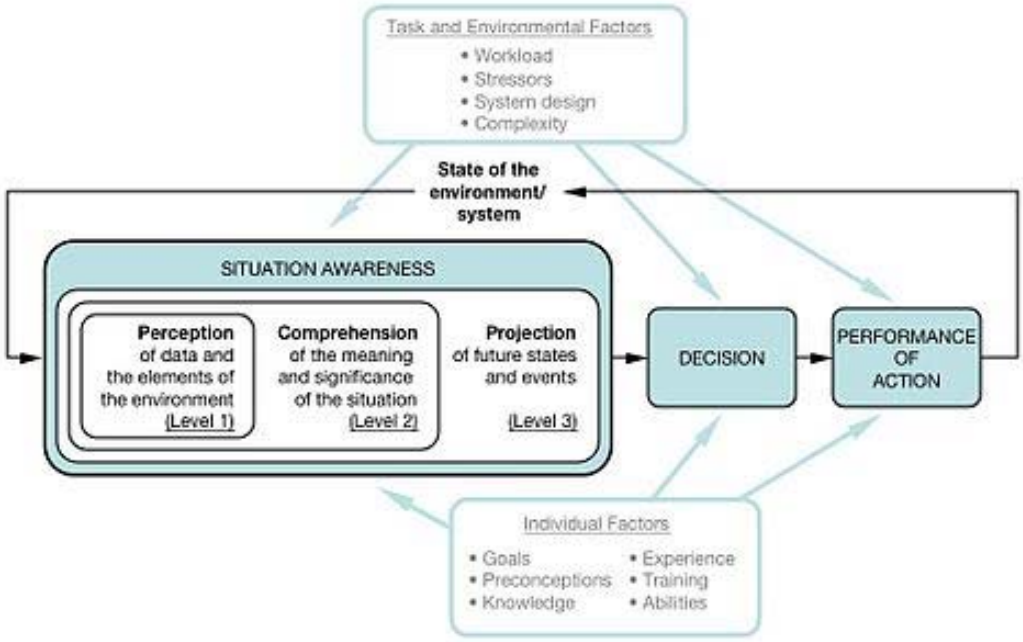

Figure 8. Endsley Model

Table 3. Data Fusion Level Definitions

Data Fusion Level	Endsley Model	Function	Attribute Estimated
0: Signal/Feature Assessment	Perception	Identify objects	Presence of a Signal
1: Object Assessment	Perception	Identify features	Attributes of Entity (e.g., an aircraft position, speed)
2: Situation Assessment	Comprehension	Develop relationships	Relationships between objects
3: Impact Assessment	Projection	Evaluate impact of objects	Future actions (Situation and Plans)

The functional analysis and allocation led to a preliminary design, along with a requirements allocation to support the integrated system design.

A. ARCHITECTURE DESIGN

Developing a system architecture for Storm Shield supports the management of complexity and change, ensuring traceability by providing multiple views to aid in communication between stakeholders. Additionally, architecture development addresses requirements in Joint Capabilities Integration and Development System (JCIDS) and the Defense Acquisition System.

The Department of Defense Architecture Framework (DoDAF) is an architecture framework that supports the development of Storm Shield. The Storm Shield architecture description uses the All View (AV), OV, Systems View (SV), and Standards View (StdV). Table 4 lists the models chosen; Figure 9 shows the development progression. These models reflect the project's focus on Conceptual Design and Preliminary Design. Further development of the system design will require the implementation of the SV-1, SV-10, and StdV-1 models from the System View and the Standards View.

Table 4. DoDAF Model List

Model	Description	Location in this paper
AV-1	Overview & Summary	Chapter 1 and 2
AV-2	Integrated Dictionary	XML Physical Exchange Specification (PES) in Innoslate not included in this paper due to length
OV-1	High-Level Operational Concept Graphic	Figure 1 Storm Shield OV-1
OV-5b	Operational Activity Model	Figure 10. Storm Shield IDEF0 Appendix A. IDEF0 Diagrams
SV-1	System Interface Description	Chapter IV.B Appendix B. System Interface Diagrams
SV-4	System Functionality Description	Appendix A. IDEF0 Diagrams

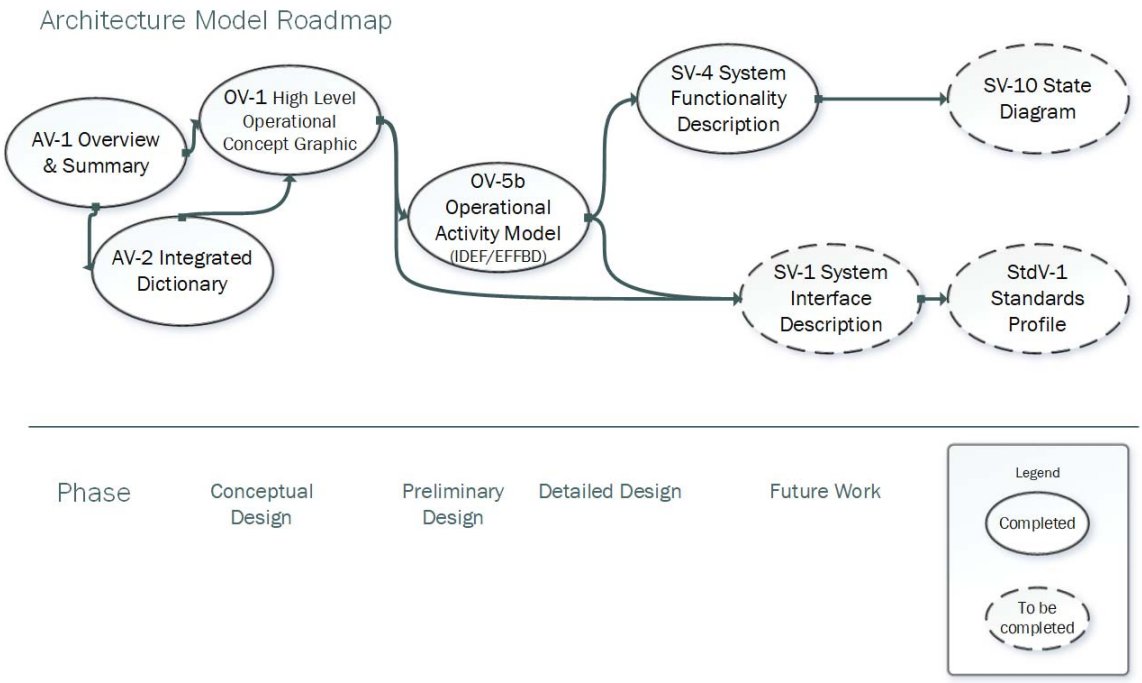

Figure 9. Architecture Model Roadmap

B. FUNCTIONAL ALLOCATION

Innoslate was the primary model-based systems engineering (MBSE) tool used for Storm Shield. It was used to develop views that provided traceability to requirements and functions, and documents design.

Figure 9 depicts the overarching IDEF0 model of the Storm Shield system. The three main functions receive and process sensor data to identify potential threats. "Fuse Data" takes the sensor data as input. It processes and translates it to an expected format that contains the entity characteristics such as size, location, speed, and radio signatures. These characteristics become elements of a target state vector or parameter set that, in turn, becomes a data point at some time on the track for a specific entity.

"Assess Threat" uses the tracking parameters provided by "Fuse Data." This second function also uses historical data from identified threats to assess possible threats. This information is stored for comparison against new tracks in the future. The current engagement doctrine will be used to make recommendations. "Assess Threat" outputs predicted UAS type and intent, projection data, and alternative decisions.

The outputs from “Assess Threat” serve as a control for the function “Provide Decision Support.” The described controls along with the decision support mechanism produce the final outputs of this system: the identified threat and assigned weapon. This output serves as feedback to the previously-mentioned functions but more importantly to “Assign Weapons.”

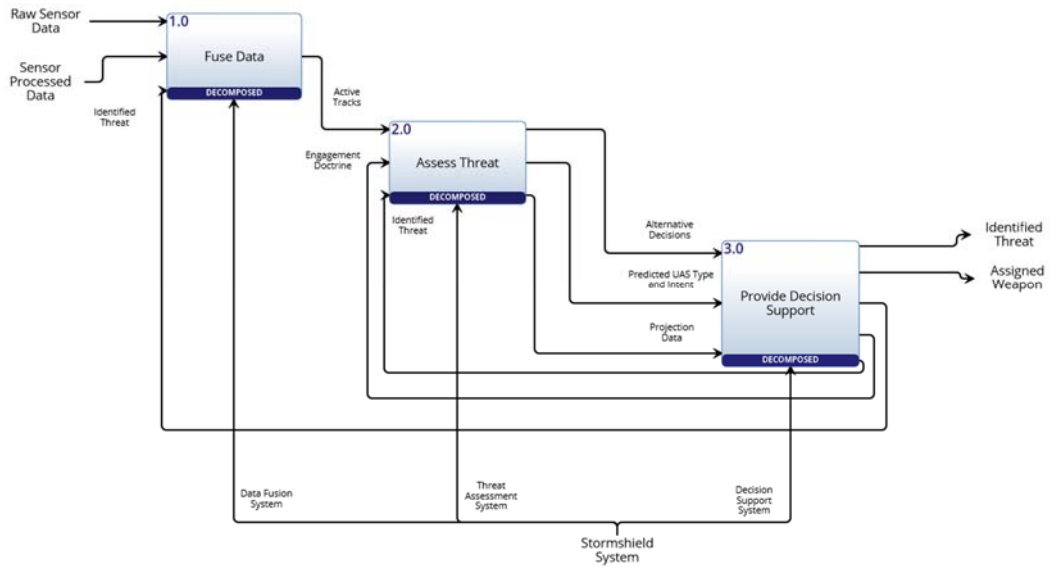

Figure 10. Storm Shield IDEF0

1. Fuse Data

“Fuse data” creates active tracks by parsing and combining data from multiple external sensors. Active tracks contain the history of the current contacts. The sensors either send raw or processed sensor data. The first step is to process it to identify any potential contacts then align the data based on the time stamps. Data is used to either propagate an existing track or create a new one as necessary. Those contacts will have different characteristics such as location, speed, size, or signal strength. The possible characteristics will vary depending on the sensor type.

Each potential contact becomes part of an active contact by comparing these characteristics with the list of active tracks. It either updates an existing active contact track, or is added as a new active track. The active tracks also include a history of the sensor readings associated to that contact.

Figure 11 shows the decomposition of the first level tier function, "Fuse Data." The IDEF0 at this level illustrates the functions needed to satisfy the requirements R2.1.1 and R2.1.2 shown in Chapter II. The data from identified threats, going into the Fuse Data function along with the sensor data undergo a series of algorithms within the functions shown below. The data is processed, associated, and scored to determine the quality and confidence of the track information.

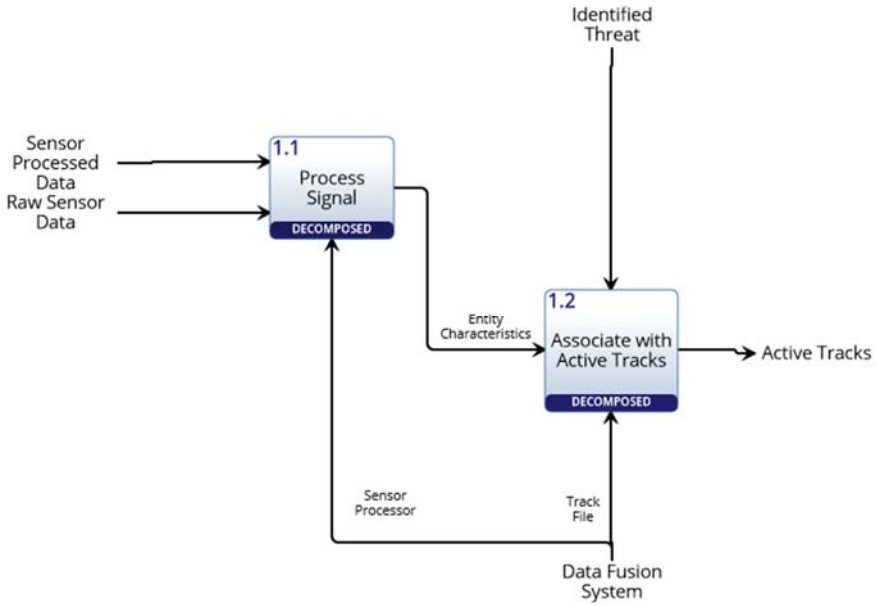

Figure 11. Fuse Data IDEF0

2. Assess Threat

"Assess Threat" receives inputs from the data stream of the collected and integrated sensor data from "Fuse Data" and a list of identified threats, from "Provide Decision Support," to associate with each active track a capability, intent, projection, and alternative decisions to handle the track. This function relies heavily on previously collected information that can identify and categorize the potential threat; the Storm Shield system leverages this information for the "Assess Threat" function. The function's main goal is to assess active tracks of collected data including tactics and capabilities to provide decision alternatives based on rule sets such as the rules of engagement defined in the rules of engagement and doctrine. At this level, Storm Shield is painting the picture

of the potential threat based on the information gathered from data fusion and the different procedures and rules to output the necessary information for decision support. Figure 12 depicts this process.

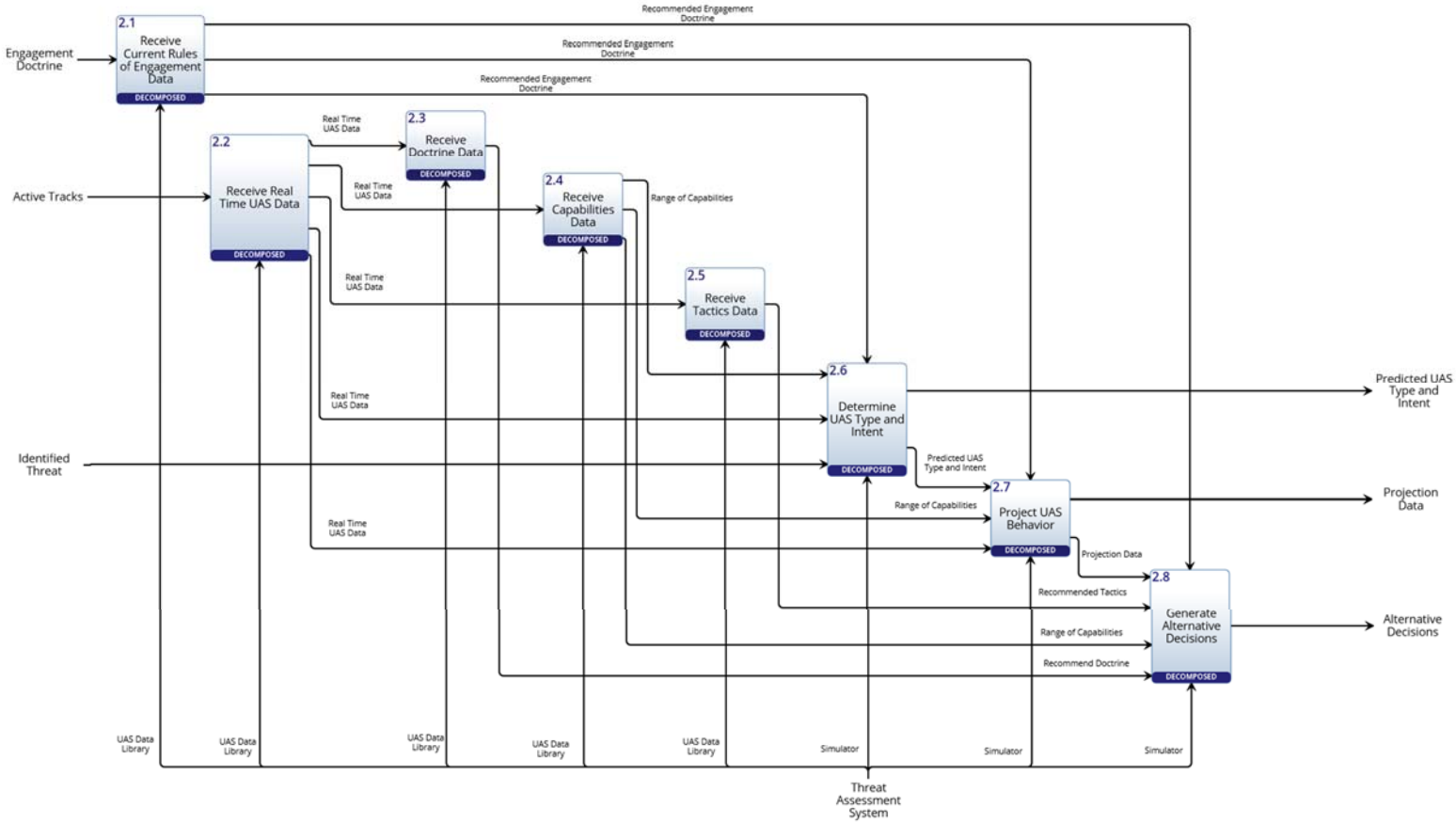

Figure 12. Assess Threat IDEF0

a. Receive Functions

Functions 2.1 through 2.5 involve the retrieval of data based on inputs beginning with the active tracks resulting from the Fuse Data function. As information from Fuse Data is received, 2.2 “Receive Real Time Data” compares this to previously collected information and retrieves relevant identifications. This information is used by “Receive Doctrine Data,” “Receive Capabilities Data,” and “Receive Tactics Data,” which retrieve doctrine data related to the threat, possible threat capabilities, and possible threat tactics. The results of these functions are used by the simulation functions, which aim to use these results to make determinations and predictions.

b. Analyze and Simulate

The analysis functions including “Determine UAS Type and Intent,” “Project UAS Behavior,” and “Generate Alternative Decisions” are accomplished through analysis and simulation. The algorithms behind these functions work on data from active tracks, the range of capabilities, the range of tactics, and doctrine rules to predict UAS type and intent and recommend a set of alternative decisions to deal with the UAS.

3. Provide Decision Support

The goal of decision support is to take in fused data, assess the situation, and determine a course of action. The outputs mentioned in the previous section (predicted UAS type and intent, projection data, and alternative decisions) serve as inputs to this function as shown in Figure 13. The functions that receive the outputs from “Assess Threat” are: “Visualize UAS Threat,” “Visualize Projections,” and “Visualize Alternative Decisions,” respectively. These functions build on the data provided by “Assess Threat” to provide useful abstractions to the decision maker. These abstractions are fed to “Provide Situational Awareness,” which allows the decision maker to process the data and develop an awareness of the situation. “Assess Situation” works on an awareness of the situation, including entity states, predicted future states, and alternative decisions to respond with, and makes decisions to identify targets as threats or non-threats. This function operates iteratively, providing continuous updates.

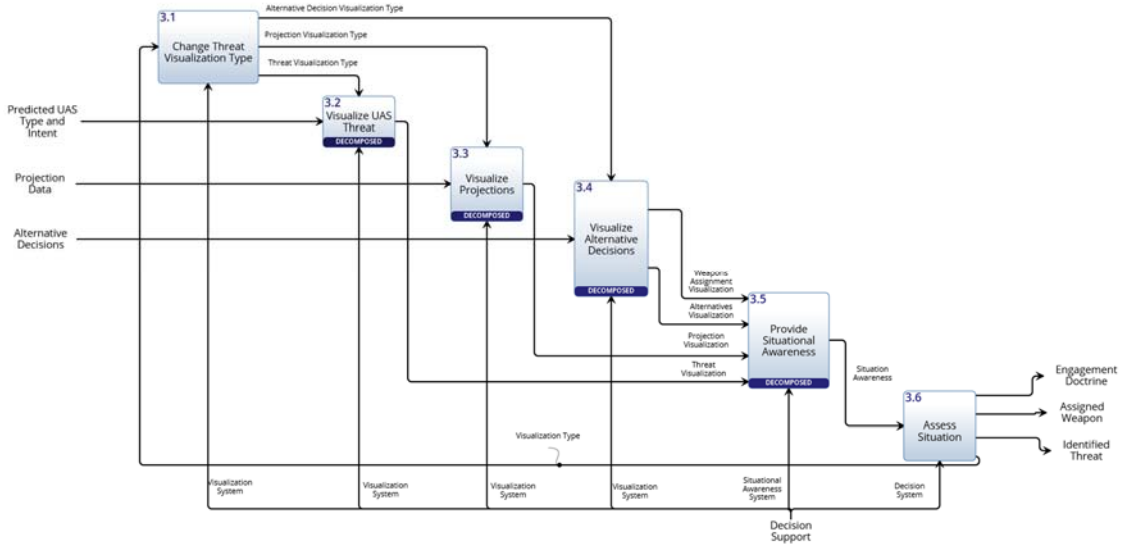

Figure 13. Provide Decision Support IDEF0

a. Visualization

The Visualization functions provide a preview for how Storm Shield predicts UAS type and intentions, applies alternative decisions and suggests a course of action to the decision system. Outputs from “Assess Threat” provide data for abstractions such as threat cones, map views, and resource views for the “Provide Situational Awareness” function.

b. Situational Awareness

The Situational Awareness System uses Visualization System outputs for decision maker consumption and decision guidance. Derived data from “Assess Threat” and abstracted data from internal visualization functions inform the decision maker and provide situational awareness.

c. Assess Situation

The “Assess Situation” function works on a combined situational awareness output, consisting of visualizations for the threat capability and intent, projections,

alternatives, and weapons assignment, to ultimately decide the course of action for the target.

C. REQUIREMENTS ALLOCATION

A requirements allocation process was undertaken to maintain requirements traceability, allocating requirements to functions. Low-level requirements refine higher level requirements through mapping to their corresponding functions. A top-down process mapped each function to a requirement. The process maintains a pedigree of requirements and a continuity of design constraints from the high to low level.

The requirements allocation was an iterative process of developing functional decompositions which defined the functional architecture as shown in Figure 14. The process facilitates the screening of requirements for duplications of allocation, the absence of allocation, and incomplete or incorrect allocation.

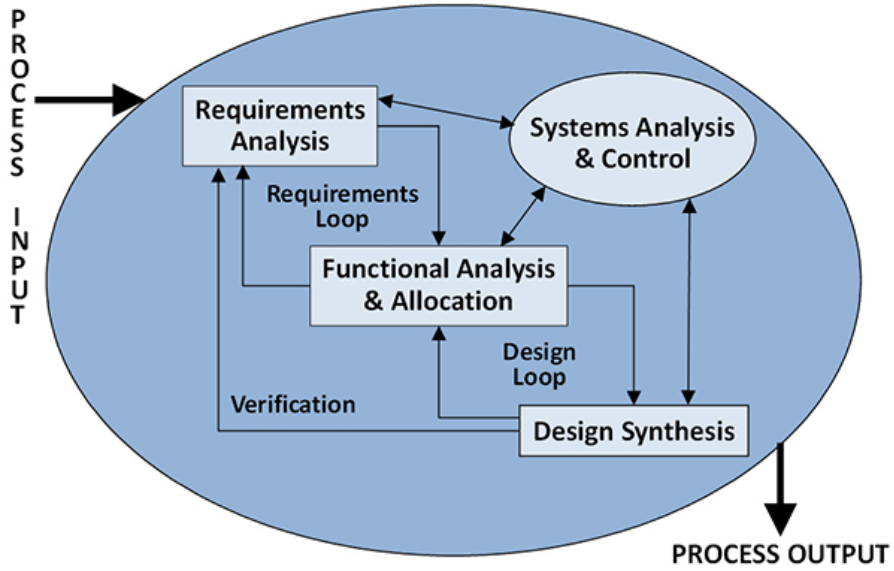

Figure 14. Requirements Allocation Process. Source: DAU (2008).

Modeling the requirements allocation was performed in Innoslate using spider diagrams, shown in Figure 15. In the case of the system level spider diagram, three primary requirements decompose the top-level requirement. Each of the primary

requirements is then further decomposed by their child requirements and mapped to the function that satisfies that requirement. This nested approach allows easy visualization of the possible secondary effects of a change to the requirements or functionality of the system. Allocation matrices mapped the same requirements to functions in a tabular format depicted in Table 5. The process ensured that missing, duplicated, or incorrect allocation could be easily spotted.

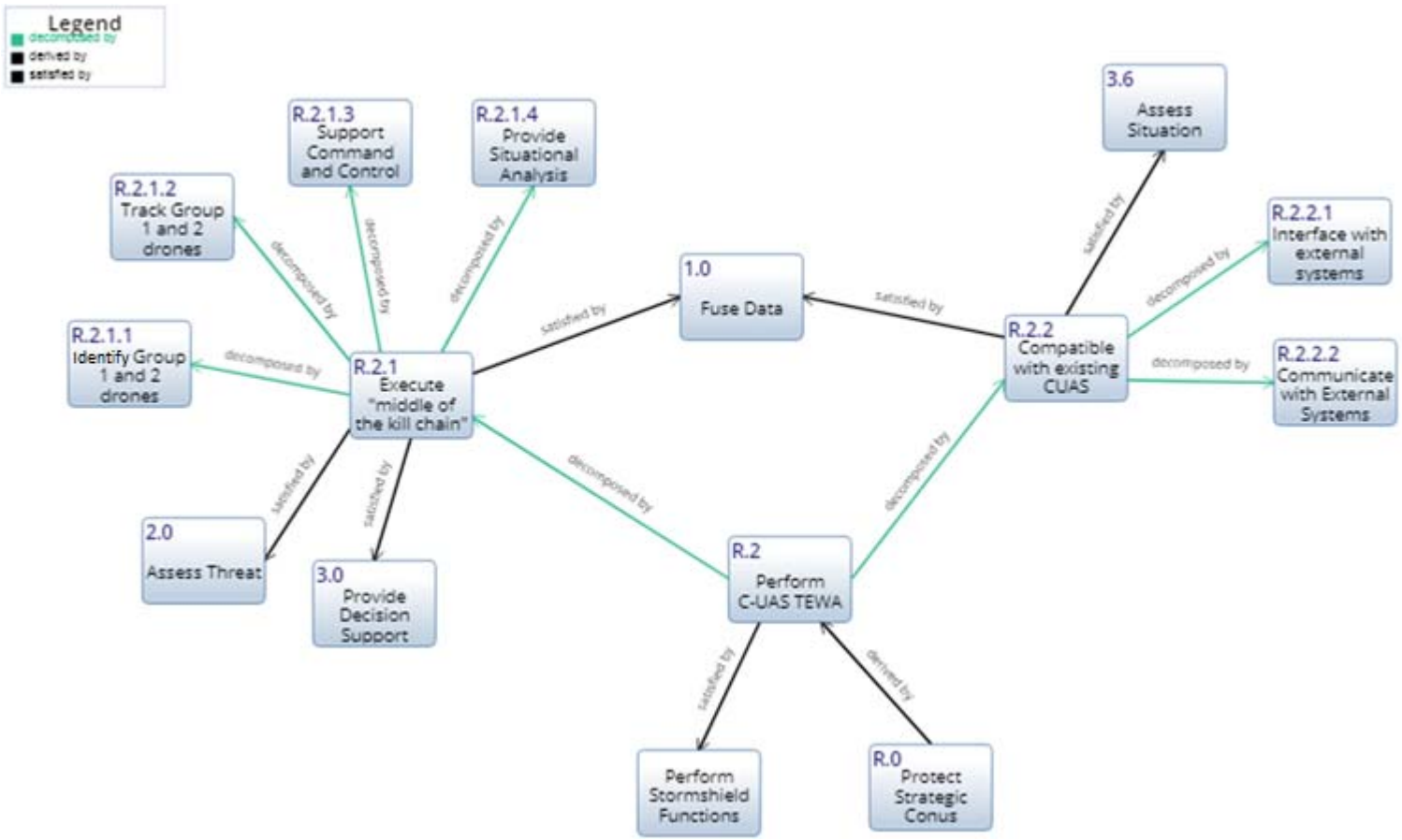

Figure 15. System Level Spider Diagram

Table 5. Functions to Requirements Traceability Matrix

Stormshield Functions to Requirements	R 0 Protect Strategic Conus Facilities from UAS threat	R 2 Perform C-UAS TEWA	R 2.1 Execute "middle of the kill chain" TEWA	R 2.1.1 Identify Group 1 and 2 drones	R 2.1.2 Track Group 1 and 2 drones	R 2.1.3 Support Command and Control (Decision Support)	R 2.1.3.1 Provide Decision Interface	R 2.1.3.2 Provide Situational Awareness	R 2.1.4 Provide Situational Analysis	R 2.1.4.1 Provide Threat Capability	R 2.1.4.2 Provide Threat Intent	R 2.1.4.3 Provide Weapon Assignment	R 2.2 Compatible with existing CUAS systems.	R 2.2.1 Interface with external systems	R 2.2.1.1 Interface with sensor systems	R 2.2.1.2 Interface with neutralization systems	R 2.2.2 Communicate with External Systems	R 2.2.2.1 Communicate with Sensors	R 2.2.2.2 Communicate with Neutralization Systems
Perform Stormshield Functions																			
Perform Stormshield Functions	X																		
1.0 Fuse Data		X	X	X	X								X	X	X	X	X	X	X
1.1 Process Signal				X										X	X	X	X	X	
1.2 Associate with Active Tracks					X														
2.0 Assess Threat		X	X																
2.1 Receive Current Rules of Engagement Data											X								
2.2 Receive Real Time UAS Data											X								
2.3 Receive Doctrine Data									X										
2.4 Receive Capabilities Data										X									
2.5 Receive Tactics Data											X								
2.6 Determine UAS Type and Intent										X	X								
2.7 Project UAS Behavior									X			X							
2.8 Generate Alternative Decisions						X		X	X			X							
3.0 Provide Decision Support		X	X			X	X	X	X										
3.1 Change Threat Visualization Type						X	X	X											
3.2 Visualize UAS Threat						X	X	X											
3.3 Visualize Projections						X	X	X											
3.4 Visualize Alternative Decisions						X	X	X											
3.5 Provide Situational Awareness			X			X	X	X											
3.6 Assess Situation													X	X	X	X	X	X	X

IV. DETAILED DESIGN

Storm Shield is a processing-intensive system that primarily relies on software. The three top-level functions of Fuse Data, Assess Threat, and Provide Decision Support, were each allocated their own module. The IDEF0 in Figure 10 shows these functions. The top-level modules include: the data fusion engine, the threat assessment system, and the decision support system. Figure 16 shows the hierarchy of the entire Storm Shield system. These systems rely heavily on processing, modeling, algorithms, and databases, which require sophisticated information systems. They also have specific hardware needs, to be able to process, combine, format, and display all necessary data. The functions of these three systems will all be carried out primarily by software. Various software modules will be used to carry out all the necessary functions of the system.

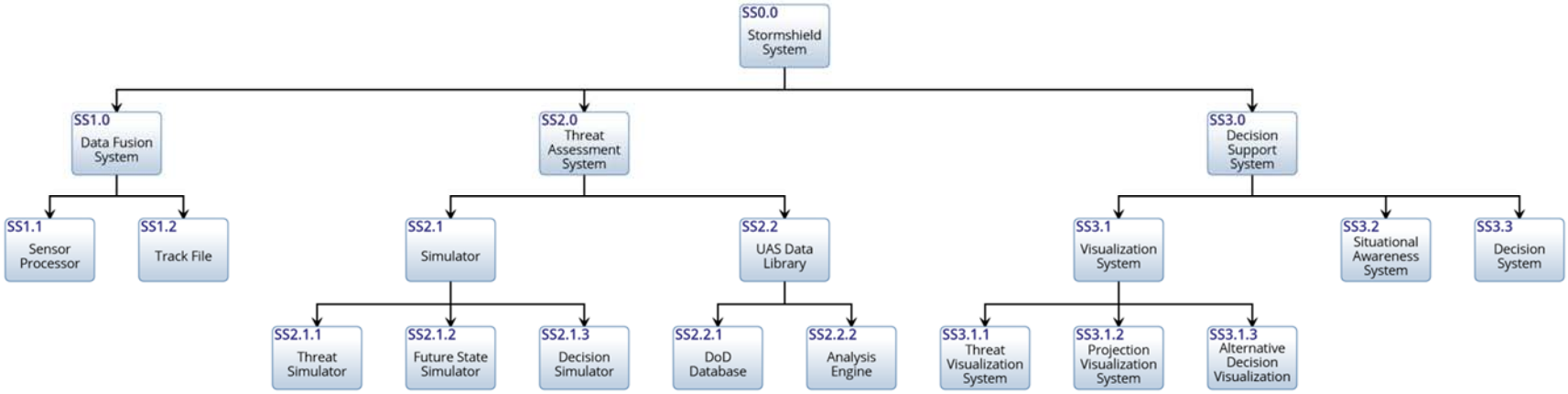

Figure 16. Storm Shield Module Hierarchy

A. MODULE ALLOCATION

1. Data Fusion

The data fusion system is comprised of two modules as shown in Figure 17. The sensor processor receives inputs from the external sensors and converts it into characteristic data about the entity. These characteristics include location, speed, size, signal frequencies, and other data captured by the sensors. The track file is the database of active tracks and contains all contacts that Storm Shield is interested in.

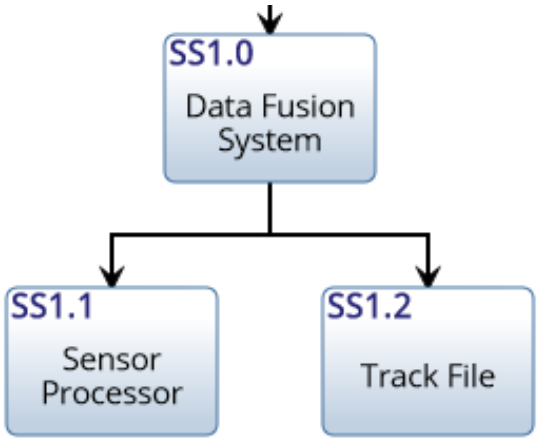

Figure 17. Data Fusion Module Hierarchy

The sensor processor accepts raw or processed data from a variety of sensor inputs. It is important that Storm Shield can accept input from many sensors so that it can use the hardware already in place at the facility, while still providing the most accurate data to identify threats. Figure 18 illustrates how this is accomplished. The sensor processor module provides the translation from either raw or processed data into the data format expected by the rest of the system. In the case of raw data, that will mean processing to determine entity characteristics. With data pre-processed by the sensor, the sensor processor will only need to put it into the proper format.

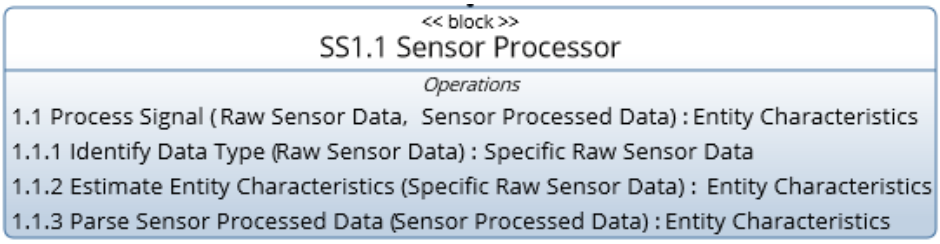

Figure 18. Sensor Processor Block Diagram

The track file is the list of all contacts recorded by the sensors, and in the module context it also includes the business logic for updating those contacts. Figure 19 shows the functions for merging or updating contacts. The track file module accepts the properly formatted characteristics about the entity.

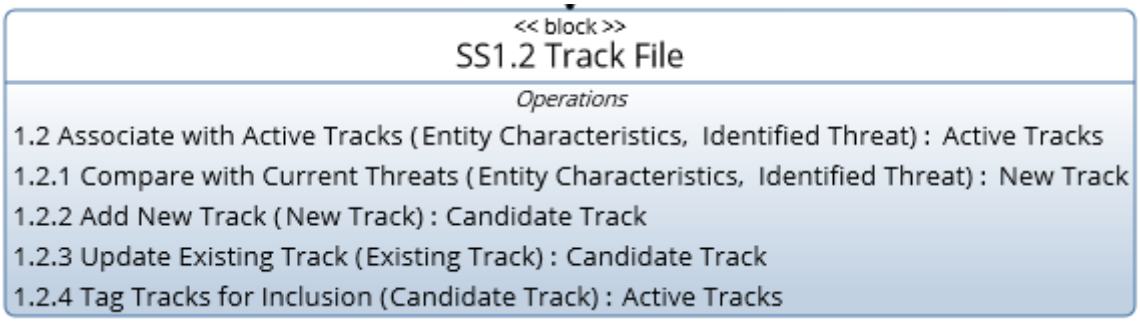

Figure 19. Track File Block Diagram

Each entity coming into the track file is from a single sensor, and the data fusion happens by associating the new characteristics measured from that sensor with an existing contact in the track file. Sensor data is fused as it is merged into the track file, rather than fusing multiple sensors and then inserting. This is because there is no assurance that all sensor readings for the contact will happen at the same time, so each reading is logged as it comes in. If no match is found, a new track is created and it will be there for any future measurements.

The final step is to attempt to reduce some of the noise by tagging contacts which the sensors measured but would not normally display. It is included in the track as

potentially useful data, but not processed by the threat assessment module until a genuine reading is recorded. One of the major problems facing C-UAS now is determining the proper filters to distinguish small UAS from birds and other factors usually discarded as signal noise. Capturing this data could help to improve those filter functions.

2. Threat Assessment

The threat assessment system is composed of seven subsystems, as shown in Figure 20. Two top-level mechanisms primarily perform these functions; a UAS data library consisting of existing UAS data, and a software intensive simulator used to determine UAS type and intent, project UAS behavior, and provide alternative decisions.

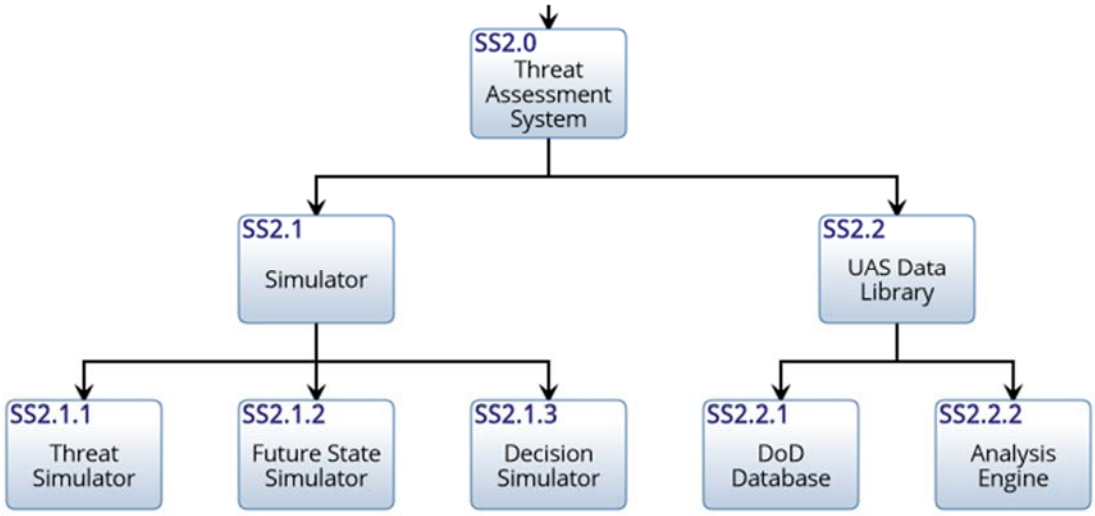

Figure 20. Threat Assessment Module Hierarchy

The UAS data library consists of two lower-level subsystems, including the Department of Defense (DOD) database and the analysis engine. The DOD database stores historical UAS data, which can be accessed by the analysis engine to assess the current threat effectively. The top-level simulator consists of a threat simulator, future-state simulator, and decision simulator, each intended to perform unique operations required for successful neutralization of the UAS threat. Each of these simulators will require the development of a custom software module.

The UAS data library contains the physical hardware and software systems that are required to retain and extract UAS data relevant to the current observed scenario. Figure 21 is a block definition diagram that provides a description of the UAS data library and lists the tasks intended to be carried out by this element of the physical architecture.

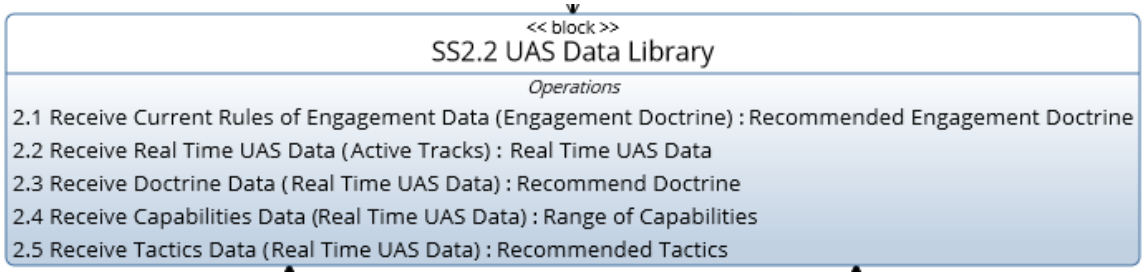

Figure 21. UAS Data Library Block Diagram

At the second level, the UAS data library consists of the DOD database and the analysis engine. The interfaces between these two subsystems allow the Storm Shield system to store, search, and send relevant information to the simulators. Figure 22 and Figure 23 describe the DOD database and analysis engine, respectively.

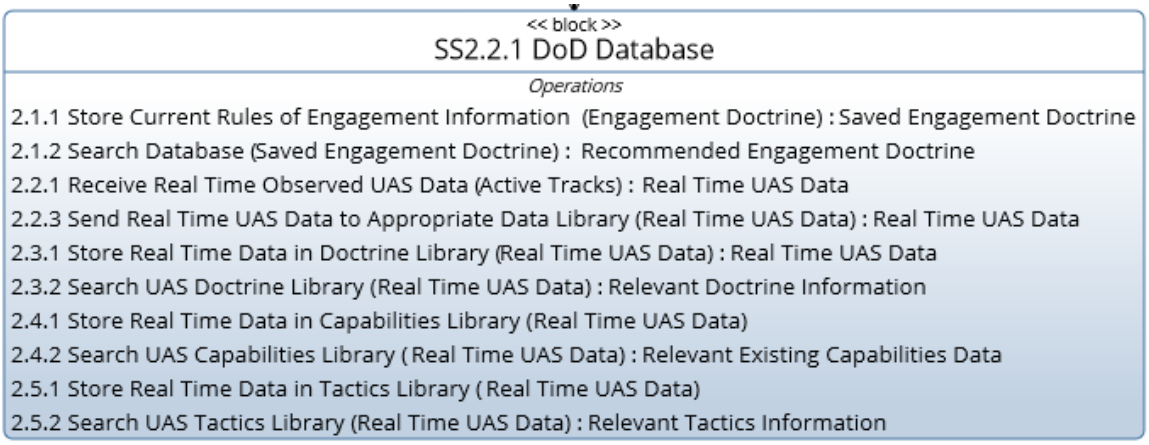

Figure 22. DOD Database Block Diagram

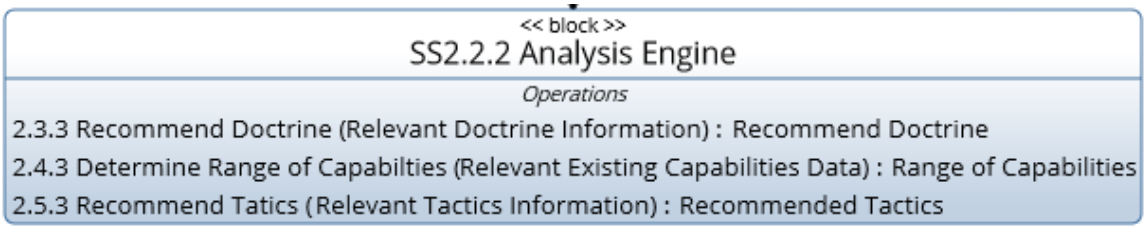

Figure 23. Analysis Engine Block Diagram

In addition to the UAS data library, the top-level of the physical architecture is comprised of a software intensive simulator, which serves as the mechanism responsible for performing the remaining threat assessment operations. Figure 24 provides a description of the tasking that is to be performed by this physical subsystem.

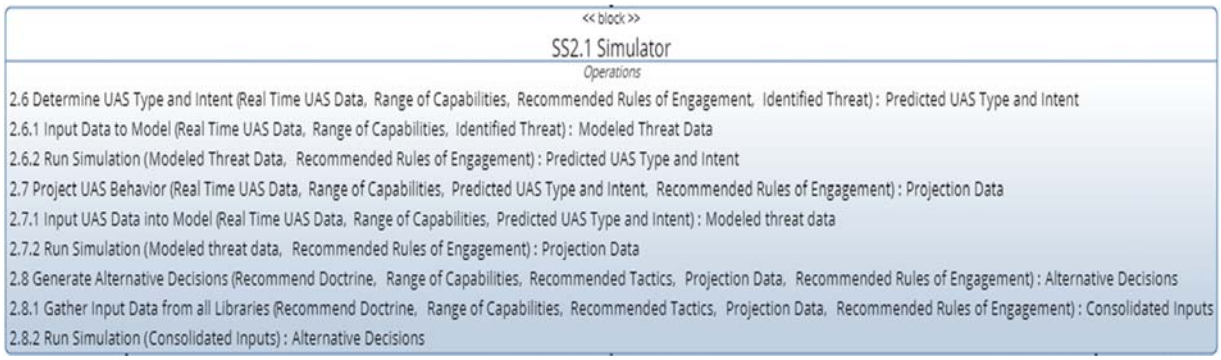

Figure 24. Simulator Block Diagram

At the second level of the physical architecture, the top-level simulator can be decomposed to include three distinct simulators. The threat simulator, future state simulator, and decision simulator are each required for successful neutralization of the UAS. The simulators are linked through software interfaces, which allow information to be shared until a decision regarding neutralization has been reached. The future state simulator receives input from the threat simulator and the decision simulator uses inputs from the previous two simulators to generate an output. Figure 25, Figure 26, and Figure 27 are block definition diagrams intended to provide a breakdown of these three subsystems.

Figure 25. Threat Simulator Block Diagram

Figure 26. Future State Simulator Block Diagram

Figure 27. Decision Simulator Block Diagram

3. Decision Support

Decision support functions were allocated into a decision support system. Within this system, similar functions were grouped into modules. This resulted in three main modules: a visualization system, a situational awareness system, and a decision system as shown in Figure 28. A more detailed view of this, including function allocations, can be found in Appendix C, Figure C-1. Each of these modules takes in data and applies an algorithm to generate output. As is the case for the other Storm Shield modules, the decision support system is software-intensive.

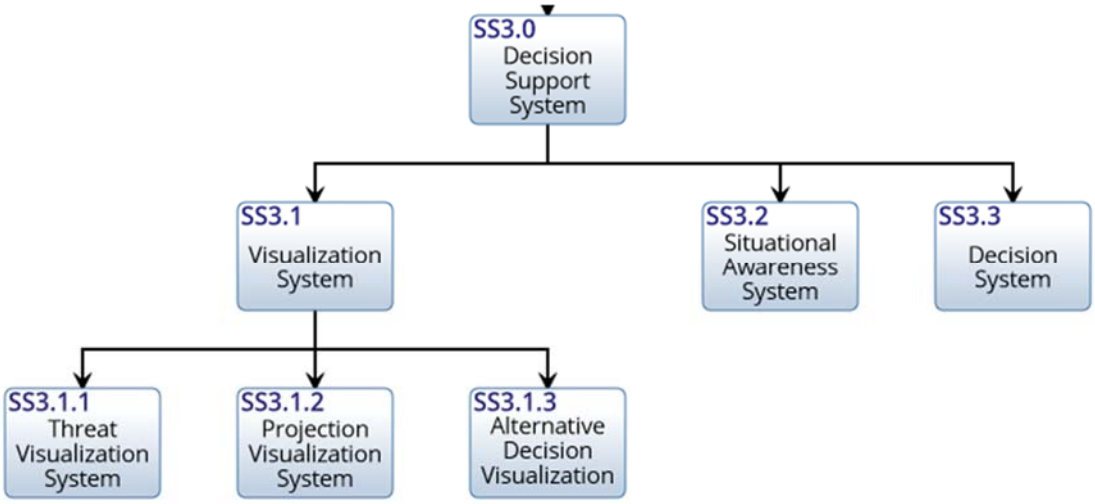

Figure 28. Decision Support Module Hierarchy

The block diagram in Figure 29 illustrates the allocation of functions to the visualization system. These include the three main visualization functions and the option to change the type and format of the visualizations. The IDEF0 for this system is illustrated in Chapter III.

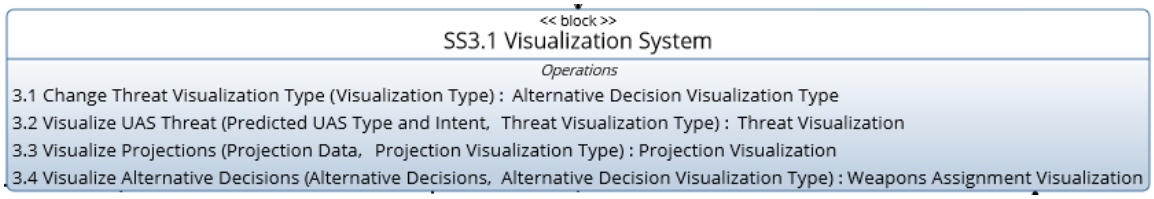

Figure 29. Visualization System Block Diagram

In the case of a human operator making decisions, the field of operations would be abstracted into a visual construct such as a map or resource view. Information about UAS capability, intent, and future states would be displayed in the context of the previously-mentioned constructs. Examples of these include threat cones, visualized paths, and gauges. In the case of algorithm-driven decisions, the visualization system becomes an interface layer that parses relevant information from the threat assessment system and passes it to the decision system in a format the decision system understands.

Figure 30 shows the functions allocated to this system. The Situational Awareness System takes in various visualizations and presents them to the decision maker. In the case of a human operator, this requires human factors engineering to ensure that visual, spatial, and audio abstractions enable communication of the different situational awareness levels.

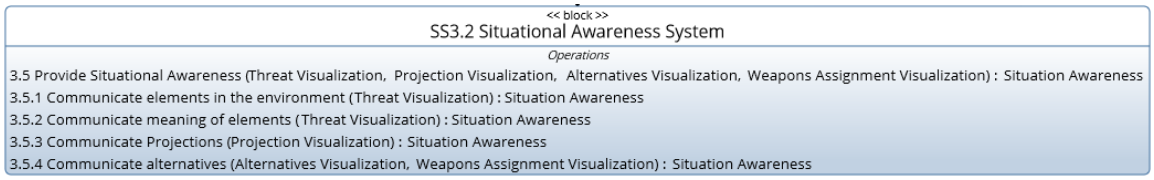

Figure 30. Situational Awareness System Block Diagram

The main driver of the implementation for the visualization system and situational awareness system is the decision support system. Table 6 describes the three options for the decision support system implementation.

Table 6. Decision Type Descriptions

Decision Type	Description
Human-driven decisions	A human operator makes identification and neutralization decisions
Automated decisions	The system makes identification and neutralization decisions
Automated decisions with a human supplement	The system makes identification and neutralization decisions but allows human intervention.

In the case of a human-driven decision support system and the automated decisions with a human supplement, the visualization system and situational awareness system must format data for human use. The human interface involves significant human

factors engineering and requires the use of various algorithms and abstractions to interface with a human operator through visual feedback and human-machine input methods.

Development is significantly simplified in the case of an automated decision system because the visualization system does not need to rely on visual abstractions to pass data to the situational awareness system. In the simplest case, data can merely be passed on to the situational awareness system, which parses relevant information for the decision system.

B. INTERFACES

The Storm Shield system will have interfaces with external systems such as sensors and neutralization systems. Additionally, the three major subsystems will require interfaces to pass information between them.

1. External Interfaces

Storm Shield will need to communicate with a suite of sensors to receive sensor data for fusion. Storm Shield will also need to interface with a neutralization system to eliminate the detected threats.

a. Interface between Sensors and Data Fusion

Storm Shield will interface with external sensors through the data fusion module. This interface shall support data rates and bandwidth necessary to support the sensor data. It needs support a variety of sensor types, such as radars, cameras, radio receivers, acoustic sensors, and EO/IR turrets. The system shall support raw or processed sensor data. The data fusion module will convert the data to the format required by the rest of the system. The module can be upgraded via software to support additional sensor types. This provides a level of abstraction to allow for new sensors to be added, preventing the system from becoming obsolete.

b. Interface between Decision Support and Neutralization System

To connect to external neutralization systems, Storm Shield will need to support multiple interfaces, depending on the neutralization system configuration. As the number of neutralization systems increase so does the development effort for this interface.

2. Subsystem Interfaces

Storm Shield is made up of three distinct subsystems: data fusion, threat assessment, and decision support. Data will pass through the data fusion system to threat assessment and finally to decision support before exiting the system boundary.

a. Interface between Data Fusion and Threat Assessment

The interface between the data fusion and threat assessment systems will be unidirectional going from the data fusion system to the threat assessment system. Logical inputs/outputs include active tracks, which contain any active contacts identified by the sensors being fused.

b. Interface between Threat Assessment and Decision Support

This interface is bi-directional and involves the multiple data fusion levels provided by threat assessment and the decisions provided by the decision support system. These are data-intensive inputs/outputs (IOs) and can be supported by a data stream.

C. SYSTEM VERIFICATION AND VALIDATION

Storm Shield must be able to recognize, identify, and respond to threats with adequate time to neutralize them with minimal impact. A radially inbound threat heading directly for the protected facility is the most stressing scenario Storm Shield will face and could pose a physical threat to the safety of the protected facility. This provided a threshold requirement for the system response time.

Using the known performance parameters of the UAS threat system and the detection ranges of the sensors gave a rough estimate of the threshold value. A stochastic model factoring in additional parameters such as probability of detection increased the fidelity of that threshold value.

The model included factors like engagement window. This represented the reality of legislative restrictions on when drones can and cannot be engaged. Figure 31 shows the approaching range of a radially inbound target, with corresponding detection range, engagement window, and an intercepting projectile. This figure is notional, to display the general concept. The model also factors in system processing time and operator response time, which will appear as a delay between detection and possible response. Different neutralization methods can also be chosen. The initial threshold value assumed signal jamming would be used and effective, since the threat was commercially available drones.

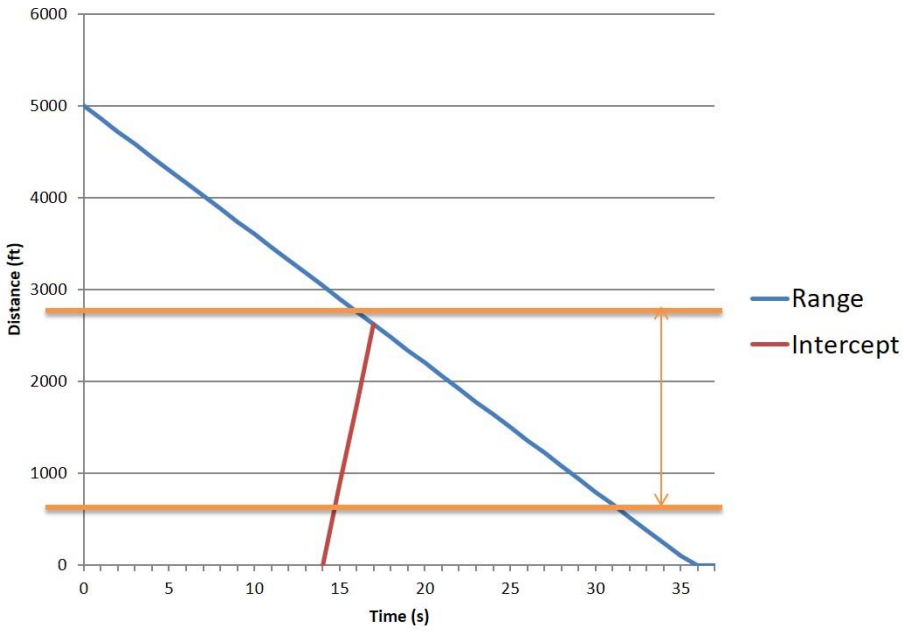

Figure 31. Time Range Graph

This model provided the tools to determine the threshold system performance. A second model examined the internal system behavior to determine the expected system performance. These two models were developed to understand and explore the functionality and performance trade space of the C-UAS TEWA system; representing both a top-down and bottom-up approach to functionality. The first model is a top-level

abstraction of the system, built using ExtendSim. The second model is built from the component level up, based on the functional architecture of the system, using the Innoslate web application. The purposes of these two models are to define and investigate system performance, respectively.

The Innoslate model was built to give a potential system designer a tool with which to define system-level performance parameters, which are used by the ExtendSim model for performance testing. Since the system is both novel and notional, the construction of the model occurred in tandem with the development of the system architecture. The Innoslate application facilitated this concurrent development, allowing for each element in the functional architecture to be defined with performance parameters. As the operational environment continues to change, this model will be easily adaptable to new configurations and allocations, as it is based on the functionality of the system. The model allows future designers to define the performance trade space, by estimating system-level parameters of various configurations.

The ExtendSim model, Figure 32, was developed to allow future designers to make performance predictions based on the system-level parameters generated by the Innoslate model. As an abstraction of the high-level functionality of the system, it can be used to simulate use-case scenarios and stochastically generated conditions. The resulting data gives designers a statistical prediction of system performance, based on a configuration. The intuitive key performance parameter at the system level is the probability of kill (p_K), therefore the ExtendSim model was designed such that p_K was the primary output.

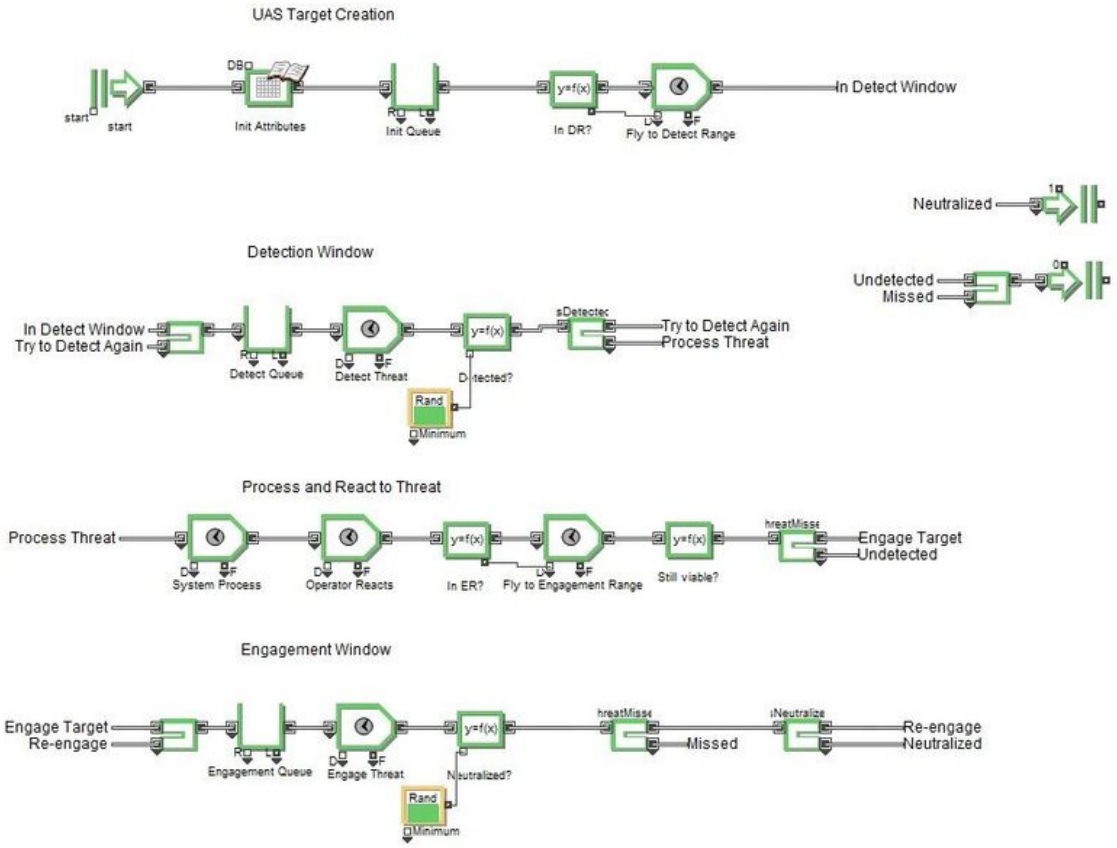

Figure 32. ExtendSim Model

It is crucial to note that these two models are complementary, representing top-down and bottom-up approaches to modeling the system. The Innoslate model builds on functional complexity from the component-level to the system-level. The ExtendSim model is an abstraction of the core functionality of the system, at the system of systems level. As more detail is added to components, the Innoslate model becomes more precise for defining the performance of the system. As the ExtendSim model is developed further, it becomes more effective for investigating the performance trade space. This dual approach allows a designer to identify, investigate, and compare design options easily.

The comprehensive, functional model that has been created and described would serve as the principal instrument for a full design effort of the C-UAS TEWA system. The model was built in such a way as to fulfill this role; having an open architecture,

generic interfaces, and clear system boundaries. The inputs required to make the model a usable design tool are performance parameters. The model is designed to run at various levels of fidelity, defined by the level of decomposition, to facilitate a spiral systems engineering approach. Performance parameters can be input for each level independently: system, subsystem, or component. The result is a progressively more detailed and accurate modeling of system performance. Deriving the performance parameters will be the topic of future work, but there are readily identifiable factors that will influence that effort, including choice of key performance parameters, the choice of decision system configuration, as well as the number and type of sensor and neutralization systems that the TEWA system will interface with.

1. Sensitivity Analysis

A sensitivity analysis was performed to assess the probability of kill against changes to system and target parameters. The analysis was based on a relatively stressful scenario, in the interest of skewing any insight in a conservative direction. A design of experiments (DOE) was built and analyzed using MiniTab statistical software and carried out using the ExtendSim model.

a. Experimental Design

A DOE was designed to test the probability of kill sensitivity to system parameters, against a relatively stressful target profile. The scenario was constructed to emulate a drone flying in a straight line, toward the interceptor, at maximum speed for a Group 2 drone of 422 ft/sec. Initial range was varied from essentially zero to ten miles. Table 7 includes a full list of performance parameters.

Table 7. Sensitivity Analysis Performance Values

System	Parameter	Minimum Value	Maximum Value	Nominal	Rationale
Independent Variables					
Target	Initial Range	1 ft	52800 ft	--	Based on scenario.
Target	Target Speed	1 ft/sec	422 ft/sec	--	Maximum speed for a Group 2 drone
C-UAS	Process Time	.1 sec	100 sec	--	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
C-UAS	Total System Reaction Time (Human-in-the-loop)	0.1 sec	100 sec	--	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
C-UAS	Detection Probability	0.5	.99	--	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
C-UAS	Neutralization Time	.1	100	--	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
C-UAS	Neutralization Probability	0.5	.99	--	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.

System	Parameter	Minimum Value	Maximum Value	Nominal	Rationale
Constants					
C-UAS	Detection Time			1 sec	
C-UAS	Maximum Intercept Range	--	--	>= maximum value for initial target range	This assumes that a neutralization system would be capable of neutralizing targets located at any distance within the military installation boundaries.
Target	Target Count	--	--	1	Dictated by problem statement and scope of project; multiple targets out of scope.
System	Detection Range			>= maximum value for initial target range	This assumes a sensor system that can detect a target at any distance within the kill zone.
System	Minimum Intercept Range	--	--	1 ft	This value is set to essentially no distance, to accommodate possible EW neutralization system modalities.
System	Interceptor Velocity	--	--	1,000,000 ft/sec	This makes the neutralization action instantaneous. In this scenario, the neutralization action is rolled into the neutralization time. This could be differentiated

System	Parameter	Minimum Value	Maximum Value	Nominal	Rationale
					in future iterations, as necessary.
System	Engagement Distance (minimum engagement distance)	--	--	52800 ft	This is the outer boundary of the kill-zone.

The DOE is a seven-factor, four-level, general full-factorial design. The levels are approximately even distributions across the range. The output is a continuous variable, the probability of kill. Table 8 lists the DOE factors for the sensitivity analysis.

Table 8. Sensitivity Analysis DOE Factors

Factor	Level 1	Level 2	Level 5	Level 4
Target Initial Range	1	17600	35200	52800
Target Speed	1	140	281	422
Process Time	.1	1	10	100
Total System Reaction Time	.1	1	10	100
Detection Probability	.5	.66	.82	.99
Neutralization Time	.1	1	10	100
Neutralization Probability	.5	.66	.82	.99

b. Results

Analysis of the data suggests that the primary driver of system effectiveness is Target Initial Range. Notably, the variables that comprise the total response time of the system, from detection to neutralization seem to have little effect below ten seconds. Neither detection probability nor neutralization probability has a notable effect. This is likely due to the configuration of the model, allowing the system to "retry" every cycle,

or once a second if it misses the first time. This configuration was intended to mimic a system that utilizing electronic sensors and EW neutralization systems. Figure 33 shows the results of the sensitivity analysis.

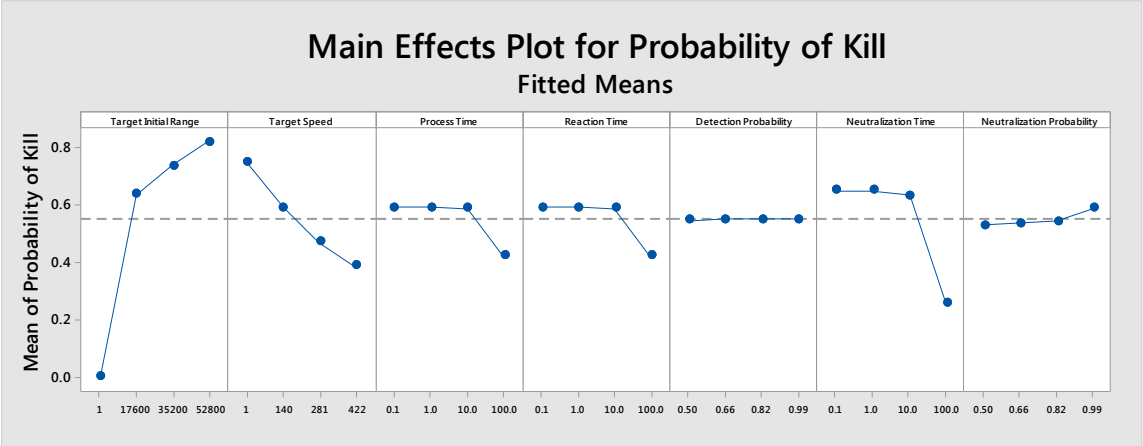

Figure 33. Sensitivity Analysis Results

2. Determination of Effect for Human-in-the-Loop

The effect of reaction time on the probability of kill was investigated to determine if it would be feasible, from a system effectiveness view, to include a human operator in the functioning of the system. To make a broad and conservative assessment, a DOE was used to analyze the effects of reaction time and target initial range.

a. Experimental Design

The DOE used for this study was based on the same scenario used for the sensitivity analysis, except for target speed which was chosen as one-third the maximum speed for a Group 2 UAV. Values for the remaining variables were chosen with the goal of nominal system performance. For example, processing time was set to ten seconds, the threshold of effect noted in the sensitivity analysis. Table 9 lists the performance values used in the DOE.

Table 9. Human-in-the-Loop Performance Values

System	Parameter	Minimum Value	Maximum Value	Nominal	Rationale
Independent Variables					
Target	Initial Range	1 ft	52800 ft	--	Based on scenario.
C-UAS	Total System Reaction Time (Human-in-the-loop)	0.1 sec	100 sec	--	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
Constants					
C-UAS	Detection Time			1 sec	
C-UAS	Maximum Intercept Range	--	--	>= maximum value for initial target range	This assumes that a neutralization system would be capable of neutralizing targets located at any distance within the military installation boundaries.
Target	Target Count	--	--	1	Dictated by problem statement and scope of project; multiple targets out of scope.
System	Detection Range			>= maximum value for initial target range	This assumes a sensor system that would be capable of detecting a target at any distance within the kill zone.
System	Minimum Intercept Range	--	--	1 ft	This value is set to essentially no distance, in order to accommodate possible EW neutralization system modalities.
System	Interceptor Velocity	--	--	1,000,000 ft/sec	This makes the neutralization action instantaneous. In this scenario, the neutralization action is rolled into the neutralization time. This could be differentiated in future iterations, as necessary.

System	Parameter	Minimum Value	Maximum Value	Nominal	Rationale
System	Engagement Distance (minimum engagement distance)	--	--	52800 ft	This is the outer boundary of the kill-zone.
C-UAS	Detection Probability	--	--	0.5	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
C-UAS	Neutralization Time	--	--	1	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
C-UAS	Neutralization Probability	--	--	.5	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.
Target	Target Speed	--	--	140 ft/sec	One-third the maximum speed of a Group 2 drone.
C-UAS	Process Time	--	--	10 sec	A wide range for the purpose of sensitivity analysis; not intended to emulate existing solutions.

The DOE is a two-factor, four-level, general full-factorial design. The levels are approximately even distributions across the range. The output is a continuous variable, the probability of kill. Table 10 lists the DOE factors for Human-in-the-Loop analysis.

Table 10. Human-in-the-Loop DOE Factors

Factor	Level 1	Level 2	Level 5	Level 4
Target Initial Range	3000	3500	4000	4500
Reaction Time	10	12.5	15	17.5

b. ***Results***

The study revealed results similar to those in the sensitivity analysis, suggesting that Target Initial Range is a driving factor. In this run, both range and reaction time were varied to determine the effect of both on the chance to stop the target. The slope of the range seems to be slightly steeper than the slope of the reaction time, and in opposite directions. Keep in mind that the slice will change that: in this set of runs, the initial range used a step of 500 feet while reaction time increased by 2.5 seconds. Also, keep in mind that this relationship will be directly affected by the speed of the threat. For this set of values, 140.6 ft/sec. was used to be representative of the upper end of the threats anticipated. Depending on the actual mission parameters, the graph indicates that an operator is a viable option. In a subsequent run, the initial range was held constant at 5,280 feet and in the scope of seven seconds (from 20 to 27 seconds of reaction time), the probability of kill dropped from 100% to 0%. Figure 34 shows the results of the human in the loop analysis.

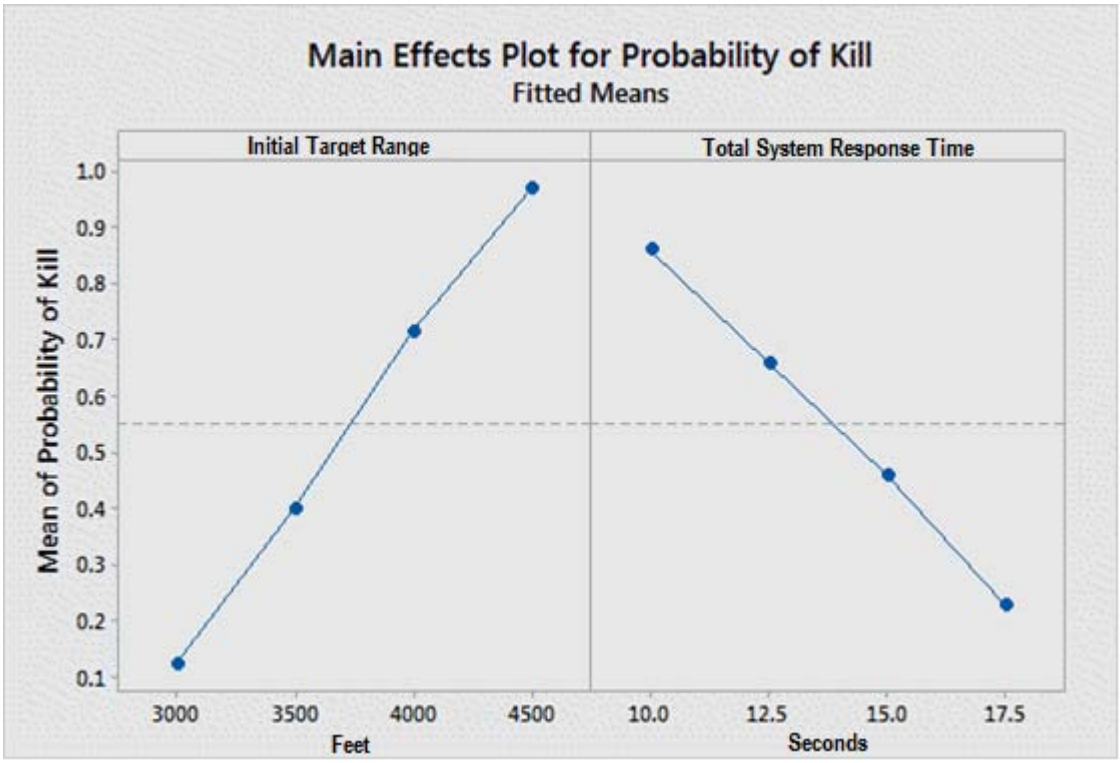

Figure 34. Human in the Loop Analysis Results

3. Probability of Kill versus Target Initial Range

The effect of probability of kill was investigated as a function of the target's initial range, based on the results of the sensitivity analysis. Functionally, this is equivalent to a minimum effective range. This variable is of interest in determining the suitability of a C-UAS system to a specific configuration and implementation, as existing facility boundaries are set.

a. Experimental Design

The model was configured with nominal parameter values, identical to those in the human-in-the-loop study except for reaction time, which was set to ten seconds. The target's initial distance was then set to values ranging from 10 to 52,800 feet in ten feet increments. The model was run 100 times at each increment to yield a probability of kill.

b. Results

Variability in the probability of kill, being anything other than 0 or 1.0, exists only over a small range of initial target range values from approximately 3,000 to 4,000 feet, during which it climbs steeply. For example, if a threat was detected at 3,000 feet the probability of kill is approximately 0.2, if that same threat was detected at 3,150 feet the probability of kill goes up to 0.5. The increase of 150 feet more than doubles the probability of kill for the threat. The results shown in Figure 35 suggest that the system could be highly effective in engagements with initial standoffs of one mile or greater.

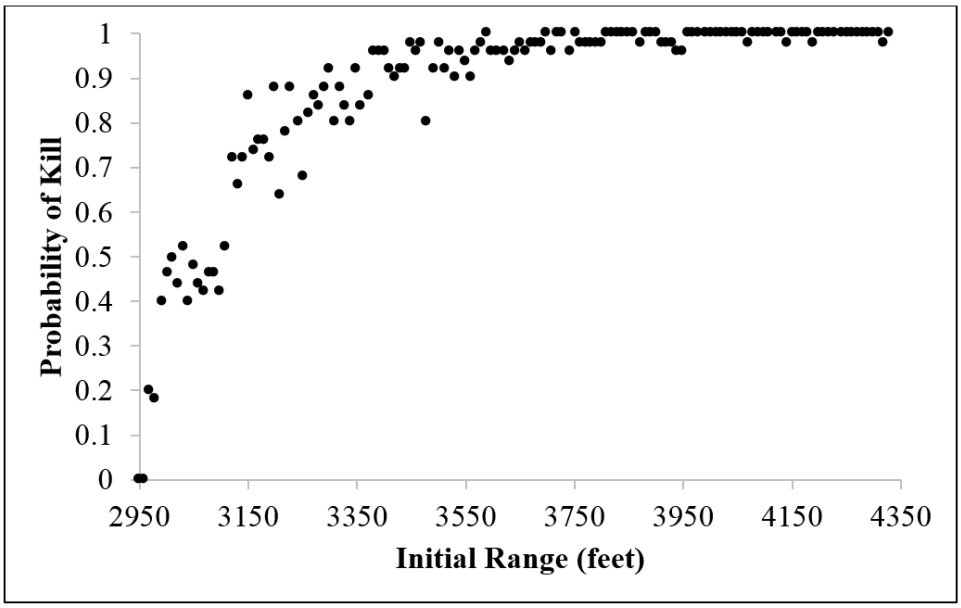

Figure 35. Probability of Kill as a Function of Initial Range

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

Storm Shield is a C-UAS system architecture that illustrates the requirements of the TEWA process for the command and control piece of the kill chain. The system design focused on providing emergent security and C-UAS capability for strategic U.S. Navy facilities, primarily focused on Group 1 and 2 drones. The driving need for this system is the rapid proliferation of UAS technologies by state and non-state actors, and the threat UAS represent to military facilities.

A. FUTURE WORK

Collaboration with major C-UAS stakeholders needs to occur to obtain the most current intelligence on emerging threats. Collected information may then be used to update Storm Shield models as subsystem functional requirements will likely change. Further data sharing will also be necessary to establish and maintain interoperability between Storm Shield, the facilities where Storm Shield will be installed, and future C-UAS capabilities. Intelligence will need to be uniform for dissemination and decoding. The Storm Shield blueprint will need to be reviewed and revised by Naval Air Systems Command (NAVAIR) C-UAS working groups before receiving funding and resources to manage the effort. This effort should include generating the SV-1, SV-10 and StdV-1 DoDAF views, as described in Figure 9, the Architecture Model Roadmap. The research-based architecture in place should be iterated for further progression.

B. CONCLUSION

The Storm Shield project team modeled a focused concept of operations to provide the necessary information to achieve a robust system design. The operational quality of the Storm Shield hardware and software integration is dependent upon the fidelity of the data fusion, threat assessment, and decision support subsystems.

When including a human operator, a system with the Storm Shield architecture is most effective when targets are detected at ranges greater than 4,000 feet. Therefore, it is

recommended to utilize sensors that can detect outside of 4,000 feet and hardware that can react and neutralize the UAS threat within 20 seconds.

APPENDIX

The appendix includes IDEF0 diagrams, system interface diagrams, and functional block diagrams. The IDEF0 diagrams found in Appendix A include level 1 and level 2 descriptions of Storm Shield. The system interface diagrams in Appendix B illustrate the interfaces between the top-level systems of Storm Shield. In Appendix C, the functional block diagrams capture system functionality for each subsystem.

A. IDEF0 DIAGRAMS

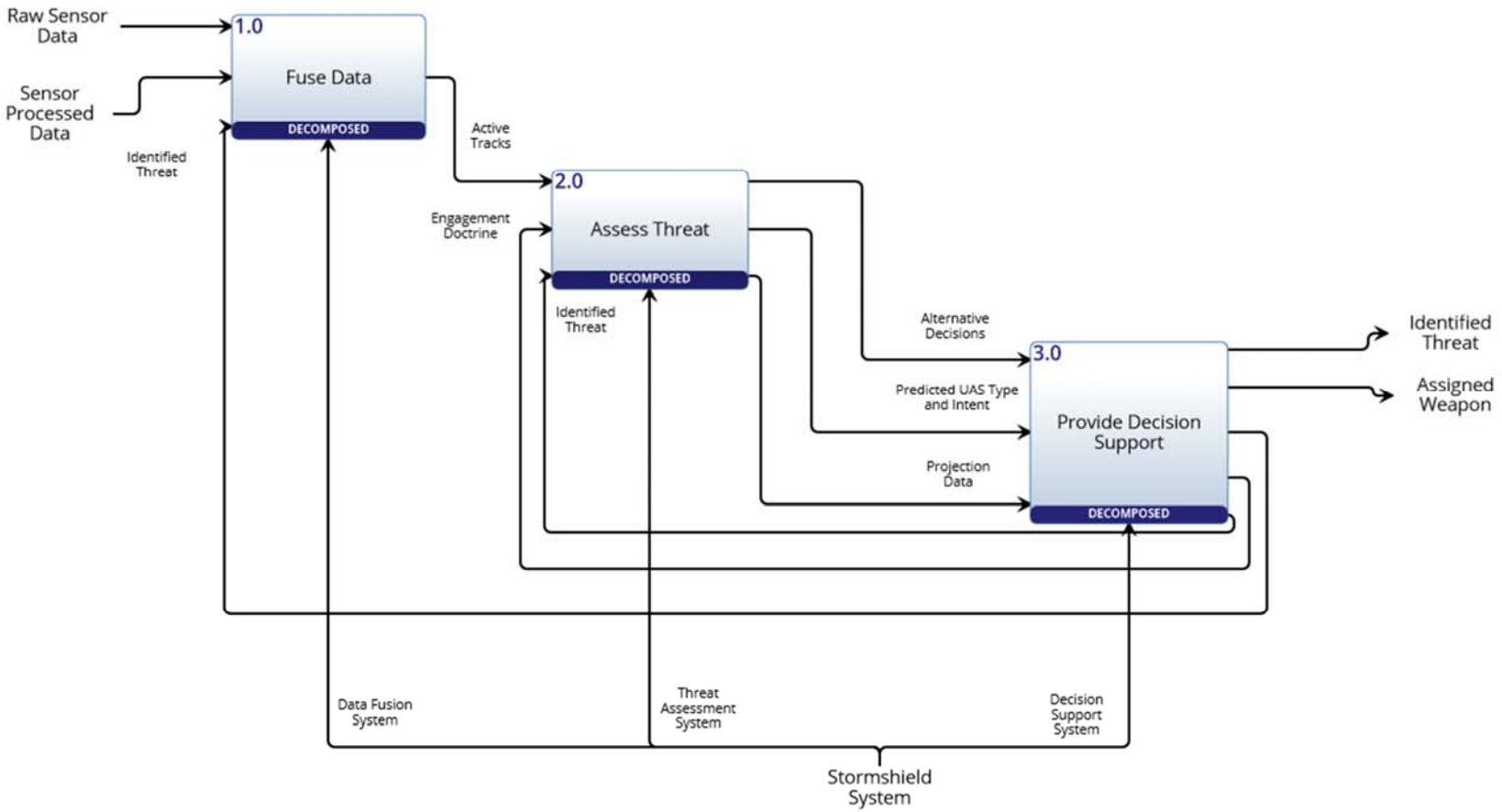

Figure A-1

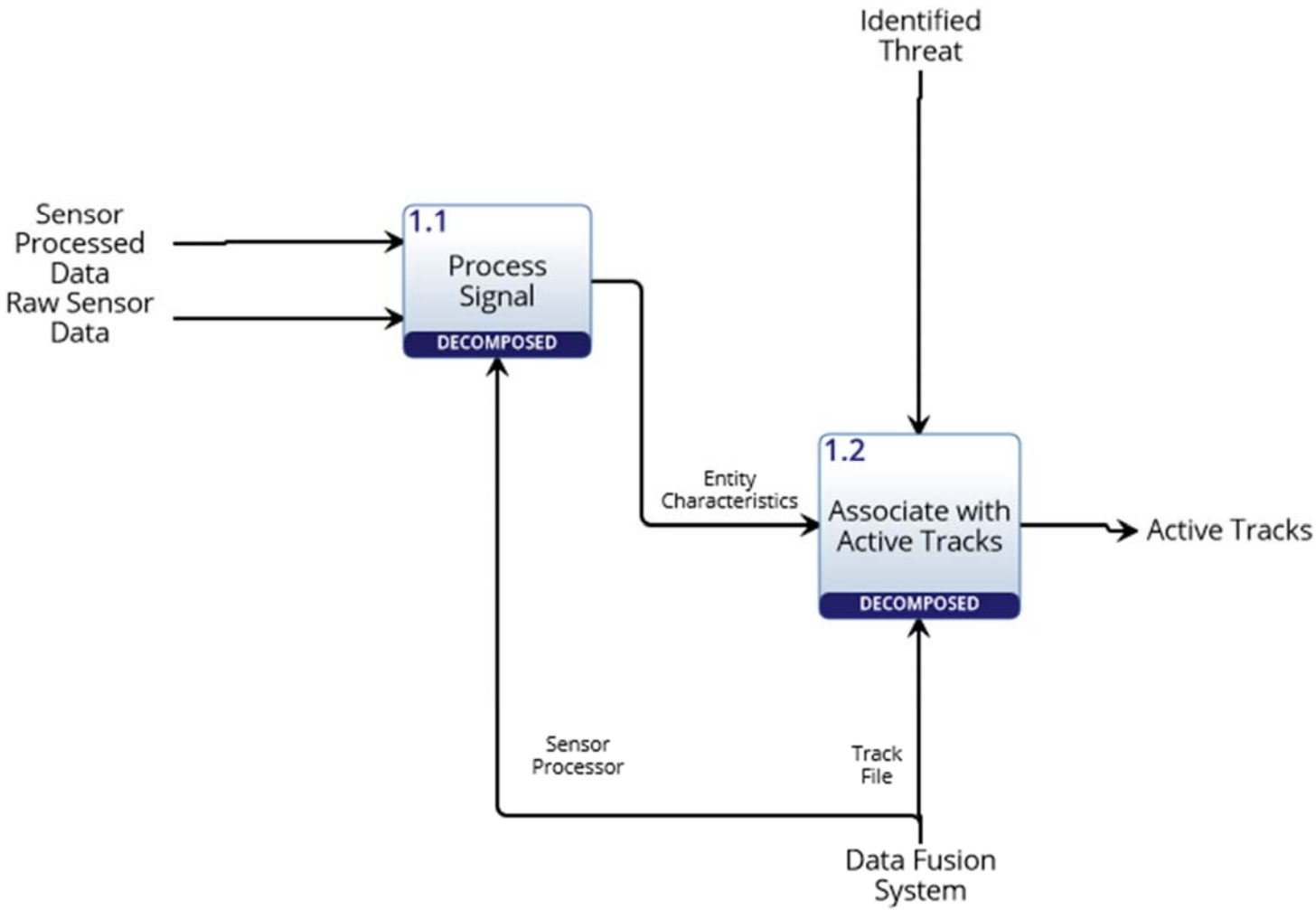
Identified
Threat
Sensor
Processed
Data
Raw Sensor
Data
1.1
Process
Signal
DECOMPOSED
Entity
Characteristics
1.2
Associate with
Active Tracks
DECOMPOSED
Active Tracks
Sensor
Processor
Track
File
Data Fusion
System

Figure A-2

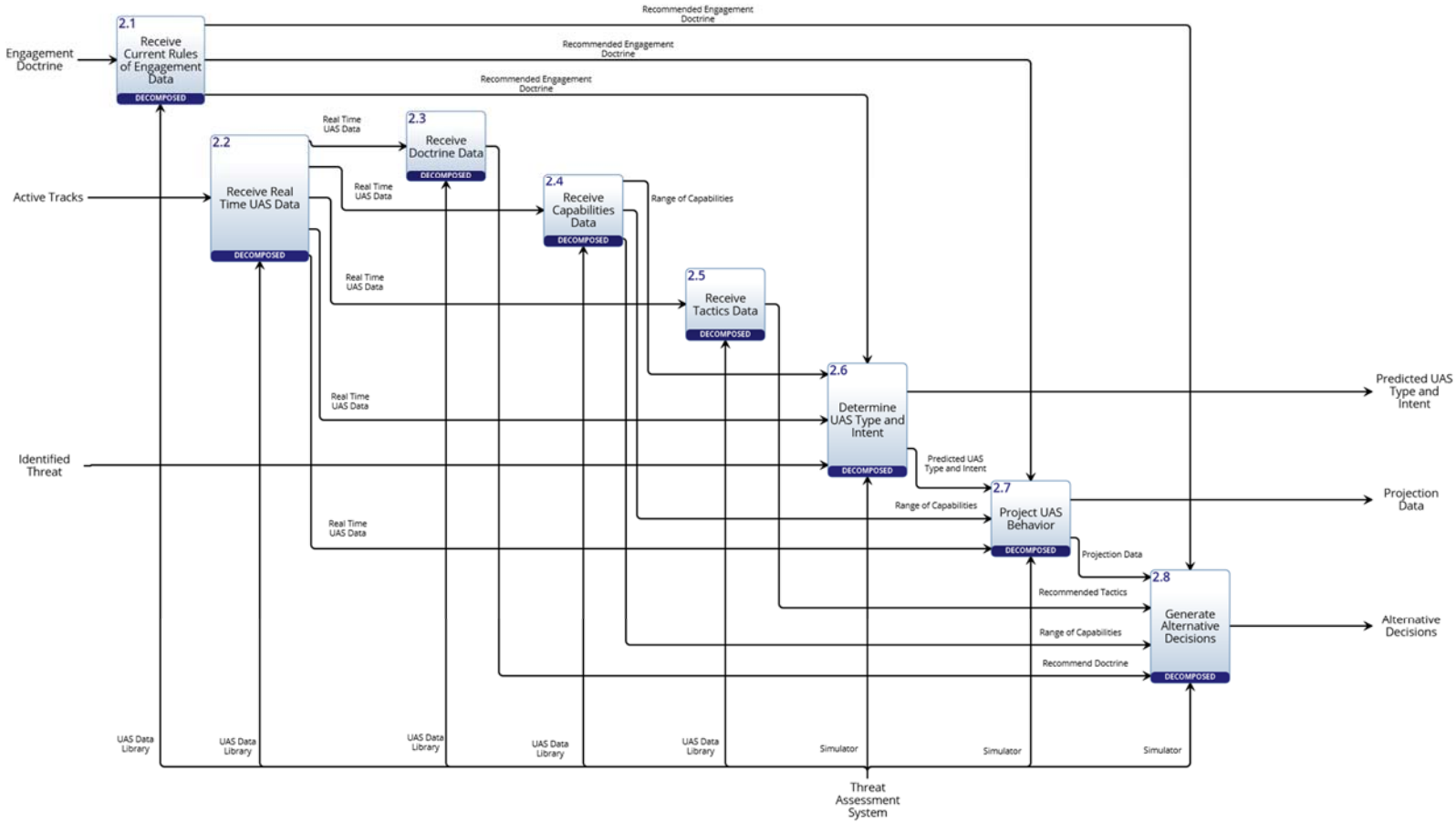
2.1
Receive Current Rules of Engagement Data
DECOMPOSED
2.2
Receive Real Time UAS Data
DECOMPOSED
2.3
Receive Doctrine Data
DECOMPOSED
2.4
Receive Capabilities Data
DECOMPOSED
2.5
Receive Tactics Data
DECOMPOSED
2.6
Determine UAS Type and Intent
DECOMPOSED
2.7
Project UAS Behavior
DECOMPOSED
2.8
Generate Alternative Decisions
DECOMPOSED
Engagement Doctrine
Active Tracks
Identified Threat
Recommended Engagement Doctrine
Recommended Engagement Doctrine
Recommended Engagement Doctrine
Real Time UAS Data
Real Time UAS Data
Real Time UAS Data
Real Time UAS Data
Real Time UAS Data
Real Time UAS Data
Range of Capabilities
Predicted UAS Type and Intent
Range of Capabilities
Projection Data
Recommended Tactics
Range of Capabilities
Recommend Doctrine
Predicted UAS Type and Intent
Projection Data
Alternative Decisions
UAS Data Library
UAS Data Library
UAS Data Library
UAS Data Library
UAS Data Library
Simulator
Simulator
Simulator
Threat Assessment System

Figure A-3

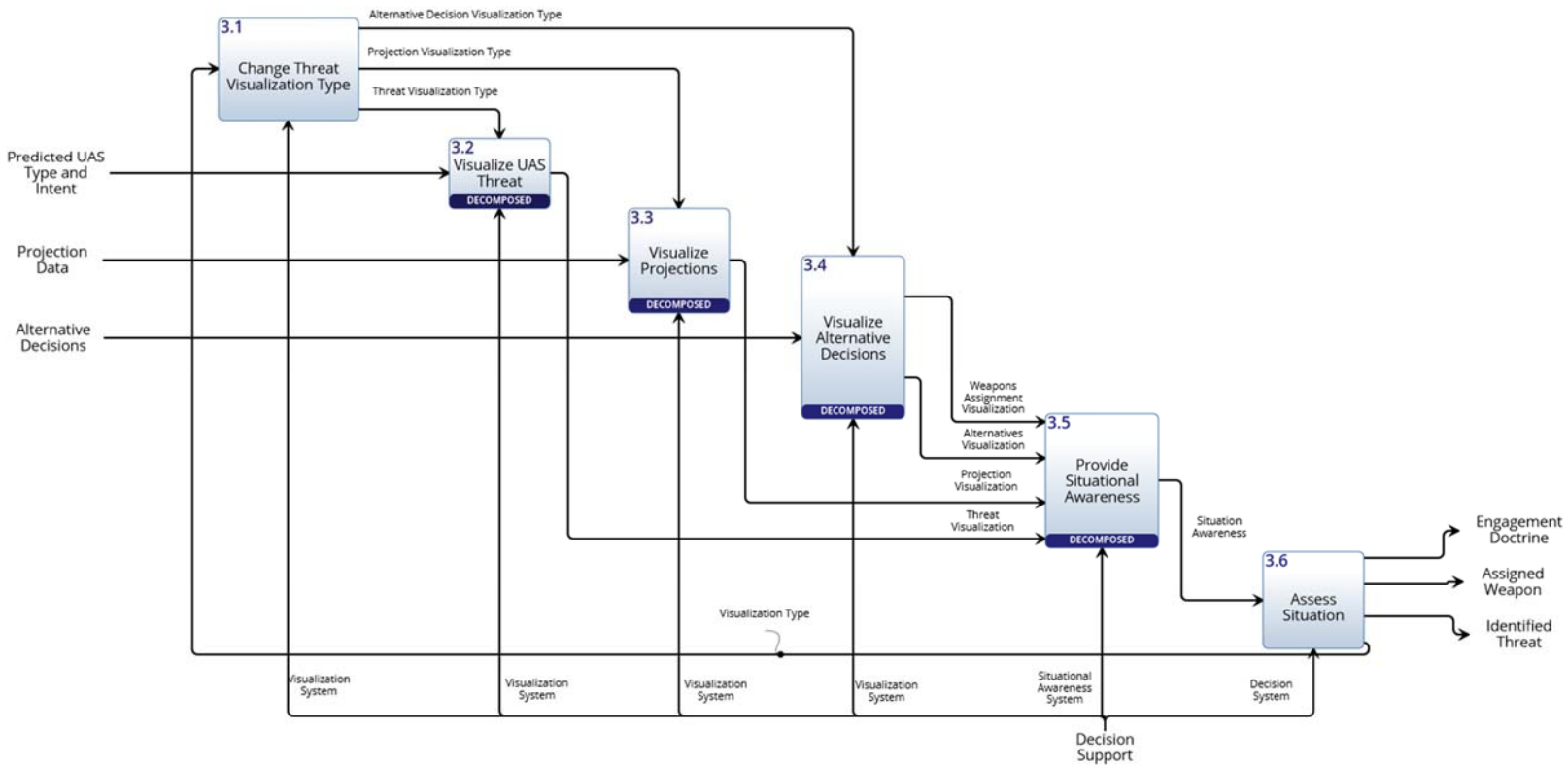
3.1
Change Threat Visualization Type
Alternative Decision Visualization Type
Projection Visualization Type
Threat Visualization Type
3.2
Visualize UAS Threat
DECOMPOSED
Predicted UAS Type and Intent
3.3
Visualize Projections
DECOMPOSED
Projection Data
3.4
Visualize Alternative Decisions
DECOMPOSED
Alternative Decisions
Weapons Assignment Visualization
Alternatives Visualization
Projection Visualization
Threat Visualization
3.5
Provide Situational Awareness
DECOMPOSED
Situation Awareness
3.6
Assess Situation
Engagement Doctrine
Assigned Weapon
Identified Threat
Visualization Type
Visualization System
Visualization System
Visualization System
Visualization System
Situational Awareness System
Decision System
Decision Support

Figure A-4

B. SYSTEM INTERFACE DIAGRAMS

Figure B-1

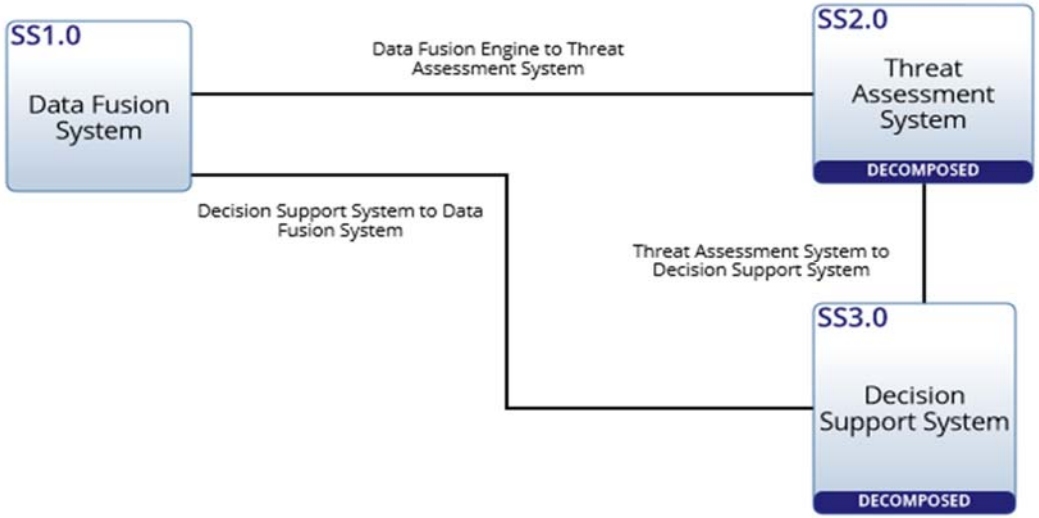

Figure B-2

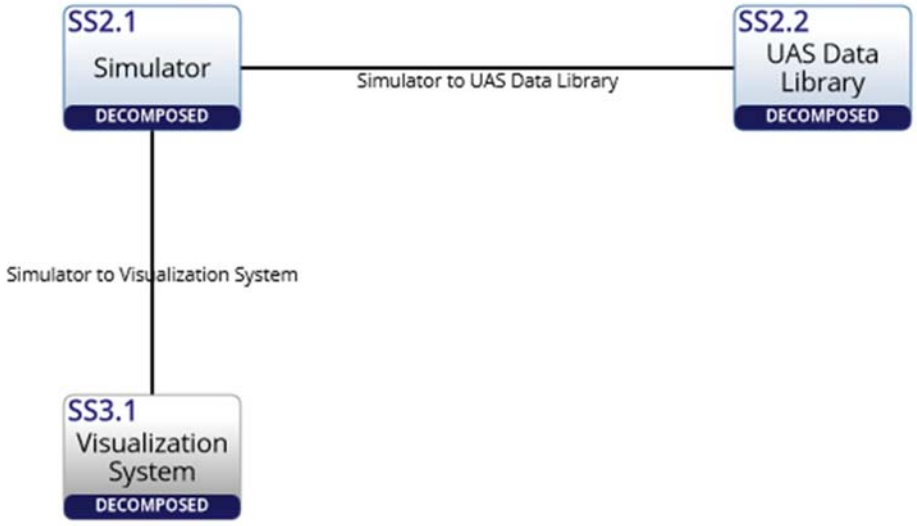
SS2.1
Simulator
DECOMPOSED
Simulator to UAS Data Library
SS2.2
UAS Data Library
DECOMPOSED
Simulator to Visualization System
SS3.1
Visualization System
DECOMPOSED

Figure B-3

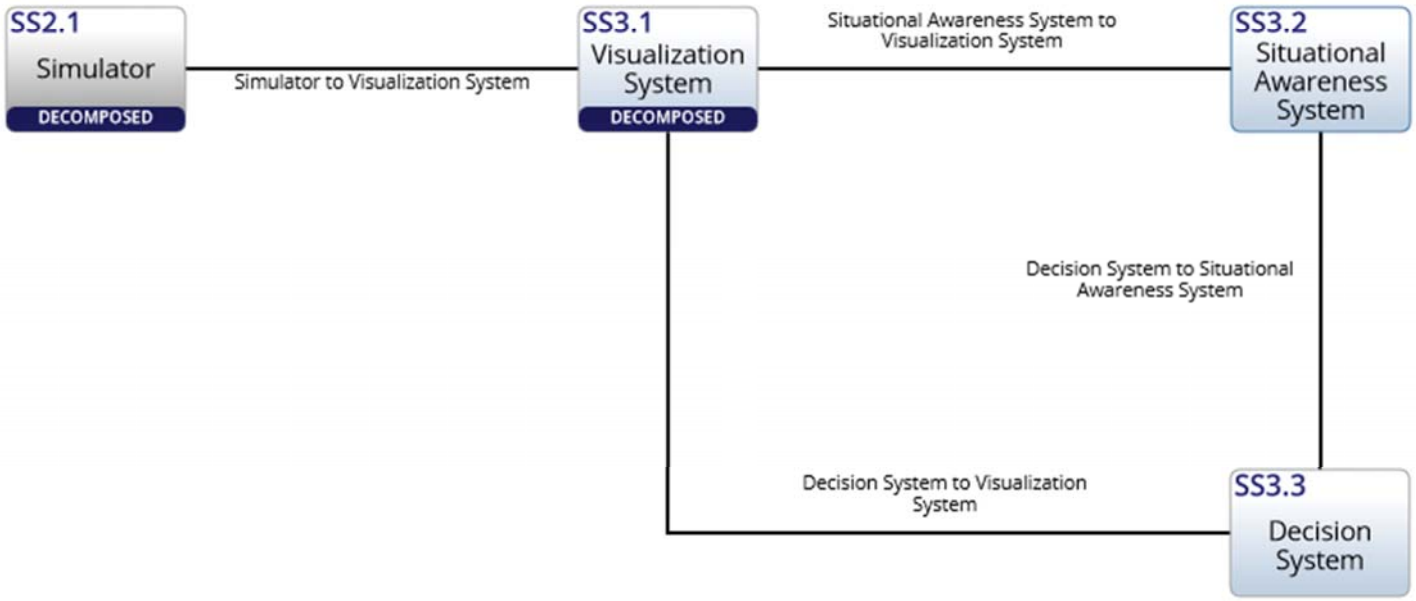
SS2.1
Simulator
DECOMPOSED
Simulator to Visualization System
SS3.1
Visualization System
DECOMPOSED
Situational Awareness System to Visualization System
SS3.2
Situational Awareness System
Decision System to Situational Awareness System
Decision System to Visualization System
SS3.3
Decision System

Figure B-4

C. SYSTEM-FUNCTION BLOCK DIAGRAMS

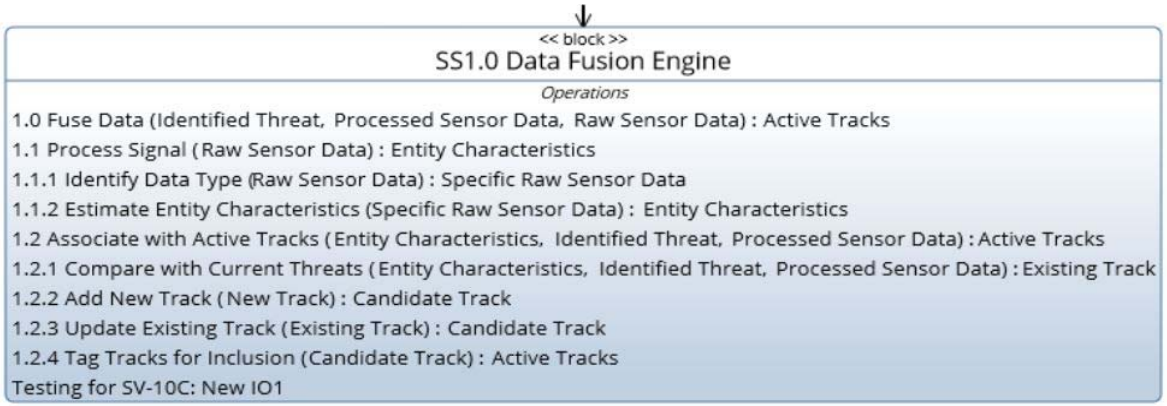

Figure C-1

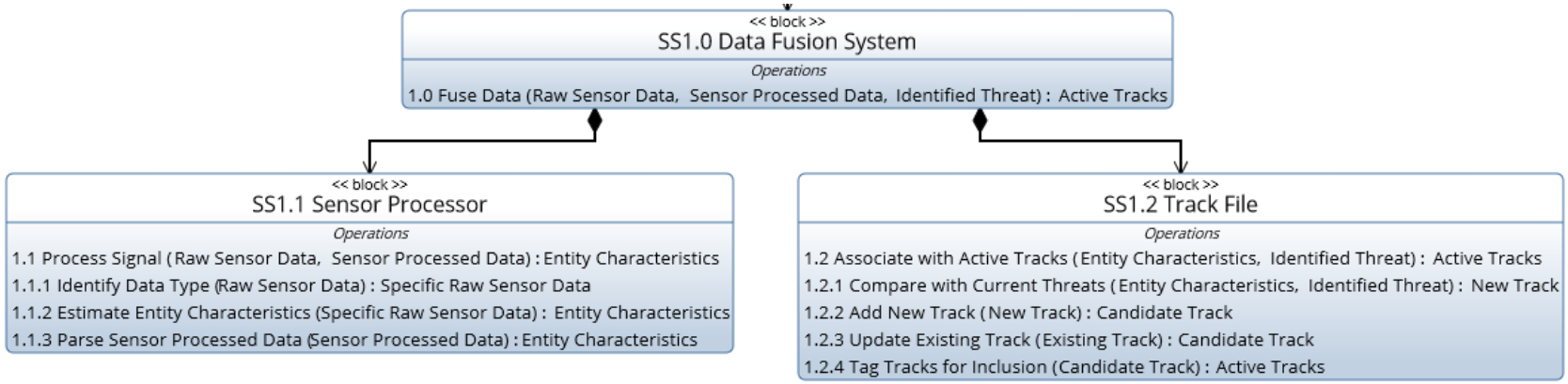

Figure C-2

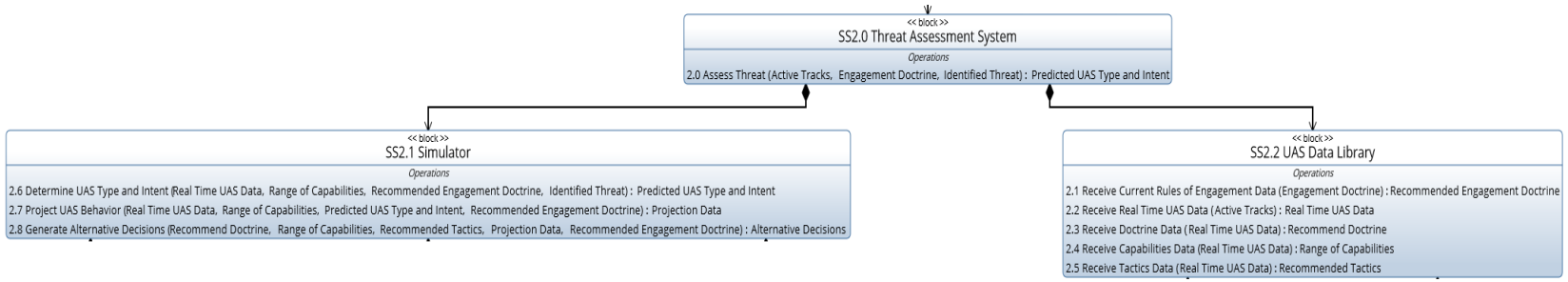

Figure C-3

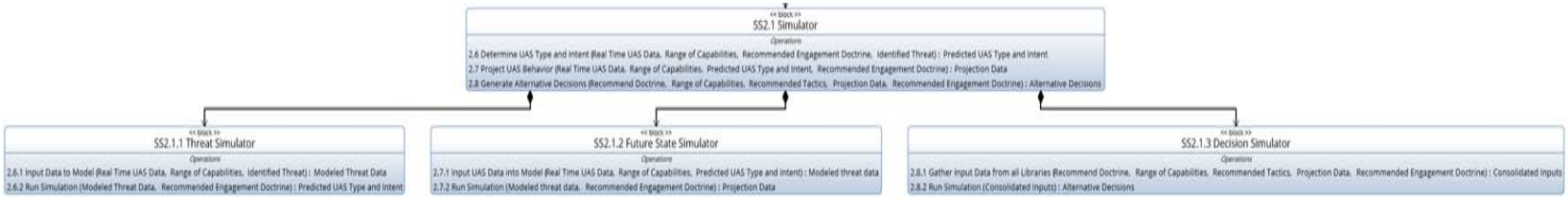

Figure C-4

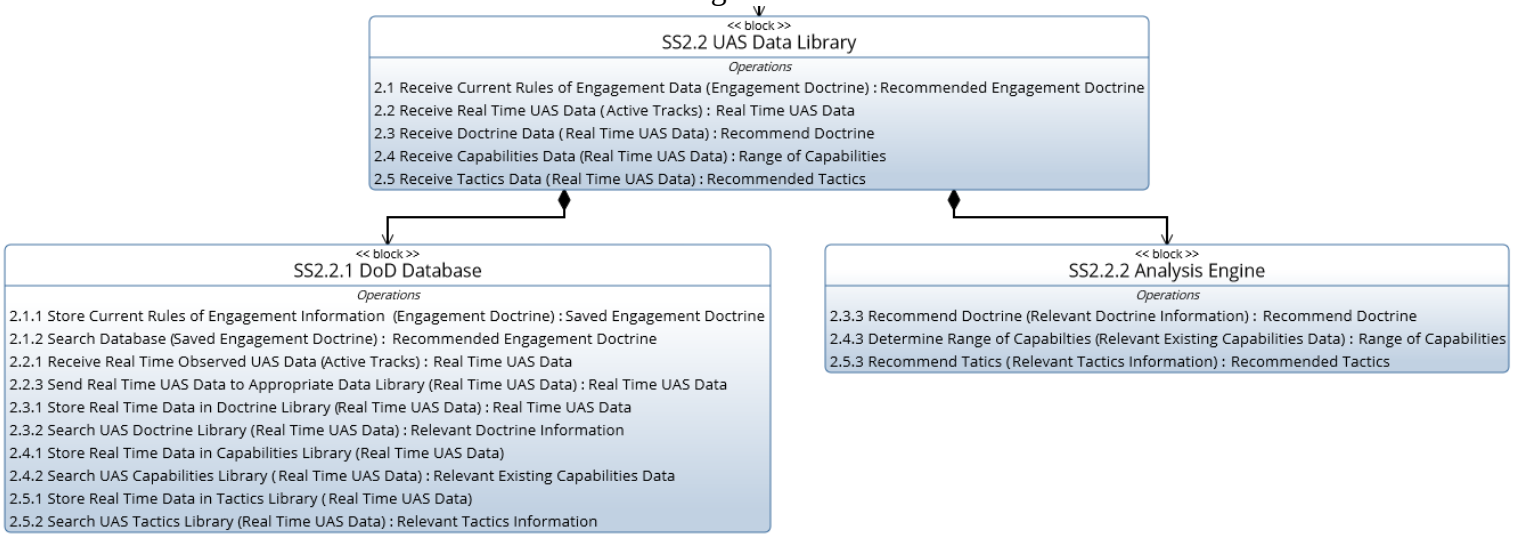

Figure C-5

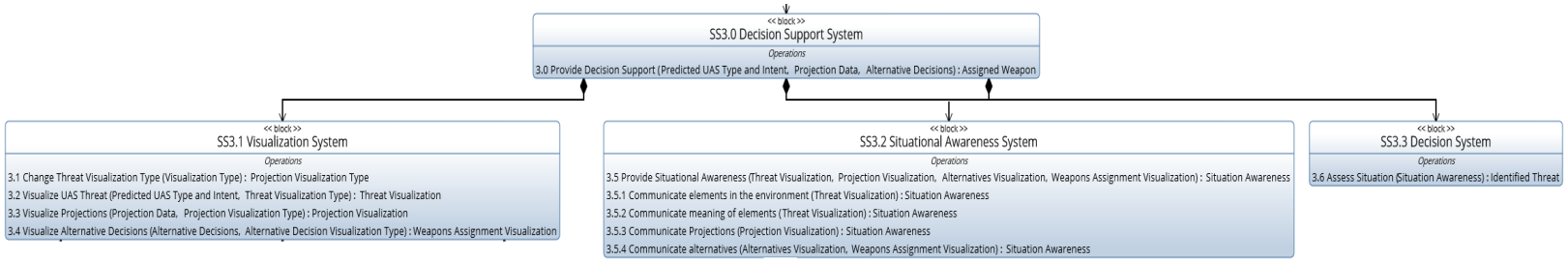

Figure C-6

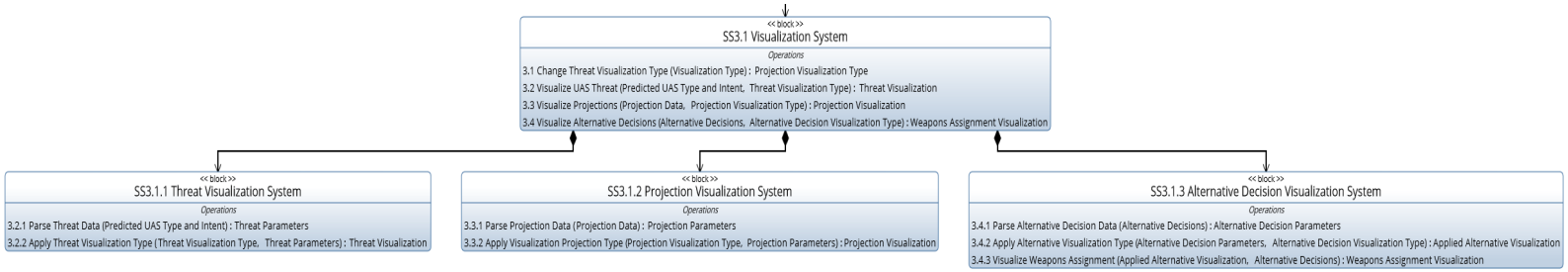

Figure C-7

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bergen, Peter, Sterman, David, Sims, Alyssa, Ford, Albert and Mellon, Christopher. 2017. “World of Drones.” New America. Accessed Aug 31, 2017, https://www.newamerica.org/in-depth/world-of-drones/.

Commander, Navy Installations Command. 2017. “Strategic Weapons Facility, Atlantic.” CNIC Naval Submarine Base Kings Bay.” Accessed July 7, 2017, https://cnic.navy.mil/regions/cnrse/installations/navsubbase_kings_bay/about/tenant_commands/strategic_weapons_facility_atlantic.html.

DAU. 2008. “Initial DOD SE Process Model.” accessed 30 January 2017, https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=9c591ad6-8f69-49dd-a61d-4096e7b3086c.

Desjardins, Jeff. 2016. “Here’s how Commercial Drones Grew Out of the Battlefield.” *Business Insider*., http://www.businessinsider.com/a-history-of-commercial-drones-2016-12.

Endsley, Mica R. 1995. “Toward a Theory of Situation Awareness in Dynamic Systems.” *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37 (1): 32–64. doi:10.1518/001872095779049543.

FAA. 2017. “UAS Sightings.” https://www.faa.gov/uas/resources/uas_sightings_report/.Joint Chiefs of Staff. 2013. Joint Publication 3–60.

Rosenburg, Jenny, and Brown, Laura. 2016. “Press Release – FAA Registered nearly 300,000 Unmanned Aircraft Owners.” https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19914.

Schaufele, Roger, D. Jr. 2015. “FAA Aerospace Forecast: Fiscal Years 2016–2036.” Statewide Agricultural Land use Baseline 2015. doi:10.1017/CBO9781107415324.004.

Steinberg, Alan N., Christopher L. Bowman, and Franklin E. White. 1999. “Revisions to the JDL Data Fusion Model.” http://www.dtic.mil/get-tr-doc/pdf?AD=ADA356422.

UAS Task Force: Airspace Integration Integrated Product Team. 2011. *Unmanned Aircraft System Airspace Integration Plan*. Department of Defense. doi:1-7ABA52E. http://www.acq.osd.mil/sts/docs/DOD_2011_UAS_Airspace_Integration_Plan_(signed).pdf.

Van Vuuren, J. H., and J. N. Roux. 2007. “Threat Evaluation and Weapon Assignment Decision Support: A Review of the State of the Art.” Orion 23 (2): 151–187. http://reference.sabinet.co.za/sa_epublication_article/orion_v23_n2_a5.

Webster, Bob. (2001). “Naval Submarine Base Kings Bay.” Wikipedia., https://en.wikipedia.org/wiki/Naval_Submarine_Base_Kings_Bay.

Whitlock, Craig. 2014. “Close Encounters on Rise as Small Drones Gain in Popularity.” *Washington Post*. http://www.washingtonpost.com/sf/investigative/2014/06/23/close-encounters-with-small-drones-on-rise/?utm_term=.fe6b353906ba.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California