NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RULES OF ENGAGEMENT POLICIES AUTOMATION FOR BALLISTIC MISSILE DEFENSE SYSTEM

by

Joshua Sanders

December 2009

Thesis Co-Advisors: Man-Tak Shing
James Bret Michael

Approved for public release; distribution is unlimited

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

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE: Rules of Engagement Policies Automation for Ballistic Missile Defense System	**5. FUNDING NUMBERS**
6. AUTHOR: Joshua Sanders	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT (maximum 200 words)

Military decision making in this current age of Warfare requires the most effective and expedient action in response to threats. In the domain of Ballistic Missile Defense (BMD), response actions must be near automatic in order to be effective. This work discusses policy automation systems and suggests a BMD System that takes into account the automation of Rules of Engagement (ROE) policies and presents an architecture for such a system.

Automated policies govern the decision-making processes of the system. Given accuracy/success and elapsed time in missile defense, it is not feasible for humans be in the decision loop other than for making overrides. The computer is required to do all the policy checking, monitoring and enforcement. The ROE policy automation is a vital link to the ultimate success or failure of a BMD program.

14. SUBJECT TERMS Policy, Policy Automation, Rules of Engagement, ROE, Ballistic Missile Defense System, BMD	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RULES OF ENGAGEMENT POLICIES AUTOMATION FOR BALLISTIC MISSILE DEFENSE SYSTEM

Joshua J. Sanders
Lieutenant Commander, United States Navy
B.S., Savannah State University, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2009

Author: Joshua J. Sanders

Approved by: Dr. Man-Tak Shing
Thesis Co-Advisor

Dr. James Bret Michael
Thesis Co-Advisor

Dr. Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Military decision making in this current age of Warfare requires the most effective and expedient action in response to threats. In the domain of Ballistic Missile Defense (BMD), response actions must be near automatic in order to be effective. This work discusses policy automation systems and suggests a BMD System that takes into account the automation of Rules of Engagement (ROE) policies and presents an architecture for such a system.

Automated policies govern the decision-making processes of the system. Given accuracy/success and elapsed time in missile defense, it is not feasible for humans be in the decision loop other than for making overrides. The computer is required to do all the policy checking, monitoring and enforcement. The ROE policy automation is a vital link to the ultimate success or failure of a BMD program.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY

Acquisition: The process in which the Department of Defense obtains materiel solutions to identified problems in mission need statements.

Active component: A component that will execute based on external conditions and a defined set of rules.

Architecture: the collection of logical and physical views, constraints, and decisions that define the external properties of a system and provide a shared understanding of the system design to the development team and the intended user of the system.

Automation: is the use of control systems such as computers to control industrial machinery and processes, replacing human operators.

Availability: The probability that a system is operating correctly and is ready to perform its desired functions.

Backward Chaining: Beings with a list of goals (or a hypothesis) and works backwards from the consequent to the antecedent to see if there is data available that will support any of these consequents.

Battle management: The decisions and actions executed in direct response to the activities of enemy forces in support of the Joint Chiefs of Staff’s precision engagement concept.

Battlespace constraints: The forces, facilities, and other features that serve to restrain, restrict, or prevent the implementation of proposed military improvements in the

defined battlespace. Constraints may include natural and physical forces, doctrine, potential adversary threats, and environmental features.

Battlespace: The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest.

Capability: The ability to perform a course of action or sequence of activities leading to a desired outcome.

Chain of command: The succession of commanding officers from a superior to a subordinate through which command is exercised.

Close-air-support: Air action by fixed- and rotary-wing aircraft against hostile targets that are in close proximity to friendly forces and that require detailed integration of each air mission with the fire and movement of those forces.

Coalition: An ad hoc arrangement between two or more nations for common action.

Combatant command (command authority): Non-transferable command authority established by title 10, United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) is the authority of a combatant commander to perform those functions of command over

assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command.

Combatant command: One of the unified or specified combatant commands established by the President.

Command and control system: The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.

Command and control: The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (JCS/J7/Joint Doctrine Division memo dated 20 Oct 94).

Completeness: A logical system is complete if everything that we want can be derived in it. Thus a formalization of logic is complete if all logically valid forms of argument are derivable in the system.

Component: A software unit of composition with contractually specified interfaces and explicit context dependencies.

Computer Network Operations: Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Control: Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations.

Correctness: A characteristic of a system that precisely exhibits predictable behavior at all times as defined by the system specifications. That is, a system that is said to demonstrate correctness does the right thing all the time.

Cyber Engagement: an engagement that takes place in the domain of cyberspace.

Data: A representation of individual facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. [IEEE]

Dependable system: One that provides the appropriate levels of correctness and robustness in accomplishing its mission while demonstrating the appropriate levels of availability, consistency, reliability, safety, and recoverability.

Design: The details of planned implementation which are defined, structured, and constrained by the architecture

Distributed system: A system that has multiple processors that are connected by a communications structure.

Engagement: 1. In air defense, an attack with guns or air-to-air missiles by an interceptor aircraft, or the launch of an air defense missile by air defense artillery and the

missile’s subsequent travel to intercept. 2. A tactical conflict, usually between opposing lower echelons maneuver forces.

Forward chaining: It is one of the two main methods of reasoning when using inference rules starts with the available data and uses inference rules to extract more data until an end state is reached.

Information: The meaning that a human assigns to data by means of the known conventions used in their representation.

Intelligence: The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

Interoperability: The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.

Model: A representation of a physical system or process intended to enhance the software engineer’s ability to understand, predict, or control its behavior.

Multiple inheritance: refers to a feature of some object-oriented programming languages in which a class can inherit behaviors and features from more than one super class

Requirement: A criterion that a system must meet. A requirement may define what a system must do, characteristics it must have, and levels of performance it must attain.

Rules of engagement: Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered.

Subsystem: A testable collection of classes, objects, components, and modules that typically share a common attribute or contribute to a common goal.

System-of-Systems: An amalgamation of legacy systems and developing systems that provides an enhanced military capability greater than that of any of the individual systems within the system-of-systems.

LIST OF ACRONYMS AND ABBREVIATIONS

AKO	A Kind Of
BMD	Ballistic missile defense
C2	Command and Control
C3	Command, Control and Communication
COCOM	Combatant Commander
CP	Control Panel
CU	Control Unit
DIU	Deployment Interface Unit
GUI	Graphical User Interface
ICP	Interface Connector Panel
ICBM	Intercontinental Ballistic Missile
IRBM	Intermediate Range Ballistic Missile
JCS	Joint Chiefs of Staff
LA	Lexical Analyzer
MDA	Missile Defense Agency
NCA	National Command Authority
OOB	Operational order of battle
PWB	Policy Workbench
ROE	Rules of engagement
ROEU	Rules of Engagement Unit
SDI	*Strategic Defense Initiative*
SLBM	*Submarine-Launched Ballistic Missile*
SROE	*Standing* Rules of Engagement
SSBN	Submarine Ballistic Nuclear
USJFCOM	United States Joint Forces Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Thank God for the strength and the opportunity. To my wife, Valorie, thank you for all your support and encouragement allowing me the time away from the family, and inspiring me to accomplish this work. To Gabrielle and Joshua, this is for you, I love you. To my parents and family, thank you for believing in me. Thank you Pastor Lusk and Harold for helping me stay focused. To Jay, Brandy and Michelle, thank you. To professors Shing and Michael for your guidance and patience. You have been a blessing to me, thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

As far back as the events that took place in the bible, there was the concern of war or the threat associated with such events. Overtime, the weapons used to wage war have evolved from merely throwing fists, to rocks, to cannon balls, to bullets, and now, to highly precise and extremely destructive nuclear capable missiles. In addition to the threats of particular weapons systems, there is an increasing concern of leaders who have professed to be willing to use them. In the period of the Cold War, 1947–1991, there was fear of the weapon, but also there was the unspoken knowledge that neither side really intended to resort to that level of conflict with one another due to the catastrophic results. In this new era, when there are countries with those capabilities and leaders who have the professed willingness to use it, there is heightened concern to protect oneself from the potential that a missile strike could be pointed in our direction. This threat is not limited just to countries that posses these capabilities but also from terrorist groups that aim to disrupt and destroy our way of life.

An effective missile defense will guard the U.S. and her allies against becoming susceptible to the nuclear or any other type of threat initiated by other nations or rouge actors. The United States needed to pursue a system for defense of the homeland, as well as its allied

countries. This defense is against a limited attack by a rogue nation or unauthorized or limited objective attack (ULOA).

Despite the research and development effort taken in the past eight years, even today as reflected in the latest discussions on missile defense, we still have not accomplished the goal of establishing a viable Missile Defense System for the United States. This fact was best illustrated on September 29, 2009, when John Issacs was quoted in an Associated Press article by Richard Lardner titled *New missile defense plan bets on Navy interceptors* stating "I don't think you can really count on any missile defense system at this point." John Issacs is the executive director of the Center for Arms Control and Non-Proliferation in Washington.

B. PURPOSE OF THE STUDY

The task of this work is to use software engineering methods to analyze and propose the design of a Ballistic Missile Defense System that takes into account the automation of Rules of Engagement (ROE) polices. We apply use case analysis to understand the roles ROE plays in various missile defense scenarios. We study the architecture of existing policy automation systems for various domains and develop a design for a Rules of Engagement Unit (ROEU) necessary for the Battle Manager of the Ballistic Missile Defense System with ROE polices automation capabilities. We also present the architecture of a “Generic Intercept System” to show how the proposed ROEU system, when interfaced appropriately, can work with existing components of the missile defense.

1. What is a Policy?

As we begin the discussion, we need to explore the general idea of policy automation for distributed systems. This will bring us closer to realizing the complete creation of the proposed system. Automated ROE policies, as a system or a component, can be effectively utilized in any environment whether that is missile defense or defense of weapons in the non-kinetic realm of Computer Network Operations. The main premise to understand is that automated ROE policies are necessary and vital for BMD or intercept system success.

We begin this discussion with a generalized definition of policy, created by Strassner (2004) to be extensible for various domains, including the military domain. Policy is a set of rules that are used to manage and control the changing and/or maintaining of the state of one or more managed objects. Reis et al. sees policies as generic and reusable rules that allow definition of: syntactic properties for process models (static); instantiation strategies (instantiation); and reaction strategies in response to dynamic events. Policies are best understood as the rules that govern or influence the behavior of a particular system.

C. ORGANIZATION OF THE THESIS

At the end of Chapter I, the reader will walk away with a solid foundation and understanding of the purpose for this work. They will know what a policy is. Chapter II begins with a review of what work has already been done with regards to missile defense. We then discuss ROE and why automation of ROE is so important. Chapter III

provides examples of policy automation systems. We will present the primary model for our suggested Ballistic Missile Defense System, which we call a “Generic Intercept System.” We have identified processes and systems that are already in existence to realize our proposed design. In Chapter IV, we will discuss the ROE Unit (ROEU) that will be designed and used as an automated policy system. The discussion will cover the development of a design for such a system. There will be a discussion of the process for creating the ROE policies. Specific components of the proposed system are addressed. Scenarios will be created in order to evaluate the system in a perceived environment—from these scenarios use case and activity diagram will be presented. Such diagrams reflect the interfaces with the system and the process or actions of the system given a particular situation. We will provide examples of key elements of the ROEU to include a proposed ontology for the Missile Defense Domain, as well as rules for the ROE polices that are compatible with a Policy model. Finally, in Chapter V, we will conclude with a summary of this work and recommendations for future research. We show one primary example being the requirements analysis of a policy automation system and then list out a few other future work areas.

II. MISSILE DEFENSE AND ROE

A. BACKGROUND OF MISSILE DEFENSE AND THE "ABM"

1. What Work has Been Done?

In March of 2005, Dr. Dale Scott Caffall wrote his doctorial dissertation on the topic "Developing Dependable Software for a System of Systems." There are many roads open before us, but none that are paved now started without a beaten path. Dr. Caffall was not the first, but his direction has provided significant influences for this thesis. With regards to the specific contributions that were made by his work in the area of missile defense, there are quite a few. These contributions include the identification of distributed-system attributes for controlling software in a system-of-systems, and the identification of real-time attributes for real-time controlling software in a reactive system-of-systems. He contributed to the development of system-of-systems architecture views from system-of-systems view to component view in controlling software. He also addressed the use of a kernel in controlling software for system-of-systems to shape dependable behavior of said system-of-systems. He has proposed to reduce the complexity of a monolithic software program with a component-based construct in which the active components are decoupled by data stores. He discussed the development of assertions using collaboration diagrams (Caffall, 2005).

Dr. Caffall's research shows the possibility of developing a system-of-systems architecture from which we can analyze/develop the controlling software for a system-

of-systems. It demonstrates that we can realize the controlling software from a system-of-systems architecture through the concepts of component-based software engineering. More importantly, we are able to apply formal methods in the design and development of the controlling software for a system-of-systems by specifying the requirements for the software components with assertions and employing a runtime verification tool to verify the desired behavior specified in the assertions.

In addition, Caffall's work addresses some of the challenges posed by David Parnas in 1985 to the Department of Defense on the Strategic Defense Initiative (SDI). David Parnas was one of the original pioneers in the efforts to develop a successful missile defense program. Parnas' six major concerns are articulated as:

> 1. Discrimination of the threat objects from decoys and debris is a significant challenge. 2. Software developers cannot predict the behavior of the battle-management software with confidence of system given the actual configuration of weapons, sensors, and battle managers are not known until the moment of battle. 3. Software developers cannot test the battle-management software under realistic conditions. 4. The duration of the defense engagement will be short. It will not allow for either human intervention or debugging the software to overcome software faults at runtime. 5. Battle-management software will have absolute real-time deadlines. 6. Battle-management software must integrate numerous dynamic software systems to the extent that has never before been achieved. (Caffall, 2005)

It is clear that there is a direct relation between policy automation, the development of the battle manager and further development of the controlling software for a

system of systems. In Caffall's work, the automated ROE policies are just a small function of the whole and the specific policies that will be housed exist in the ROE data store. Automated ROE policy of the BM for a Generic Intercept System will be similar. According to Caffall's work, the "ROE data store contains the rules of engagement (ROEs) as set in the BMD planning phase to include shot doctrine, firing trigger (e.g., first available shot, Ninety percent probability of kill (P_K), desired interceptor reserve)" (Caffall, 2005). In Figure 1, the ROE Data store is identified by the blue arrow, as it is a small portion of the Weapons Assignment System.

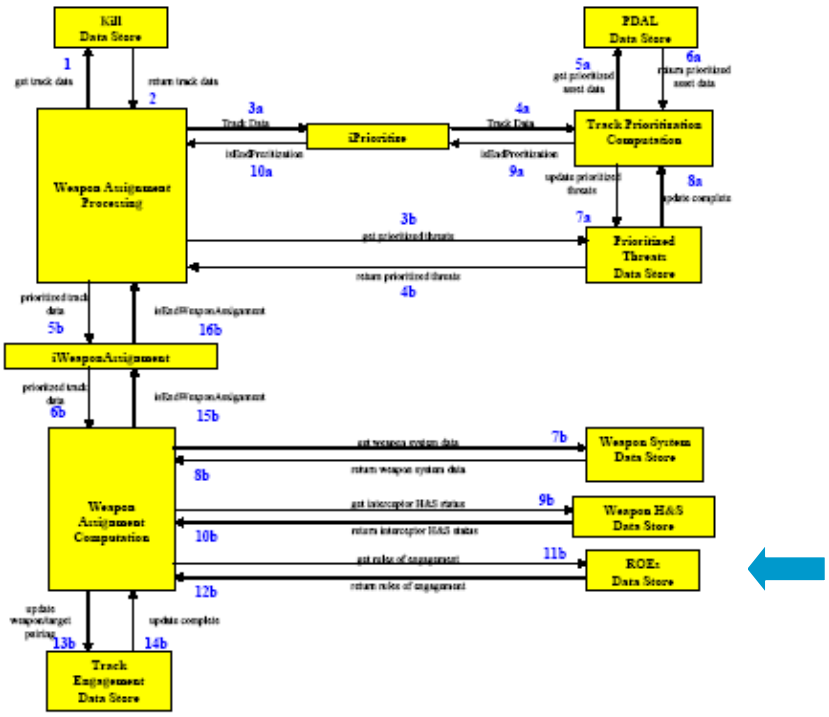

Figure 1. Weapon Assignment (From Caffall,2005)

In Dr. Caffall's work, the command and control (C2) subsystem is the system that sets the parameters for the battle manager. These parameters are, in essence, the policies that are discussed in this thesis. Depending on the particular C2 subsystem, each battle manager will employ the appropriate C2 parameter or policies assigned to it. He gave an example of a theater battle-manager being filled with rules of engagement policies that are specific to that theater but not applicable to the Homeland Battle Manager. The ROE are defined for the theater battle manager must be transferred into that specific theater battle-manager and no others. Caffall calls this process, the tailoring of a battle manager to its specific mission, in the BMD battlespace.

Before moving forward with this discussion, it is important to understand what ROE are, how ROE will affect the battlespace, and why it is necessary for them to be automated.

B. GENERAL ROE DISCUSSION

1. What are Rules of Engagement?

According to the Joint Pub 1-02, *Dictionary of Military and Associated Terms, ROE is defined* in the following manner:

> ROE are directives issued by competent military authority to delineate the circumstances and limitations under which its own naval, ground, and air forces will initiate and/or continue combat engagement with other forces encountered. They are the means by which the National Command Authority (NCA) and operational commanders regulate the use of armed force in the context of applicable political and military policy and domestic and international law.

Through the development of ROE, the President and National Command Authority (NCA) are able to meet national objectives. ROE governs the military's use of force to ensure that those objectives are met. During peace and wartime, *Standing* Rules of Engagement (SROE) serve as the baseline for military personnel to follow. They provide guidance, define the right to defend oneself, and act as the guidelines for the use of force. Given this, commanders are alleviated of the need to request the use of force from the higher echelon of military and/or government leadership. Based on world situations, however, these ROE may need to be altered. Life does not fit neatly in a box, and ROE are most often changed due to operational situations that require different operational tactics. The requirements, therefore, are that ROE remains consistent with national policy, military strategy, and the missions assigned by the higher authority. In order to obtain a successful outcome, it is important that those that fall within the C2 structure strictly adhere to the rules of engagement set forth by the Combatant Commanders (COCOMs).

ROE will always recognize the inherent right of a unit or an individual's self-defense. ROE must be unambiguous and therefore must: (1) fit the situation, (2) be reviewed for legal sufficiency and (3) be included in training. Rules of Engagement vary from operation to operation and often can vary midstream. Generally, ROE provides guidance and imposes limitations on the use of force by commanders and individuals based on three primary considerations. These three considerations are legal, political, and military.

The legal considerations of ROE are set forth to affirm order and discipline during the facilitation of our governmental relationships and partnerships abroad. Rules are only useful if everyone agrees to them; otherwise, they are nothing more than words. Consequently, ROE are reflections of national policy and international and domestic law.

Uniquely, political considerations drive the acceptance of missions and operations. ROE must reflect the political will of the government. A mission that lacks the general support of the people and their elected officials is doomed to failure.

If legal considerations represent the mind of Rules of Engagement, political considerations would then represent the heart, and then military considerations would serve as the arm of ROE. ROE help military personnel accomplish the mission by ensuring the use of force is executed in a manner consistent with the overall military objective. In other words, it helps to keep the military on track and in focus. It also must implement the inherent right of self-defense. ROE help prevent the unintended escalation of hostilities prior to achieving a desired readiness posture. This is achieved by developing an economy of force and preventing the destruction of enemy infrastructure that could prove important at a later date.

It cannot be overstated how important it is to understand what ROE are and their impact to the ultimate success of operations; whether they be for BMD, an amphibious assault operation or even future non-kinetic cyber engagements. Without the ROE, there is no regard for

ultimate war and complete destruction is the result. In essence, ROE keeps everything in order and on track. The ROE policies or parameters are the buffer between rational decisions and careless exchanges such as launching missiles with total disregard.

C. ROE AUTOMATION IN MISSILE DEFENSE

1. Why Automate ROE?

When drafting and implementing ROE, it can be a very difficult endeavor; however, it is a critical issue when planning and executing various types of operations. As stated earlier, in any operation ROE must be liberal enough to allow commanders operational flexibility while ensuring friendly forces stay within the mission's legal, political, and operational boundaries. When analyzing the necessity of automation, we look at the example and process of developing ROE. There are a few issues that need to be taken into consideration.

When drafting missile defense ROE, tension exists between operational efficiency and necessary constraints in ROE. This tension can be attributed to the proximity of civilians in the battlespace. Careful consideration must be given to weapon system capabilities and C2 assets when crafting these ROE. The degree of positive control of assets and surety of target identification that is both desirable and possible must be carefully considered. In planning, ROE must be strictly cross-examined using possible and probable scenarios.

When all of the planning and considerations are taken into account, we must consider a few essential points which

include but are not limited to the following general considerations. With operations conducted in the air, which will have a potential impact on urban environments that may be in proximity to missile defense operations, there exists the major concern of time. Time constraints become a concern at the event identification and verification phases. The sensor systems must, in a timely manner, make notifications to tactical assets and C2 platforms that possess the ability to assign the appropriate platform to handle the threat. The weapons selection and its evaluation of its effectiveness against the particular threat is a concern as well. The issue of time clearly is a major driving force for the automation of ROE policies. The ROE policies provide the decision points that are part of the identification of an event or threat, and lead to the ultimate decision to Kill or NOT. In order to be effective, there is no time to delay at any point in this process as missile defense is not a zero sum game. A 99 percent success rate for the defender is still considered a failure, but a 99 percent failure rate for the attacker can still be considered a success, if only one of the launched missiles was a success. A single enemy missile striking and destroying its target can have disastrous effects that can transcend the actual level of damage inflicted at the point of impact. We must, therefore, be prepared for potential threats at a high level of defensive effectiveness. This requires a well-planned and automated set of ROE policies.

III. POLICY AUTOMATION SYSTEM FOR MISSILE DEFENSE

A. DISCUSSION OF APPLICABLE SYSTEMS

1. Background

In this section, it is important to understand policy automation from the perspective of systems in other domains. What automated policy systems exist and what are their architectures? We identify the benefits of using policy automation, and in particular, benefits from automated ROE policies. We generally will ask: What does it look like? How do the components work and what are its interfaces? In this pursuit of knowledge, we will discuss the Policy System proposed by Buibuish et al., as a automated policy solution for Net-Centric Warfare, the Policy Work Bench (PWB) and finally the proposed Generic Intercept System. These systems show that automated policies are clearly possible. Once we understand these systems, we will have a good reference point for the proposed uses of automated ROE policies and prelude the deeper discussion of how the policies will be automated and what that means for the BMD System and its structure. As we look at an automated policy system, it is clear that the varying layers of interaction must be smooth and efficient in order for the outcome to be successful.

At this point, we must move from one level of abstraction, the overarching, to the next level that delves further into the ROE unit itself. We will also discuss policy automation and the tools that will be used to make this a reality.

We know what policies are from the previous section, but we have yet to evaluate what automation is, in order to make our foundation complete. Automation is defined in the Encarta World English Dictionary as simply the replacement of human workers by technology. This is the key reason for automation with regards to weapons, war and such engagements. It must possess the capability to automatically make a decision and pass that decision on to the appropriate component or components. This is the core of policy automation; the policies or constraints in the automated policy component must be automatic as its necessary feature and functionality.

The idea for the automation of policies and automated aspects management in distributed components stems from the size and complexity of the distributed systems with which we deal with today. However, every action has its own consequence and with the automation of distributed components comes loss of flexibility in some cases, as the only way to make changes to the behavior at that point is to recode. One way to avoid this problem is to have a design that only requires the operator to revise the policy specifications files without recoding the policy automation engine.

In Table 1, we list the definitions and levels of automation as provided by Ensley and Kris (1995).

Automation Level	Type	System Function	Operator Tasks
1	Manual	No automation support or information	Decide, act
2	Decision support	Automated system provides information but does not execute actions	View recommendation, decide, act
3	Consensual automation	Automated system highlights recommended choice; user makes any selection	Concur or select other option
4	Monitored automation	Automated system executes the choice. User has veto power for some fixed period of time, but system defaults to its choice if the user does not act.	Veto if nonconcur
5	Full automation	System acts and provides no veto authority to the user.	Observe full automation

Table 1. Automation Table (From Ensley, 1995)

2. Policy System

The first policy system that we will be exploring is one that was proposed by Buibish, Lange and Woitalla in their paper titled, “Responsive Decision Making Through Automated Policy-Enabled Systems.” They identified that policy systems, such as the one suggested, are necessary when one considers the military battlespace, an increasingly a more complex and dynamic policy environment.

After evaluating a very comprehensive scenario, it was clear to see that the policy system given this dynamic environment must be one that is flexible and adaptive. It

must be automated, so that it will interpret and act on new relationships without having to make changes to the procedural logic of the system. The appropriate action and response is a threat is the key.

The system is a solution for automated policy for Net-Centric Warfare. The general policy architecture is provided in Figure 2. The components include Domain Knowledge, Policy Console, Policy Broker/Expert system and a Policy Consumer.

1. The Domain Knowledge is the component that allows the common operating picture to be presented. It stores the problem space for the specific domain in which this policy system will interact. They set the bases for the constraints that the Policy Console will operate within. The Policy Broker uses it to help determine applicable rules based defined relationships.

2. The Policy Console is the initial human-to-computer interface with which the commander’s intent, in the form of policy rules, is translated for the system to upload for interface.

3. The Policy Broker is the Expert System that acts as the repository for the policy rules that were uploaded via the Policy Console. It will be the point at which the rules are verified and de-conflicted, or, at the very least, conflicts with rules are identified.

4. The Policy Consumer can be a system or a human. It is the aspect of the system or component that makes the request of the policy system based on the threat, action or response required. When the Policy Consumer is an expert

system, it allows for flexibility in decision making automatically adjusting to the changing domain knowledge.

The proposed system and architecture is one that can be applied to various domains and could be chosen as the policy component for our Generic Intercept System (Buibish et al., 2005).

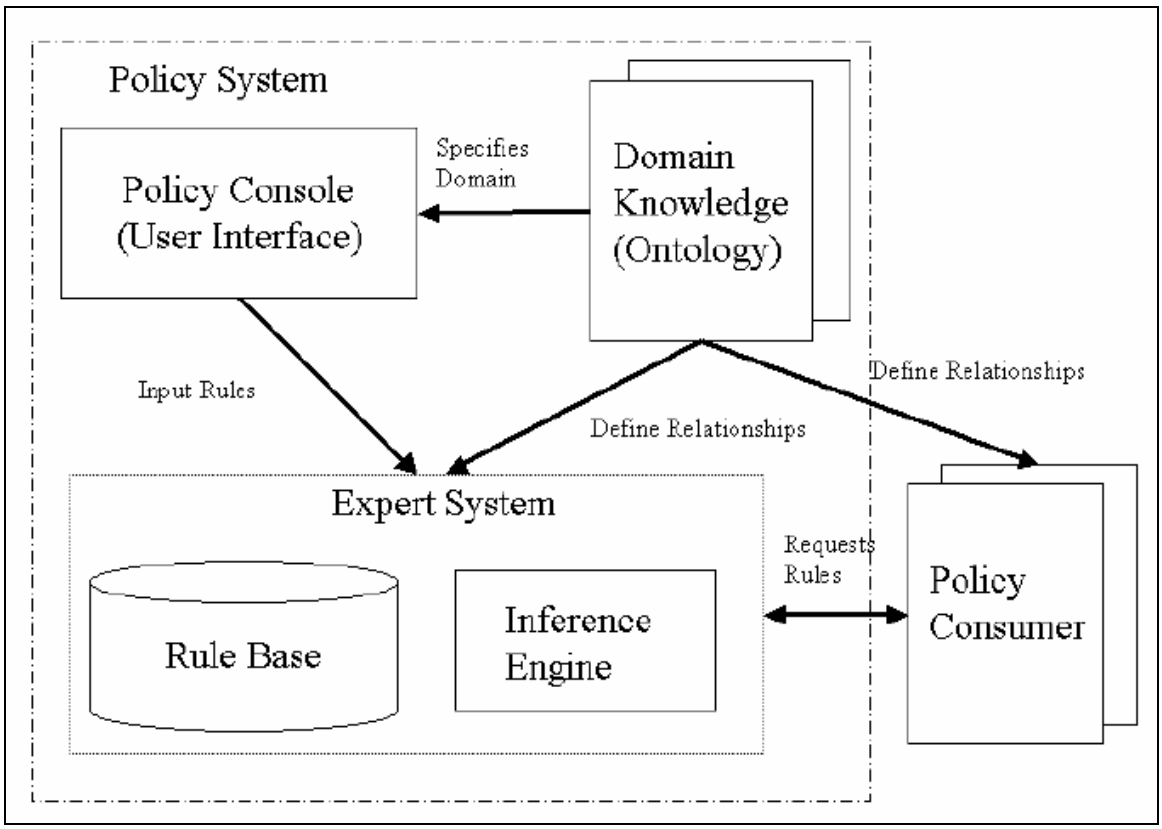

Figure 2. General Policy Architecture(From Buibish et al., 2005)

3. Policy Workbench

It is time to introduce the Policy Workbench (PWB), the idea of an architecture that was proposed by Sibley, Michael and Wexelblat. The PWB is the tool that will be used to allow for policy automation within a system of systems such as is being proposed. According to Michael et al., a policy workbench is an automated knowledge-based system comprised of a suite of tools designed to assist the user in the representation of policy; reasoning about the properties of policy such as consistency, completeness, soundness, and correctness; refinement of policy into systems; maintenance of policy; and enforcement of policy. There are five major actors and interfaces of the workbench as defined by Sibley et al., from which we have derived a version suitable for what the Battle Manager requires of its tactical and routine maintenance evaluation procedures.

1. The policy maker enters policy by means of evaluation of current facts, figures, population and climate, which in turn provides a baseline for consistency when responding to ROE.

2. The policy maintainer maintains live testing continuously to manage the cause and effect, as well as correctness and completeness in the means of protection. Because of the live updates, it is modified accordingly in order to maintain accuracy and soundness within the system.

3. The policy implementer is a responsible unit that is designed to act as a ROE facilitator that both interprets and disperses ROE effectively, while maintaining an accurate tracking of all inter-relations amongst policies.

4. The policy enforcer is responsible for maintaining an efficient procedure that will enable ROE to be maintained and fulfilled.

5. The policy evaluator routinely runs checks-and-balances through various queries, data analysis and strategic implementation procedures.

As seen in Figure 3, there are three important subsystems of the PWB. They are the Policy and Real World Analyzer, the Dictionary Handler System and the Reasoning System. In Sibley's early work, both the Policy and Real World Analyzer and the Dictionary Handler System consist of a Lexical Analyzer (LA), an important aspect as we have yet to discuss how the policies will get into the system from the User interface. When policies are input, they will go through the LA which accepts policy statements and translates them into a common data interchange format based on an Object Oriented Model. This aspect is a key point when developing and using automated policies. The policies are in most cases going to be created by someone other than the programmer, who will not speak the computer language. In order for full automation to be accomplished, the policies, whether they are ROE or other, will need to be translated from the common spoken language to computer language and back again. This is the function of the LA. More work is being done in the realm of Natural Language processing support, but we will shelve that discussion for now. The dictionary handling system acts as a database; it will organize, store and be the point of refinement for the policies. The triggers of the dictionary system allows for the update of its schema to signal any needed changes to

other components. With a fully populated Dictionary, the Reasoning System will evaluate queries to answer questions such as: “what level of refinement is necessary to enable effective future processing of policies?” and “what reasoning techniques will best allow for standard and important policy queries and must be used to respond to a request for information or a specific query?”

Three mechanisms we must also address, which are part of the PWB, based on prior studies, are the automated theorem prover; an expert system having forward and backward chaining capabilities; and an object-oriented system, incorporating, at least, the ability to specify multiple inheritances and message passing between objects.

Based on the research of this work, the PWB has proven to be the logical choice when considering the need of the intercept system to have automated policies. The workbench’s flexibility will allow any type of policies to be stored. With the internal function of checking for correctness and completeness in the policy, it makes it ideal for the automated ROE policies.

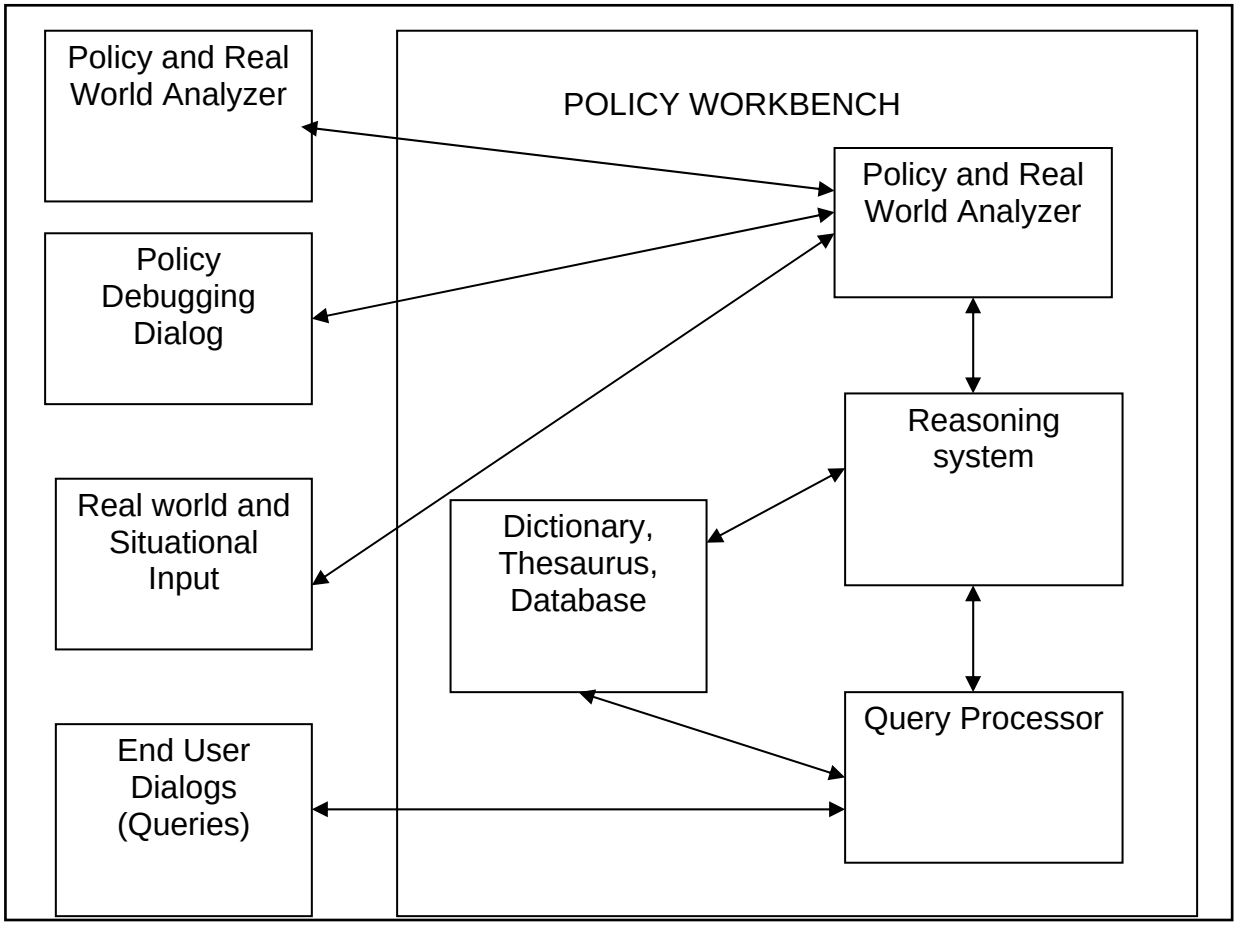

Figure 3. Policy Workbench (From Sibley et al.,1992)

4. Generic Intercept System

The architecture of an intercept system will hold the same general characteristics of the systems described earlier. It is a distributed system, as previously defined. When we began to develop the model, we used one with which we were familiar. In studying the Rapid Action Surface-to-Air Missile (RASAM) System, it gives us a baseline model to which to refer with the creation of our GENERIC INTERCEPT SYSTEM (Michael, 2006).

The generic intercept system architecture is a software intensive system that is made up of three primary subsystems; the Weapons Deployment subsystem, the Weapon and the Battle Manager (Figure 4). Supplementary equipment that could be associated with this system is the loader, weapons deployment interface test kit and the weapon interface test kit.

The Battle Manager is the primary component of the intercept system. The BM interfaces with the host Command and Control (C2) system. The type of C2 will vary depending upon the operation environment or domain. The type of intercept system that would be attached to a ship for missile intercept, the C2 may even vary by class of ship. The BM will accept target designations and engagement orders from the C2 system. It will also issue commands to the weapons deployment subsystem via the most expeditious means of communication, such as Satellite, Fiber-Optic cable, wireless capabilities or others as available.

Major subsystems of the battle manager are the Interface Connector Panel (ICP), which is the primary point for all interfacing. It is the switch board for the Battle manager taking requests and passing along the appropriate data to the right components within the system. It interfaces with the software of the host combat system, and the sensors, internal and external to the host. This idea of a host will remain generic and vary based on environment or domain. The ICP will interface between the BM for execution of actions as prescribed by the Rules of Engagement Unit (ROEU). Another function of the ICP is that

it will format message traffic for the Control Unit (CU). The CU and the ROEU represent the remaining major subsystems of this system. The CU is where the operator interface happens, and will, for most systems, be a Graphic User Interface (GUI). At this panel the operator can select the operational mode (e.g., Off, Standby, Test, Training or Tactical), view and input data. It is where the operator can monitor the operation of the systems similar to that of the task manager in today's personal computer. The ICP will also interface between the BM for execution of actions as prescribed by the ROEU. As for the ROEU, this is where our automated ROE policies are housed. This is the equivalent to Dr Caffall's ROE Data Store. This unit will have interface with the CU and the ICP on the lower subsystem level but will also have an interface with the Battle Manager directly. The ROEU will be the decision-making hub through which the output will produce a decision to "Shoot," "Don't Shoot," or "Wait, based on its various interfaces, the knowledge base or policy repository. Once the output data is processed from the ROEU, it will pass it to the BM to carry out the actual engagement or intercept again depending on environment.

The intercept systems' other main leg is the Launcher/Deployment Subsystem, which will also constitute a major subsystem. The Launcher is the unit where the tools or weapon is housed. It is also responsible for the positioning of the weapon for a successful engagement. The Launcher, in this case, can be a ship, a standalone weapons system, a CPU (in the case a cyber engagement), or whatever would be considered the weapons deployment unit.

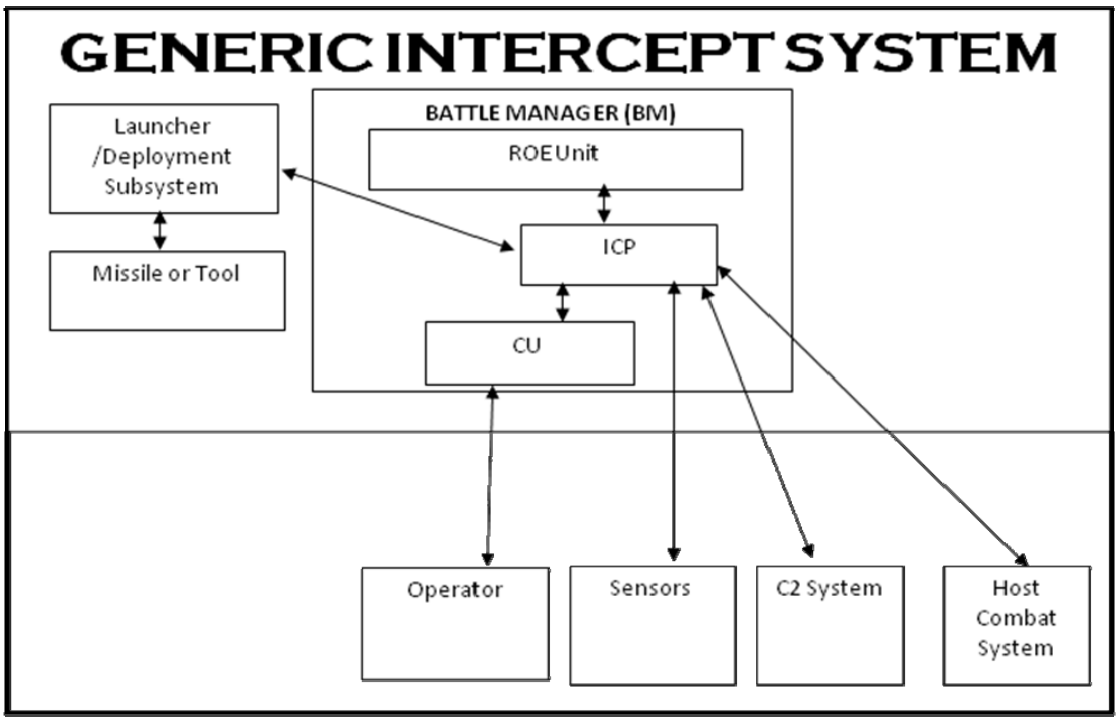

Figure 4. Generic Intercept System

IV. THE ROE UNIT OF THE BATTLE MANAGER

A. BACKGROUND

As shown in the Generic Intercept System architecture, it is clear that the ROE Unit is the primary component of the Battle Manger for the suggested Ballistic Missile Defense system. As we have explored the two policy systems and further suggested the architecture for a Generic Intercept System, we must choose the policy system that will support the architecture for our ROE Unit. In this section, we have chosen the policy system and will be presenting a design that will allow for the development of the ROE Unit for our Battle Manger.

The first step in designing the ROE Unit for the Battle Manager is to perform a use case analysis to identify the actor and features of the proposed software. The second step in designing the ROE Unit for the Battle Manger is to choose the policy system, for which we have chosen the general policy architecture as presented by Buibish et al., 2005. In choosing this system, we must next develop two key elements needed for its functionality: 1) the Domain Knowledge, which will be realized by the creation of an ontology for the domain of Missile Defense; and, 2) the development of rules for the Expert System, which will be compatible with a Policy model that we will also select.

For the ontology development, we will explore the existing ontologies of Sensors, Weapons and Command and Control Systems (C2). Much of this work has been researched and created independently. We will show

examples of these ontologies. We will show the ROE policies that we have created of which will be translated into our rules. In order to understand what the domain will consist of and the interfaces associated with the system, we examine a general set of Missile Defense scenarios which we will use to develop use case and activity diagrams. These diagrams and analysis products give us greater insight into the domain of Missile Defense.

Before we get into the use case analysis and the development of the key elements of our ROEU, this next section will present the proposed architecture for the ROEU.

B. ARCHITECTURE

In this section we will recall the architectural models provided for both the Policy system in Figure 2 and the Generic Intercept System in Figure 4. Our Generic Intercept system was a black box view, in other words we could not see the internal component of that Unit. We have to reconcile with each model the components that will be reused or modified to ensure compatibility and then show what that architecture will look like as the ROE Unit.

As we study the architecture presented by Buibish et al., 2005, we see the key components include the Policy Console, which is the user interface, the Domain Knowledge (ontology), the Expert System that consists of the Rule Base and Inference Engine, and the Policy Consumer, which is the component that makes requests of the rules.

The Generic Intercept Systems architecture again shows a black box view of the ROE Unit that interfaces with the

Interface Connector Panel (ICP), which is responsible for all interacting with internal and external consumers of the system to include the Host Combat systems, the Sensors and even the C2 systems. The ICP is responsible for formatting the requests of the external systems, as well as internal components in a manner that the ROE Unit or Policy system can understand. The other component to address that interacts with the ROE Unit is the Control Unit (CU). It acts as the user interface with a GUI much like the Policy Console.

Figure 5 presents the architecture for the ROE Unit, which takes into account the functionality of both architectures in a manner in which we don't lose the integrity of the systems, their necessary interfaces or operations. The ROEU has two internal components, the Expert System, which consists of the Rule Base and Inference Engine. This Expert System allows flexibility, since decisions can automatically adjust to the changing domain knowledge. The second component is the Domain Knowledge, which is used to relate rules to the request criteria. The request or data must fit within the knowledge of the environment or be added to that domain knowledge. Both the Expert System and the Domain Knowledge components communicate with the ICP. It will take a request for a given set of criteria and provide a response action. This communication is all automated between software. The CU is the interface with the Operator or the User where it can operate, monitor and interact with the system in all modes of operations. The CU will normally interface with the ICP in order to pass and receive information, but in the case of maintenance

trouble shooting or testing, the CU will communicate directly with the ROEU's Expert System and Domain Knowledge via a secondary communication path, as reflected by the dotted lines. This is a precautionary means of communicating with the ROEU.

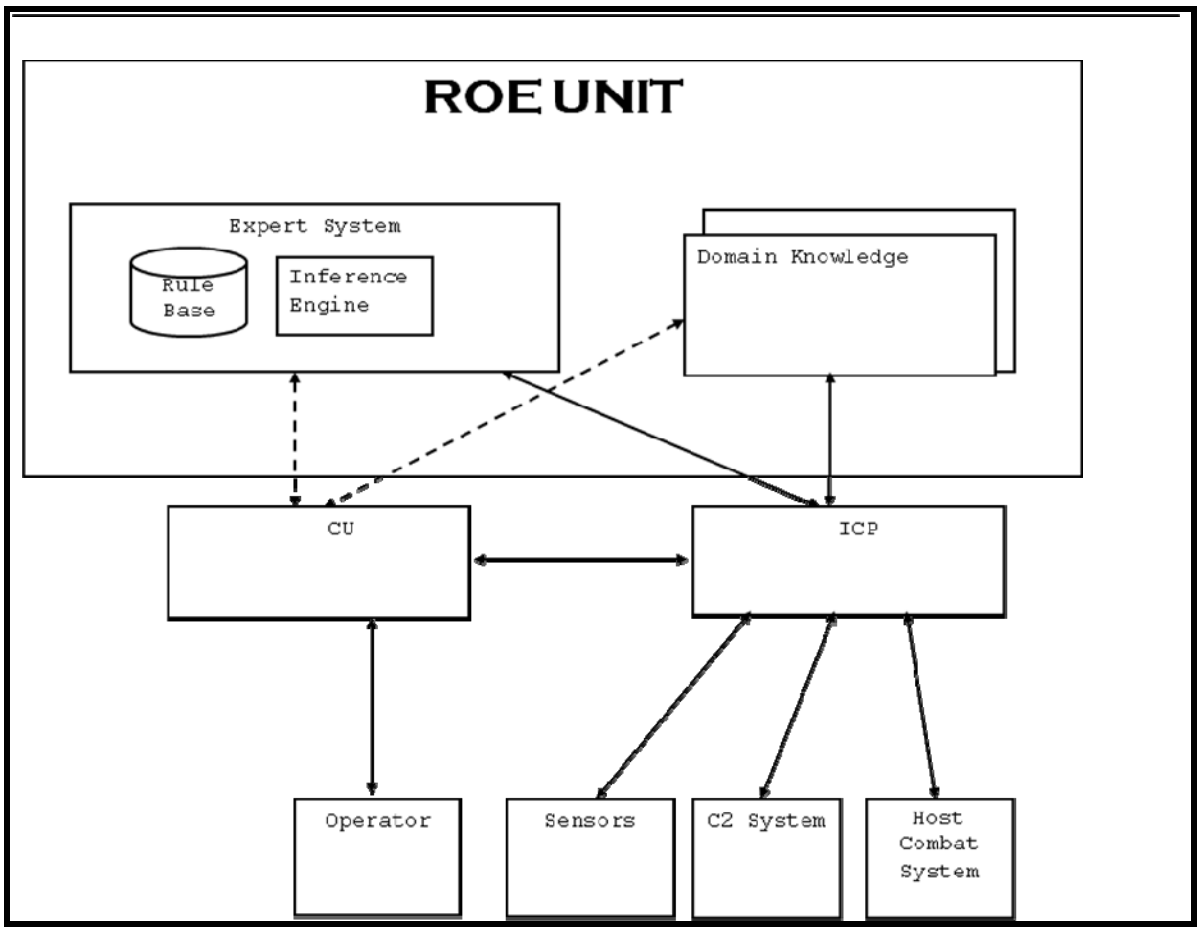

Figure 5. ROE Unit

C. USE CASE ANALYSIS FOR THE DEVELOPMENT OF RULES

In this section, we will look at the elements needed to derive our rules for the Expert System. The foundation of the rule development comes from a holistic understanding

of the domain or environment, the Commanders Intent, the system itself, and the components internally and externally that interact with this system. We examine a general set of scenarios from which we develop our use case and activity diagrams.

The production of these diagrams will yield a general set of ROE policies, constraints, Commanders concerns, or intent. These rules need to be understood clearly in order to proceed with the appropriate action. It is from this ROE set and the adaption of the policy model that we will create a few sample Rules that our system will be able to process.

1. High Level System Use Case Analysis

Development of general scenarios based on discussions with individuals that work in the realm of Ballistic Missile defense is paramount in developing use cases. The scenarios help us also create rules of engagement as we understand what actions and interfaces the system will be involved in. The readers will see from the activity diagrams covered in the next section how these rules will be derived. All Rules of Engagement policies are derived from scenarios and situations that extend beyond those covered by the CJCS Standing Rules of Engagement. The scenarios for use case analysis help show the basic operations of the system and help define the interfaces with the system. This is one of the primary purposes of use case analysis.

The scenarios chosen are used to understand the environment in which the Generic Intercept System and the ROE Unit will operate in. Many scenarios are derived from

experience and at this time we do not have any to glean from. With that being the case, we have chosen simple scenarios centered on the premise that actions are imminent. What can be further identified in this section is that the scenarios drive the use cases, but likewise in evaluating the use cases, we can derive new scenarios as it allows us to ask a series of ‘what if’ questions of the system interfaces that will allow for greater discussion and understanding of the system.

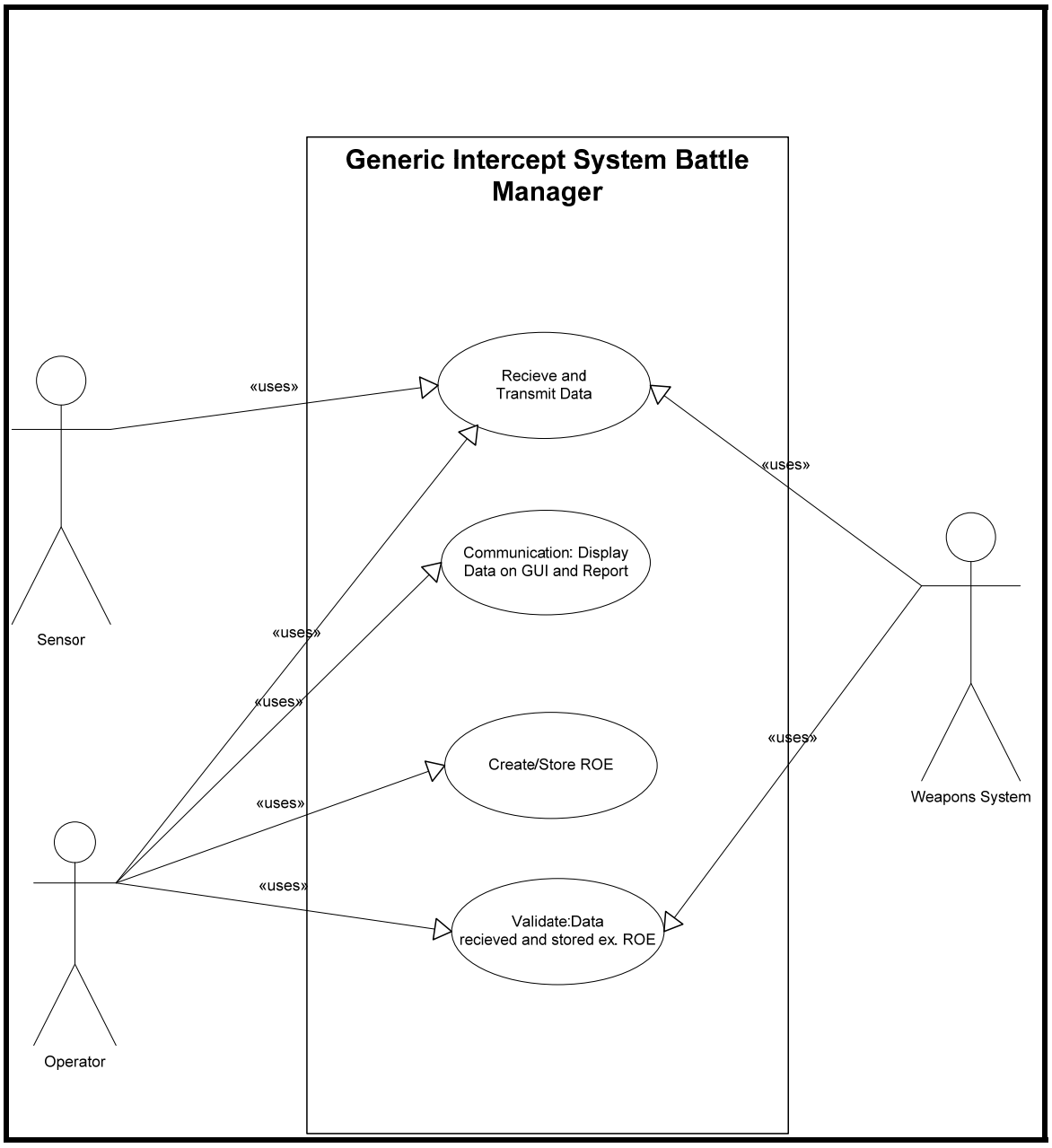

Figure 6. Intercept System Use Case

The primary actors that we have identified in this first iteration of the use case analysis for the high level system are the sensors, the user (or C2 platform) and the weapons system. With each of the listed scenarios, there

are specific concerns that each actor has to take into consideration. There can be more actors given a specific situation, but these three are our focus for the limited scope of the scenarios provided.

2. Use Case for ROE Unit

We now create a use case that specifically identifies the interfaces of the ROE Unit using the same set of scenarios but adding more detail to best flush out the actors, the interfaces and the actions of the system. This level of refinement will help in the design of the ROEU.

In this scenario, the sensor identifies a ballistic missile. The sensor is an infrared equipped sensor that detects the heat signature. The data is instantly received by the generic intercept system alerting the User via the GUI and the Intercept Control Panel, which will communicate this data received to the ROEU to determine that the information is in the Domain Knowledge and to the Expert System if so to determine base on the rule inference what action can be taken. The system will be receiving information steadily as the event is still in an active mode. The validation of the information and a determination of actions have been identified sent to the ICP and the CU for review. Once the actions are determined, the ICP will communicate with the Host Combats System or appropriate C2 platform to execute actions. The message sent will have all coordinates, weapons information and execute considerations as flagged by the ROEU. Information that is of a higher classification than the platform being assigned the task will be further flagged or stripped.

The use cases shown in Figure 7 review the key actors are the CU and ICP component of the Battle Manager.

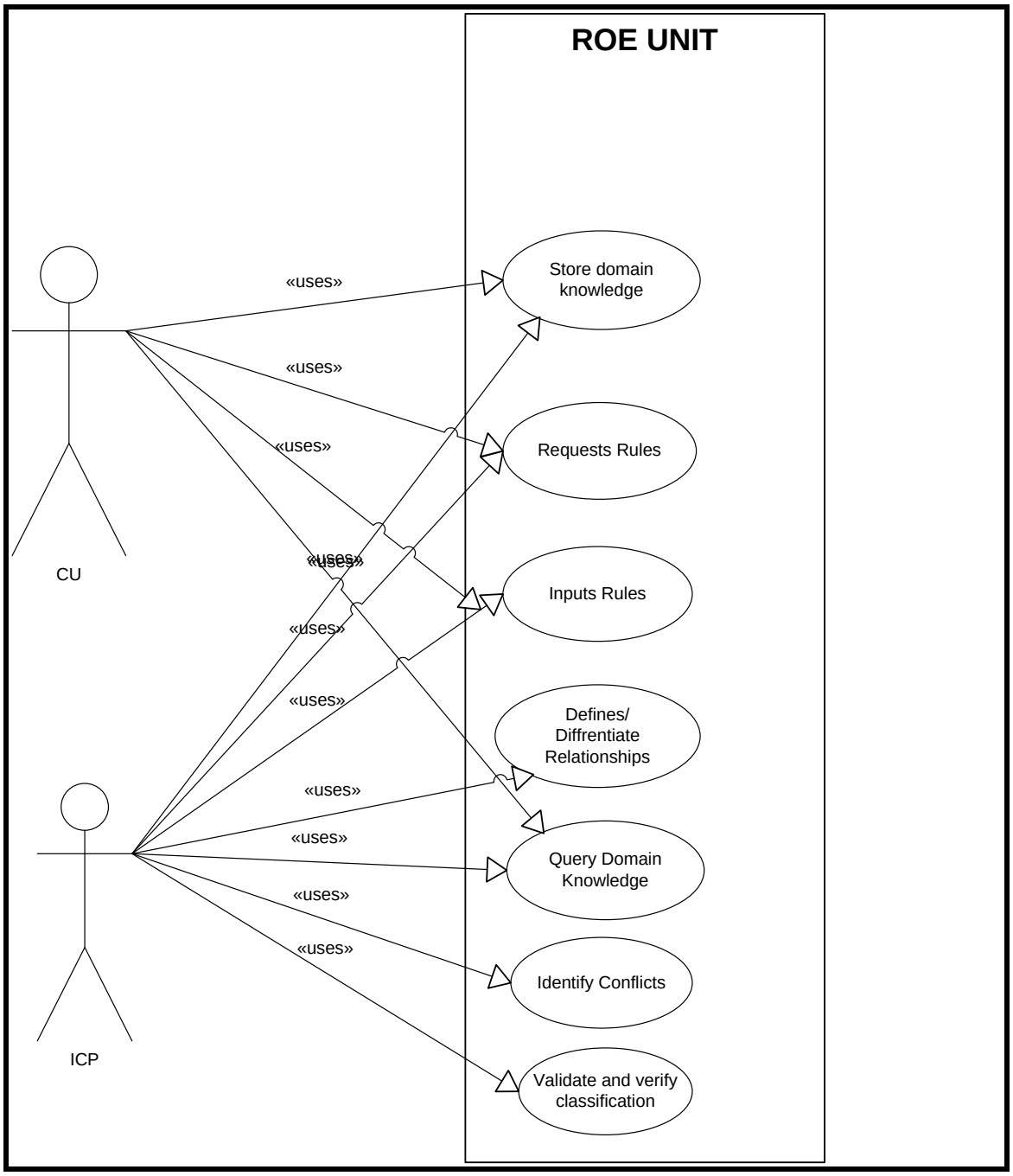

Figure 7. Use Case for ROEU

As we analyze the uses cases for the ROEU, we see that the actors interface with the system to execute seven different actions. These are as follows.

1) Store Domain Knowledge: Both actors will interface with the system in order to load or store the ontology for the domain into the ROEU in particular the Domain Knowledge component. It is under that instance of maintenance, testing or as a backup to adding to the ontology that the CU will interface with the ROEU for this action.

2) Requests Rules: Both actors will again make rule requests of the Expert System however in the case of the CU it will not be the primary interface for this action.

3) Inputs Rules: The ICP and the CU will interact with the system in order to input rules into the Rule Base of the Expert System.

4) Defines and Differentiates relationships: As the data is initiated or requested by the ICP, the systems will determine where in the ontology it fits and then determine a relationship to help best differentiate the rules and response actions that are most suitable.

5) Query and Input Domain Knowledge: Both the CU and the ICP will need to input and query the domain knowledge. In this case, the ontology will be queried.

6) Identify Conflicts: a primary function of an automated system is that it will allow for the identification of conflict as the ICP interfaces with the ROEU, for example, when the data received is in conflict with the knowledge about the domain.

7) Validate and verify classification of data: In this case, data is passed to the ICP and interfaces with the ROEU. If the response action requires passing data that may be of a level of classification greater than that of the C2 element then that information will need to be flagged and or striped.

3. Deriving Rules for Expert System

The general flow of action for our scenarios within this domain follows. 1) Sensors or other indications and warning systems identify a threat. This information is automatically uploaded to the intercept system. 2) The intercept system will process all the information checking and evaluating data received. 3) The system will make a determination based on the data received, information existing in systems database, and repositories. 4) That information will be passed along to the designated asset that will accomplish the desired effect, which, in the case of an intercept system, is to shoot or not to shoot. The set of rules or constraints are consistent with the ROE policies for the particular domain given all of the information that is known at the present time or otherwise at the time of ROE policies creation.

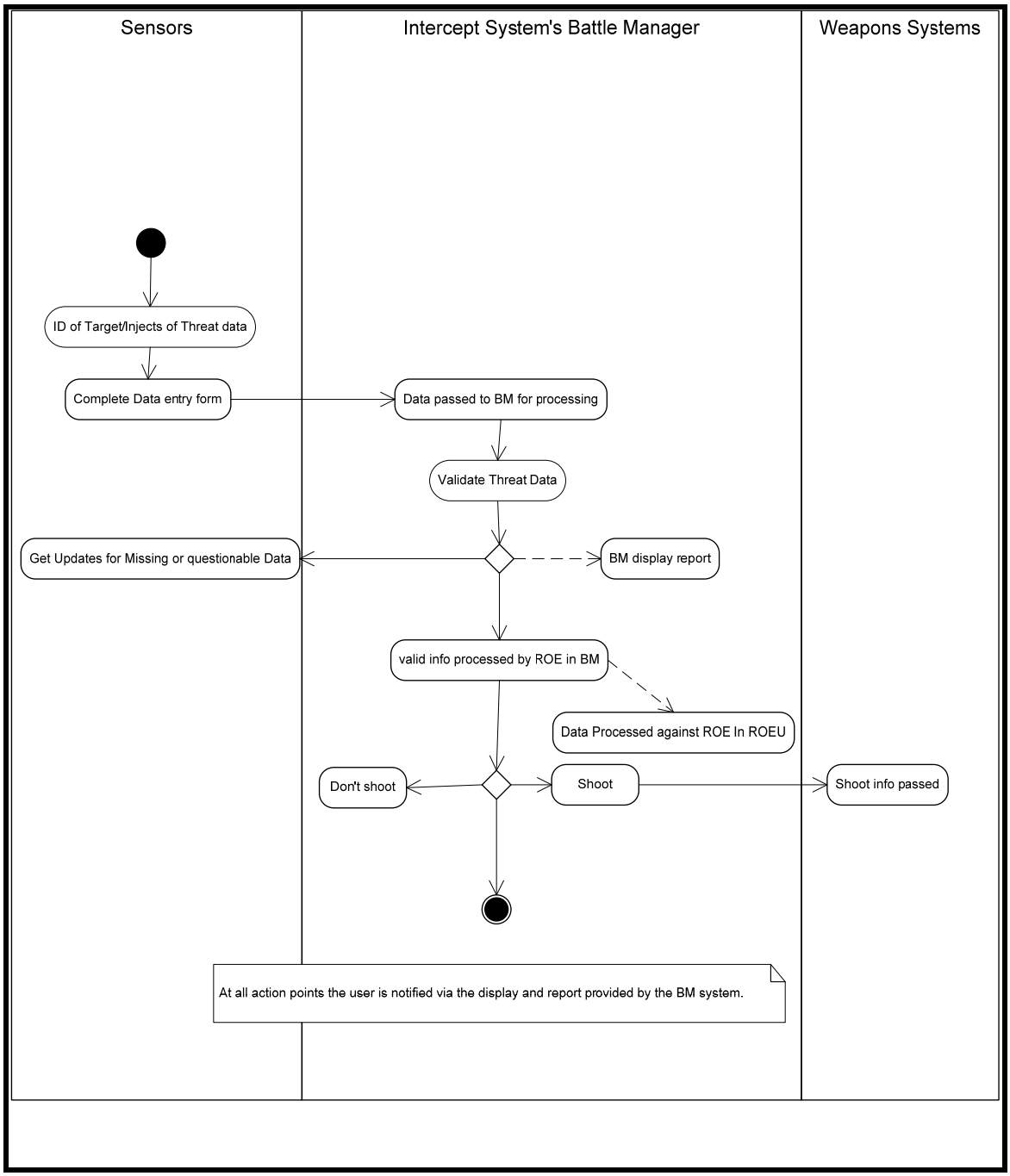

Figure 8. Activity Diagram for Intercept System

The flow of each scenario, again, is generally the same as the one shown in Figure 8, which begins with the identification of an event. The sensors are the primary source of indications and warning. In this case, there can be various types of sensors on multiple platforms, but for purposes of this work we, again, are being very general. At this point we see the flow as 1) user is informed of the situation to the millisecond; 2) user monitors the system as it runs through the policies and processes of determining the credibility of the threat; 3) the ROE unit determines whether to shoot based on the credibility of the threat; based on weapon system(s) capability, 4) the ROE unit then assigns the weapon system(s) with the responsibility to execute, as appropriate. The communication between all actors and the system must be clear and concise, as time is a critical factor in matters of missile defense. If a weapons system does not successfully execute and destroy the target, another may be required to execute but alludes to the fact that the sensors will be tracking and communicating as the event continues. This is the general flow to consider for the four scenarios below all have the same desired outcome of 100 percent destruction of all threats prior to entering a point in the U.S. that could cause any effect.

1. Multiple Warheads with Saber Rattling

All sensors are tuned to particular areas of the world based on known and expected tensions. The assets that would react to the threat of missile attack are ready and positioned to do so; these are known as Defense Assets. The Order of Battle for the stated enemy is known. The

origin and firing point of the missile will not be a surprise, but the type of missile and firing time are still relevant questions, and the location and time of impact are important to calculate.

2. Multiple Warheads with No Prescience

A sensor detects the launch of multiple missiles or deployment of multiple weapons systems. The communications link must be open for C2 to ensure verification of missile launch, coordinates, type, and time, among other data. In this case, the assignment of the most appropriate asset must be selected and notified in the most expeditious manner.

3. Detection of Unidentified Weapon or Missile

Sensors and or intelligence have detected a missile or intercept event. The weapon is not identified, but the data that is provided includes time and coordinates for the missile or weapons system data. Through continued tracking, we obtain the speed, coordinates and other important data updates.

4. Detection of a Non-Threat Event

The system and its sensors determine that there is a launch or trigger event, but with additional intelligence, a determination is made that the event is a Non-Threat event.

a. Proposed ROE Policies

Listed in this section, the readers will find a set of policies that were derived from the scenarios. The

policies would be run through an appropriately configured system for correctness and completeness. The assumption is that when the BM is in tactical mode, it is ready to shoot. The policies are the constraints of the system or parameters that will or will not let the automated ROE policy unit produce a result that will forward instructions to the BM to shoot or otherwise engage. Before we show the policies, it is important to see how from the scenarios the policies are derived. Using the first scenario as an example, we see that there are many factors that are known like general location of the threat, assuming all intelligence assessments are correct, we should be able to determine that easily. Consideration of this naturally falls within the ROE; the actor shooting and their location will determine how and if we can act in response. This is ROE: constraints that allow us to conduct warfare in the best possible manner. The second scenario brings into question the constraint of action based on unclear information due to a possible lack of communication. In general, it would be irresponsible to risk so much as shooting a missile at a target that may or may not be validated. With regards to our third scenario, it is clearly a question of weapons selection. If the target specifics are unknown the operator may chose a weapon that may not be effective. We must consider measures of effectiveness, as well as measures of performance concerns. Did we hit our target and how well we did? Will we be able to execute intercept with an appropriate weapons system in the right window of engagement? Finally, in the last scenario, we have a situation in which the sensors are reporting one thing, yet the supporting intelligence is

reporting something different. This would be a situation when the operator would want to consider the source of the data before shooting. Again, through this scenario, it helps identify constraints or things that the commander may need to consider before taking action. We must remember that there are Standing ROE, we have to come up with ad hoc ROE based on the commander, or situation, which in this case is specifically missile defense.

Policy 1) Shoot if there is data intercept information from three sources,

Policy 1b) Shoot if you have data intercept information from two sources and an approved insufficient source count override by an authorized operator.

Policy 2) Shoot if there is tracking data for moving engagements such as missiles that are identified as a threat; we must obtain coordinates, time, speed, and weapon system type.

Policy 3) Shoot if engagement is within preset window of engagement. Lat/Longs for all areas will be stored in the database list. If the engagement takes place outside of the appropriate window, there may be grave consequences to consider, such as the loss of life if engaged over highly populated areas or environmental issues.

Policy 4) Shoot if engagement window will be a determinant distance outside of foreign airspace or territory other than enemy territory. E.g., 300 Mile outside.

Policy 5) Shoot if location or tracking data has been validated.

Policy 6) Shoot if domain knowledge or system knowledge database has been updated or refreshed within 10 days. This is necessary when taking into consideration enemy Order of Battle (OOB) and weapons inventory. Different operating battlespaces may have a high operational tempo and 10 days may have to be reduced to 1 or 2 for a refresh.

Policy 7) Shoot if interceptor calculations reflect a chance of success at 80 percent or greater.

Policy 8) Shoot if the identified weapon is exhibiting the normal capabilities, speed, flight pattern, etc., as defined by domain knowledge.

Policy 9) Shoot if you can identify threat or if a non-threat event is determined threat event.

Policy 10) Shoot if higher echelon leadership does not override system. E.g. in the case that the engagement is being handled in U.S. Pacific Command, the Secretary of Defense can override.

As it is clearly understood, ROE are limitations and circumstances delineated by higher authorities that govern the decision making of forces initiating and prosecuting combat engagements with enemy forces. The environment in which the engagement is to take place will determine what the specific ROE will be. Build further on the idea to predict the scenarios that could be realized, and then determine what ROE policies should be created and added to the knowledge base of the system.

Policies are developed by a collaborative effort. When you look at a scenario, you can determine what the

concerns are and derive the appropriate policies. The hands involved in policy-creation include, but are not limited to, those of the President, Secretary of Defense, Combatant Commands (COCOMS), and lawyers and, in the case of automated policies, the system maintainer who will be loading these policies. Before we move further, we must briefly address the research on Natural Language Processing support. Michael, Ong, and Rowe propose the use of the natural language to interact with the PWB. The foundation behind this idea is that the people creating the policies are not going to be computer scientists, but rather politicians, military and other civilians. This system must be able to take inputs that are close to modern English and push it to the repository translated into computer language for interface with the system. This is where the backward and forward chaining is vital to the system.

4. A Policy Model

We have selected a policy model that uses general terminology, which will enable policies, ideas, and data that will be used in the military domain (Buibish, 2005). It is important to use this particular model as many others were created for domains, such as networking where the terminology is not compatible. The key elements of this model are the Policy Rule, the Policy Condition and the Policy Actions (Figure 9). The Policy Rule is where the data that defines how the Policy Rule is used in a environment, as well as, a specification of behavior that dictates how the managed entities that it applies to will interact. The Policy Condition will define the necessary

state and/or prerequisites that define whether the associated Policy Actions should be performed. The Policy Action is where the necessary action that should be performed if the Policy Condition is met is represented. Figure 13 shows our model and it will be from this form and function that our rules, which will be presented in our example, have to fit.

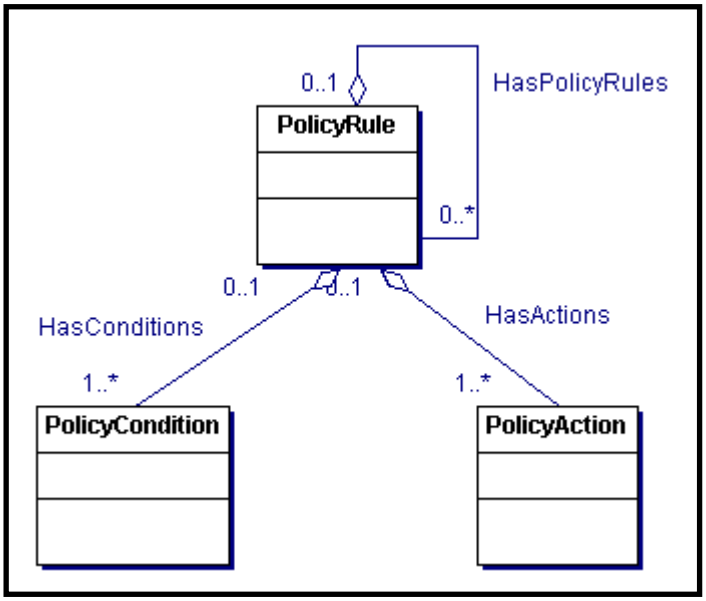

Figure 9. Policy Model Primary Classes (From Strassner, 2004)

a. Example of Policy Model for ROE Unit

The Policy model is important to the ROEU, as it is how the rules will be formatted for the Expert System. In order for the Expert System to understand the Commanders Intent or the ROE policies, it will need to be reflected in a manner in which the system can identify. As we have chosen the policy model reflected in Figure 9, we now provide a set of sample rules. This will be in a format that can be used for any relational database or Object

Oriented Database. Table 2 provides an example of the rules that are derived from the ROE polices.

Policy Rules	Policy Condition	Policy Action
1)	Three sources provide intercept data.	Shoot
1b)	No override submitted in event that there are only 2 sources provided for intercept data.	Don’t Shoot
2)	coordinates, time, speed, and weapon system type exist for moving engagement	Shoot

Table 2. Sample Rules for ROEU

D. UNDERSTANDING DOMAIN KNOWLEDGE USING AN ONTOLOGY

We must begin this section by defining what an ontology is. Gruber defines ontology as an explicit formal specification of terms in the domain and relations among them (1993). In general, ontologies help you understand an environment or specific domain with better clarity as it lays out also a common vernacular for all that are interested in research with that domain to understand. Noy, et al. gives five specific reasons for developing ontologies: 1) This will allow for the sharing of a common understanding of the structure of information among people or software agents. 2) To enable reuse of domain knowledge. 3) It will allow you to make domain assumptions explicit.

4) It will allow you to separate domain knowledge from the operational knowledge. 5) It allows you to analyze domain knowledge.

When we look at the ontology for the missile defense domain, we understand that this should be a composite of the information known about the domain. In the most general look at such a missile defense ontology, we focus on three key elements; Sensors, Weapons, and C2. In the next three sections, you will see examples of ontologies that have been created for each of these individual domains. Portions of these ontologies will be used in the development of our proposed Missile Defense Ontology later in this chapter.

1. Ontology for Sensor Domain

The first example of an ontology in the sensor domain was provided in the undergraduate work titled Ontology Development as Undergraduate Research by Antonio Lopez, Jr. His work gives examples of ontologies and identifies why they are suited for undergraduate research. This ontology presented is a partial sensor ontology that focuses on the Thermal Infrared Multi-spectral Scanner (TIMS), which is an instance of an infrared device that is a kind of (ako) sensor (Figure 10). The nodes sensor and platforms both have many features and subsystems. There are two kinds of sensors, radar and infrared and various types of platforms including aerial, land-based and space-based. This is a simple sensor ontology that can be used to build out the complete sensor domain (Lopez, 2002).

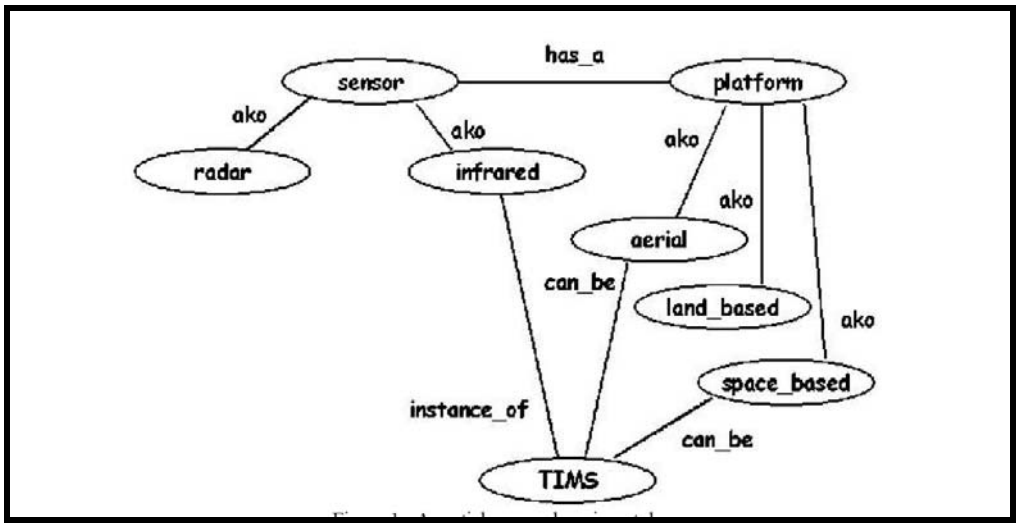

Figure 10. Partial Sensor domain ontology (From Lopez, 2002)

In Figure 11, we present another example of a sensor ontology developed by Davis. In this case, we see a different orientation of the nodes reflecting a bottom up approach to understanding the relationships within the domain. Note, that in the case of radar, the author further built out its relationship to include an instance of radar being the x band type of radar. Davis even identifies the signals that are emitted from the radar in this case the electromagnetic wave that is further identified as a sub-class of the electromagnetic signal. This sensor ontology covers the aspects of the sensor domain that would be of most importance with respect to tracking incoming missiles (Davis, 2004).

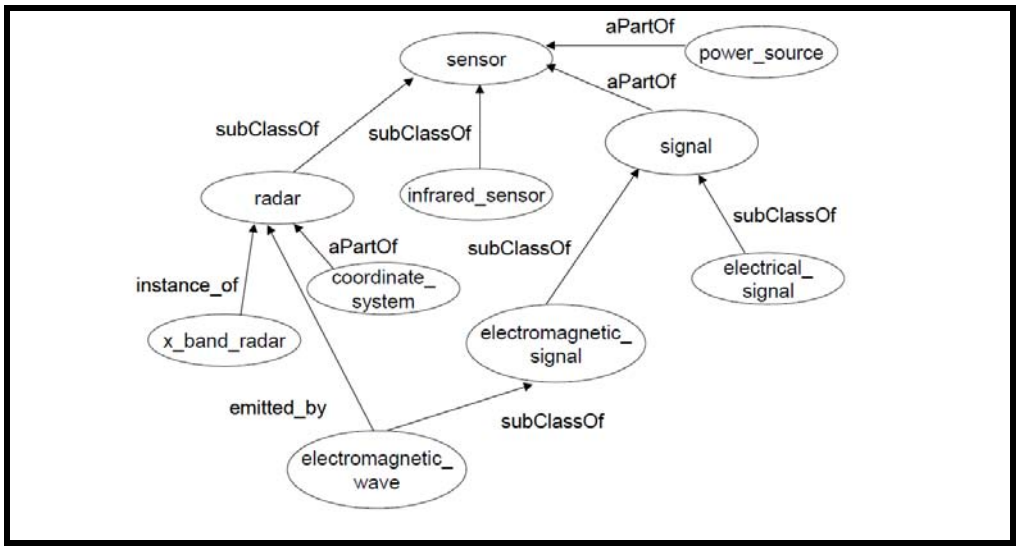

Figure 11. Partial Sensor Ontology (From Davis,2004)

As illustrated by the previous two examples, there are many approaches to developing an ontology for sensors. Depending on the context in which the researchers are looking at the problem, two researchers can independently develop two different ontologies for the same domain. In general, it is clear to see that the full development of a sensor ontology would be a very challenging and labor-intensive task, as we would need to identify the reason for the domain knowledge in order to relate the different sensor information.

2. Weapons Related Ontology

In the example below, Andrade and Brandsma present an example of an ontology that will be part of their future development of a semantic enabled orchestration in support of Ballistic Missile Defense System contexts. What we take from this example is the beginning of the Missile relationships and how they relate to Missile Defense. In

his example, the Missile has a type in which one is the ICBM (Figure 12). It shows us that, with regard to Missile Defense, two key functions are the Missile's Signature and its Type. This will be the starting point for our sample Missile Defense Ontology.

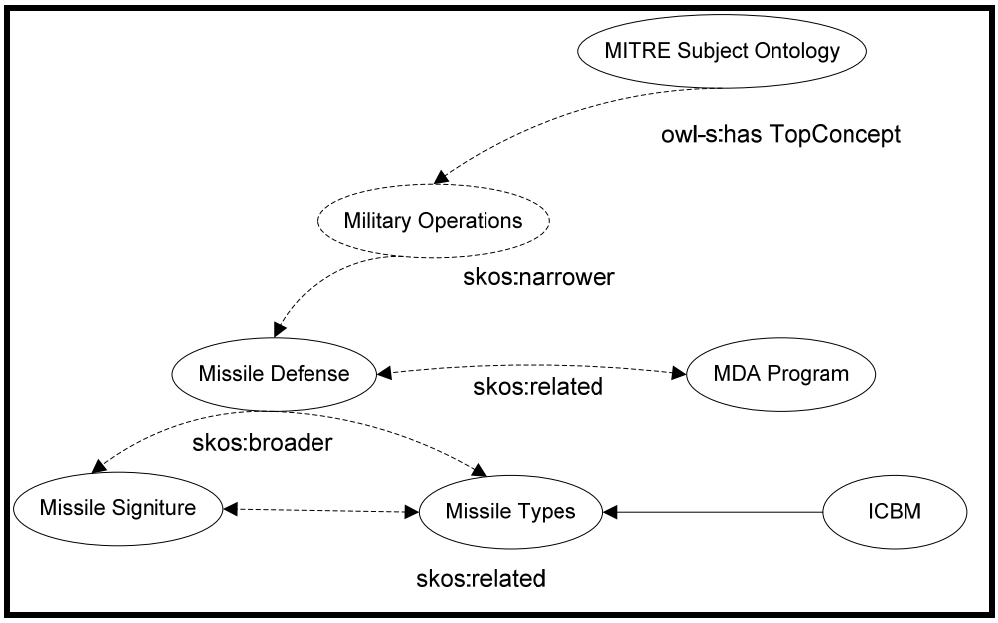

Figure 12. Remake of Semantic-Enabled Orchestration (From Andrade,2007)

3. C2 Related Ontology

Currently, a published C2 Domain Ontology does not exist to date, but Ms. Leslie Winters, U.S Joint Forces Command (USJFCOM) and Dr. Andreas Tolk, of Old Dominion University, have presented a number of very viable reasons for such an ontology, as well as steps to realizing it with the work presented in the paper titled "C2 Domain Ontology In Our Lifetime" (Winters, 2009).

For the purposes of this work, we will suggest a partial C2 ontology that will be associated with our

Missile Defense Ontology example. As shown in Figure 13, the C2 elements begin with the Secretary of Defense (SECDEF) who delegates to the subordinate COCOM. The types of Missile Defense Platforms are further subordinate to the COCOMS. In the case of the Nuclear Powered Ballistic Missile Submarine (SSBN), you see that it is a kind of subsurface platform, and one instance of SSBN is SSBN 43, a specific boat. There are many layers of C2 missing from this example, but a simplistic view allows readers to understand what the C2 domain ontology would consist of.

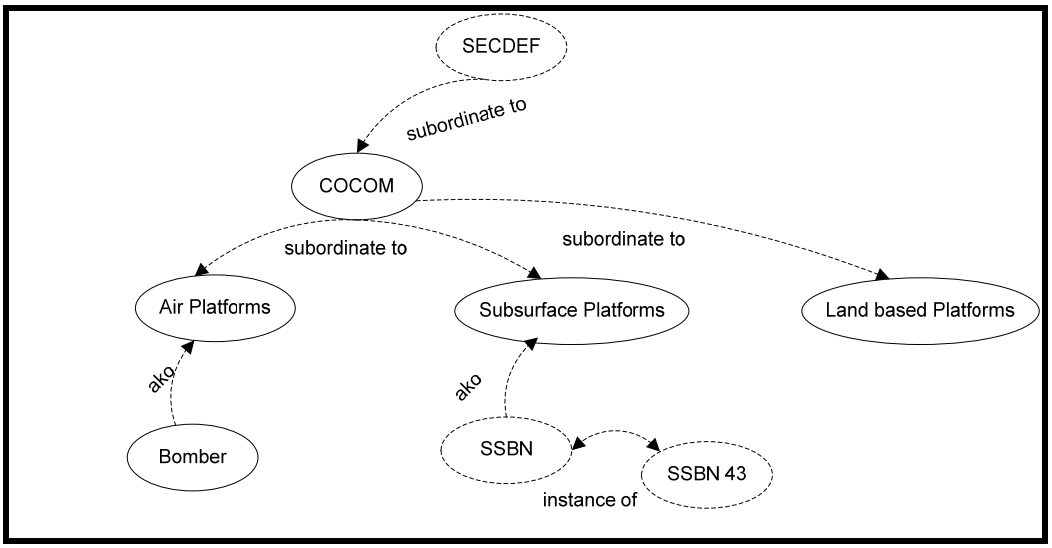

Figure 13. Sample C2 Domain Ontology

These sample ontologies give a better understanding of the complexity that we face when we consider a missile defense domain ontology will be inclusive of all three of these domains. It is also clear that more work will need to be done on the individual development of these ontologies but at this time we will use them as a foundation to build from, and they are reflected in the next section.

4. Sample Ontology for Missile Defense Domain

One of the more subjective portions of designing a ROEU is developing the Missile Defense Domain Ontology. Based on our use case analysis, we determine that there are three primary actors: the Sensors, the Missiles or Weapons and the C2. As stated earlier, an ontology consists of the relationships and knowledge about a particular domain. In this section, we will provide a sample Missile Defense Ontology that will be stored as the Domain Knowledge for the ROEU. The Domain Knowledge is necessary when one considers how things such as the requests levied on the system, the rules and the response actions.

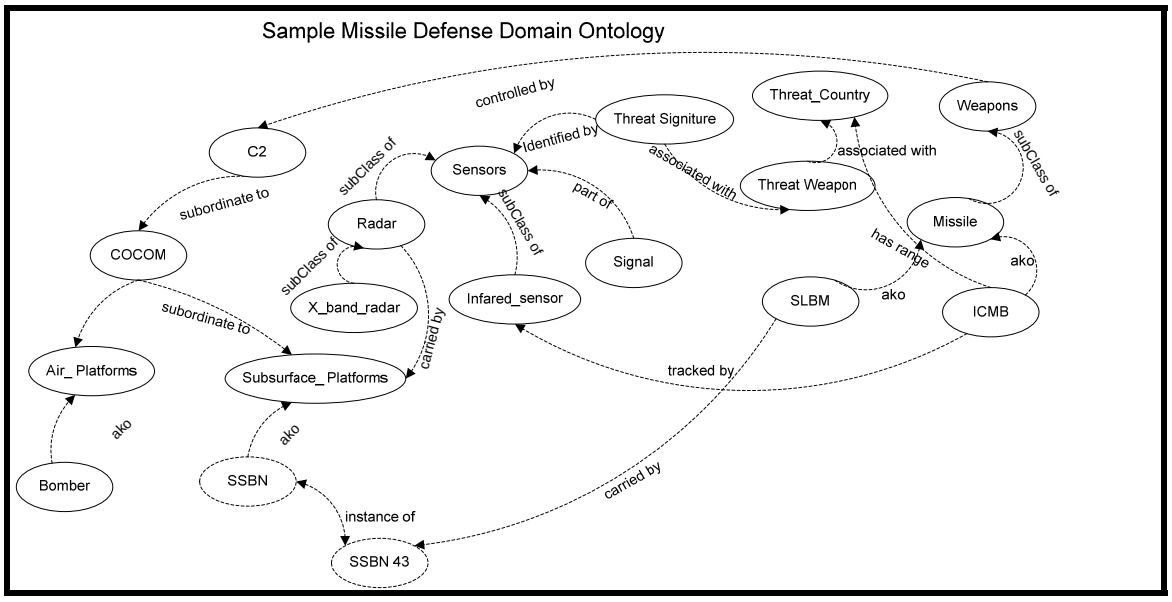

Figure 14. Sample Missile Defense Domain Ontology

5. Example of a Threat Engagement by ROEU

To understand how the sample ontology in Figure 14 and the rules in Table 2 are used by the ROEU, consider the scenario in which the Radar identifies or detects a Threat Signature; this signature is associated with a particular Threat Weapon and further associated with a particular Threat Country. We see that the sensor is on the subsurface platforms, which are equipped with, or carry Submarine-launched Ballistic Missiles (SLBMs). At this time, the specific submarine that could be assigned to respond is the SSBN 43. It is particularly important to note that the weapons system that has a range to action against the particular Threat Country is the Intercontinental Ballistic Missile (ICBM). Using this ontology, the Expert System will have to identify that there are no missiles that are in the domain knowledge that can respond to the threat, or we will have to reflect that the SLBM has the range to action against the threat. While this is going on, the system itself is running all of the data through the Expert System's Rule Base and Inference Engine to ensure we can execute and that it is in accordance with the ROE of missile defense for example Policy 1 needs to be met where three sources are tracking the threat.

E. CONCLUSION

In conclusion, what we derive from this chapter is a design for the ROEU. We have taken the time to propose an architecture that will best suit the adaptation of the architectures for the generic intercept system and the policy system that we have chosen. We then used the use

case analysis to understand the high-level software features of the system and conducted use case analysis to do the same for the ROE Unit specifically. We have discussed the scenarios used for this operation, as well as how those scenarios are used to develop ROE policies that were subsequently used to become the rules for the Expert System. We ensured that the rules where compatible with the Policy model that was chosen. Once we had our Rules, we then explored the Domain Knowledge by understanding ontology and presenting a sample ontology for the missile defense domain.

Now, by seeing this proposed design for the ROEU, we see that the Domain Knowledge requires an ontology of the domain space and that ontology will be called upon to understand the rules, which are reflected in the Expert System.

V. CONCLUSION AND RECOMMENDATIONS

A. REVISITING THE ISSUES

The need for a Ballistic Missile Defense system exists. This system, as a result of the domain, as well as the threats and actors associated with such threats, needs to be able to appropriately respond with the greatest level of accuracy, expedience and reliability. The framework for such a system must be one that has enabled automated ROE policies.

We have expressed through this work the importance that Rules of Engagement (ROE) play in the engagement of targets no matter what the situation. When looking at today's technology, the changing battlespace and the weapons systems that are in existence, full automation is required, and with full automation, any intercept system must be enabled with automated ROE policies as a component in its Battle Manager.

To realize and design this ROEU for the BM, we were able to explore and select a policy system that would allow the functionally required to accomplish the desired effect of Missile Defense. With the proposed architecture, we see its key component being the Expert System, which again includes the Rule Base and Inference Engine, and the Domain Knowledge. Key features of this work was the outline of the systems functions as defined using use case analysis to show what the system will do and the actor that interface with the system. We then presented examples of the key elements of the Expert System and Domain Knowledge, which

is represented by the Sample Missile Defense Domain Ontology, and the development of the sample rules for the system.

The remainder of this section is devoted to briefly reflecting on some ideas of future research areas with regards to the ideas covered with this body of work.

B. FURTHER DEVELOPMENT OF REQUIREMENTS FOR THE ROE UNIT

1. Functional Requirements

Functional Requirements simply relay the specific functionality that defines *what* we desire the unit or system to accomplish. Listed below are a general set of Functional Requirements. These will need to be further refined as a result of more extensive use case analysis and further design and testing of the proposed ROE Unit.

A. The unit shall display and differentiate data and rules as established by the domain.

B. The unit shall evaluate its behavior at the update of new data that may change the battlespace picture. New data may come from weapons, sensor, the battle manager itself, or even User-made injects.

C. The unit shall accept in test mode injects that present as realistic a view of the battlespace as possible.

D. The unit shall display and notify User immediately of software faults at runtime.

E. The unit shall provide a User with diagnostic presentation in test mode and operational mode.

F. The unit shall allow a User or maintainer to add, delete, or modify data, in particular the Rule of Engagement policies.

G. The unit shall be compatible, integrating numerous dynamic software systems, based on its various interfaces.

H. The unit shall have the capability to perform backward and forward chaining.

2. Non-functional Requirements

Non-functional requirements define how a system is supposed to *be*. Non-functional requirements are also considered the qualities or constraints of the system being created. These too would need to be further refined as the software development processes on this system evolves.

A. Utility

1. The training program and manual must be extensive but designed for all levels of users to become proficient at operating all aspects of the system.

2. The Graphic User Interface (GUI) must be user friendly and meet all Human Computer Interface (HCI) standards (Bevan, 1995). There must be no confusion as to the most important displays, buttons or how to navigate and maneuver.

3. All symbols and displays will need to be approved and meet all DoD standards.

B. Reliability

1. The unit shall have highest priority with all communication sources. In operational mode, no connectivity will take priority over data transfer to and from the system.

2. Maintainers and maintenance of systems must be available for 24/7 support.

3. One hundred percent accuracy is necessary for all transmissions validity.

4. One hundred percent of all messages will need to report transmission success or transmission failure.

C. Performance

1. The unit shall have absolute run time deadlines.

2. The unit will have the highest level of processing capability as to allow for the processing of massive amounts of simultaneous data transfer without the system getting hung processes.

3. The unit’s database capacity must be large enough that if it reached critical size, it would not stop processing, but rather, would pop the data from the stack into an external repository.

D. Interfaces

1. The components of the unit must be scalable as it evolves and grows interfaces must not be affected. This is a system of systems, and as such will interact with weapons systems, navigation systems and sensors.

E. Legal

1. The loaded and stored ROE policies in ass part of the domain knowledge must reflect national policy and international and domestic law. They will need to be approved by the appropriate COCOM's in compliance with Joint Chiefs of Staff instructions and guidance.

F. Security

1. The minimum required clearance level for the system is SECRET. This may vary depending on the environment and the test of targets or the approved ROE stored in the ROCU.

2. A minimum of SECRET-level security clearance will be required for all personnel who work on the development of this system and the associated Rules of engagement.

C. FUTURE WORK

Many follow-on topics are available in ROE automation including, but not limited to, the following topics:

1) Develop a complete ontology for Missile Defense domain.

2) Refine the rules for the Expert System.

3) Further architecture discussion as automated policies can be used in various domains. Some of those domains may be non-kinetic and require different interfaces and as such different requirements. What domains or environments can

actually benefit from policy automation systems and in particular, ROE policy automation?

4) Identify platforms will handle such a system of systems and explore their compatibility.

5) What is the level of knowledge and training programs for such a system?

6) How would you use and automate policy systems in Computer Network Operations?

7) Creation of the security portion of the system as some components may have multiple levels of security.

8) How can one maintain and test such a system?

9) Will the system support a rapidly changing environment? How many different threats can the system process?

10) Reliability studies to determine a level of confidence in the accuracy of the system.

11) Deconfliction of the policies and rules within the system. Will that be by the system itself or a maintainer? Does the technology exist for the system to identify and correct conflicts?

In the near term, additional research needs to be done to determine if the work presented can be reasonably developed. We have shown architecturally that the components can be interfaced, but as a system of systems that will be ready to appropriately respond to the threat needs further developing.

LIST OF REFERENCES

Bevan, N. (1995). Usability is Quality of Use. Anzai & Ogawa (Eds.) *Proceedings of the 6th International Conference on Human Computer Interaction.* Yokohama: Elsevier.

Buibish, A., Lange, A. & Woitalla, M. (2005). *Responsive Decision Making through Automated Policy-Enabled Systems In 10th ICCRTS, Track 1*. VA.

Caffall, S.D. (2005). *Developing Dependable Software for a System-of-Systems*. Ph.D. Dissertation, Monterey, CA: Naval Postgraduate School.

Davis, S.D., & Walton, T.B. (2004). Engineering Knowledge ACM Southeast Regional Conference archive. *Proceedings of the 42nd annual Southeast Regional Conference* (pp. 406-407).

Duminda, W.M., James, B., & Nerode, A. (2005). An Agent-based Framework for Assessing Missile Defense Doctrine and Policy. *Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'05).*

Garwin, R.L. (2004). Holes in the Missile Shield, *Scientific American* (pp. 70–79).

Gruber, T. (2003). *What is an Ontology?* From http://www-ksl.stanford.edu/kst/what-is-an-ontology.html (access date, September/09).

Department of Defense (2001). *Joint Publication (JP) 1-02: Department of Defense Dictionary of Military and Associated Terms.* Washington DC: Joint Doctrine Division.

Michael, J.B., Ong, V.L., & Rowe, N.C. (July 30 through August 2, 2001). *Natural-Language Processing Support for Developing Policy-Governed Software Systems*. 39th International Conference on Technology for Object-Oriented Languages and Systems. Santa Barbara, CA: IEEE Computer Society Press.

Michael, J.B., Nerode, A., & Wijesekera, D. (June 13-16, 2005). *Agent-Based Framework to Model Ballistic Missile Defense Strategies, An*. Tenth Command and Control Symposium. McLean, VA.

Michael, J.B. Weapons Systems Software Safety*. Rapid Action Surface-to-Air Missile (RASAM) System*. Fall, 2006 Naval Postgraduate School Course: SW4582.

Noy, N. & McGuinness, D. (March 2001). Ontology Development 101: A Guide to Creating Your First Ontology. *Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880*. From http://protege.stanford.edu/publications/ontology_ development/ontology101-noymcguinness html.

Silbey, E.H. (1993). Experiments in Organizational Policy Representation: Results to Date. In *Proceedings of the International Conference on Systems, Man and Cybernetics*. (pp. 337-342) Los Alamitos, CA: IEEE Computer Society Press.

Silbey, E.H., Michael, J.B. & Wexlblat, R.L. (1992). An Approach to Formalizing Policy Management. In P. Bourgine & B. Walliser (Eds.) *Economics and Cognitive Science* (pp. 155-169). Oxford: Pergamon Press.

Silbey, E.H, Michael, J.B. & Wexlblat, R.L. (1992). Use of an experimental policy workbench: Description ad Preliminary results. In Landwehr, C. E. & Jajodia, S. (Eds.), *Database Security, V: Status and Prospects* (pp. 47-76). Amsterdam: Elsevier Science (North-Holland).

Silbey, E.H, Wexlblat, R.L., Michael, J.B., Tanner, M.C., & Littman, D.C. (1993). The Role of Policy in Requirements Definition: the Next Challenge for Knowledge-Based Software Engineering. In *Proceedings of the IEEE International Symposium on Requirements Engineering* (pp. 277-280). Los Alamitos, CA: IEEE Computer Society Press.

Strassner, J. (2004). *Policy-Based Network Management; Solutions for the Next Generation*. Boston: Morgan Kauffman Publishers.

Weller, D.B., Boger, D.C., & Michael, J.B. (2004). Command structure of the Ballistic Missile Defense System. In Savoie, M.J., Chu, H.-W., Michael, J., and Pace, P., (Eds.) , *Proc. Int. Conf. on Computing, Communications and Control Technologies* (pp. 42-48). Austin, TX: Int. Institute of Informatics and Systemics.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Man-Tak Shing
   Naval Postgraduate School
   Monterey, California

4. Professor James Bret Michael
   Naval Postgraduate School
   Monterey, California