NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE SYSTEMS ENGINEERING DESIGN OF A SMART FORWARD OPERATING BASE SURVEILLANCE SYSTEM FOR FORWARD OPERATING BASE PROTECTION

by

Timothy L. Craft
June 2013

Thesis Advisor: Rachel Goshorn
Thesis Co-Advisor: Deborah Goshorn

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: THE SYSTEMS ENGINEERING DESIGN OF A SMART FORWARD OPERATING BASE SURVEILLANCE SYSTEM FOR FORWARD OPERATING BASE PROTECTION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Timothy L. Craft	
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 Protocol Number _____N/A_____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT

Forward operating bases are vulnerable to terrorist activity due to their location and limited resources. Threat awareness under these conditions is paramount to the safety of the personnel and to mission accomplishment. In the absence of the manpower required to maintain complete and continuous monitoring of the FOBs surroundings, an automated surveillance system is needed. The Smart FOB Surveillance System (SFSS) employs a multi-agent behavior analysis and decision system with Swarm Intelligence (SI) through a network-centric systems engineering method of development to create a robust surveillance system. The SFSS provides the capability of an intelligence automated system for continuously monitoring areas for certain behaviors, linking individuals, predicting future behaviors, and taking appropriate action against them to eliminate threats and the possibility of future threats. Environments, such as insurgent urban areas, Forward Operating Bases, country borders, and other high-value target areas all require constant personnel behavior surveillance and monitoring.

The SFSS utilizes a complex network of aerial, fixed and mobile terrestrial units, capable of identifying and processing audible, visual, and signal intelligence in order to determine personnel behavior in a given area of interest as well as recording and processing intelligence data. The focus is on creating a system to protect Forward Operating Bases (FOB) by providing continuous and autonomous surveillance and threat alerts. In this manner, a Smart FOB Surveillance System (SFSS) will be designed in this thesis using the systems engineering process.

14. SUBJECT TERMS Systems Engineering, Autonomous Systems, Surveillance, Force Protection.	**15. NUMBER OF PAGES** 107
	16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE SYSTEMS ENGINEERING DESIGN OF A SMART FORWARD OPERATING BASE SURVEILLANCE SYSTEM FOR FORWARD OPERATING BASE PROTECTION

Timothy L. Craft
Lieutenant Commander, United States Navy
B.A., Miami University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2013

Author: Timothy L. Craft

Approved by: Rachel Goshorn
Thesis Co-Advisor

Deborah Goshorn
Thesis Co-Advisor

Clifford Whitcomb
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Forward operating bases are vulnerable to terrorist activity due to their location and limited resources. Threat awareness under these conditions is paramount to the safety of the personnel and to mission accomplishment. In the absence of the manpower required to maintain complete and continuous monitoring of the FOBs surroundings, an automated surveillance system is needed. The Smart FOB Surveillance System (SFSS) employs a multi-agent behavior analysis and decision system with Swarm Intelligence (SI) through a network-centric systems engineering method of development to create a robust surveillance system. The SFSS provides the capability of an intelligence automated system for continuously monitoring areas for certain behaviors, linking individuals, predicting future behaviors, and taking appropriate action against them to eliminate threats and the possibility of future threats. Environments, such as insurgent urban areas, Forward Operating Bases, country borders, and other high-value target areas all require constant personnel behavior surveillance and monitoring.

The SFSS utilizes a complex network of aerial, fixed and mobile terrestrial units, capable of identifying and processing audible, visual, and signal intelligence in order to determine personnel behavior in a given area of interest as well as recording and processing intelligence data. The focus is on creating a system to protect Forward Operating Bases (FOB) by providing continuous and autonomous surveillance and threat alerts. In this manner, a Smart FOB Surveillance System (SFSS) will be designed in this thesis using the systems engineering process.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- **A. MOTIVATION 1**
- **B. PURPOSE 1**
- **C. QUESTIONS RESEARCHED 1**
- **D. OVERVIEW 2**
- **E. APPLICATION 5**
- **F. PROBLEM DEFINITION 6**
- **G. PROPOSED SOLUTION 7**
- **H. THESIS ORGANIZATION 8**

II. NETWORK-CENTRIC SYSTEMS ENGINEERING APPROACH 11
- **A. OVERVIEW 11**
- **B. NETWORK-CENTRIC SYSTEMS 11**
  - **1. Network-centric Systems 12**
  - **2. What is Network-centric Systems Engineering? 12**
    - ***a. Top-down System 13***
    - ***b. Bottom-up System 14***
    - ***c. Middle System 14***
    - ***d. Side View (Disadvantaged User) System 14***
- **C. NETWORK-CENTRIC ARCHITECTURE 15**
  - **1. NetOps Agility 15**
  - **2. Data and Services Deployment 15**
  - **3. Computing Infrastructure Readiness 16**
  - **4. Communications Readiness 16**
  - **5. Secured Availability 16**
- **D. CAPABILITIES AND ATTRIBUTES 16**
  - **1. Network-centric Capabilities 17**
  - **2. Network-centric Attributes 18**
- **E. WARFARE AND OPERATIONS 19**
  - **1. Network-centric Warfare 19**
  - **2. Network-centric Operations 23**
    - ***a. FBCB2 – Blue Force Tracker 23***
    - ***b. Horizontal Fusion 23***
    - ***c. Collaborative Information Environment 24***
- **F. ENGINEERING THROUGH AGENTS 24**
  - **1. Network-centric Science and Technology 24**
  - **2. Agent-based Science and Technology 25**

III. THE SYSTEMS ENGINEERING PROCESS 27
- **A. SYSTEMS ENGINEERING PROCESS 27**
- **B. SYSTEMS ENGINEERING V-MODEL 27**
  - **1. Operational Requirements 28**
  - **2. Operational Concept 29**

3. Operational Scenarios 29
4. External Systems Diagram 29
5. Requirements 29
6. Functional Architecture Hierarchy 30
7. Functional Architecture Decomposition 30
8. Physical Architecture Hierarchy 30
9. Operational Architecture 30
C. DOD SYSTEMS ENGINEERING V-MODEL 30
D. PROBLEM DEFINITION AND SYSTEM CONCEPT 31
E. SYSTEM LEVEL DESIGN REQUIREMENTS AND ARCHITECTURE 32
1. Analysis of Alternatives 33
F. ITEM LEVEL DESIGN REQUIREMENTS 33
G. FABRICATE, INTEGRATE, AND TEST 33
IV. SWARM INTELLIGENCE AND MULTI-AGENT SYSTEMS 35
A. OVERVIEW 35
B. INTELLIGENCE AUTOMATION 36
1. Intelligence Automation 38
C. MULTI-AGENT SYSTEM 38
1. Agent Design 38
2. Environment 38
3. Perception 39
4. Control 39
5. Knowledge 39
6. Communication 39
D. DISTRIBUTED ARTIFICIAL INTELLIGENCE (DAI) 40
E. WHY DISTRIBUTED AI? 40
F. DIPR AS A MAS 41
1. Detection 41
2. Identification 42
3. Prediction 43
4. Reaction 44
V. SYSTEM ENGINEERING SOLUTION FOR A SMART FOB SURVEILLANCE SYSTEM (SFSS) 47
A. OPERATIONAL NEED 47
B. OPERATIONAL CONCEPT 47
C. OPERATIONAL OVERVIEW 48
D. OPERATIONAL SCENARIOS 50
E. EXTERNAL SYSTEMS DIAGRAM (ESD) 55
F. REQUIREMENTS 56
G. GENERIC SYSTEM FUNCTIONAL ARCHITECTURE 57
H. GENERIC SYSTEM PHYSICAL ARCHITECTURE 66
1. The Fixed Sensor System 67
2. The Smart Mobile Sensor System 71
3. The NOC System 73

I. GENERIC SYSTEM OPERATIONAL ARCHITECTURE 74
VI. SUMMARY AND CONCLUSIONS 77
A. SUMMARY 77
B. CONCLUSION 77
LIST OF REFERENCES 81
INITIAL DISTRIBUTION LIST 83

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. NCSE Core and Four Approaches Tree (From Goshorn et al., 2011)..... 13
Figure 2. JNO Tier 2 Capability Areas ((From JNO, 2007)..... 18
Figure 3. Information Age Warfare Domains of Conflict (From DoD, 2005)..... 21
Figure 4. Tenets of NCW within the Warfare Domains (From DoD, 2005) 22
Figure 5. Systems Engineering Vee (From Forsberg and Mooz, 1992)..... 28
Figure 6. Systems Engineering V-Model (From DoDAF, 2007)..... 31
Figure 7. The Need for Intelligence Automation, and the Four Approaches Required to Implement Automation (From Goshorn et al., 2011)..... 37
Figure 8. DIPR System (From Goshorn et al., 2011)..... 41
Figure 9. Feature Space Matrix (From Goshorn et al., 2011) 42
Figure 10. Identification Subsystem of the DIPR System (From Goshorn et al., 2011) 43
Figure 11. Prediction Subsystem (From Goshorn, 2011)..... 44
Figure 12. Intelligent Hierarchy Implements DIPR System (From Goshorn, Goshorn, Goshorn & Goshorn 2010)..... 45
Figure 13. System Operational View 50
Figure 14. External Systems Diagram for SFSS 55
Figure 15. Generic Functional Architecture Hierarchy for SFSS 58
Figure 16. Top-level Function for the Generic System for SFSS 59
Figure 17. First-level Decomposition of the System Function Provide SFSS Services for SFSS 60
Figure 18. Decomposition of the Provide Fixed Sensor Services Function for SFSS 61
Figure 19. Decomposition of the Provide Mobile Sensor Services Function for SFSS 62
Figure 20. Decomposition of the Provide NOC Services Function for SFSS..... 63
Figure 21. Decomposition of the Provide Swarm UAV Control Function for SFSS 64
Figure 22. Decomposition of the Process Video Function for SFSS 65
Figure 23. Decomposition of the Process Sensor Data Function for SFSS 66
Figure 24. Generic Physical Architecture Hierarchy for SFSS..... 67
Figure 25. Super Night Vision Outdoor AF 30X Zoom Camera (From Security Camera World, 2012)..... 68
Figure 26. Long Range Listening Devices (From Mesinnovation.com, 2005)..... 69
Figure 27. Agilent N6841A RF Sensor (From Agilent Technologies, Inc., 2000–2013) 71
Figure 28. Dragon Flyer X6 (From Draganfly Innovations Inc., 2013)..... 72
Figure 29. NOC System Components 73

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Net-Centric Attributes (From JNO, 2007) 19
Table 2. Operational Architecture Matrix for SFSS 74

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARPA	Advanced Research Projects Agency
AI	Artificial Intelligence
CBA	Capabilities Based Assessment
CIO	Chief Information Officer
CIE	Collaborative Information Environment
C2	Command and Control
CIR	Computing Infrastructure Readiness
COI	Communities of Interest
COI	Contact of Interest
COP	Common Operational Picture
CR	Communications Readiness
DIPR	Detect Identify Predict React
DoD	Department of Defense
DSD	Data and Services Deployment
DAI	Distributed Artificial Intelligence
EBO	Effects-Based Operations
FAA	Functional Area Analysis
FOB	Forward Operating Base
GIG	Global Information Grid
GPS	Global Positioning System
GWOT	Global War on Terrorism
IED	Improvised Explosive Device
IDEF0	Integrated Definition for Function Modeling
ISA	Intelligent Software Agent
JCA	Joint Capability Area
JFDID	Joint Force Development and Integration Division
JFC	Joint Functional Concept
JNO	Joint Net-Centric Operations
INCOSE	International Council on Systems Engineering
MAS	Multi-Agent System

NCE	Net-Centric Environment
NCOE	Net-Centric Operational Environment
NCOW	Net-Centric Operations and Warfare
NCO	Network-Centric Operations
NCSE	Network-Centric Systems Engineering
NCW	Network-Centric Warfare
NOA	NetOps Agility
NOC	Network Operations Center
OI	Object of Interest
OIF	Operation Iraqi Freedom
OV	Operational View
RF	Radio Frequency
RM	Reference Model
SFSS	Smart FOB Surveillance System
SOA	Service-Oriented Architecture
SoS	System of Systems
SI	Swarm Intelligence
TPPU	Task, Post, Process, and Use
UAV	Unmanned Aerial Vehicle

EXECUTIVE SUMMARY

Forward Operating Bases (FOBs) are vulnerable to terrorist attacks and intelligence gathering by terrorists. Current methods of surveillance are manpower intensive and are unnecessarily dangerous to those performing these functions. FOBs must be provided with an effective surveillance system that can continuously monitor threat activity.

The purpose of this thesis is to advise systems engineers in uniting Swarm intelligence and Multi-Agent intelligent systems in a Detect, Identify, Predict, React (DIPR) infrastructure to further enable our Network-Centric capabilities. Additionally, this thesis will present a systems engineering approach to the design of a Smart FOB Surveillance System (SFSS) with emphasis on a Network-Centric System application. This research will aid in the future unmanned systems and cyber world, where a paradigm shift is required toward intelligence automation.

Future Network-Centric Warfare will be accomplished via unmanned systems, whether unmanned airborne, small satellites, unmanned carriers, unmanned ground systems, etc. With this paradigm shift, intelligence automation is a necessity to autonomously control these systems. In addition, the sensor data acquired from these systems, or any sensor network, must be analyzed through intelligence automation software, as opposed to intelligence automation analysts. There will never be enough facilities, humans, and bandwidth to handle the vast amount of data these unmanned systems will produce (Goshorn, Goshorn, Goshorn, & Goshorn, 2011). This thesis proposes to develop a Network-Centric Systems Engineering Solution, for intelligence automation, through applying the systems engineering process to design a Smart FOB Surveillance System (SFSS).

The use of a multi-agent behavior analysis and decision system, with swarm intelligence through a network-centric systems engineering method of development, will create a robust and highly intelligent surveillance system. The system provides the capability of an automated and autonomous means of continuously monitoring areas for certain behaviors, linking individuals, predicting future behaviors, and taking appropriate

action against them to eliminate threats and the possibility of future threats. Environments, such as insurgent urban areas, Forward Operating Bases, country borders, and other high-value target areas all require constant personnel behavior surveillance and monitoring.

The system utilizes a complex network of aerial, fixed and mobile terrestrial units, capable of identifying and processing audible, visual, and signal intelligence in order to determine personnel behavior in a given area of interest, as well as recording and processing intelligence data. The focus is on creating a system to protect Forward Operating Bases (FOBs) by providing continuous and autonomous surveillance and threat alerts. In this thesis a Smart FOB Surveillance System (SFSS) will be developed using the systems engineering process.

Figure 1 is the Operational View of the Smart FOB Surveillance System (SFSS). There are three main signals that the system is intended to detect: visual signals, audible signals, and RF signals. The video data is taken by both the mobile UAV platforms that patrol the vicinity of the Forward Operating Base (FOB) and the fixed sensors located along the perimeter of the FOB. The video is analyzed for facial recognition to alert the Network Operations Center (NOC) operator, who is stationed within the FOB, of known threats based on local and remote database comparisons. Video is further analyzed by behavior recognition software. Behaviors deemed potential threatening such as unknown personnel approaching the FOB, persons in prone positions, and others will result in alerting the NOC operator for further disposition. Fixed sensors located along the perimeter of the FOB detect audio near the perimeter of the FOB. The audio received is sent to the NOC, within the FOB, for threat criteria evaluation. To meet a threat criterion, the audio received is evaluated by the NOC against audible threat profiles. The intent is to primarily detect gunfire and explosions. The audio source can also be located through simple triangulation based on the audio signal, received at the various audio sensors. Finally, radio frequency (RF) is detected by fixed sensors located along the perimeter of the FOB. The RF signal will be analyzed by three methods. First, the source of the RF signal can be determined by triangulation based on the RF signal received at various location sensors. Secondly, the RF signal will be compared to a database of threat

profiles. The intent is to detect jamming attempts, electronically guided munitions, electronically actuated Improvised Explosive Devices (IED), and finally, in the case of RF communications, to intercept the voice transmissions for recording and evaluation by the NOC operator.

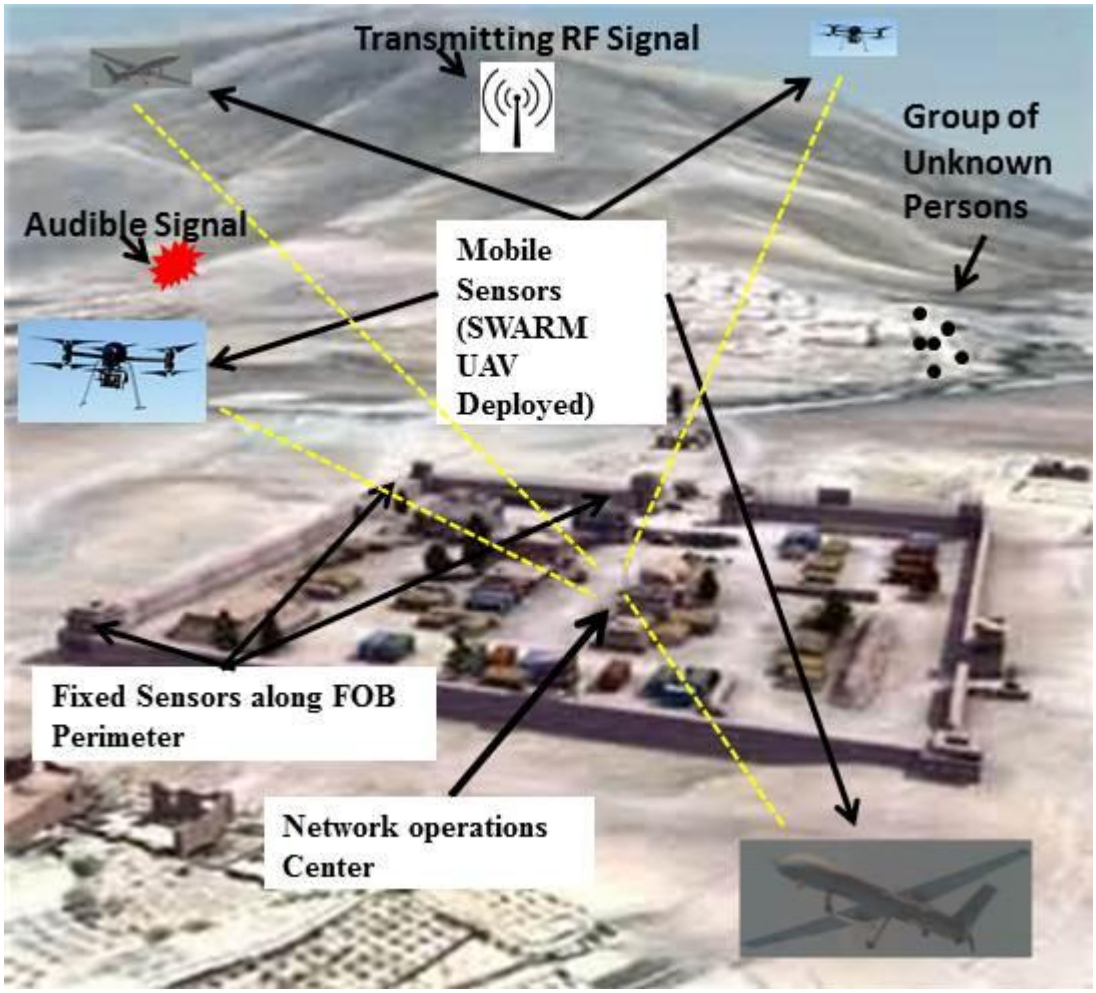

Figure 1. System Operational View of the SFSS.

In any event where the Smart FOB Surveillance System (SFSS) generates an alert, the FOB will initiate defensive protocols to mitigate the risk of the threat and the NOC operator will be required to resolve the condition causing the alert. In addition, the FOBs headquarters will automatically be notified of the potential threat in order to provide assistance and to establish situational reporting with the operational chain of command and the global intelligence community.

This thesis provides a background on multi-agent systems, DIPR systems, Swarm Intelligence, automated intelligence, and the network-centric systems engineering approach to system design. With the background for the technologies encompassed in the system established, the thesis will then present a systems engineering approach to the design of a Smart FOB Surveillance System (SFSS) beginning with the operational requirements, operational concept and scenarios, external systems design, system requirements, then culminating in a complete design through the functional architecture hierarchy, functional architecture decomposition, and physical architecture hierarchy.

LIST OF REFERENCES

Goshorn, R. E., Goshorn, D. E., Goshorn, J. L., & Goshorn, L. A. (May 2011). "The Need for Distributed Intelligence Automation Implemented through Four Overlapping Approaches: Intelligence Automation Software, Standardization for Interoperability, Network-Centric System of Systems Infrastructure (with Advanced Cloud Computing) and Advanced Sensors," GMU–AFCEA Symposium.

ACKNOWLEDGMENTS

The author wishes to thank Professors Rachel Goshorn and Deborah Goshorn for their guidance during the writing of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

Future Network-Centric Warfare will be accomplished via unmanned systems, whether unmanned airborne, small satellites, unmanned carriers, unmanned ground systems, etc. With this paradigm shift, intelligence automation is a necessity to autonomously control these systems. In addition, the sensor data acquired from these systems, or any sensor network, must be analyzed through intelligence automation software, as opposed to intelligence automation analysts. There will never be enough facilities, humans, and bandwidth to handle the vast amount of data these unmanned systems will produce (Goshorn, Goshorn, & Goshorn, 2011). This thesis proposes to develop a Network-Centric Systems Engineering Solution, for intelligence automation, through applying the systems engineering process to design a Smart FOB Surveillance System (SFSS).

B. PURPOSE

The purpose of this thesis is to provide a systems engineering approach to systems engineers, through uniting Swarm intelligence and Multi-Agent intelligent systems in a Detect, Identify, Predict, React (DIPR) infrastructure, to further enable our Network-Centric Capabilities (Goshorn, Goshorn, & Goshorn, 2009). Additionally, this thesis will present a systems engineering solution to the design of a Smart FOB Surveillance System (SFSS) with emphasis on a Network-Centric System application. This will aid in the future unmanned systems and cyber applications, where a shift is required toward intelligence automation.

C. QUESTIONS RESEARCHED

1. How can Swarm technology be paired with a Multi-Agent Behavior Analysis and Decision System through a Network-Centric Systems Engineering Approach?
2. What is Swarm Intelligence (SI)?

3. What is a Multi-Agent System (MAS)?
4. What is behavior modeling for Detection, Identification, Prediction, and Reaction (DIPR) in AI Systems?
5. What is Network-Centric Systems Engineering (NCSE)?
6. How can Swarm Intelligence be used to implement a Multi-Agent DIPR AI System?
7. What NCSE solution would best illustrate proof of concept for a Multi-Agent Behavior Analysis and Decision System with Swarm Intelligence?
8. What are the systems engineering architectures for the NCSE solution?
9. What is the systems engineering solution for a Smart FOB Surveillance System (SFSS)?
10. What is the Operational Concept for Smart FOB Surveillance System (SFSS)?
11. What is the Operational View (OV-1) for Smart FOB Surveillance System (SFSS)?
12. What are the operational scenarios for the Smart FOB Surveillance System (SFSS)?
13. What are the external systems for the Smart FOB Surveillance System (SFSS)?
14. What are the system requirements for the Smart FOB Surveillance System (SFSS)?
15. What is the Functional Architecture for Smart FOB Surveillance System (SFSS)?
16. What is the Physical Architecture for Smart FOB Surveillance System (SFSS)?

D. OVERVIEW

A highly automated system that is designed to provide continuous surveillance for a FOB must be very adaptable and scalable. FOB environments in terms of the local populace, terrain, and surrounding threats vary widely. Therefore, the system should be intuitively tailored to match the needs of the FOB it serves. The application of swarm intelligence (SI) is a possible solution for built-in adaptability and scalability without the need for each SFSS to be independently designed for each individual FOB. Swarm intelligence (SI) is based on the interactions of animal colonies found in nature. Some colonies are found to behave as a collective group in the performance of a task instead of

a large number of individuals reacting independently. An individual, in this discussion, is one that only reacts to its environment; decisions and actions by an individual are carried out independently of the actions of other individuals (Bonabeau, Dorigo, & Theraulaz, 1999). In order to accomplish this, the individuals interact with their environment as well as all other individuals that comprise the group in order to determine their own behavior in terms of the performance of tasks. SI is a specialized application of artificial intelligence (AI) (Ferby, 1999). In general, all types of AI systems react to the environment and choose an appropriate response or action based on the program application. The difference with SI is that instead of single AI agents acting independently, it acts collectively within the group for a common goal. In an AI environment, this can result in a substantial improvement in a systems performance and efficiency. Instead of directing each agent directly, the entire swarm can be directed and then able to self-organize to better accomplish its mission (Bonabeau et al., 1999).

Recent Artificial Intelligence (AI) research has shown that intelligent software systems are the future in the design and development of next generation computing. Intelligent Software Agents (ISAs) are complex computer programs that on their own accord that do not require operator input to carry out their functions on the way to accomplishing a task. More frequently, applications of this technology require that multiple agents work together in a system. The result is the creation of an advanced multi-agent system (MAS) comprised of a collection of interfacing ISAs that perform at a much greater level than capabilities of their single agents. ISAs that are interfacing with their environment as well as each other are the foundation of SI. This form of distributed AI allows for maximum adaptability, redundancy, and scalability (Ferby, 1999).

In the future, Network-Centric Command and Control Systems will rely heavily on the use multi-networked ISAs and MASs. The standard for the future development of U.S military based network-centric systems is the Net-centric Operations and Warfare Reference Model (NCOW RM) (DoDAF, 2007). The purpose of this model is to create net-centric systems that provide information dominance in that they link all users to receive and provide data on demand at any location and in any environment. There are four basic capabilities that such systems will have: Artificial Intelligence, automated or

semi-automated resource management, business enterprise services, and user interface. To satisfy the requirements of the Net-Centric Operations and Warfare Reference Model (NCOW RM), the use of ISAs and MSAs will be a necessity (DoDAF, 2007).

To further enable these systems, decision-making must move from an operator function to an automated function. The ability of AI systems to mimic human decision-making has been modeled in the Detection, Identification, Prediction, and Reaction (DIPR) process (Goshorn et al., 2011). Analogous to a human operator, information is received from the environment, then it is identified or classified, then analyzed to predict future actions based on what has already occurred, and finally acted upon. In the detection phase, various sensors provide input into the system, where raw data is initially processed by feature extraction algorithms (Goshorn et al., 2011). The identification subsystem carries out fusion of the features into an intelligent symbol. Prediction occurs in the following subsystem by analyzing the sequence of intelligence symbols, representing a behavior over time and space, identified in the environment. These predictions then solicit reactions based on predefined parameters; reactions could be automated "rules of engagement" or recommended reactions (Goshorn et al., 2011).

In a net-centric system, users and local applications depend upon common services for functionality and data. This type of system provides an information architecture that comprises communication, processing, and data exchange that can be used by a vast array of platforms. Engineering of this type of system will require that these systems be more centered on data-sharing versus application-sharing, which is currently more commonly used. A data centered architect will require an interface link between users as well as uniform input and output formatting to ensure compatibility. This net-centric systems approach results in a system capable of providing data to and from any station at any time automatically.

There have been numerous frameworks, approaches, and methodologies for modeling and developing Multi-Agent intelligent systems and swarm intelligence. This thesis will focus on how a net-centric systems engineering approach can produce a superior union between Swarm intelligence and Multi-Agent intelligent systems in a

DIPR infrastructure. Models, architectures, and design and implementation of a proposed proof of concept tactical system will be discussed.

Overall, this thesis will apply the systems engineering process to propose a systems solution through development of an operational concept and scenarios, external systems diagram, requirements, functional architecture, physical architecture, and operational architecture.

E. APPLICATION

A Swarm-based Multi-Agent Behavior Analysis and Decision System could provide a platform for civil, government, and military environments, which require constant surveillance in order to mitigate the threat of attacks of various types; most notably from within the civilian indigenous population who do not normally stand out as a recognizable threat. Such a system could provide a means of performing the task of constant monitoring in these environments to observe the numerous personnel, which may transit an area. The SFSS has the ability to identify behaviors classified as "Abnormal" for the purposes of detecting potential threat behavior. Simple human monitoring of audio, visual, or other media-based systems is severely limited in extended duration and capability, due to finite human useful attention span and identification of behaviors. However, the SFSS can perform these functions autonomously, indefinitely, and accurately.

By providing a networked system of automated "smart" sensors, the system can continuously monitor areas for certain behaviors and alert authorities to react to those behaviors in order to interdict the threat. With this type of system, the manpower required would be significantly reduced; additionally, potential friendly casualties will be reduced that could have resulted from the mission execution through man-power (not smart systems). This thesis research will focus on the use of this system in a Forward Operating Base (FOB); although this system can be used in any number of civil or military applications such as government installations, military bases, buildings, and other potential targets considered as high-value to an enemy, where the capability of constant personnel behavior surveillance and monitoring would be advantageous.

Integrating Swarm Intelligence (SI) into a Multi-agent Analysis and Decision System would further improve the degree of autonomy inherent in the SFSS Current efforts have focused on the capability to locate, classify, and track a Contact of Interest (COI); then identify "Abnormal" behaviors, out of many other so-called "Normal" behaviors, discern which of the abnormal behaviors could be classified as posing a threat, and then notify the appropriate personnel via various means (visual, electronic, audio, etc.) to react to the threat. However, the capability of a system- or operator-initiated reaction for obtaining additional information required for a specific COI does not exist. That is, a single command whether initiated by the system or its operator, only results in the action commanded. Integrating Swarm Intelligence (SI) into a Multi-agent Analysis and Decision System could result in a single command carrying out a series of commands aimed at following an event to resolution. Similarly, the legacy systems and approaches are incapable of reacting to other organic assets within the network in order to improve mission effectiveness. This thesis proposes a solution to this problem. The problem definition is discussed next.

F. PROBLEM DEFINITION

Currently, there are numerous environments in the civil, government and military spheres that require constant surveillance in order to mitigate the threat of attack from threats of various types; threats are mostly from the civilian indigenous population who do not normally standout as a recognizable threat (Woo, 2009). The task of monitoring these environments, to observe the numerous personnel that may transit an area, and have the ability to identify certain behaviors that would classify as abnormal, for the purposes of detecting potential threat behavior, is not possible using conventional humanized techniques. Simple human monitoring of audio, visual, or other media-based systems is severely limited in extended duration and capability, due to finite human attention span, identification of behaviors, and limited memory. Additionally, it is extremely dangerous for humans to carry out the monitoring by foot around bases.

To protect our vital national interests, high-value assets at sea and ashore must be protected, and are therefore often nested within a network of internal and external,

organic and inorganic sensors. This arrangement provides a Common Operational Picture (COP) around the high-value units. These types of sensor networks increasingly have the ability to fuse some of the sensors' data flooding in to detect, track, and, to a certain extent, classify the surface vessels in the vicinity of these units. Currently, humans in the loop of these sensor networks monitor the contact tracks of these vessels; however, their dense number and irregular, indiscernible, and unpredictable movements prevent an early and/or accurate detection of threat-like activity by the many contacts that must be monitored in the COP. Automation of these vital, yet mundane, monitoring and threat-detection activities could potentially greatly enhance the awareness for the protection of friendly forces.

G. PROPOSED SOLUTION

A Smart FOB Surveillance System (SFSS) could give us the capability of an automated and autonomous method for continuously monitoring areas for certain behaviors, linking individuals, predicting future behaviors, and taking appropriate action against them to eliminate threats and the possibility of future threats. Environments, such as insurgent urban areas, Forward Operating Bases, and other high-value target areas all require constant personnel behavior surveillance and monitoring. A complex network of aerial, fixed and mobile terrestrial units capable of identifying and processing audible, visual, and signal intelligence in order to determine personnel behavior in a given area of interest would fill the capability gap identified.

This thesis will develop the following Systems Engineering products: Operational concept, operational scenarios, external systems diagram, requirements, functional architecture hierarchy, functional architecture decomposition using IEDF0, physical architecture hierarchy, and operational architecture…

This chapter provided an overview of the technology required to solve the problem presented and provided an introduction to a Multi-Agent Behavior Analysis and DIPR System with Swarm Intelligence. The next chapter will provide a literature survey for the background and provide a discussion on Network- Centric Systems Engineering methods, including how NCSE differs from traditional Systems Engineering and

Software Engineering, and it will discuss the NCSE methodologies and selection of desired methodology.

H. THESIS ORGANIZATION

This thesis is organized as follows:

1. Chapter I Introduction: This chapter will include the overview, questions researched and the thesis outline to include: Problem to Solve, Application, Motivation, and Proposed Solution for a Multi-Agent Behavior Analysis and DIPR System with Swarm Intelligence.
2. Chapter II Network-Centric Systems Engineering Approach: This chapter will provide a literature survey for the background and provide a discussion on Network-Centric Systems Engineering methods, including how NCSE differs from traditional Systems Engineering and Software Engineering.
3. Chapter III Application Of The Systems Engineering Process: This chapter will also discuss the Systems Engineering "V" model used in the development of the functional architecture from the system level design requirements to the completed system. Finally, it will discuss the NCSE methodologies and selection of desired methodology.
4. Chapter IV Swarm Intelligence and Multi-Agent Systems: This chapter will provide a background for swarm intelligence and multi-agent systems. The chapter will also discuss the need for Intelligence Automation (IA), the Detect, Identify, Predict and React (DIPR) method, and distributed Artificial Intelligence (AI), which is a form of DIPR.
5. Chapter V System Engineering Solution for a Smart FOB Surveillance System (SFSS): This chapter will focus on the development of the Smart FOB Surveillance System (SFSS) by using the left side of the Systems Engineering Vee model. Beginning with the operational need an operational concept will be identified. This will trace into the various operationals scenarios that will be used to bound and scope the SFSS system design. From there, further Systems Engineering products, of the

SFSS, will be developed. This begins with the formation of the External Systems Diagram and flows into the requirements of the system. Finally, the functional, physical, and operational architectures are developed.

6. Chapter VI Summary and Conclusion: This chapter will summarize the proposed systems solution of a Smart FOB Surveillance System (SFSS) and draw conclusions from the research performed. Additionally, future research recommendations to continue the proposed systems solution, are presented.

THIS PAGE INTENTIONALLY LEFT BLANK

II. NETWORK-CENTRIC SYSTEMS ENGINEERING APPROACH

A. OVERVIEW

Understanding of Network-centric systems is fundamental to the solution required in this thesis. Taking the network-centric systems engineering approach in the development of a solution will aid in defining the architecture vision, capabilities and attributes, warfare and operations, and engineering network-centric systems using agent-based technology.

The Joint Force Development and Integration Division defines the network-centric capability as the ability to create an infrastructure that allows for the interaction of users and systems while providing data and information exchange freely and in a protected environment. Network-centric capability provides users with the information needed, when needed, and in a format that is coherent and useful (JCCD, 2011). There are three key elements that comprise a network-centric system that in order to provide service-based information sharing and processing (NESI, 2009): 1) be functional to the user by providing intelligence based processing of information, 2) be completely interoperable with other systems and platforms, and 3) carry out its network operations independently (NESI, 2009).

In order to engineer and implement these types of interconnected complex systems it is important to understand the following topics discussed later in this chapter in terms of their net-centric applications:

- Architecture
- Capabilities and Attributes
- Warfare and Operations
- Engineering through Agents

B. NETWORK-CENTRIC SYSTEMS

This section discusses relationship between network-centric systems and network-centric systems engineering. The section delves into the various network-centric systems

engineering types such as top-down systems, bottom-up systems, middle systems, and side view systems; to include the differing information flows and under what circumstances one may be used of another.

1. Network-centric Systems

A network-centric system is the collaboration of humans and computers (hardware and software) in the performance of a task or function within a network environment. Network centric systems function in a human and computer framework to provide a more efficient use of resources while acting to synchronize actions necessary to accomplish a mission. The term "network-centric" implies that the system contains the attributes and can perform the capabilities discussed here in the following sections.

2. What is Network-centric Systems Engineering?

Network-Centric Systems Engineering (NCSE) is simply the design and development of a system created to operate in network-centric environments. This environment may be a local intranet or wide area network. The primary concern is whether the system enables discovery and access to its information; can another system within that environment find and access information. To operate in a network-centric environment a system must contain the network-centric attributes and enable the network-centric capabilities described in this chapter.

The Network-centric Systems Core contains the basic fundamental components that any network or system of networks is built from; networks, communications, distributed computing and real-time processing. The major elements of network centric system engineering core evolved from three distinct functions: Communications (including an established network), real-time data processing, and distributed intelligent computing. There are four distinct but complementary NCSE systems: top-down, bottom-up, middle, and side view/disadvantaged users (Goshorn et al., 2011). Each system can be viewed as a system. Therefore, NCSE is a system of systems (SoS). These four overlapping systems are integrated by the NCSE Core and Four Systems seen in Figure 2.

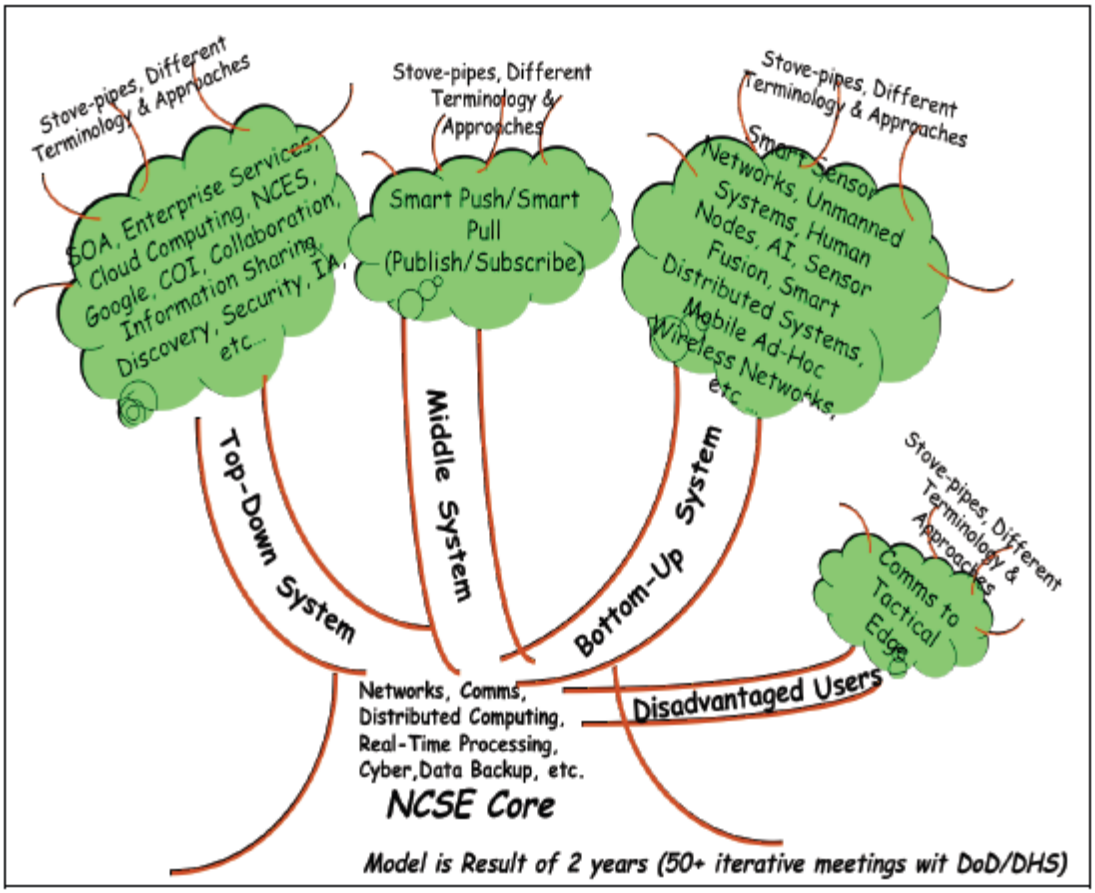

Figure 1. NCSE Core and Four Approaches Tree (From Goshorn et al., 2011)

a. Top-down System

The Top-down System describes the high-level functions and provides the boundaries of the requirements and capabilities of a system. Each major system is broken down individually into subsystems until the most basic low-level requirements of the system are defined. The Top-down system focuses on how the system will share information. The way information is shared will depend by the design of the service oriented architecture (SOA), enterprise services, cloud computing, network capability, hardware/software employed, and user familiarity. The top-down system represents the collaboration environment, with the highest level of intelligence, that pertains to the users mission. In the top-down system the flow of information begins at the bottom and is pulled up (Goshorn et al., 2011).

b. Bottom-up System

The emphasis of the Bottom-up System is on the actual elements of the network-centric system and the requirements and capabilities it provides to the warfighter. This systems represents the origination of data; whether from a sensor, manned or unmanned system, or human, etc. This system relies on the use distributed smart systems, which is done in part by the use of smart sensors. The bottom-up system collects and pushes data to a common location by the detection agents and software employed. The bottom-up system relies heavily on distributed intelligent systems and smart sensors. The goal is to provide processed data in the form that the user understands automatically to any location in the network (Goshorn et al., 2011).

c. Middle System

The Middle System fuses the top-down and bottom up views. Within this system is the data domain that uses the smart push/publish (top-down system) and smart pull/subscribe (bottom-up system). "Smart" refers to the Artificial Intelligence (AI) used in this system to automate the push or pull of data. Smart systems are those enabled with AI decision support to perform the analyses typically performed by an operator. The goal of the middle system is to funnel data into a repository using a bottom-up system, and then retrieve the data from a top-down-system. This middle system is the world of "smart distributed clouds." Distributed clouds will need to receive the information from the bottom-up system, store and process the data, and allow for top-down systems to pull from these smart clouds. This is done without prompting by the user (Brandon, 2009).

d. Side View (Disadvantaged User) System

The Side View, or Disadvantaged User, system examines how communications is provided to and from a user that has disadvantaged communications; also known as a user at the tactical edge. A disadvantaged user could be have network connectivity, interoperable communications, incompatible security, stealth communications by choice). A user may have limited network connectivity due to their operating environment, mission, platform, or security posture. By definition these users

are coined “disadvantaged users.” The success of a units mission relies heavily on their ability to communicate on a tactical network. The side view system focuses on the disadvantaged user in order to fill the resource gap (Brandon, 2009). A network-centric system must incorporate the disadvantaged users into the system design; it often becomes a create communications design problem to interoperate with disadvantaged users.

This section described the four NCSE systems, from a system of systems view. The next section discusses the DoD Network-centric Architecture Vision.

C. NETWORK-CENTRIC ARCHITECTURE

The DoD Information Enterprise Architecture (DIEA) describes the goal of Network-centric Operations (NCO) and the priorities required in order to remove significant obstacles that must be overcome. The architecture outlined brings the DoD closer to realizing true Network-centric Operations (NCO). The DoD network-centric transformation is realized by setting priorities to focus on fundamental requirements. Five priorities are identified as areas of attention and investment to achieve network-centric based information sharing; NetOps Agility, Data and Services Deployment, Computing Infrastructure Readiness, Communications Readiness, and Secured Availability (DoD CIO, 2007). These priorities are briefly described in this section to understand the foundation for the network-centric capabilities and attributes.

1. NetOps Agility

NetOps Agility (NOA) allows the user access to information on demand from any node along a network. The user can also process, share, send or receive information in a secure computing environment. The operation and management of the GIG is set by NOA policy and protocols (DoD CIO, 2007).

2. Data and Services Deployment

Data and Services Deployment (DSD) removes the link between applications and the data and services they provide. This idea is based in part from moving from application-centered networks to information-centered networks to provide more accessibility. The goal of net-centricity is to remove the information stovepipes and

increase decision-making agility and speed to enable users to access information regardless of time or place (DoD CIO, 2007).

3. Computing Infrastructure Readiness

Computing Infrastructure Readiness (CIR) provides a common framework to ensure interoperability among DoD networks. This allows for the necessary processing and storage required of these networks. Computing Infrastructure Readiness (CIR) also ensures that data flow along networks can be controlled efficiently for the most efficient through-put (DoD CIO, 2007).

4. Communications Readiness

Communications Readiness (CR) provides the framework for uninterrupted communications throughout the Global Information Grid (GIG). This includes ensuring that the infrastructure is capable of handling the necessary bandwidth and information flow between all users on the GIG (DoD CIO, 2007).

5. Secured Availability

Secured Availability (SA) provides the needed security on the network. It allows users to access the network at any location and ensures that data received or sent has not been compromised.

In this section, the DoD Information Enterprise Architecture and priorities to enable network-centric information sharing were discussed; the next section will discuss the capabilities and attributes of network-centric systems (DoD CIO, 2007).

D. CAPABILITIES AND ATTRIBUTES

The DoD Office of the Chief Information Officer (CIO) vision is to create a tactical military advantage by information dominance for us and our partners. This requires two fundamental elements (DoD CIO, 2003):

- Creation of an infrastructure where data is shared, available and trusted throughout the Collaborative Information Environment (CIE).

- Creation of an agile Global Information Grid (GIG) that is information centered and operates seamlessly with all users across the enterprise.

This vision is accomplished through the establishment of official capabilities and attributes for DoD network-centric systems. This section identifies the capabilities and attributes of network-centric systems.

1. Network-centric Capabilities

In an ideal network-centric environment, agents whether human or computer, can better protect assets by more effectively processing information and more efficiently utilizing resources. This will streamline the efforts of our forces and improve mission accomplishment. (NESI, 2007).

Robust network-centric capabilities ensure an information advantage and gives our war fighting commanders a more clear picture of the battle space, which results in better decision making. Our joint forces and allies require access to relevant and accurate information in real-time. In parallel, they must be able to share battle space information securely in order to make the most informed decisions in an environment flooded with unprecedented quantities of operational data (DoD CIO, 2007). The Joint Net-Centric Operations (JNO) Tier 1 Joint Capability Area (JCA) is described as the ability exploit all components in a battle space, both human and technological, by the unit and their allies by creating a rich information environment that is secure and dynamic in any operational environment (JNO, 2007). Figure 3 is the JNO Tier 2 Capability Areas and is broken down into five key elements:

- *Network Management*: The ability to install and deploy the network in any environment and to ensure the network is optimized to maintain all network functions and utilize available resources.
- *Knowledge Management*: The ability to share information and enable collaborative decision making in order to improve situational awareness. It also discusses the ability to create organizational hierarchies.
- *Information Transport*: The ability of the network infrastructure to provide secure and continuous communications from anywhere to anywhere.

- *Enterprise Services*: The ability to identify, process, store, and share data and information.
- *Information Assurance*: The ability to defend the network from attack to maintain security and continuity. It also outlines the ability to create and produce information in a smart environment.

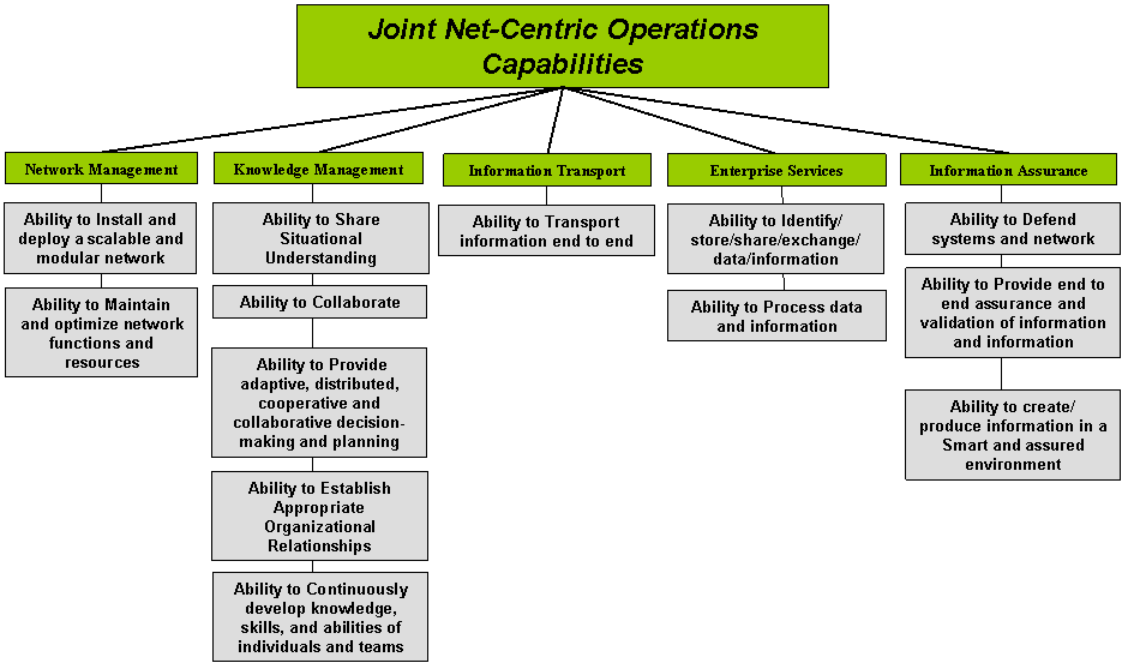

Figure 2. JNO Tier 2 Capability Areas ((From JNO, 2007)

2. Network-centric Attributes

The Network-centric concept of operations, enabled by information superiority, improves war-fighting ability by linking sensor information to the decision makers directly. This connectivity between warfighters creates a clearly defined battle space that improves awareness and reaction time. This contributes to improved joint force survivability, lethality, and overall effectiveness (DoD CIO, 2003). To enable NCO, a system must possess certain attributes to ensure the required net-centric capabilities can be provided to the warfighters.

The nine official net-centric attributes are seen in Table 1 (JNO, 2007):

Net Centric : Attributes	
Attribute	**Description**
Internet & World Wide Web Like	Adapting Internet & World Wide Web constructs & standards with enhancements for mobility, surety, and military unique features (e.g. precedence, preemption) .
Secure & available information transport	Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service.
Information/Data Protection & Surety (built-in trust)	Producer/Publisher marks the info/data for classification and handling; and provides provisions for assuring authenticity, integrity, and non-repudiation.
Post in parallel	Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g. raw, analyzed, archived).
Smart pull (vice smart push)	Users can find and pull directly, subscribe or use value added services (e.g. discovery). User Defined Operational Picture vice Common Operational Picture.
Information/Data centric	Information/Data separate from applications and services. Minimize need for special or proprietary software.
Shared Applications & Services	Users can pull multiple applications to access same data or choose same apps when they need to collaborate. Applications on "desktop" or as a service.
Trusted & Tailored Access	Access to the information transport, info/data, applications & services linked to user's role, identity & technical capability.
Quality of Transport service	Tailored for information form: voice, still imagery, video/moving imagery, data, and collaboration.

Table 1. Net-Centric Attributes (From JNO, 2007)

In this section, the capabilities and attributes of network-centric systems were discussed; the next section will introduce Network-centric Operations and Warfare.

E. WARFARE AND OPERATIONS

1. Network-centric Warfare

Network-centric Warfare (NCW) is the attempt to by the DoD to exploit the use of network based information systems in the current modern environment. The mission is also to enhance our war fighting capabilities by improving our network capabilities while

denying their use by others. The focus of NCW is on the behavior of humans in the networked environment. The hypothesis of the NCW theory is that force structure and protocols linked in a networked environment is more capable than forces that do not use net-centric information exchange (DoD, 2005).

NCW leverages an information advantage to create a decisive war fighting advantage created by a complex network of tactical commanders apprised of the battle space in order to share information and improve awareness. When commanders share tactical awareness through net-centric information exchange they gain an advantage over the opposing force. This war-fighting strategy is supported by net-centric based systems, but is only made successful when used collectively and at the same time (DoD, 2005).

Successful implementation of the NCW theory demands recognition of the four domains of warfare in which conflict takes place: physical, information, cognitive, and social. The interactions between these domains of conflict are illustrated in Figure 4. A brief description of the four domains from (DoD, 2005) is given below.

1. *Physical Domain*: The physical domain is the traditional domain where troops physically exist. Elements in this domain can be measured comparatively easier than other domains.

2. *Information Domain*: This is the area where information is received and processed. Communication, or information exchange, among commanders occurs here. This domain also encompasses methods of information gathering such as sensors, information that is shared, and the infrastructure that allows for sharing.

3. *Cognitive Domain*: The cognitive domain is in the mind of the warfighter where decisive battle space concepts and tactics emerge.

4. *Social Domain*: The social domain describes human interactions, understanding, awareness, and decision-making.

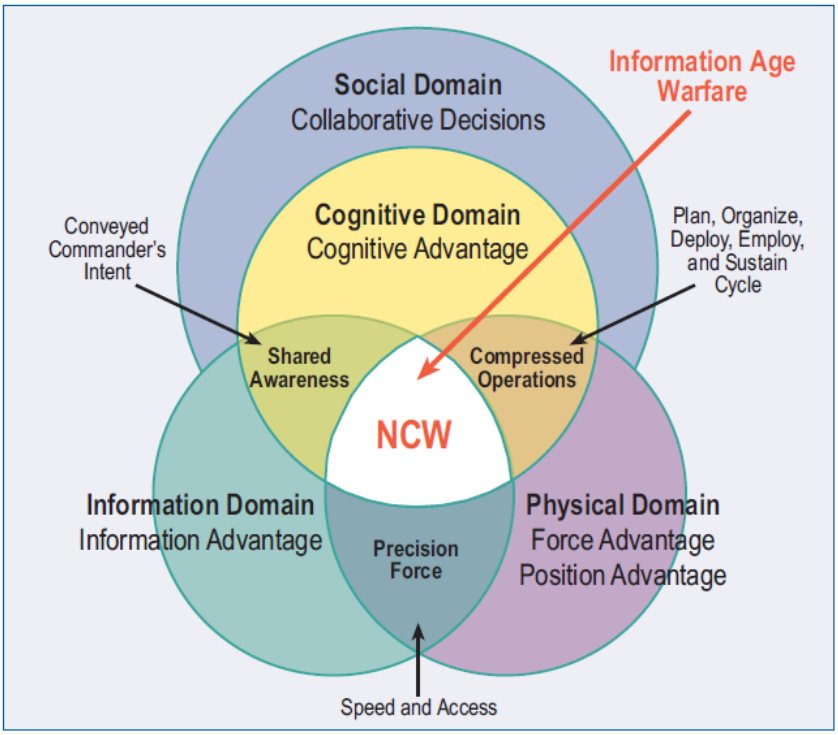

Figure 3. Information Age Warfare Domains of Conflict (From DoD, 2005)

The concepts of NCW help to explain how this theory provides enhanced power of networked forces and the associated source of war fighting advantage. These four tenets of NCW as defined in (DoD, 2005) are:

1. Net-centric communications improves the ability to share information.

2. When information is shared, the collective situational awareness is improved.

3. Collective situational awareness improvement results in a faster reactions and improved cooperative efforts.

4. Faster and improved cooperative actions result in greater capabilities.

The four basic tenets of NCW represent a realization of this new theory of war as a source of transforming an information advantage into a combat advantage. Figure 5 shows how the tenets of NCW may be applied to the warfare domains.

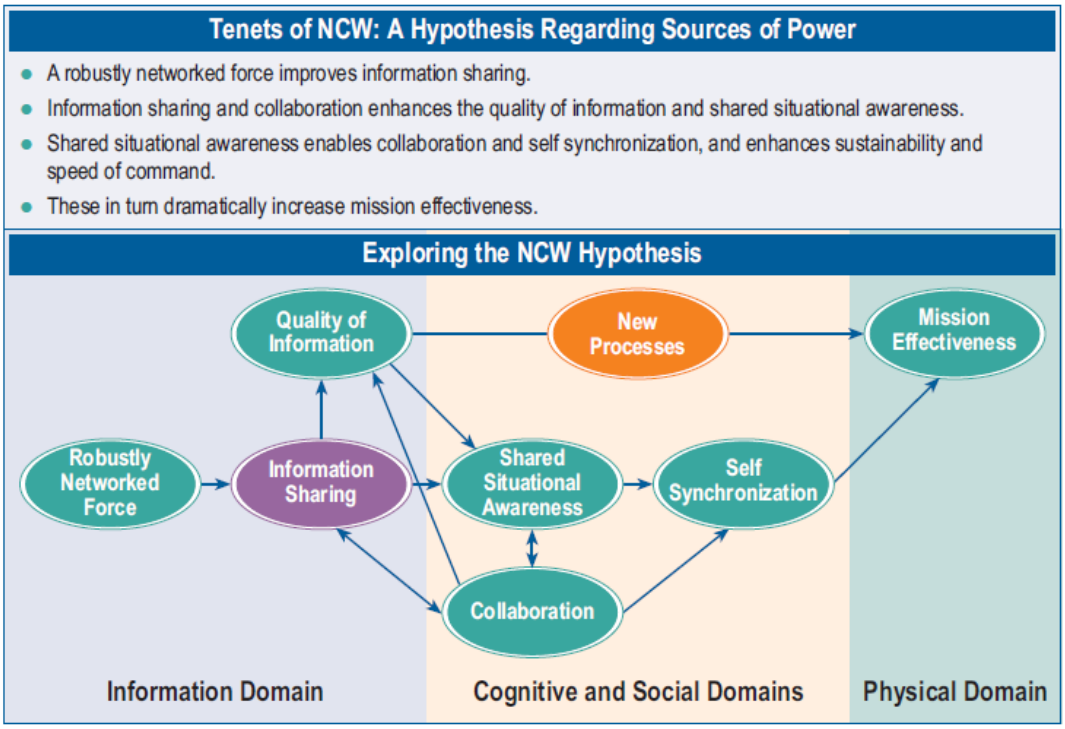

Figure 4. Tenets of NCW within the Warfare Domains (From DoD, 2005)

The requirements of a net-centric joint force are illustrated in terms of the individual domains in which their most basic requirements lie. This in turn describes how they operate, function, and are integrated as a single unit (DoD, 2005). The requirements are defined as follows:

- *Physical Domain*:
  - Networking of all elements; achieving secure and seamless connectivity.
- *Information Domain*:
  - Receive and share information.
  - Process information to improve awareness.
- *Cognitive/Social Domains*:
  - Improve collective situational awareness.
  - Collaboration of efforts

The fundamental idea to support the sources of power hypothesis of the NCW theory of war is that if the following three requirements are met, then the joint force will be capable of greater effectiveness in combat (DoD, 2001):

- Improved collaboration in mission execution.
- Improving responsiveness to the battle space environment.
- Improving combat survivability and lethality.

2. Network-centric Operations

Network-centric Operations (NCO) is the application of NCW theory. Simply, NCW is the theory; NCO is the theory in action. NCO is the implementation of the concepts of NCW: Improved collaboration, responsiveness, survivability, and lethality (DoD, 2005).

a. FBCB2 – Blue Force Tracker

The Blue Force Tracker monitors the location of vehicles and aircraft using Global Positioning System (GPS) transmitters. The location is then tracked to create awareness within the battles space by the sharing of information through satellite networks. Friendly fire has been reduced as a direct result of FBCB2 implementation (DoD, 2005).

b. Horizontal Fusion

Horizontal Fusion provides the warfighter the ability to pull information to them as they move using a "smart-pull" process, to provide near-real time situational awareness, sense making tools, collaboration, and critical intelligence information sharing. As a result, troops on the ground are better prepared to execute missions (DoD, 2005). It is horizontal in that information is received from a level in various domains that makes sense to the user. This information is received from the fusion of sensors and other gather methods in a net-centric environment (DoD, 2005).

c. Collaborative Information Environment

The Collaborative Information Environment (CIE) describes the infrastructure used to create the GIG. It encompasses the hardware and software that allows connectivity in information centered network. It is through this infrastructure that information sharing, collaboration, decision-making, and synchronization can occur.

F. ENGINEERING THROUGH AGENTS

Engineering through agents is an approach in which the network-centric capabilities and attributes identified are paired with available agent-based technologies. The following section discusses the use of agents to satisfy network-centric capabilities.

1. Network-centric Science and Technology

A host of information technologies provide capabilities needed to facilitate collaboration and information sharing. These technologies fall into the following categories: collection, exploitation, storage, retrieval, distribution, collaborative environments, presentation, Information Operations and Assurance, and the technologies that help extract knowledge and understanding from data and information. These knowledge-related technologies include a variety of analyses, modeling, simulation, problem solving, and other decision support tools (DoD, 2001). The implementation of NCW will require investment in technologies to facilitate the ability to enable the required capabilities to perform NCO. Some of these technologies include (DoD, 2001):

- Agile and maintainable networks.
- Information exchange.
- Seamless interoperability.
- Reliable Connectivity
- Information management and distribution.
- Information Assurance.

It is now possible to consider the relationship between these technologies and the network-centric capabilities and attributes previously presented. Analyzing these

technologies provides insight into to what types of components may be required to achieve these capabilities within a network-centric system.

Many of these technologies could best be implemented using agent-based systems. Agents are essentially the building blocks of AI. Distributed AI, Swarm Intelligence will be discussed in great detail in Chapter IV. Agent technology has been used for information integration, decision support and sensor data processing, as well as distributed collaboration and information management for rapid and accurate decision-making and predictive planning. These are potential areas where autonomous software agents and multi-agent systems could be utilized for the development of network-centric systems (Jennings & Wooldridge, 1995).

2. Agent-based Science and Technology

The Department of Defense cited that in order to reach the network-centric capabilities outlined research must be done in the following areas (DoD, 2001):

- Cooperative Processing/Decision Support Technology
  - − Information integration (fusion & correlation)
  - − Computer-aided reasoning
  - − Co-operative software agents
  - − Mediation agents
- Human-machine Interface
  - − Explanation agents
  - − Alerting and cueing agents
  - − Knowledge elicitation agents
  - − Input/output for a stressing environment
- Rapid, distributed modeling and simulation
  - − Robust stochastic algorithms and processes
  - − Automated learning
  - − Distributed intelligent agents

Applying these specific agent technologies listed to the network-centric capabilities and attributes previously identified demonstrates the types of agent-based

systems that could be employed within a network-centric system to achieve the required capabilities needed for these complex, interconnected systems.

In this chapter, an overview of what is meant by network-centric was presented; including the architecture vision, capabilities and attributes, warfare and operations, and engineering network-centric systems using agent-based technology. The next chapter will discuss the application of the systems engineering process.

III. THE SYSTEMS ENGINEERING PROCESS

This chapter will discuss the systems engineering process used to design and develop the systems engineering solution for the Smart Fob Surveillance System (SFSS), which includes identifying the operational need, concept, and scenarios as well as the development of the external systems diagram and requirements. From these systems engineering products the functional, physical, and operational architectures are developed.. These products will then be utilized to develop the proposed system solution. This chapter will discuss the Systems Engineering "V" model on a step-by-step system to provide the foundation of the system from design, which is then taken into the right-half of the "V" of fabrication, installation, and testing of the system. This thesis develops solutions corresponding to the left side of the "V," introduced in this chapter.

A. SYSTEMS ENGINEERING PROCESS

Systems engineering is an engineering approach that incorporates all other engineering disciplines in which design and implementation is based on the system as a whole (Maier and Rechtin, 2000). In order to maintain the required engineering discipline, a process must be utilized that details system requirements so that when implemented, the design meets the requirements of the system. The eventual goal, of this thesis, is to produce an actual system that fulfills the requirements of enhancing continuous monitoring of high-value targets previously discussed, while not eliminating much of the traditionally required personnel. The concept, external systems diagram, requirements, and functional architecture, physical architecture and operational architecute for such a system is provided in Chapter V. This chapter gives a background on these systems engineering products. After a brief analysis of alternatives, a specific solution will be proposed in Chapter V.

B. SYSTEMS ENGINEERING V-MODEL

This thesis will carry out the top left part of the systems engineering "V." The specific systems engineering products that will be developed are described next. Figure 6 illustrates the Forsberg and Mooz Systems Engineering Vee. The left side is the

decomposition and definition phase. It begins at the very top left with understanding the user requirements and developing the system concept and validation plan. In the next phase, which moves from the bottom to the top right, the system is developed and performance specifications are defined (Forsberg and Mooz, 1992). To reach these goals, several systems engineering products must be developed; they are explained generically in the next sections (Buede, 2000).

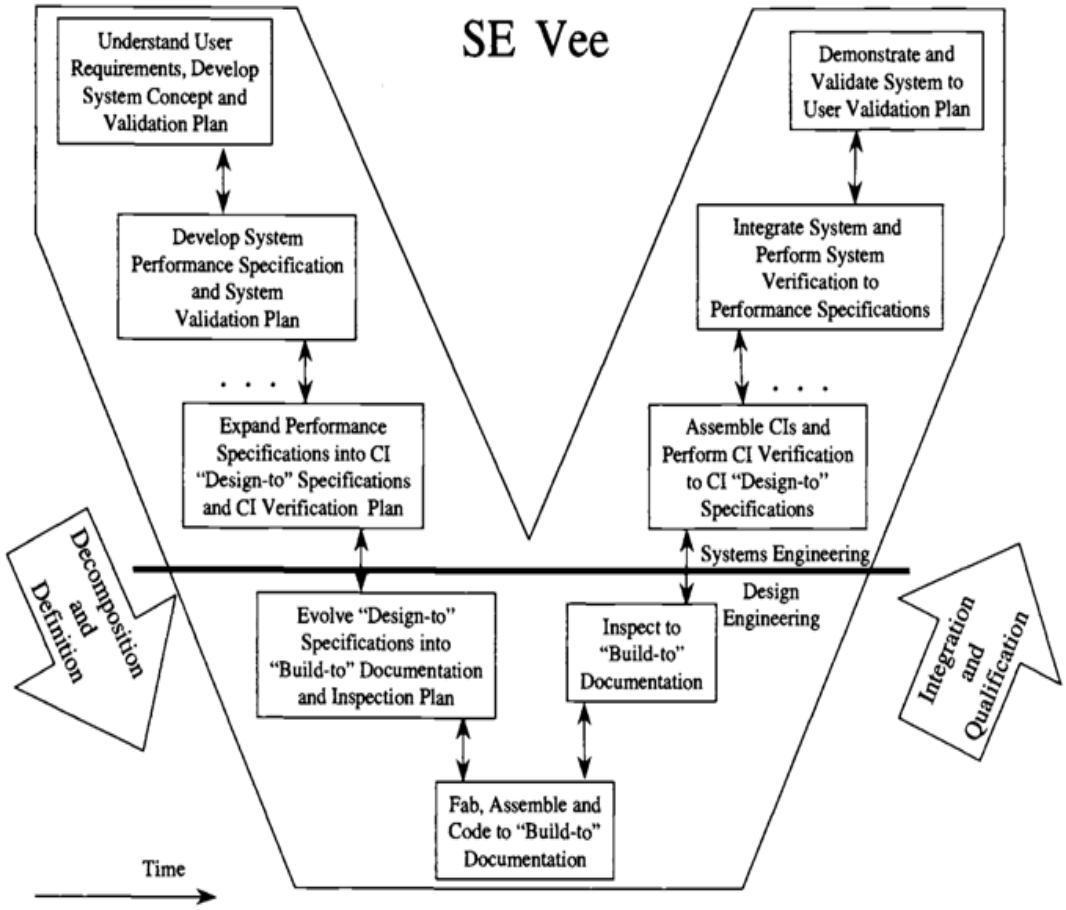

Figure 5. Systems Engineering Vee (From Forsberg and Mooz, 1992)

1. Operational Requirements

To fill a capability gap or need, a solution must be developed that satisfies the condition. In order to do this the solution must be bound in scope. These are the operational requirements. They define what must be done in order to fill the need. They

must be very succinct and exclusive to eliminate ambiguity in the systems development. This is in essence the purpose of the system (Buede, 2000).

2. Operational Concept

Once the purpose of the system is defined, then the vision for what the system is to become is developed. Operational concept is also known as the concept of operations (CONOPS). This includes how the system will operate, in its planned operating environment, from the stakeholders' perspective. The operational concept should discuss how the system is to operationally function in order to satisfy the stakeholder needs and how it will be manned, maintained, and deployed. The operational concept also includes a list of scenarios for which the system is designed to operate and meet (Buede, 2000).

3. Operational Scenarios

Operational scenarios describe every situation for which the system is designed to perform. The scenarios define how the system will respond to various environmental inputs and the resulting outputs. They do not describe how the system will perform these tasks, but rather how the system will process inputs and produce outputs (Buede, 2000).

4. External Systems Diagram

The External Systems Diagram (ESD) bounds the system in the design space. The external systems that interact with the system are defined as well as the system inputs, outputs, and constraints. The ESD models the system interactions at the boundaries of the system as they reach outside the system and into external systems (Buede, 2000).

5. Requirements

The requirements define system specifications, which the system design is required to meet, based on the needs and objectives of the stakeholders. The system design must meet these specifications. Requirements trace back to ESD, CONOPS and scenarios.

6. Functional Architecture Hierarchy

The functional hierarchy depicts what the system must do. The functional architecture hierarchy contains the hierarchy of the functions performed. The functions are based on the requirements needed to implement a system that can perform the scenarios previously described.

7. Functional Architecture Decomposition

Using IDEF0 modeling, each level of the functional architecture hierarchy is decomposed and modeled in terms of input and output requirements to specific functions. Each level of the functional architecture decomposition is traceable to the previous functional architecture hierarchy level (discussed in 6 above). The modeling of the system also illustrates all of the associated inputs to and outputs of the systems functions. This process is continued until the system has been decomposed to a single functioning component.

8. Physical Architecture Hierarchy

The physical architecture is modeled in a hierarchal format. It defines the physical resources that map to each individual function illustrated in the functional architecture hierarchy.

9. Operational Architecture

The operational architecture is where the physical and functional architecture map to each other. Each element of the physical architecture must match to a function, in a one-to-one fashion. It is the complete description of the system design.

C. DOD SYSTEMS ENGINEERING V-MODEL

In addition, the systems engineering "V" can be viewed from a Department of Defense (DoD) acquisitions point of view. The Systems Engineering Process is a problem solving approach (Department of Defense, 2001, 31). In the development of the generic architecture, proposed system solution, and implementation of an instantiated physical architecture, the systems engineering V-model was utilized (DoDAF, 2007). The

generic architecture is a simplified approach that identifies and focuses on only the key elements of the system. This model can be broken down into distinct phases as displayed in Figure 3. A new system design should start on the left side of the "V" with the system concept to establish the system level design requirements. Then continuing down the upper-left side of the "V," item level design requirements are established. This Systems Engineering V-model has predetermined review points along the way, where a detailed review is conducted to ensure the system is ready to move into the next phase. Once the design is completed at the bottom of the "V," then the fabrication, integration, and testing phases can begin, at the bottom of the "V" and moving up the right side of the "V."

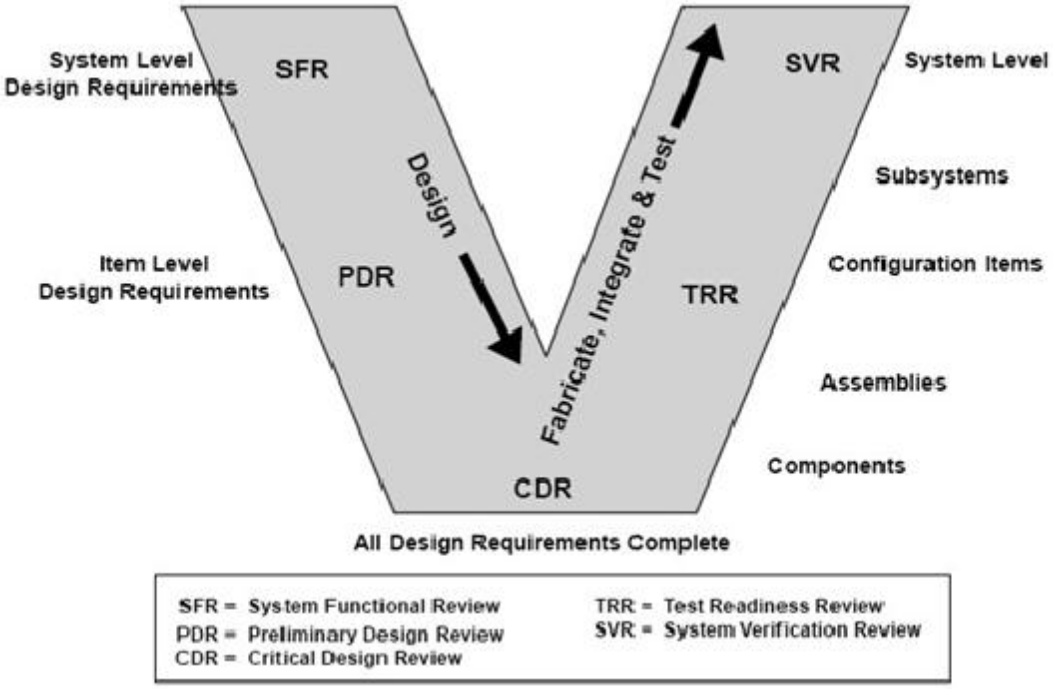

Figure 6. Systems Engineering V-Model (From DoDAF, 2007)

D. PROBLEM DEFINITION AND SYSTEM CONCEPT

The initial phase of a project starts with defining a problem or identifying a capability gap that needs to be filled. This phase describes what could be built or procured in order to fill the need and can result in the formulation of the idea for a

system. This initial phase does not establish that a system will be built; it only states that a system could fill a need and that further evaluation should be conducted.

Maintaining security and situational awareness over high value areas is a difficult and man-power intensive task based on the force structure of our military and other government agencies. A need exists for a system for use in the civil, government, and military environments that require constant surveillance in order to mitigate the threat of attacks of various types; most notably from within the civilian indigenous population who do not normally stand out as a recognizable threat. The Smart FOB Surveillance System (SFSS) provides a means of performing the task of constant monitoring in these environments to observe the numerous personnel who may transit an area. The system must have the ability to identify behaviors classified as "Abnormal" for the purposes of detecting potential threat behavior, is daunting, to say the least. The system should autonomously perform what simple human monitoring of audio, visual, or other media-based systems is severely limited in extended duration and capability, due to finite human useful attention span and identification of behaviors.

The solution for FOB protection should provide a networked system of automated "smart" sensors, which can continuously monitor areas for certain behaviors and alert authorities to react to those behaviors in order to interdict the threat. This system can be used in any number of civil or military applications such as government installations, military bases to include Forward Operating Bases (FOB), buildings, and other potential targets considered as high-value to an enemy where the capability of constant personnel behavior surveillance and monitoring would be advantageous.

E. SYSTEM LEVEL DESIGN REQUIREMENTS AND ARCHITECTURE

The requirements and architecture phase is where the generic architecture for system development is created and the system requirements are defined. The architecture provides a top-down view of the system. This phase results in a well-defined system architecture that has clear linkages to requirements. The architecture properly links to the previous phase, so that the system to be built meets the original needs. In the case of the system solution, an operational concept was developed, which provides all of the

necessary information in order to create scenarios in order to perform future simulations. The simulations can then be run utilizing different solutions to address the problem defined at the beginning of the operational concept. From the operational concept, the generic system architecture is created. The generic system architecture consists of the external system diagram, requirements, and functional architecture for the generic system.

1. Analysis of Alternatives

The analysis of alternatives (AOA) is a process that looks at the required need, the generic architecture, and identifies potentially viable solutions. Assessments are performed on each possible solution evaluating for effectiveness, achievability, cost, and viability (United States Air Force, 2008). Once an AOA is complete and a solution has been chosen for further development then the item level design can begin.

F. ITEM LEVEL DESIGN REQUIREMENTS

After one executes an AOA, the next step is to define the proposed alternatives physical architecture through the item level design requirements phase. These detailed specifications provide the bottom-up system design by breaking up the larger system into individual sub-systems and then breaking up the subsystems into components. This thesis selects a particular solution and provides its instantiated physical architecture. Additionally in this phase of the "V," the test and evaluation plans, to include acceptance tests, are developed. The acceptance must ensure that the needs described in the initial phase are satisfied. At the conclusion of this part of the process, all design requirements are complete, the upper-left side of the Systems Engineering "V," and the system is ready to begin fabrication, integration and test phases.

G. FABRICATE, INTEGRATE, AND TEST

As one moves from the bottom of the "V" and up the right side of the "V," the design that was formulated in the previous sections is turned into a real system. First, individual components are acquired or built and assembled into sub-systems (Buede, 2000). Then, unit tests are performed on these sub-systems. After the sub-systems have

been created and their unit tests have been satisfactorily performed, these sub-systems are ready for integration into the larger system (Buede, 2000).

The systems integration step is where all of the components and sub-systems are assembled and integrated into a complete working system (Blanchard & Fabrycky, 2006). The integration includes debugging of all software and testing of the complete integrated system. The complete system operation is verified when an acceptance test is demonstrated to and approved by the stakeholders. The acceptance test is the same test that was agreed upon earlier with the systems stakeholders, but due to any engineering change orders, the acceptance test may have incurred minor changes during the build cycle. All parties involved must agree upon any changes that have occurred. Upon successful completion of the acceptance test, the system is delivered to the entity that paid for its construction, and a determination for further orders is made. Fabrication and integration is where the majority of the time and work on the system occurs. However, it will only be successful if the earlier design was performed correctly.

To conclude, a Systems Engineering V-model yields an achievable roadmap for system creation. Additionally, the Systems Engineering V-model will be utilized in this thesis for the design of a generic architecture for the Smart FOB Surveillance System (SFSS). The next chapter discusses the basic concepts of Multi-Agent Systems (MAS) and introduce Artificial Intelligence (AI), Detection, Identification, Prediction, and Reaction (DIPR) Process, ISA, and MAS as an employment of distributed artificial intelligence.Swarm Intelligence and Multi-Agent Systems.

IV. SWARM INTELLIGENCE AND MULTI-AGENT SYSTEMS

This chapter discusses the use of intelligent automation as a method of data collection and processing. Intelligent automation provided by Multi-agent Systems (MAS) is desired because it provides more capability albeit more complexity. This chapter then discusses MAS characteristics that must be considered for proper implementation and the benefits of using distributed vice centralized artificial intelligence. Finally, this chapter will discuss the culmination of these ideas in the concept of Detect, Identify, Predict, React (DIPR) as an MAS, which is essential to the Smart FOB Surveillance System (SFSS) design.

A. OVERVIEW

Swarm Intelligence (SI) is an example of a Multi-agent System (MAS). A MAS is one that is comprised of many individual intelligent agents. The agents are autonomous; however, they interact within the network and communicate with other agents on the network. This includes interaction with human operators, the hardware, and software that comprise the MAS system. These intelligent agents can be anything from an individual software program to a collection of hardware and software that make up a robotic entity. The agents contain the necessary software for decision making in order to eliminate the need for human operation. Engineering through agents, which was discussed in Chapter II, is an approach in which the network-centric capabilities and attributes identified are paired with available agent-based technologies. This chapter will introduce and discuss Artificial Intelligence (AI), Detection, Identification, Prediction, and Reaction (DIPR) Process, ISA, and MAS as an employment of distributed artificial intelligence. In this chapter, the following topics will be covered:

- What is Intelligence Automation?
- What is a MAS?
- Why distributed AI?
- What is a DIPR?

B. INTELLIGENCE AUTOMATION

In today's environment, there is a significant need for automation of our data collection and processing capabilities. It is no longer practical or possible to gather the required actionable intelligence through conventional methods. The volume of data that must be processed is too immense for our current resources. Figure 7 below describes the three driving factors that require a change in our data gathering approach. Predicting and preventing terror or crime, Consumer needs, and the current economic crisis all push for intelligent automation as a solution (Goshorn et al., 2011).

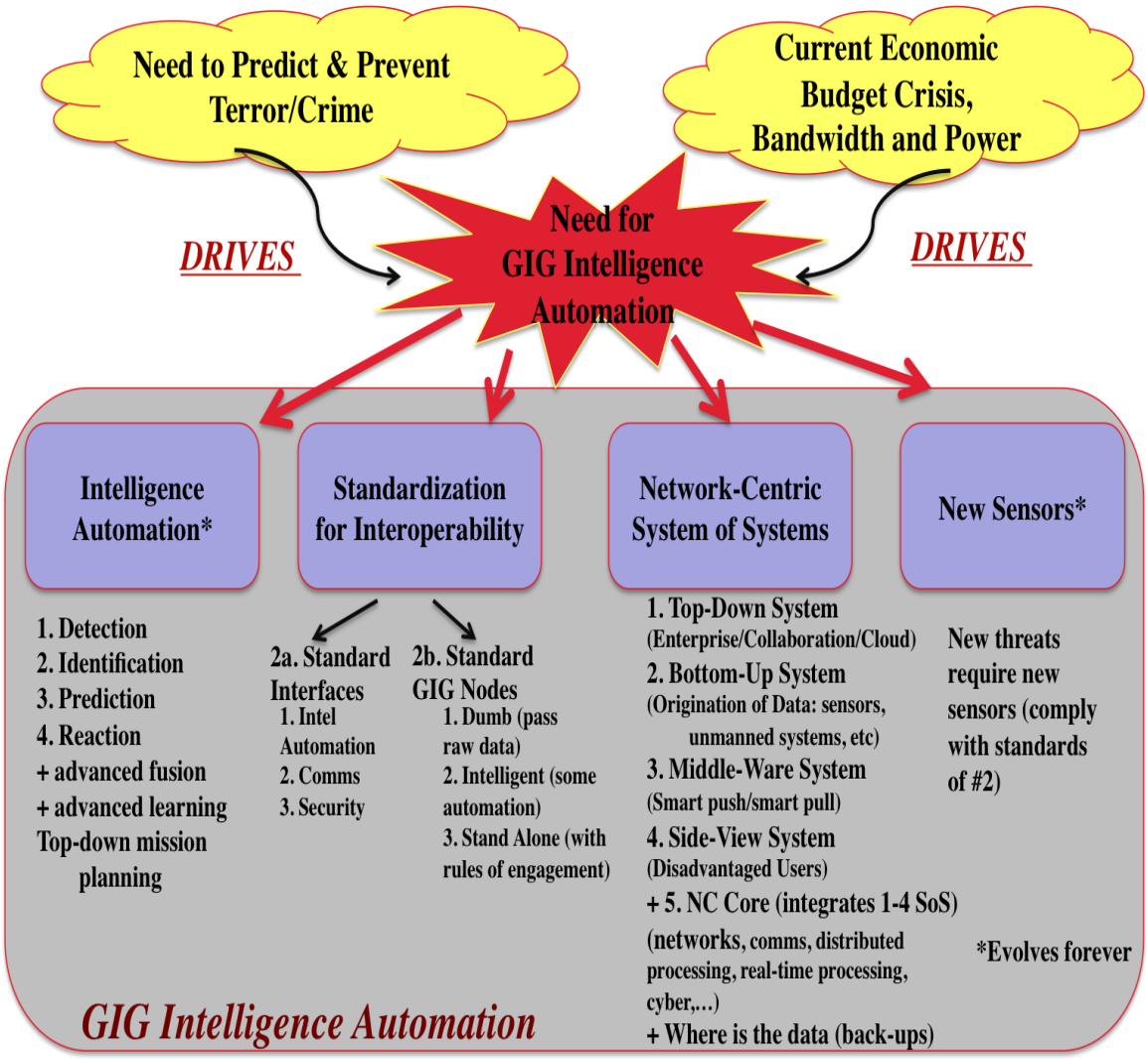

Figure 7. The Need for Intelligence Automation, and the Four Approaches Required to Implement Automation (From Goshorn et al., 2011)

There are four approaches designed to meet the need for automation: The need for intelligence automation, the need for standardization for interoperability, the need for network-centric system of systems, and a need for new sensors. In the development of the Smart FOB Surveillance System (SFSS) the first approach is being used (Goshorn et al., 2011).

1. Intelligence Automation

Intelligence automation is needed in order to rely less on manpower to carry out data collection and processing functions. In systems that are laden with various sensors and processing requirements, the bandwidth required could quickly overwhelm a systems network. An autonomous intelligent automation system designed for efficiency could alleviate this problem (Goshorn et al., 2011).

C. MULTI-AGENT SYSTEM

A multi-agent system (MAS) is defined as a system comprised of many individual intelligent agents that interface and operate collectively in the performance of a single overarching goal. These individual agents each carry out their own functions, which cumulatively perform the larger task (Padhy, 2005). The use of a MAS system is much more complicated than an individual agent. The interaction of individual agents that make up the MAS must be analyzed to ensure the proper application of groups of agents. Typically a bottom-up approach is taken to determine the interactions of the agents. As a result, multi-agent system (MAS) system design is much more complex. Relationships and the method that the ISAs communicate with one another must be considered. In addition, task hierarchy and responsibilities must be defined and incorporated into the overall system. Finally, software applications must be specifically designed with MAS applications in mind (Weiss, 1999).

The general MAS characteristics are as follows (Vlassis, 2007):

1. Agent Design

The individual agents that comprise MASs are not required to be alike. They may be the same or similar, or they may also be very dissimilar; which is the case in a complex MAS. The only requirement is that they have the ability to interact seamlessly.

2. Environment

Static environments generally only require a simple individual agent. The AI embedded technology is capable of handling these types of scenarios. However, the solution to dynamic environments requires a complex MAS.

3. Perception

Each agent perceives sensed information at their own location, time, and context. This results in each agent receiving bits and pieces of the actual environment. This data must have the ability to be melded in order to create a clear picture of the information received.

4. Control

Command and control of the individual agents in an MAS is done from within the agent. The MAS has the capability of deciding which actions to perform. Control is distributed among each agent instead of being centralized.

5. Knowledge

Due to the differing perceptions of each agent, it is necessary for the individual agents to share knowledge about their environment and with input from other agents, have the ability to coalesce perceptions to reach common environmental knowledge.

6. Communication

Every agent of an MAS must have the ability to transmit as well as receive data from other agents. This requires that they have a common communications format to include software compatibility.

Robust intelligent systems tend to use many agents for the following reasons (Vlassis, 2007):

- Speed is improved due to parallel processing.
- Reliability is improved since single agent failures do not cause system failure.
- Interoperability is improved since agents from one MAS can be used interchangeably with agents from another
- Application flexibility is improved because the number of agents can be changed based on the operational needs of the environment.

D. DISTRIBUTED ARTIFICIAL INTELLIGENCE (DAI)

Distributed Artificial Intelligence (DAI) is the decentralization of the tasks performed by individual agents. Although the individual agents act collectively as a group to perform a common goal, the processes and functions performed are spread out among the collection of agents. This concept lends itself NCW applications especially when implementing a system composed of numerous systems and subsystems within a single unified system.

E. WHY DISTRIBUTED AI?

As discussed previously Intelligent Automation is necessary in todays environment. For very similar reasons, distributed intelligence is also needed in complex sensor-based MASs. The reasons for this are outlined in the following section (Ferber, 1999):

- Distributed systems are more flexible. They can adapt to environmental changes as well as system requirements more easily.
- Military applications generally encompass many locations or a widely dispersed area.
- Distributed systems can be sized according to the required capability.
- Networking and interfaces among networks inherently require distribution.
- Networking of forces (and sensors) compels a distributed view.
- The problem solving for which these systems are designed for require that multiple parallel and serial steps be performed.
- To reach the level of automation required by todays surveillance based systems, detection, identification, prediction, and reaction (DIPR) systems must be automated.

Distributed Automated Intelligence is an absolute necessity for future NCW systems. The Global War on Terrorism (GWOT) has resulted in our requirement to process more information than ever before. Current resources prevent adequate detection and prevention of these threats unless these functions can be highly automated. In addition, behavior prediction models such as detection, identification, prediction, and

reaction (DIPR) systems must distribute automation in order to handle the necessary processing required to stay with demand of these sensor-based systems (Goshorn et al., 2011).

F. DIPR AS A MAS

A DIPR system inherently contains many MASs. Each function of DIPR is comprised of an MAS in that they carry out sub-functions that collectively perform the common overall goal, which is to receive sensor input and then process the information to provide an appropriate response (Schafer, 2009).

The concept of a Detect, Identify, Predict and React (DIPR) system is illustrated below (Figure 8). Information is received by sensors. Raw sensor data is sent to detection software that places the data in a spatial-temporal feature matrix. The identification function processes the data, by fusing these spatial-temporal features, to output intelligent states of the information received. These intelligent states are inputted to the prediction function, over time, creating a sequence. This sequence of intelligent states forms a behavior. The prediction function then classifies the behavior and then infers predicted behaviors outcomes. Finally, predicted behaviors actuate an appropriate reaction response (Goshorn et al., 2011).

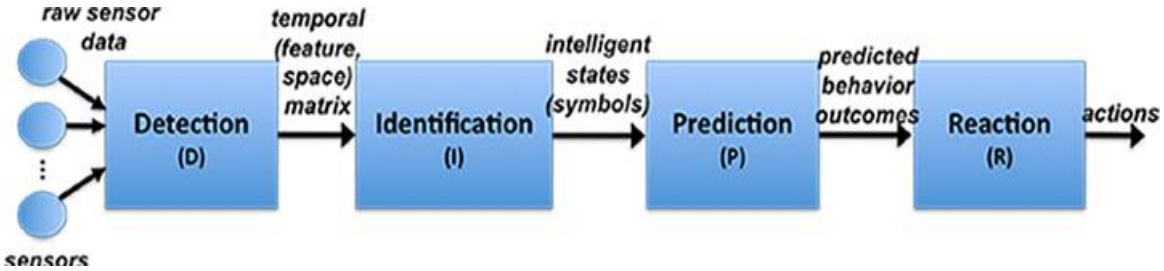

Figure 8. DIPR System (From Goshorn et al., 2011)

1. Detection

Raw sensor data feeds the detection subsystem of DIPR. This subsystem receives data from the various sensors enabled to provide input. They can be any type of sensor

including video, audio, or RF, among others. The feature information extracted from each sensor input is based on end user needs, the behavior modeling technique, and the type of signal detected. From this input, the detect function outputs a spatial-temporal matrix that captures data as packets in space and time. The result is a feature space matrix representing the data detected. Figure 9 below describes the feature space matrix. Matrices represent a single snapshot of features, over space, at a given moment in time. As time elapses, multiple matrices are formed, which create a three-dimensional matrix describing the spatial and temporal features of the data. In addition, to these features differentiation calculations can be performed to create time rate of change features (Goshorn et al., 2011).

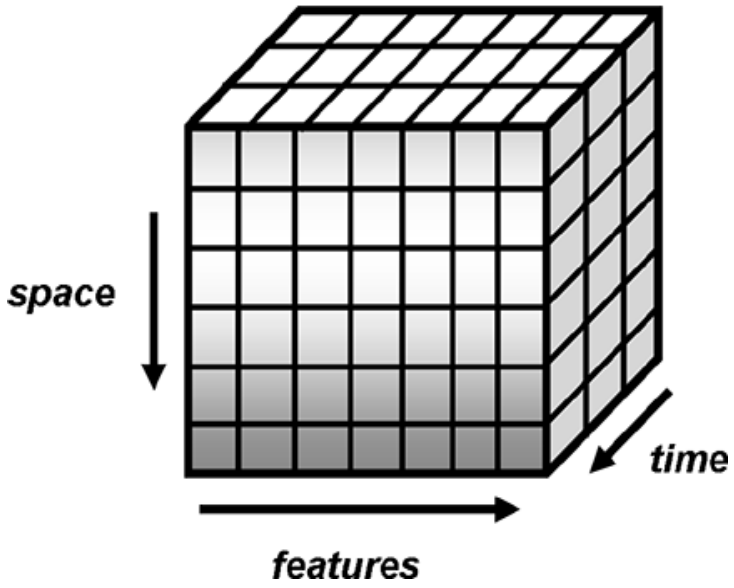

Figure 9. Feature Space Matrix (From Goshorn et al., 2011)

2. Identification

The identification subsystem receives the temporal feature space matrix from the detection subsystem and outputs an intelligent state symbol when a feature meeting threshold requirements is observed at a given time increment. These intelligent states are dictated by operating rules that are established by the operator. The intent is to sift through incoming data and pull out features that are of interest to the end user. Figure 10 illustrates the operation of the identification function. Once the features and spatial-

temporal attributes are processed by the temporal (features, space) module, the signals are fused and compared against intelligence rules to determine whether an intelligent state is triggered. If so, the intelligent state symbol is an output to the next DIPR subsystem (Goshorn et al., 2011).

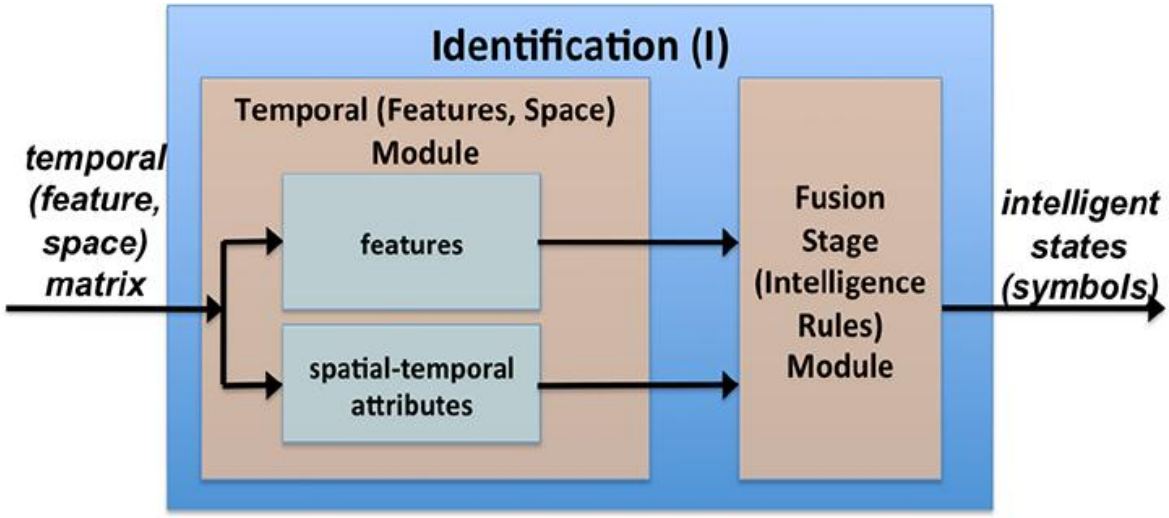

Figure 10. Identification Subsystem of the DIPR System (From Goshorn et al., 2011)

3. Prediction

Figure 11 shows the prediction subsystem of the DIPR system. The main function of this subsystem to perform the high-level behavior classification and infer future behaviors. Intelligent states outputted from the identification subsystem are inputted into the prediction subsystem. The behavior classifier module groups sequences of intelligent states and then classifies these sequences in terms of their syntactical behavior. This is where behaviors are deemed normal or abnormal. These behaviors are then paired with inferred predicted outcomes as defined by the user. This output then becomes the input to the reaction subsystem of DIPR (Goshorn et al., 2011).

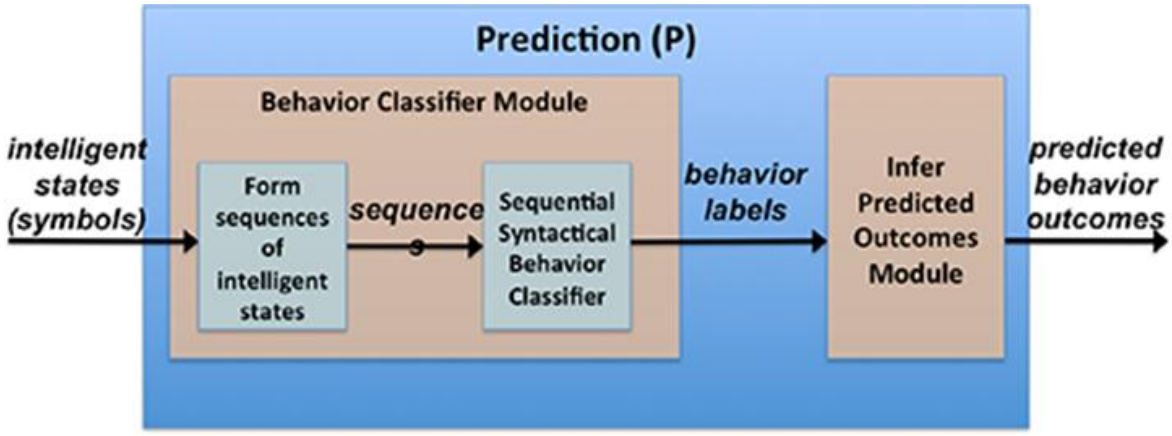

Figure 11. Prediction Subsystem (From Goshorn, 2011).

4. Reaction

The reaction subsystem matches predicted behavior outcomes to appropriate system responses. This could result in warnings or alarms. This could also prompt the system operator for further information or action. In an automated surveillance environment this could also prompt further information gathering by the systems sensors. The reaction subsystem recommends or automates "rules of engagement." The reaction subsystem can be seen as part of the entire DIPR system in Figure 13 below. This subsystem is integral in the creation of a true NCW system designed to automate decision functions previously performed by human operators.

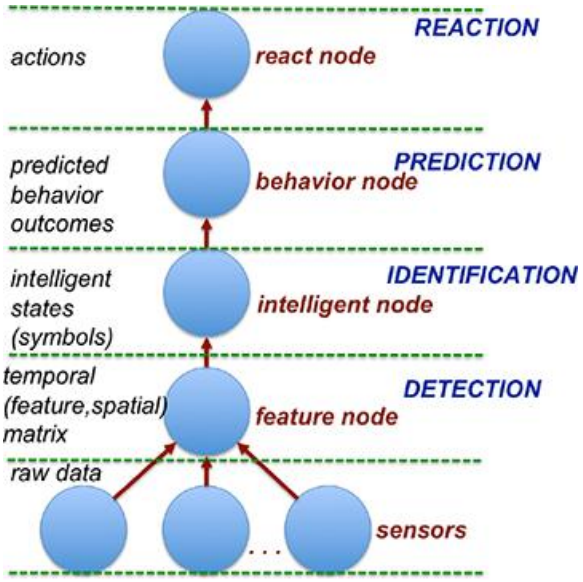

Figure 12. Intelligent Hierarchy Implements DIPR System (From Goshorn, Goshorn, Goshorn & Goshorn 2010)

This chapter discussed the need for Intelligent Automation (IA), and more specifically, the need for Distributed Intelligent Automation (DIA). The chapter also addressed the difference between a single-agent system and a Multi-Agent System (MAS) and how an MAS readily lends itself to military and sensor-based systems. Finally, the automated DIPR concept was explained. The next chapter will discuss the systems engineering solution for a Smart FOB Sensor System (SFSS).

THIS PAGE INTENTIONALLY LEFT BLANK

V. SYSTEM ENGINEERING SOLUTION FOR A SMART FOB SURVEILLANCE SYSTEM (SFSS)

This chapter will focus on the development of the system by using the left side of the Systems Engineering Vee model beginning with identifying the operational need and operational concept. From the operational need and operational concept, the various operational scenarios are defined that will be used to bound and scope the system. From there further Systems Engineering products can be developed. The External Systems Diagram is developed and flows into the requirements of the system. Finally, the functional, physical, and operational architectures are developed.

A. OPERATIONAL NEED

Forward Operating Bases (FOB) are vulnerable to terrorist attacks and intelligence gathering. Current methods of surveillance are manpower intensive and are unnecessarily dangerous to those performing these functions. FOBs must be provided with an effective surveillance system that can continuously monitor threat activity.

B. OPERATIONAL CONCEPT

A FOB will be monitored by both fixed and mobile sensors. The fixed sensors will monitor the FOBs immediate perimeter by way of video, Radio Frequency (RF), and audio sensors. The mobile sensors will be deployed as an integral part of a collection of Unmanned Aerial Vehicle (UAV) operating within a Swarm Intelligence framework. Multiple video-sensor equipped UAVs will patrol and monitor the vicinity of the FOB. The number of UAVs will be based on the approximate size and threat density specific to the particular FOB. A Network Operating Center (NOC) will be established within the protected boundaries of the FOB. The NOC will receive sensor data from both the fixed and mobile systems and process the raw fixed sensor data. The mobile sensor data will

initially be processed by the Swarm based UAVs, then send the intelligence data to the NOC for final processing. The NOC will perform all of the behavior analysis, alert functions, and database management functions based on the processed fixed and mobile intelligence data.

C. OPERATIONAL OVERVIEW

The Operational View (OV-1) is a fundamental systems engineering product. The OV-1 depicts the high-level operational concept of the mission that the system is intended to perform (DoDAF, 2007). Figure 14 describes the system in terms of the operational environment, technologies involved, equipment used, and the communication that occurs between the components.

On the most basic level, the Smart FOB Sensor System (SFSS) is a surveillance system that continuously and autonomously receives signals from the environment passively and actively. For every instance that a signal received meets the criteria for a potential threat, the source of the signal is labeled as an Object of Interest (OI). These OIs will be tracked for further evaluation until the threat criteria no longer exists. In addition, OIs initiate a heightened priority for evaluation, which results in more intensive observation by the Swarm UAVs.

There are three main signals that the Smart FOB Sensor System (SFSS) is intended to detect: visual signals, audible signals, and RF signals. Visual signals are sensed actively by both the fixed and mobile sensors. Video captured by the UAV is processed on board for facial recognition and video for behavior analysis is sent directly to the Network Operations Center (NOC). Video captured by the fixed sensors are sent directly to the NOC for facial recognition and behavior analysis processing. The multi-directional signal interaction between the UAVs and between the UAVs and NOC are represented by a dashed yellow line. The intent is to detect potential threats either by

facial recognition of known terrorist threats or by behavior analysis of the movements of the OIs. The OV-1 graphic shows six black dots, which represent a group of unknown persons that require threat evaluation. Audible signals are passively received by the fixed sensor network located along the perimeter of the FOB. The audio received is sent to the NOC for threat criteria evaluation. To meet a threat criterion, the audio received is evaluated by the NOC against audible threat profiles. The intent is to primarily detect gunfire and explosions. The audio source can also be located through simple triangulation based on the dB level of the various audio sensors receiving the signal. As with all signals that meet a threat criterion, the signal source will be labeled as an OI and initiate more intense observation by the Swarm UAVs. The OV-1 graphic shows a representation of a red explosion that requires threat evaluation. The final signal sensed is RF signals passively sensed by the fixed perimeter sensors. The OV-1 graphic shows its representation by a transmitting antenna. The RF received is sent to the NOC for threat criteria evaluation. To meet a threat criterion, the RF received is evaluated by the NOC against RF threat profiles. The intent is to detect jamming attempts, electronically guided munitions, electronically actuated Improvised Explosive Devices (IED), and in the case of RF communications, to intercept the transmission for recording and evaluation by the NOC operator. The RF source can also be located through simple triangulation based on the signal level of the various RF sensors receiving the signal. As with all signals that meet a threat criterion, the signal source will be labeled as an OI and initiate more intense observation by the Swarm UAVs.

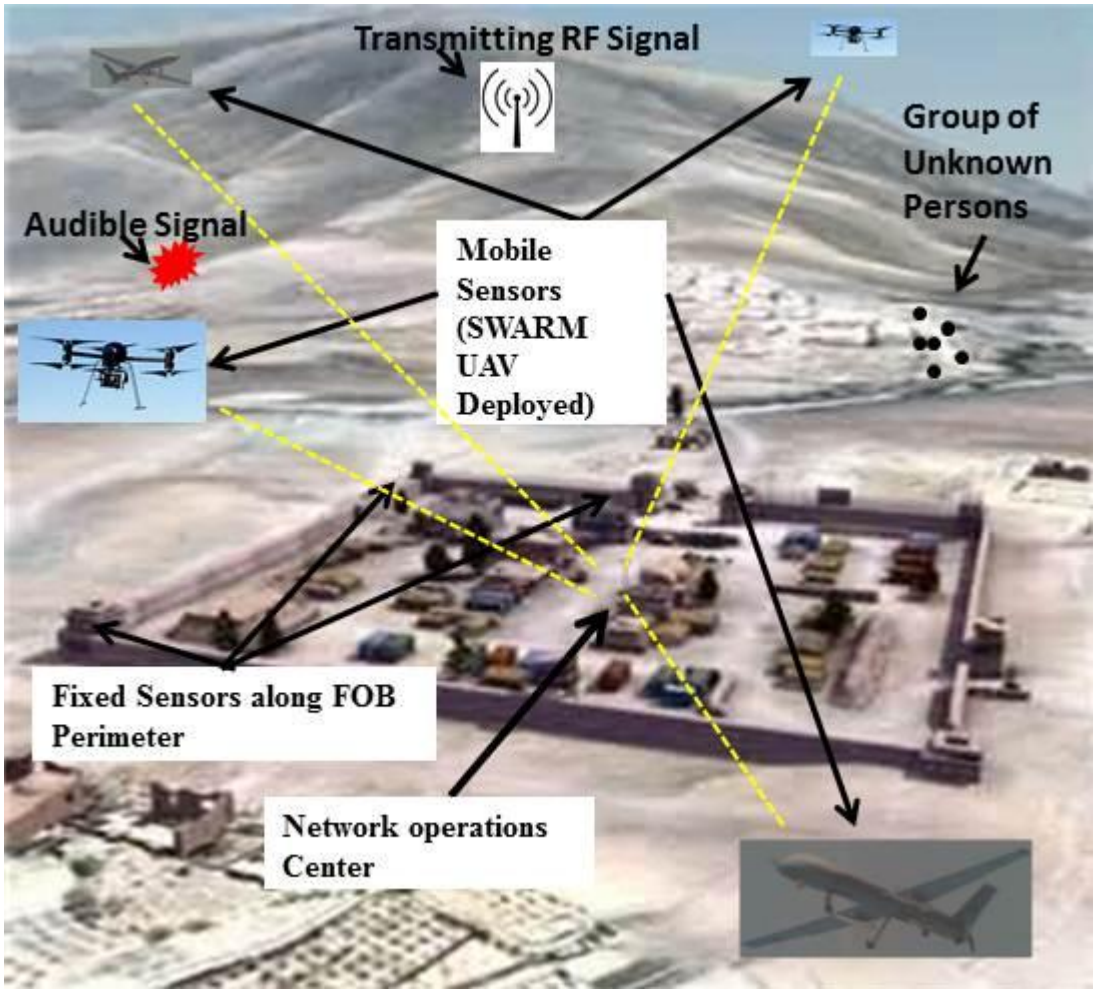

Figure 13. System Operational View

D. OPERATIONAL SCENARIOS

The operational scenarios discussed below will be used to scope the architecture design of the system. The operational scenarios will scope the operational need to the expected threat environment. The architecture of the system will include the development the external systems diagram, the functional architecture hierarchy, functional architecture decomposition, physical architecture and operational architecture.

1. Normal Steady State Operation

Normal steady state operation is defined as the system functioning and monitoring all sensory data. However, no sensory data is received that would initiate an Object of Interest (OI) protocol. The fixed sensors are scanning the immediate area of the FOB for visual, audible, and RF signals that meet criteria to initiate further investigation and signal processing by the Behavior Analysis Module. The UAV deployed mobile visual sensors are also receiving data that does not meet criteria for further processing. In this instance, the Swarm based UAV fleet will maintain normal flight patterns and no alerts are received by the Network Operations Center (NOC) Operator from the Smart FOB Surveillance System (SFSS).

2. Visual Signal Criteria Met/Facial Recognition Matches Non-threat

Persons approaching the FOB are captured on video by the mobile UAV Swarm and /or the fixed video sensors along the FOB perimeter. The video is analyzed onboard the UAVs by a facial recognition program. Video received by the fixed sensors is sent to the NOC directly for analysis. The Facial recognition images captured are sent to the NOC and compared to a database containing images of known threats and known non-threats. When a match to a known non-threat is received, the NOC operator will acknowledge the report and the system will maintain steady state operation.

3. Visual Signal Criteria Met/ Facial Recognition Matches Threat

Persons approaching the FOB are captured on video by the mobile UAV Swarm and /or the fixed video sensors along the FOB perimeter. The video is analyzed onboard the UAVs by a facial recognition program. Video received by the fixed sensors is sent to the NOC directly for analysis. The Facial recognition images captured are sent to the NOC and compared to a database containing images of known threats and known non-threats. When a match to a known threat is received, the NOC operator will receive an alert, who will in turn alert the FOB to initiate threat protocols as well as Head Quarters for reporting requirements. In addition, the known threat will be labeled as an OI and initiate more intense observation by the Swarm UAVs until the threat is resolved.

4. Visual Signal Criteria Met/ Facial Recognition No Match

Persons approaching the FOB are captured on video by the mobile UAV Swarm and /or the fixed video sensors along the FOB perimeter. The video is analyzed onboard the UAVs by a facial recognition program. Video received by the fixed sensors is sent to the NOC directly for analysis. The Facial recognition images captured are sent to the NOC and compared to a database containing images of known threats and known non-threats. When the facial recognition data collected does not reveal a match when compared to the database, the Smart FOB Surveillance System (SFSS) will continue to track the contact and alert the NOC operator to determine the disposition of the contact as a threat or non-threat. The FOB reactionary force will investigate the contact to determine the threat level of the Object of Interest (OI). After the investigation, the NOC operator will update the database to reflect the threat level evaluated for that contact.

5. Visual Signal Criteria Met/Behavior Abnormal

In addition to threat evaluation by facial recognition comparison, the raw video from the fixed and mobile sensors is sent to the Network Operations Center (NOC) for behavior analysis. Behavior analysis is carried out comparing the movements of the tracks against threat criteria. Abnormal behaviors are considered as loitering, persons in prone positions, persons that appear to be traveling in a manner to not be detected, vehicles approaching the FOB, and other abnormal threats as defined by the operator. In these instances, the NOC operator will be alerted for disposition of the Object of Interest (OI). The FOB reactionary force will investigate the contact to determine the threat level of the Object of Interest (OI).

6. Visual Signal Criteria Met/Behavior Normal

Raw video data, collected by the fixed and mobile sensors, of contacts in the vicinity of the FOB that do not exhibit abnormal behavior will continue to be tracked and their behavior analyzed for abnormal behaviors. The system will maintain steady state surveillance operation.

7. Audible Signal Criteria Met/ Behavior Abnormal

The fixed sensor network located along the perimeter of the FOB passively receives audible signals. The audio received is sent to the NOC for threat criteria evaluation. To meet a threat criterion, the audio received is evaluated by the NOC against

audible threat profiles. When gunfire or on explosion is detected, the audio source will be located through simple triangulation based on the dB level of the various audio sensors receiving the signal. The NOC operator will be alerted who will in turn initiate FOB threat protocols, which may include the deployment of FOB reactionary force for further investigation. In addition, the contact will be labeled as an Object of Interest (OI) and be monitored by the Swarm UAVs at an elevated priority until the disposition of the threat is resolved.

8. Audible Signal Criteria Met/Behavior Normal

Audible signals that do not initially meet threat criteria will continue to be tracked and monitored by all other sensors as normal. The source of the audio will be located through simple triangulation based on the dB level of the various audio sensors receiving the signal. The NOC operator will determine the threat disposition of the audio detected and if it is determined that no threat exists, the Smart FOB Surveillance System (SFSS) will return to normal steady state operations.

9. RF Signal Criteria Met/ Behavior Abnormal

RF signals are passively received by the fixed sensor network located along the perimeter of the FOB. The RF received is sent to the NOC for threat criteria evaluation. To meet a threat criterion, the RF received is evaluated by the NOC against RF threat profiles. When jamming attempts, electronically guided munitions, electronically actuated Improvised Explosive Devices (IED), or other potentially threatening RF signals are detected, the RF source will be located through simple triangulation based on the dB level of the various audio sensors receiving the signal. The NOC operator will be alerted who will in turn initiate FOB threat protocols, which may include the deployment of FOB reactionary force for further investigation. In addition, the contact will be labeled as an Object of Interest (OI) and be monitored by the Swarm UAVs at an elevated priority until the disposition of the threat is resolved.

10. RF Signal Criteria Met/Behavior Normal

RF signals that do not initially meet threat criteria will continue to be tracked and monitored by all other sensors as normal. The source of the RF will be located through simple triangulation based on the dB level of the various audio sensors receiving the

signal. The NOC operator will determine the threat disposition of the RF detected and if it is determined that no threat exists, the Smart FOB Surveillance System (SFSS) will return to normal steady state operations.

11. RF Signal Criteria Met/ Communication Intercept

RF signals that are determined to be voice or data communications will be intercepted and evaluated by the NOC operator to determine the treat level. The location of the source will be determined by triangulation and labeled as an Object of Interest (OI) until the operator completes the threat disposition. If the source is considered a threat, FOB protocols will be initiated to combat the threat. If the source is determined to be non-threatening, then the Smart FOB Surveillance System (SFSS) will return to normal steady state operations.

12. Global Intelligence Data Communication with Head Quarters

The Network Operations Center (NOC) is in constant two-way communication with the FOBs Headquarters by way of a satellite data link, which is a service provided by the FOB infrastructure for the Smart FOB Surveillance System (SFSS). Global Intelligence Data is sent from Head Quarters to the FOB to alert the Network Operations Center (NOC) operator of impending threat alerts as well as updates to the NOC database for facial recognition, behavior analyses, audible threat profiles, RF threat profiles, and RF communications decryption. In addition, positive threat alerts by way of video, audio, RF, or NOC operator determination will automatically alert Head Quarters to initiate reporting of the threat condition to resolution. In situations where the NOC has discovered a new threat profile, the NOC will also update Global Intelligence data via Head Quarters. A new threat profile is a signal or Object of Interest (OI) previously determined to not be a threat criterion, but subsequently was determined to be potentially threatening. For example, a person who did not previously match the facial recognition database, but recently was determined to be a threat by the FOB reactionary force would now be entered into the facial recognition database.

E. EXTERNAL SYSTEMS DIAGRAM (ESD)

From the operational scenarios, the External Systems Diagram (ESD) is developed. The ESD is a representation of the inter-relationship between the SFSS system and the external systems at the system boundaries with regard to the systems inputs, outputs, and constraints (Buede, 2000). The Integrated Definition for Function Modeling (IDEF0) format is used to depict the ESD for the Smart FOB Surveillance System (SFSS). The ESD (Figure 14) consists of five distinct parts: Constraints (FOB Standards and Environment) are listed at the top of the figure and constrain each function. System Functions are listed in the boxes (Provide Infrastructure for SFSS, Operate SFSS, Provide SFSS Services, Provide Global Intel for SFSS, and Maneuver within FOB Area of Operation). On the left side of each function are the inputs. The Smart FOB Surveillance System (SFSS) inputs are the outputs from the external systems. On the right side of each function are the outputs. The Smart FOB Surveillance System (SFSS) outputs are inputs to external systems. Finally, the bottom of the graphic shows the system and external systems (FOB, Operator, SFSS, Head Quarters, and Objects).

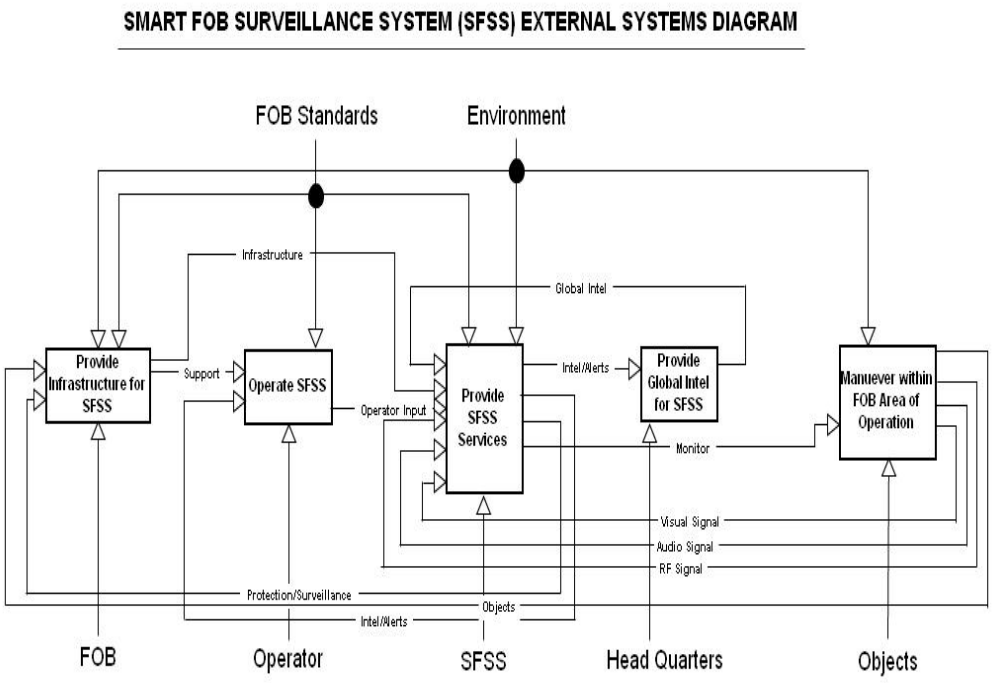

Figure 14. External Systems Diagram for SFSS

F. REQUIREMENTS

The requirements for the Smart FOB Surveillance System (SFSS) are an extension of the External Systems Diagram (ESD) discussed above. They are based on the operational concept, scenarios, as well as the External Systems Diagram (ESD) of the system and are broken down into three distinct categories: Input/output requirements, external systems requirements, and system constraint requirements.

F.1.0—Input/output requirements

F.1.1—Input requirements

F.1.1.1—The Smart FOB Surveillance System shall receive the input Global Intel.

F.1.1.2— The Smart FOB Surveillance System shall receive the input Infrastructure.

F.1.1.3— The Smart FOB Surveillance System shall receive the input Operator Input.

F.1.1.4—The Smart FOB Surveillance System shall receive the input Visual Signal.

F.1.1.5— The Smart FOB Surveillance System shall receive the input Audio Signal.

F.1.1.6— The Smart FOB Surveillance System shall receive the input RF Signal.

F.1.2—Output requirements

F.1.2.1— The Smart FOB Surveillance System shall provide the output Intel/Alerts.

F.1.2.2— The Smart FOB Surveillance System shall provide the output Alerts.

F.1.2.3— The Smart FOB Surveillance System shall provide the output Protection/Surveillance.

F.1.2.4— The Smart FOB Surveillance System shall provide the output Monitor/Surveillance.

F.2.0—External systems requirements

F.2.1— The Smart FOB Surveillance System shall interface with the external system FOB.

F.2.2— The Smart FOB Surveillance System shall interface with the external system Operator.

F.2.3— The Smart FOB Surveillance System shall interface with the external system Head Quarters.

F.2.4— The Smart FOB Surveillance System shall interface with the external system Objects.

F.3.0—System constraint requirements

F.3.1— The Smart FOB Surveillance System shall comply with constraints of FOB Standards.

F.3.1— The Smart FOB Surveillance System shall comply with constraints of the Environment.

G. GENERIC SYSTEM FUNCTIONAL ARCHITECTURE

The functional architecture of a system contains the hierarchy of the functions performed. Those functions are then decomposed further from top-level functions to the bottom-level functions (Buede, 2009). Figure 15 depicts the functional architecture for the Smart FOB Surveillance System (SFSS). The functions are based on the requirements needed to implement a system that can perform the scenarios previously described. This generic functional architecture hierarchy will be used to carry out the mission of the system as described in the operational concept and graphically displayed in the operational view.

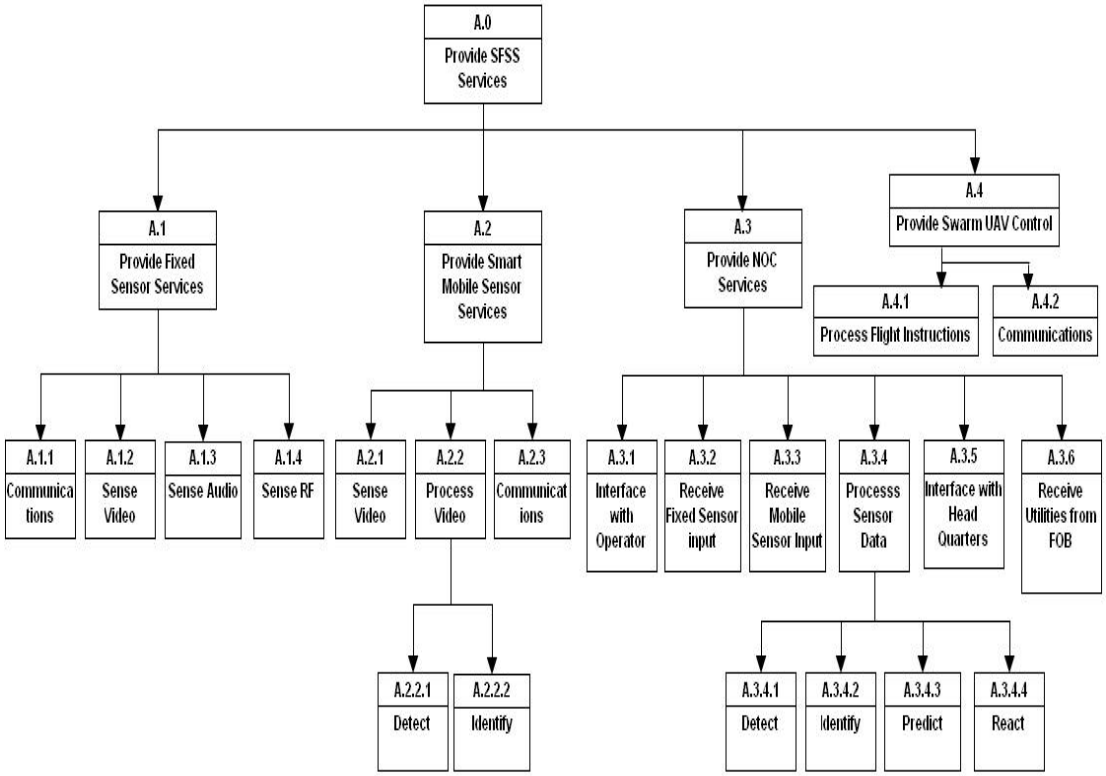

Figure 15. Generic Functional Architecture Hierarchy for SFSS

The functional architecture outlines four key subfunctions that the Smart FOB Surveillance System (SFSS) must perform in order to provide surveillance and threat detection for a FOB.

- Provide fixed sensor services
- Provide smart mobile sensor services
- Provide NOC services
- Provide Swarm UAV Control

The functional architecture decomposition is illustrated using IDEF0 modeling, beginning with the top function and then further decomposing each function into lower level functions. Figure 15 depicts four levels of function decomposition with inputs and outputs of each function. The top level function of "Provide SFSS services" can be seen in Figure 16 below. Again, using an IDEF0 diagram, the top level function is located

inside the box. The constraints of environment and FOB standards are above the box, the inputs enter the box from the left, and the outputs exit the box to the right.

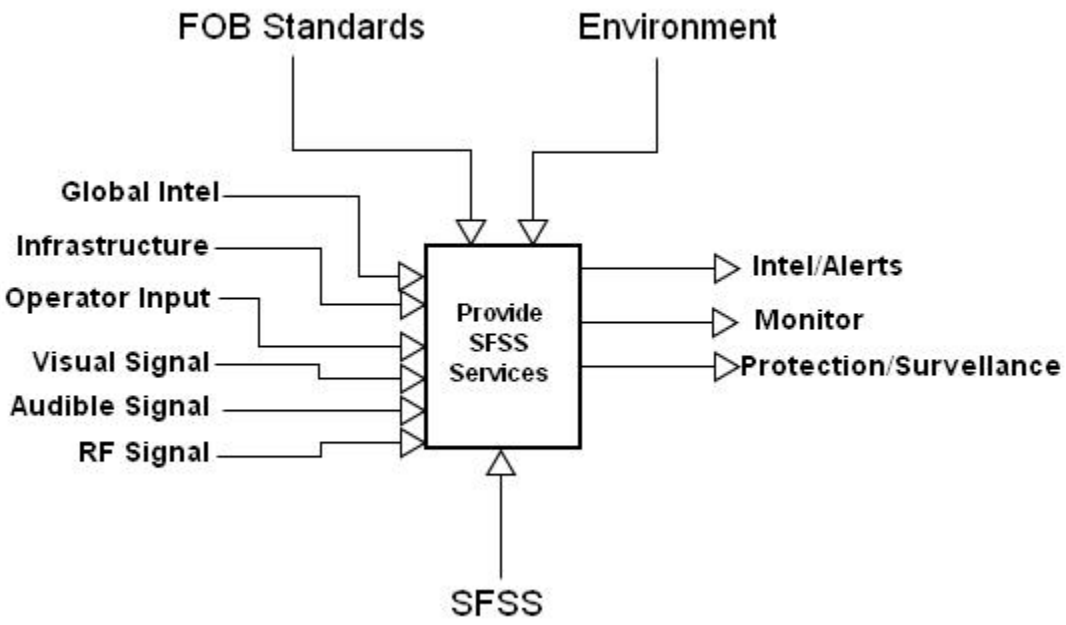

Figure 16. Top-level Function for the Generic System for SFSS

The first level decomposition of the system function "Provide SFSS Services" is depicted in the IDEF0 Figure 18. This diagram shows inputs and outputs between the first level functions and the constraints on these functions. The model demonstrates how data from the fixed and mobile sensors are received in order for the Network Operations Center (NOC) to generate alerts and ultimately warn the FOB of potential threats. The figure also depicts how global intelligence data from the FOBs headquarters can be received by the Smart FOB Surveillance System (SFSS).

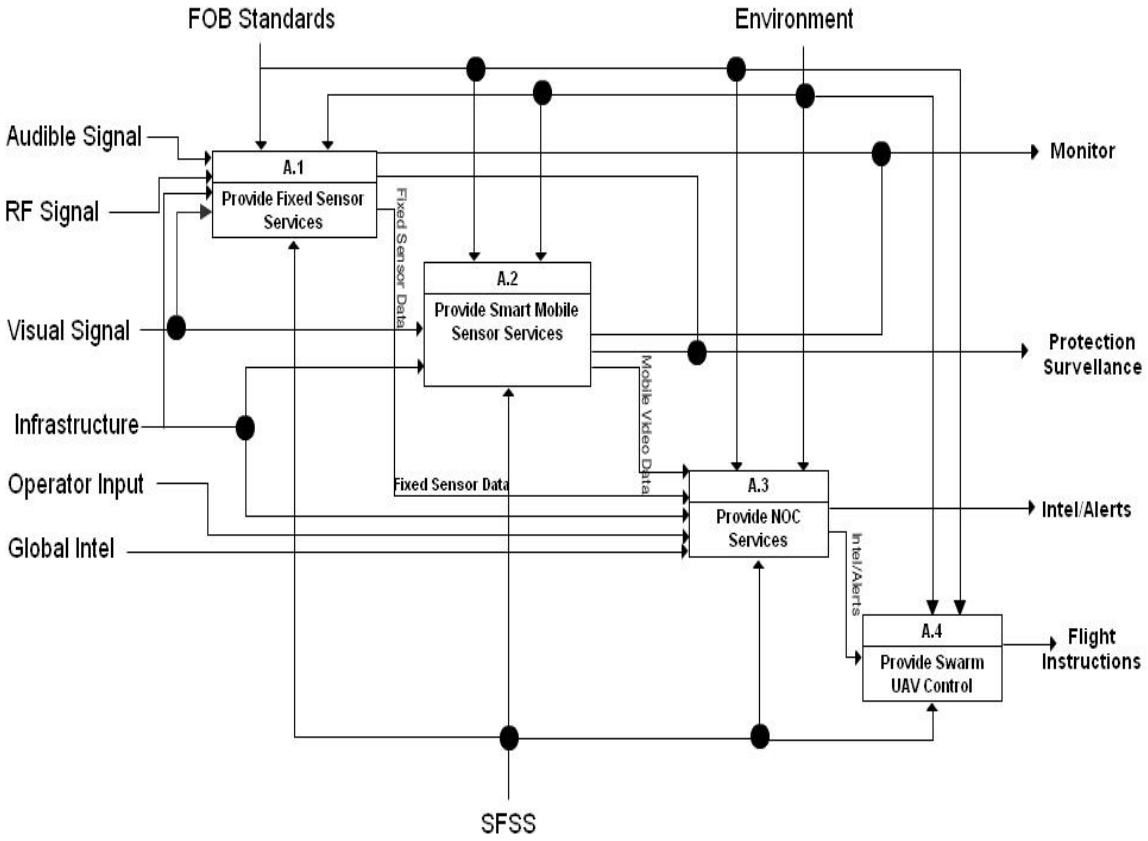

Figure 17. First-level Decomposition of the System Function Provide SFSS Services for SFSS

Figure 18 shows the decomposition of the function "Provide Fixed Sensor Services." This graphic depicts how the raw data inputs from the video, audio and RF sensors are received for further processing. The data received can also be heard and viewed in real-time by the operator for manual monitoring. The FOB infrastructure provides the necessary power requirements of the system as well as network connectivity for communications with the FOB headquarters.

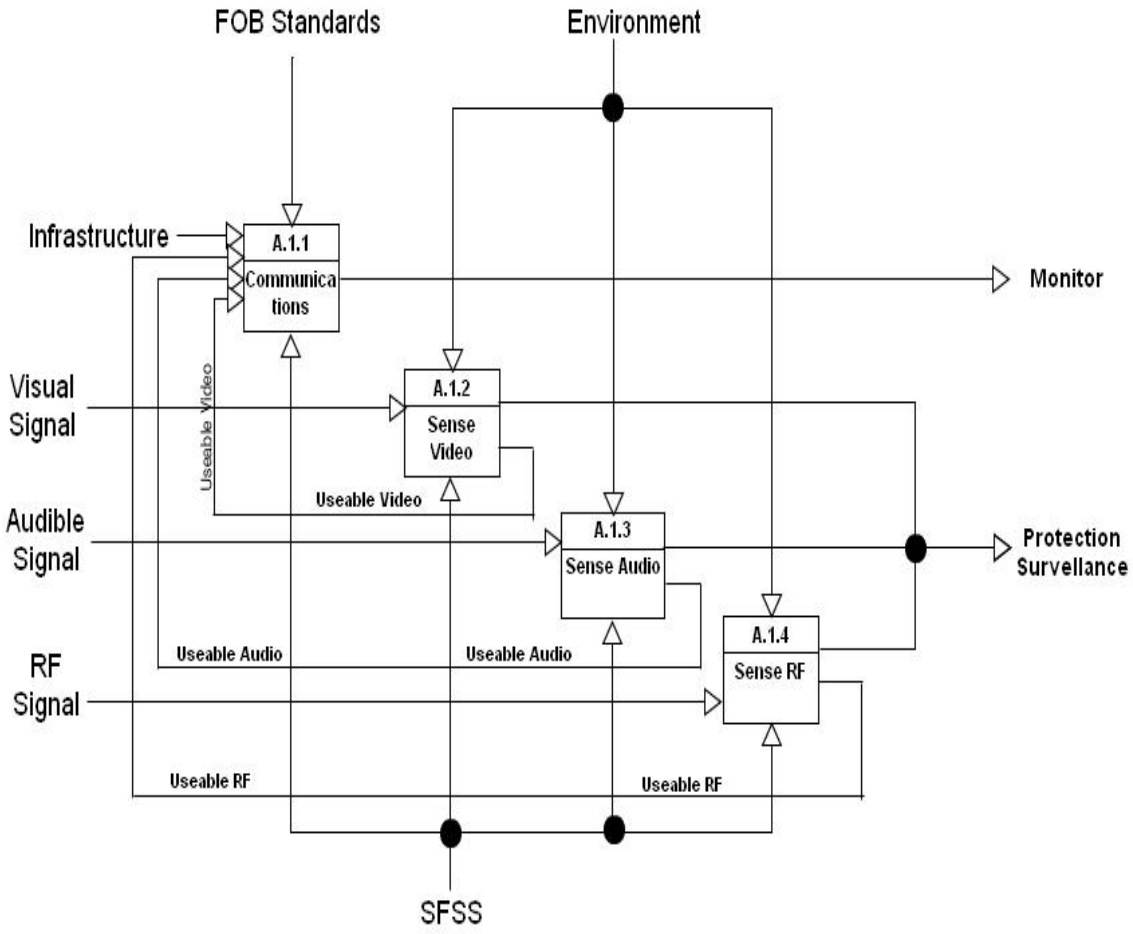

Figure 18. Decomposition of the Provide Fixed Sensor Services Function for SFSS

Figure 19 shows the decomposition of the function "Provide Mobile Sensor Services." The mobile sensors are attached to the UAVs patrolling the perimeter. The video taken by the UAVs is first processed on board for facial recognition and database comparison. The video captured by the mobile sensors is also sent to the Network Operations Center (NOC) for further behavior analysis processing and for real-time viewing by the operator.

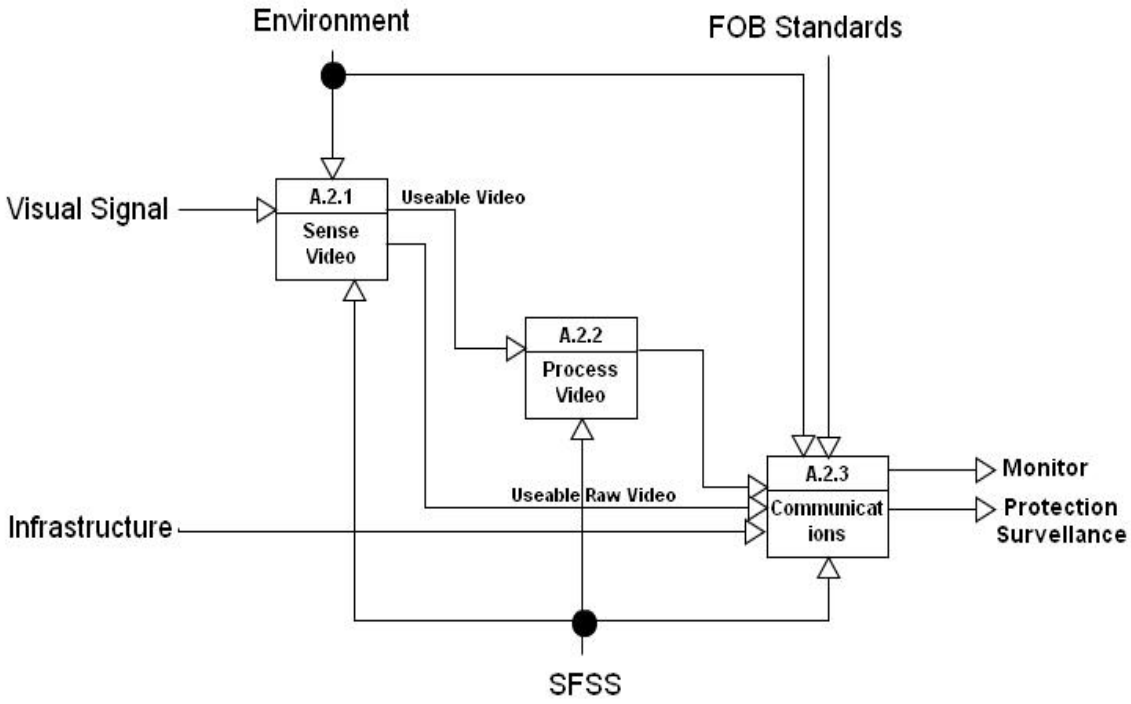

Figure 19. Decomposition of the Provide Mobile Sensor Services Function for SFSS

Figure 20 shows the decomposition of the Decomposition of the function "Provide NOC Services." This figure shows the interface of the various sensors and the processing of the sensor data being received. The model also shows the system interface with the Network Operations Center (NOC) operator, headquarters, and the Smart FOB Surveillance System (SFSS). This decomposition also further describes how the FOB infrastructure supports the Smart FOB Surveillance System (SFSS).

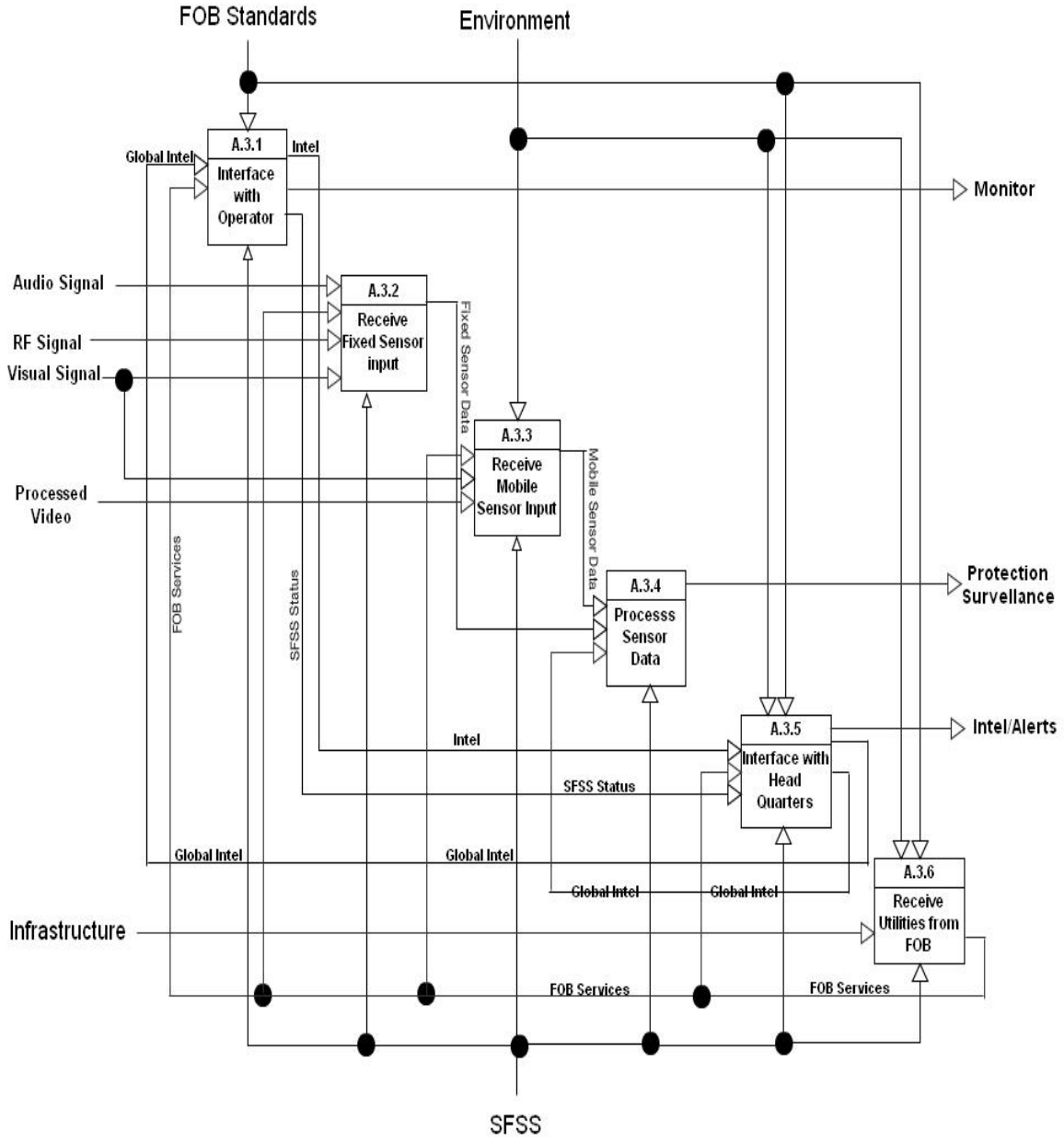

Figure 20. Decomposition of the Provide NOC Services Function for SFSS

Figure 21 shows the decomposition of the "Provide Swarm UAV Control" function. This function is performed inside the NOC, however, it is completely independent of NOC functions. The UAVs transmit their position data to Process Flight Instructions function via the NOC. The NOC also provides this function with alert data and intelligence data that would be considered when processing the proper flight paths

and organization of the UAVs during surveillance. The "Process Flight Instructions" then computes the flight orders and transmits them to each UAV in the network via the communications function.

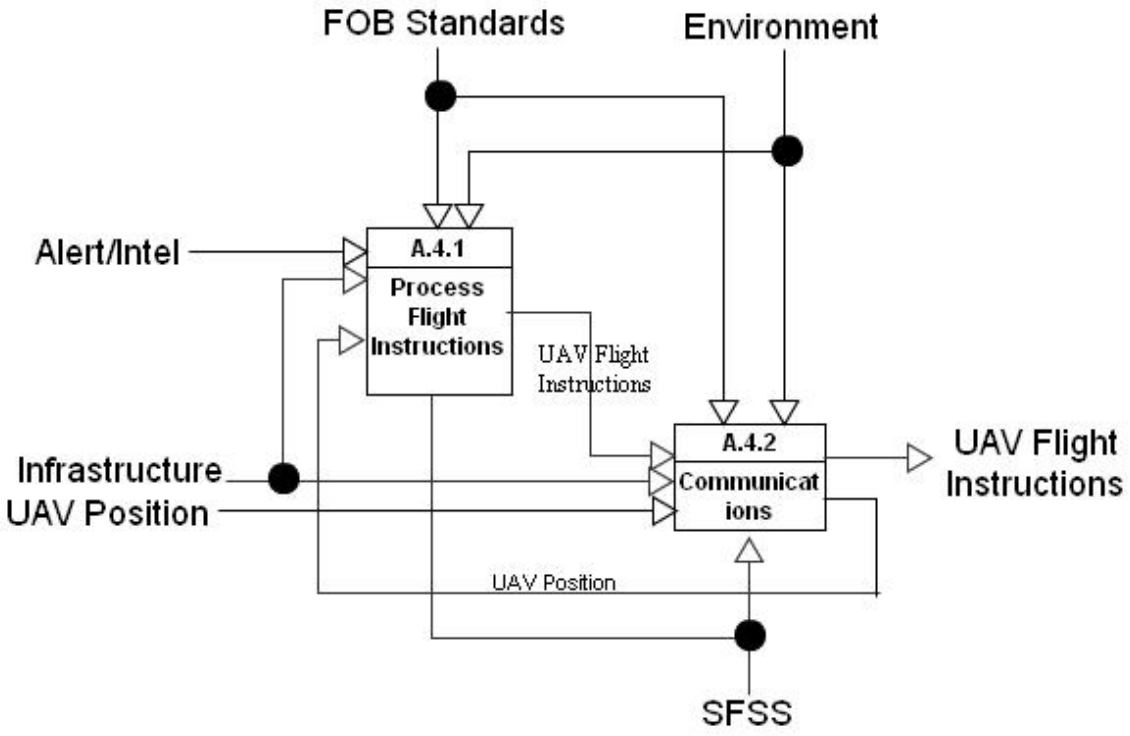

Figure 21. Decomposition of the Provide Swarm UAV Control Function for SFSS

Figure 22 shows the decomposition of the "Process Video" function. This function is performed locally on the individual Swarm UAV performing the function. The video captured is analyzed by facial recognition software and compared to a database within the identify function. The possible results are either a match to a known threat in which an alert will be generated, a match to a known non-threat in which no alert will be generated, or a non-match in which the operator must resolve by categorizing as friendly or a threat. Raw video is also sent to the Network Operations Center (NOC) for behavior analysis processing.

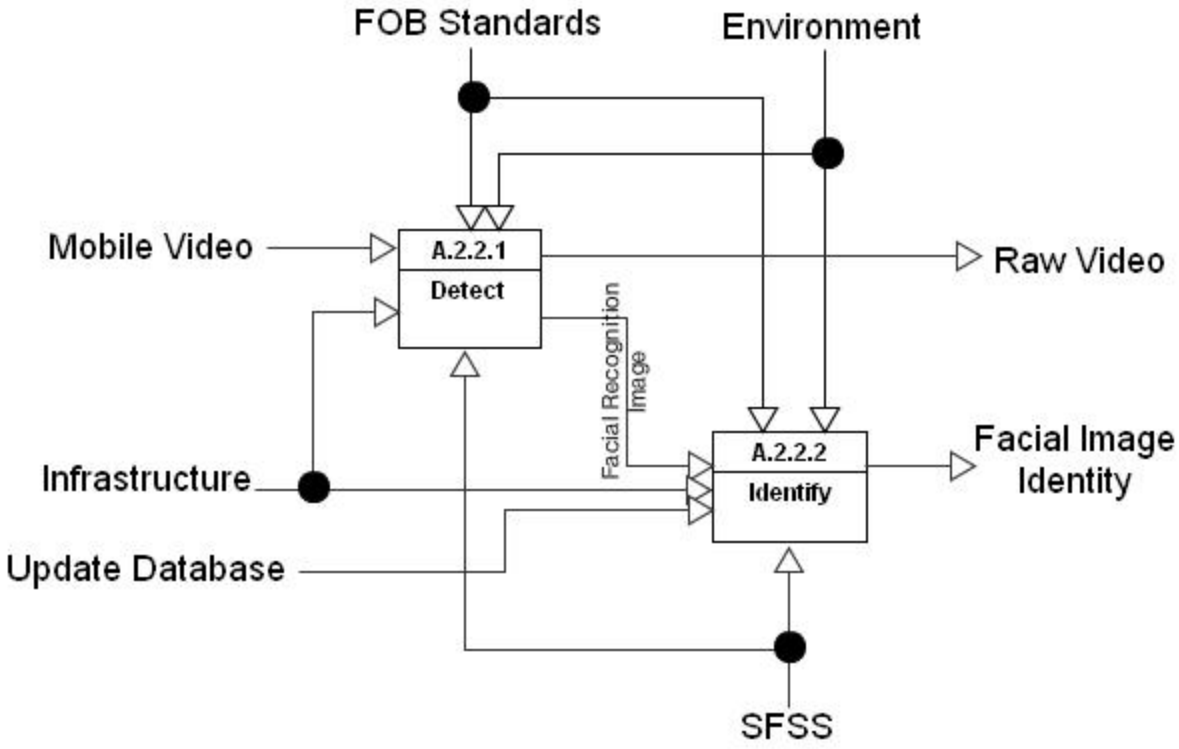

Figure 22. Decomposition of the Process Video Function for SFSS

Figure 23 shows the decomposition of the "Process Sensor Data" function. This function receives the data from both the fixed and mobile sensors. Raw video and audio can be monitored directly by the Network Operations Center (NOC) operator. The data is analyzed for threat recognition in the predict function and if the threat criteria are met for a given signal, then an alert will be issued. In the case of RF signals identified as voice communications, the RF will be demodulated for listening by the operator. The react function, will issue alerts to both the operator and headquarters as well as prompt the operator for resolution in cases where the signal processed is determined neither friendly nor hostile.

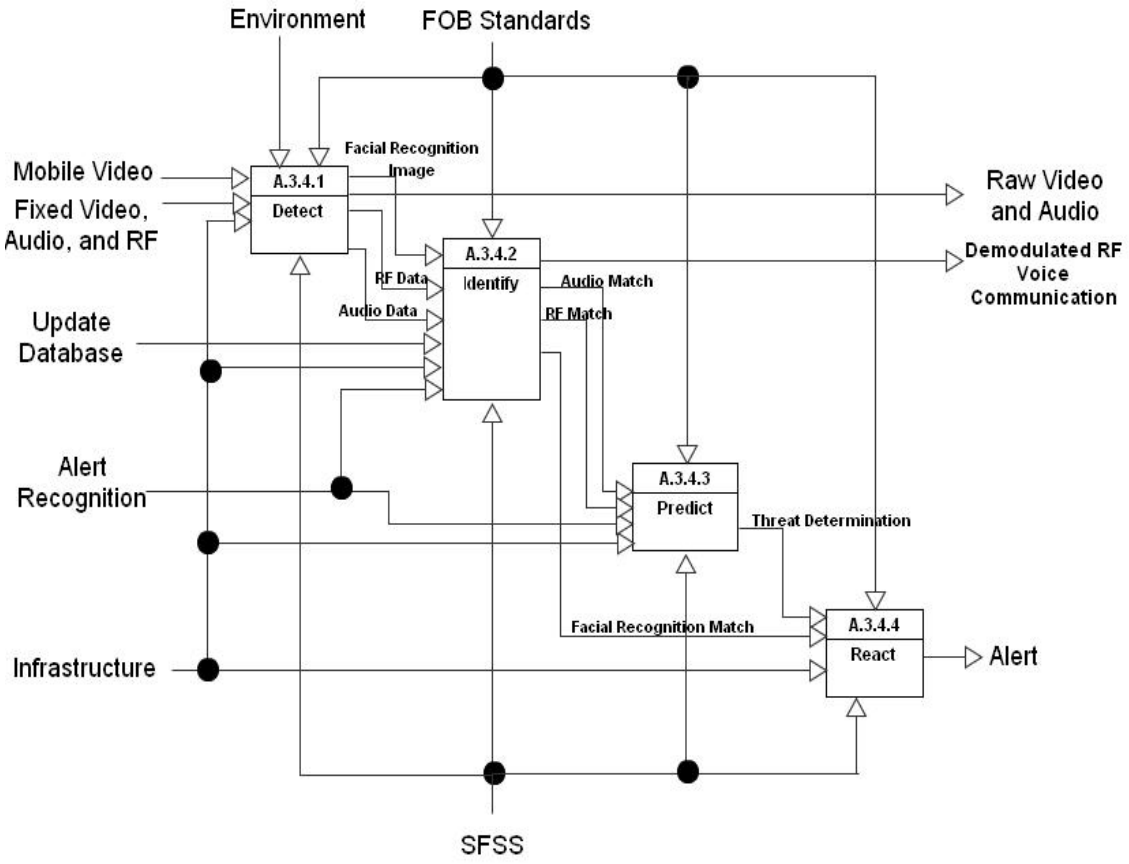

Figure 23. Decomposition of the Process Sensor Data Function for SFSS

H. GENERIC SYSTEM PHYSICAL ARCHITECTURE

The physical architecture shown in Figure 24 is modeled in hierarchal format. It defines the resources that map to each individual function illustrated in the functional architecture hierarchy. This graphic depicts how the Smart FOB Surveillance System (SFSS) decomposes from the entire system, to subsystems, components, and software modules.

Within the SFSS, the three high level systems are the Fixed Sensor system, Smart Mobile Sensor System, and the NOC System. In the subsequent sections, the vision of the physical components that comprise these sensors will be discussed.

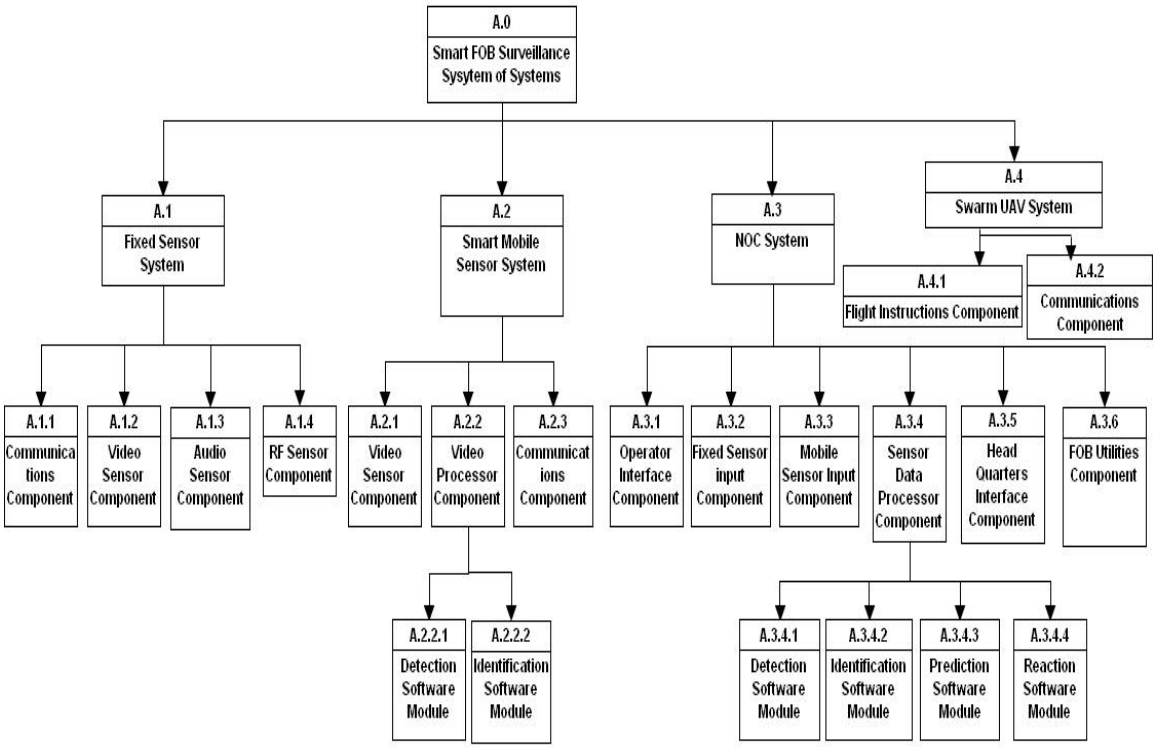

Figure 24. Generic Physical Architecture Hierarchy for SFSS

1. The Fixed Sensor System

The Fixed Sensor System is composed of three distinct sensor types. Other sensor types can be added in future development or to adapt to other applications. However, in a FOB application these were determined to provide the most fundamental level of surveillance and protection based on known threats. The three types of sensors chosen are video sensors, audio sensors, and radio frequency sensors. The sensor clusters will be physically mounted along the perimeter of the FOB to provide 360-degree coverage. The Fixed Sensor System also contains a communications component, which provides two types of signals (discussed in the functional hierarchy) by way of an Ethernet cable connected directly between the sensor and the Network Operations Center (NOC) server.

a. Video Sensor Component

Figure 25 is a picture of the Super Night Vision Outdoor AF 30X Zoom Camera. This camera has the features of the video sensor envisioned in the Smart FOB

Surveillance System (SFSS). It is capable of capturing raw video at the fidelity needed for facial recognition and behavior analysis applications. Although not a complete list of the cameras features, the following are highlights that demonstrate compatibility with the Smart FOB Surveillance System (SFSS):

- It is fully weather proof and can withstand extreme environmental temperatures.
- It is compatible with a typical FOB infrastructure.
- It has an effective range for facial recognition software of 3000 feet.
- It has an Infra-red (IR) Video range of 300 feet.
- It internally contains intelligent control technology to provide the best possible resolution for the given environment.

Figure 25. Super Night Vision Outdoor AF 30X Zoom Camera (From Security Camera World, 2012)

b. Audio Sensor Component

There are several differing technologies in todays long range listening devices. The different approaches to distance microphones result in different advantages. Some are able to focus on a very specific narrow target while others can detect noise over a large area. Examples of the three most advanced and most prevalent are shown in Figure 26 below. Acoustical amplification as seen on the left side of the figure, concentrates sound waves into a parabolic dish along a wide angled vector. Specialized software is capable of filtering out background noise as well as amplifying the signal. Shotgun microphones also seen in the figure below operate similarly to acoustical amplification; however, they sample a very narrow direction of sound and are primarily tuned to frequencies in the human voice spectrum. They are used primarily to listen to conversations. Reflective amplification and demodulation devices serve the same purpose as shotgun microphones as they also detect noise along a narrow band and they do so at a much greater range. They are based on the principle that sound waves will modulate a high frequency beam of energy when they interact. When these modulated beams are reflected back, the signal is demodulated by the device leaving the resulting sound detected. The carrier signal can be in the microwave, infrared, or laser spectrums (Mes Innovations, 2005).

Figure 26. Long Range Listening Devices (From Mesinnovation.com, 2005)

For the purposes of the Smart FOB Surveillance System (SFSS) the type of long range listening device most functional is an acoustical amplification device with a fitted parabolic dish. The purpose of the audio sensor in this system is not to detect sounds along a narrow width or to even detect and listen to voices at a distance, but rather to detect sounds in as wide a band as possible at a fidelity that can then be compared to a database of sounds that signify a contact of interest. These sounds can then be processed for threat determination and directionality, and the location of the source can be triangulated.

c. RF Sensor Component

Figure 27 is the Agilent N6841A RF Sensor. This sensor provides the radio frequency detection capabilities needed by the Smart FOB Sensor System (SFSS). It is capable of capturing a wide spectrum of radio frequencies used for identification and analysis. This particular model houses its own proprietary software, which allows it, when used in concert with additional sensors, to triangulate the RF source location. The following are some characteristics of this device that make it an ideal sensor for the Smart FOB Surveillance System (SFSS) (Agilent Technologies, Inc., 2000–2013):

- It is weather proof and can withstand temperatures -15°C to 55°C.
- It is compatible with a typical FOB infrastructure.
- It has an effective range of 3 km.
- It contains a 20 MHz to 6 GHz Wideband RF receiver with 20MHz bandwidth.
- It has two wide dynamic range switched RF inputs.
- It has a timing accuracy of less than 20ns.

Figure 27. Agilent N6841A RF Sensor
(From Agilent Technologies, Inc., 2000–2013)

d. Communications Component

The communications component of the fixed sensor system is the Ethernet cabling that runs from the sensor locations along the perimeter of the FOB to the Network Operations Center (NOC). It is required to transfer the data received by the sensors to the NOC and to provide operator interface with the sensors when required. To ensure compatibility, other components may need to be added depending on which the sensor manufacturer and the software used.

2. The Smart Mobile Sensor System

The Smart Mobile Sensor System contains a video sensing component, a video processor, and a communications component. All three of these components are contained internally to each UAV in the swarm. Figure 28 is the Dragon Flyer X6 as an onboard video platform.

Figure 28. Dragon Flyer X6 (From Draganfly Innovations Inc., 2013)

The on board video camera is a lightweight Panasonic TM-900 that captures data at 60fps, with a resolution of 1080p, and effective range of 2km. The video can be stored on a 60Gb hard drive, which correlates to about 5 hours of video or processed and transmitted directly via an FM data link that is supported by the Smart FOB Surveillance System (SFSS) (Draganfly Innovations Inc., 2013). Video processing and the initial analysis of the video is done on board the UAV. Internally, the UAV contains enough processing and storage capability to house the detection and identification software modules.

The FM data link operates in the 20–25 MHz of bandwidth, which can give connectivity to about 75 miles. However, due to the power restriction as a result of limited battery weight capacity this is reduced can be reduced to about 5 miles, which provides the intended swarm UAV coverage area around the FOB. The FM data link provides the interface for the NOC operator as well as the ability to transmit processed data to the NOC as discussed. In addition, the FM data link provides the UAV with flight

instructions with the NOC acting as the swarm node that receives flight information from all UAVs and then transmits flight directions back to each UAV.

3. The NOC System

The Network Operations Center (NOC) System is the control center for the Smart FOB Surveillance System and comprises the majority of the processing and analysis of the sensor outputs. The Operator Interface Component and the Headquarters Interface Component will consist of multiple LCD displays for ease of use and a keyboard to enter data manually into the system in order acknowledge alerts and interface with headquarters, and a headset and speakers for voice communications and audio signal listening. The Fixed Sensor Input Component, Mobile Sensor Input Component, the Sensor Data Processor Component, and associated DIPR software Modules are housed in a server rack in the NOC. The FOB Utilities Component is made up of hardware that ensures compatibility between the FOB infrastructure and the NOC and will be uniquely tailored for the given NOC. Figure 29 depicts the NOC System physical architecture.

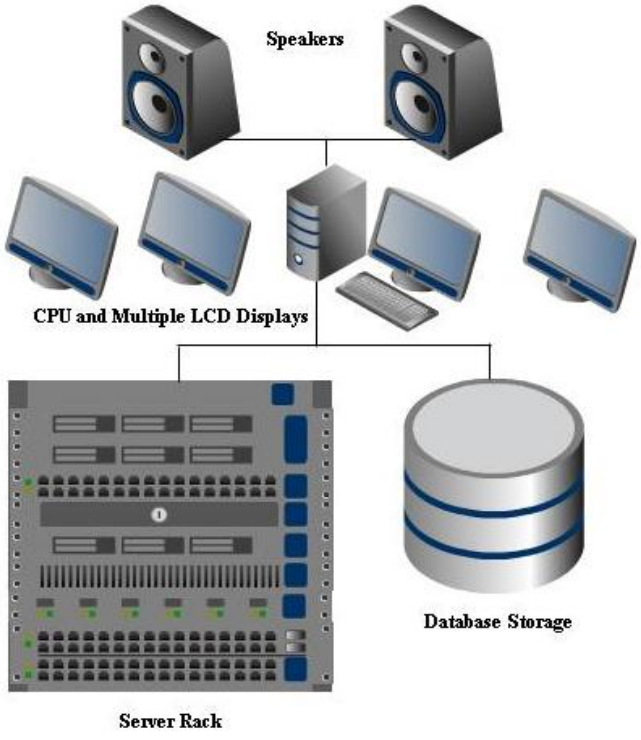

Figure 29. NOC System Components

I. GENERIC SYSTEM OPERATIONAL ARCHITECTURE

The operational architecture is where the physical and functional architecture of the Smart FOB Surveillance System (SFSS) meet. Table 1 shows how each element of the functional architecture matches to a function: system, subsystem, component, or module of the physical architecture. It is the complete description of the Smart FOB Surveillance System (SFSS) design. There are no unneeded physical parts. The operational architecture also shows that functions are carried out in the physical design.

Functional Architecture		Physical Architecture	
A.0	Provide SFSS Services	A.0	Smart FOB Surveillance System of Systems
A.1	Provide Fixed Sensor Services	A.1	Fixed Sensor System
A.1.1	Communications	A.1.1	Communications Component
A.1.2	Sense Video	A.1.2	Video Sensor Component
A.1.3	Sense Audio	A.1.3	Audio Sensor component
A.1.4	Sense RF	A.1.4	Sense RF Component
A.2	Provide Smart Mobile Sensor Services	A.2	Smart Mobile Sensor System
A.2.1	Sense Video	A.2.1	Video Sensor Component
A.2.2	Process Video	A.2.2	Video Processor Component
A.2.2.1	Detect	A.2.2.1	Detection Software Module
A.2.2.2	Identify	A.2.2.2	Identification Software Module
A.2.3	Communications	A.2.3	Communications Component
A.3	Provide NOC Services	A.3	NOC System
A.3.1	Interface with Operator	A.3.1	Operator Interface Component
A.3.2	Receive Fixed Sensor input	A.3.2	Fixed Sensor Input Component
A.3.3	Receive Mobile Sensor Input	A.3.3	Mobile Sensor Input Component
A.3.4	Process Sensor Data	A.3.4	Sensor Data Processor Component
A.3.4.1	Detect	A.3.4.1	Detection Software Module
A.3.4.2	Identify	A.3.4.2	Identification Software Module
A.3.4.3	Predict	A.3.4.3	Prediction Software Module
A.3.4.4	React	A.3.4.4	Reaction Software Module
A.3.5	Interface with Head Quarters	A.3.5	Head Quarters Interface Component
A.3.6	Receive Utilities from FOB	A.3.6	FOB Utilities Component
A.4	Provide Swarm UAV Control	A.4	Swarm UAV System
A.4.1	Process Flight Instructions	A.4.1	Flight Instructions Component
A.4.2	Communications	A.4.2	Communications Component

Table 2. Operational Architecture Matrix for SFSS

This chapter used the left side of the Systems Engineering Vee model to develop the required Systems Engineering products. Once the operational need an operational concept were derived, the various operational scenarios were defined that that were used to bound and scope the system. From there additional Systems Engineering products were developed. The External Systems Diagram led to the requirements of the system. Finally, the functional, physical, and operational architectures were developed.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY AND CONCLUSIONS

A. SUMMARY

The current method for FOB surveillance is manpower intense and unnecessarily dangerous. In our current operational environment we do not have the resources to reliably detect and recognize threats. There exists a critical need for autonomous continuous surveillance of vulnerable targets such as Forward Operating Bases (FOB). A formal analysis of this problem was performed using the systems engineering design approach. The systems engineering "V" model was used to develop the operational requirements and operational concept. From this a list of operational scenarios were developed to scope the system by creating the boundaries of the tasks the Smart FOB Surveillance System (SFSS) was to perform. From the scenarios, an External Systems Diagram was developed to illustrate how the system was to interface with the external systems of FOB. Requirements were then established for the system . By establishing the requirements of the system the Functional Architecture Hierarchy was developed. Each function contained within was then decomposed to the most basic processes, showing how inputs, outputs and constraints trace through the functions, using IDEF0 modling. In order to further define the system, the Physical Architecture Hierarchy was then developed. Finally, an Operational Hierarchy matrix was created to map each function to a subsystem, component, or software module.

B. CONCLUSION

This thesis demonstrates that a highly intelligent and autonomous surveillance and detection system will greatly enhance security and safety of a Forward Operating Base (FOB). This research shows that the possibility exists to improve the agility and effectiveness of such a system on many fronts, as compared to traditional systems that rely heavily on available resources and manpower to operate. In addition, those traditional systems have an innately high degree of error due to their many human interfaces. This is in stark contrast to the potential created when the human interfaces and

functions performed by humans are replaced with Intelligent Automation (IA). IA improves the detection quality and minimizes the quantity of people required.

The utilization of Swarm UAVs to act as a mobile sensor platform greatly enhances agility and efficiency. Operators are no longer required to operate the UAVs, nor walk the FOB surrounding areas for surveillance, which is extremely dangerous. Instead, these UAV platforms will operate independently and autonomously to react in their environment and the objects of interest in the battle space. This automation will result in more efficient patrol patterns, provide more coverage of an area, and react more quickly to potential threats. Multi-Agent Systems and Distributed Intelligence is incorporated by spreading out computing and processing requirements throughout many of the subsystems. This improves bandwidth efficiency and reduces the possibility for data and processing bottlenecks leading to a much more agile system. Utilizing the DIPR concept again reduces human interface. Raw sensor data can be processed in an intelligent system much faster than a trained operator. Use of DIPR eliminates most of the mundane tasks performed by a human operator in order manipulate the data to the point that it is actually useful. In addition, the concept of behavior analysis, in the Prediction subsystem of the DIPR system, greatly improves reaction time. This behavior analysis algorithm detects certain predefined behaviors; this is an area of significant research where “learning” behaviors in an area of operations is underway; with learning, the operator will not need to input predefined known behaviors.

These improvements in traditional surveillance, monitoring, and threat recognition methods are also done at lower man-power requirements to the commanders deploying such system. This all leads to FOB commanders having much better situational awareness, which in turn improves their ability to protect their FOB and assets as well as gather intelligence that can be shared with other commanders.

Much more work is required to further the research performed while developing this thesis in order to realize an actual working system. While this thesis focused on the left side of the Systems Engineering V-model, the right side of the model must be followed as well. This will include the detailed design and implementation for the development of a prototype followed by integration, testing and evaluation, and fielding. These systems engineering products can then be scaled to a real-world systems solution for autonomous and automated surveillance.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Blanchard, B. S., & Fabrycky, W. J. (2006). *Systems engineering and analysis*. Englewood Cliffs, NJ: Prentice-Hall.

Bonabeau, E., Dorigo, M., & Theraulaz, G. (1999). *Swarm intelligence from natural to artificial systems*. New York: Oxford University Press.

Buede, D. M. (2000). *The engineering design of systems: models and methods*. New York: John Wiley & Sons, Inc.

Department of Defense. (2007). *Architecture framework version 1.5*. Washington, DC: Author

Department of Defense Chief Information Officer Memorandum. (2003). *Department of Defense net-centric data strategy.* Washington, DC: Author.

Department of Defense. (2001). *Network centric warfare, Department of Defense report to congress*. Washington, DC: Author.

Department of Defense, Office of Force Transformation. (2005). *The implementation of network-centric warfare*. Washington, DC: Government Printing Office.

Ferber, J. (1999). *Multi-agent systems: an introduction to distributed artificial intelligence*. London: Addison-Wesley Professional.

Forsberg, K., & Mooz, H. (1992). "*The relationship of systems engineering to the project cycle*." Engineering Management Journal, 4, No. 3, pp. 36–43.

Goshorn, R. E., Goshorn, D. E., Goshorn, J. L., & Goshorn, L. A. (May 2011). "The need for distributed intelligence automation implemented through four overlapping approaches: intelligence automation software, standardization for interoperability, network-centric system of systems infrastructure (with advanced cloud computing) and advanced sensors," GMU–AFCEA Symposium.

Goshorn, R. E., Goshorn, D.E., Goshorn, J. L., & Goshorn, L. A. (2010). "*Behavior modeling for detection, identification, prediction, and reaction (DIPR) in AI systems solutions.*" for Journal of Ambient Intelligence and Smart Environments (JAISE), Springer Handbook , 2010.

Goshorn, R. E., Goshorn, D. E., Goshorn, J. L, .& Goshorn L.A. (2009). "Abnormal behavior classification and alerting through detection, identification, prediction and reaction (DIPR) system applied to a multi-camera network," submitted to the Workshop on Behavior Monitoring and Interpretation: Moving Objects in a Three Dimensional World.

Joint Concepts and Capabilities Division (JCCD). 20 September 2011. dtic.mil. Retrieved from http://www.dtic.mil/futurejointwarfare/index.html

Joint Net-Centric Operations (JNO) Capability Portfolio Management (CPM). 16 April 2007. DoDcio.defense.gov. Retrieved 20 April2011. http://DoDcio.defense.gov/Portals/0/Documents/JNO_Business_Plan.pdf

Net-Centric Enterprise Solutions for Interoperability (NESI). 07 May 2007. *Mike Dettman Deputy APEO for Engineering,*. navy.mil. Retrieved from http://www.afcea-sd.org/wp-content/uploads/2009/05/dettman-afcea-c4isr-final-20090507.pdf.

Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. 2007. Net centric attributes list. Retrieved from http://semanticommunity.info/Network_Centricity/U.S._DoD_Net-Centric_Attributes#2_ASD(NII).2FDoD_CIO_Net-Centric_Attributes

Padhy, N. P. (2005). *Artificial intelligence and intelligent systems.* New Dehli, India: Oxford University Press.

Schafer, D. C. (2009). "*A systems engineering survey of artificial intelligence and smart sensor networks in a network-centric environment*," (Master's thesis, Naval Postgraduate School). Retrieved from http://www.researchgate.net/publication/235091835_A_Systems_Engineering_Survey_of_Artificial_Intelligence_and_Smart_Sensor_Networks_in_a_Network-Centric_Environment

United States Air Force. (2008). Analysis of alternative (AoA) handbook: a practical guide to analysis of alternatives. Kirtland AFB, NM: Air Force Materiel Command (AFMCs) Office of Aerospace Studies (OAS).

Vlassis, N. (2007). "*A concise introduction to multiagent systems and distributed artificial Intelligence*," in R.J. Brachman and T.G. Dietterich (Editors), *Synthesis Lectures on Artificial Intelligence and Machine Learning,* vol. 1, San Rafael, CA: Morgan and Claypool.

Weiss, G. (1999). *Multiagent systems: a modern approach to distributed artificial intelligence.* Cambridge, MA: The MIT Press.

Woo, G.. (2009). "Terrorism threat assessment and management." Risk Management Solutions, London EC3R 8NB. Keynote lecture given at the NATO Centre of Excellence: defence against terrorism Ankara, Turkey.

Wooldridge, M. J. & Jennings, N. R. (1995). *Intelligent agents: theory and practice*. The knowledge Engineering Review, 2(10).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California