



2007-09

# An Analysis of the Open Architecture Warfare System Domain Model for surface time critical targets

Marshall, Jolene

Monterey, California. Naval Postgraduate School



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

**Dudley Knox Library / Naval Postgraduate School  
411 Dyer Road / 1 University Circle  
Monterey, California USA 93943**



# NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

**An Analysis of the Open Architecture Warfare System  
Domain Model for Surface Time Critical Targets**

by

Jolene Marshall, Eric R. LeMay, Joshua Tapp,  
Alfred T. Diotte, Daniel Quigley, John Givens,  
Kenneth Reszka, Curt Williams, and  
Mark Bonnett

September 2007

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

**NAVAL POSTGRADUATE SCHOOL  
Monterey, California 93943-5000**

Daniel T. Oliver  
President

Leonard A. Ferrari  
Provost

This report was prepared for the Chairman of the Systems Engineering Department in partial fulfillment of the requirements for the degree of Master of Science in Systems Engineering. Reproduction of all or part of this report is not authorized without permission of the Naval Postgraduate School. This report was prepared by the Masters of Science in Systems Engineering (MSSE) Cohort (Number) from the (Command(s)):

---

Jolene Marshall

---

Eric R, LeMay

---

Joshua Tapp

---

Alfred T. Diotte

---

Daniel Quigley

---

John Givens

---

Kenneth Reszka

---

Curt Williams

---

Mark Bonnett

Reviewed by:

---

J. M. Green, Ph.D.  
Project Advisor

---

C. A. Whitcomb, Ph.D.  
Project Advisor

Released by:

---

David H. Olwell, Ph.D.  
Department of Systems Engineering

---

Dan C. Boger  
Interim Associate Provost and Dean of  
Research

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> September 2007	<b>3. REPORT TYPE AND DATES COVERED</b> Joint Applied Project	
<b>4. TITLE AND SUBTITLE:</b> Title (Mix case letters) An Analysis of the Open Architecture Warfare System Domain Model for Surface Time Critical Targets			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> J. Marshall, E. LeMay, J. Tapp, A. Diotte, D. Quigley, J. Givens, K. Reszka, C. Williams, M. Bonnett				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this report are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Distribution Statement (mix case letters)			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b> This study's objective is to evaluate the Open Architecture Warfare System Domain Model (OAWSDM) against time critical targets with specific focus on command, control, and communication processes.  A functional analysis of the OAWSDM was conducted and synthesized to create the Open Architecture Time Critical Target Engagement Process Model (OATCTEPM). This model represents the notional engagement cycle of a Navy cruiser. Two scenarios were developed to exercise the system: a surprise assault from a number of personal watercraft and a saturation assault in which approximately fifty craft of varying sizes attack. Results from these scenarios were analyzed for system bottlenecks and recommendations were made to improve decision making processes and reduce engagement time.  This study concludes that while the OAWSDM may offer no technical flaws in its design, it fails to factor in the role of the human in the decision making and engagement processes. In doing so it overlooks a key factor in the effectiveness of the architecture against surface TCT engagements.				
<b>14. SUBJECT TERMS</b> Open Architecture, Time Critical Targeting, Netted Sensors			<b>15. NUMBER OF PAGES</b> 226	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU	

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

This study's objective is to evaluate the Open Architecture Warfare System Domain Model (OAWSDM) against time critical targets with specific focus on command, control, and communication processes.

A functional analysis of the OAWSDM was conducted and synthesized to create the Open Architecture Time Critical Target Engagement Process Model (OATCTEPM). This model represents the notional engagement cycle of a Navy cruiser. Two scenarios were developed to exercise the system: a surprise assault from a number of personal watercraft and a saturation assault in which approximately fifty craft of varying sizes attack. Results from these scenarios were analyzed for system bottlenecks and recommendations were made to improve decision making processes and reduce engagement time.

This study concludes that while the OAWSDM may offer no technical flaws in its design, it fails to factor in the role of the human in the decision making and engagement processes. In doing so it overlooks a key factor in the effectiveness of the architecture against surface TCT engagements.



THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
	<b>A. PROBLEM STATEMENT .....</b>	<b>1</b>
	<b>B. BACKGROUND .....</b>	<b>2</b>
	<b>1. Time Critical Targets .....</b>	<b>2</b>
	<i>What is a time critical target? .....</i>	<i>2</i>
	<i>Why is a time critical target important? .....</i>	<i>2</i>
	<i>How is a time critical target typically prosecuted? .....</i>	<i>4</i>
	<i>What deficiencies exist in targeting a time critical target? .....</i>	<i>4</i>
	<b>2. Target Engagement Process.....</b>	<b>4</b>
	<b>3. Target Kill.....</b>	<b>5</b>
	<b>4. Open Architecture Warfare System Domain Model .....</b>	<b>6</b>
	<b>C. RESEARCH OBJECTIVES .....</b>	<b>8</b>
	<b>D. SITUATION ASSESSMENT.....</b>	<b>8</b>
	<b>1. The Past.....</b>	<b>8</b>
	<b>2. Present.....</b>	<b>10</b>
	<b>3. Future.....</b>	<b>12</b>
	<b>E. APPROACH AND METHODOLOGY .....</b>	<b>15</b>
	<b>1. Research Current Naval Doctrine.....</b>	<b>16</b>
	<b>2. Identify Important Enablers.....</b>	<b>16</b>
	<b>3. Decompose and Analyze the OAWSDM.....</b>	<b>16</b>
	<b>4. Develop a TCT Engagement Model .....</b>	<b>17</b>
	<b>5. Develop Time Critical Targeting Scenarios .....</b>	<b>17</b>
	<b>6. Develop Measures of Effectiveness.....</b>	<b>17</b>
	<b>7. Obtain and Analyze Baseline Results.....</b>	<b>17</b>
	<b>8. Incorporate Model Improvements and Rerun.....</b>	<b>18</b>
	<b>9. Document Results and Recommendations.....</b>	<b>18</b>
	<b>F. SCOPE .....</b>	<b>18</b>
	<b>G. OUTPUTS.....</b>	<b>18</b>
	<b>H. ORGANIZATION OF THE PAPER.....</b>	<b>19</b>
<b>II.</b>	<b>LITERATURE SEARCH .....</b>	<b>21</b>
	<b>A. OPEN ARCHITECTURE.....</b>	<b>21</b>
	<b>B. FORCENET .....</b>	<b>23</b>
	<b>C. TIME CRITICAL TARGETING .....</b>	<b>27</b>
	<b>1. DoD Joint Perspective.....</b>	<b>27</b>
	<b>2. Service Component Perspectives .....</b>	<b>28</b>
	<i>Air Force Efforts .....</i>	<i>28</i>
	<i>Navy Efforts.....</i>	<i>29</i>
	<i>Army Efforts.....</i>	<i>29</i>
	<b>3. Private Industry Perspectives .....</b>	<b>30</b>
	<b>4. Additional Views .....</b>	<b>30</b>
	<b>D. FUTURE NAVAL FIRES .....</b>	<b>31</b>
	<b>1. First Pillar.....</b>	<b>31</b>

2.	Second Pillar .....	31
3.	Third Pillar .....	32
4.	Fourth pillar .....	32
E.	NETTED SENSORS AND EXPEDITIONARY PERVASIVE SENSING .....	33
1.	Evolution of Network Centric Concepts .....	33
2.	Beyond the Status Quo .....	34
3.	Applicability to Time Critical Targeting .....	35
F.	SERVICE ORIENTED ARCHITECTURE.....	36
G.	TARGET ENGAGEMENT AND THE OODA MODEL .....	36
H.	SUMMARY OF LITERATURE SEARCH.....	41
III.	ANALYSIS OF THE OAWSDM .....	43
A.	SYSTEMS ENGINEERING DESIGN PROCESS .....	43
B.	OPEN ARCHITECTURE WEAPONS SYSTEM DOMAIN MODEL DECOMPOSITION.....	46
1.	Search / Detect (S/D).....	47
2.	Data / Information Services (DIS) .....	48
3.	Planning, Assessment & Decision (PAD) .....	49
4.	Weapon / Asset Services (W/AS) .....	51
5.	Mission Execution (ME) .....	52
6.	External Communication (EXCOMM) .....	53
7.	Common Services (CS).....	54
8.	Training (TR) .....	55
9.	Force Planning / Coordination (FP/C).....	57
10.	OAWSDM Analysis .....	58
C.	INPUT – OUTPUT ANALYSIS .....	58
D.	SCOPE AND BOUNDS ANALYSIS.....	59
E.	FUNCTIONAL ANALYSIS .....	62
1.	Function Flow Analysis .....	63
IV.	MODEL DESIGN .....	69
A.	MODELING GOALS.....	69
B.	OPERATIONAL VIEW.....	69
C.	METRICS DEFINITION.....	71
1.	Introduction.....	71
2.	Baseline Model MOPs.....	72
3.	Total C3I Time MOP.....	73
4.	Measures of Effectiveness.....	74
5.	MOE and MOP Comparison .....	75
6.	Use of MOEs in the OATCTEPM .....	75
D.	MODEL SCENARIO DEFINITION .....	75
E.	MODEL AND SCENARIO ASSUMPTIONS.....	76
1.	Rules of Engagement .....	76
2.	ROE Based Assumptions.....	77
3.	Scenario Assumptions.....	77
4.	Scenario 1 Specific Assumptions .....	79
	Scenario 2 Specific Assumptions .....	79

5.	Overall Model Assumptions.....	80
F.	RADAR MODEL DESIGN.....	81
G.	OATCTEPM SIMULATION MODEL DESIGN.....	81
H.	LIMITATIONS.....	83
V.	RESULTS AND ANALYSIS .....	85
A.	DISCUSSION OF MOPS AND MOES USED TO ANALYZE RESULTS .....	85
1.	Discussion of Time-Based MOPs.....	86
	<i>Validate Target Time</i> .....	86
	<i>Identify Target Time</i> .....	87
	<i>Threat Evaluation Time</i> .....	87
	<i>Assign Target Priority Time</i> .....	88
	<i>Mission Evaluation Time</i> .....	88
	<i>Weapon Assignment Time</i> .....	89
	<i>Plan Approval Time</i> .....	89
2.	Discussion of MOEs .....	90
	<i>Probability of Leaker</i> .....	90
	<i>Probability of Raid Annihilation</i> .....	90
	<i>Probability of Success</i> .....	91
B.	BASELINE MODEL .....	91
C.	IDEALIZED MODEL .....	94
D.	COMPARISON OF BASELINE AND IDEALIZED MODELS.....	96
E.	ANALYSIS OF IMPROVED MODEL .....	97
F.	RESULTS OF IMPROVED MODEL .....	101
VI.	CONCLUSION .....	105
A.	STUDY CONCLUSIONS.....	105
B.	FUTURE WORK.....	105
APPENDIX I: SCENARIOS FOR TIME CRITICAL TARGETING (TCT)		
	SIMULATION .....	109
	GEO-POLITICAL SITUATION .....	109
	SCENARIO #1 - ATTACK BY A GROUP OF TYPE-1 FAST INSHORE	
	ATTACK CRAFT (FIAC).....	115
	Tactical Situation (TACSIT).....	115
	Assumptions .....	115
	Blue Force Posture.....	116
	Red Force Posture.....	116
	The Attack .....	117
	SCENARIO #2 - FIAC SATURATION ATTACK.....	119
	TACSIT: .....	119
	Assumptions: .....	121
	Red Force Posture: .....	122
	The Attack .....	122
APPENDIX II: DETAILED DISCUSSION OF OATCTEPM DESIGN .....		
1.0	SEARCH/DETECT (S/D) .....	125
2.0	DATA/INFORMATION SERVICES (DIS).....	126

3.0	PLANNING, ASSESSMENT, AND DECISION (PAD)	128
4.0	WEAPON / ASSET SERVICES (W/AS)	132
5.0	MISSION EXECUTION (ME)	133
6.0	EXTERNAL COMMUNICATIONS (EXCOMM)	138
7.0	COMMON SERVICES (CS)	139
8.0	TRAINING (TR)	142
9.0	FORCE PLANNING / COORDINATION (FP/C)	142
	OATCTEPM PROCESS VARIABLES	143
	OATCTEPM ENGAGEMENT FLOW	151
	OATCTEPM PROCESS VARIABLE INPUT DISTRIBUTIONS	163
<b>APPENDIX III: RADAR MODEL DETAILED EXPLANATION OF</b>		
	<b>CALCULATIONS</b>	<b>183</b>
	<b>PURPOSE OF THE RADAR MODEL</b>	<b>183</b>
	<b>RADAR MODEL ASSUMPTIONS</b>	<b>183</b>
	<b>DESIGN OF THE RADAR MODEL</b>	<b>184</b>
<b>APPENDIX IV: IMPROVED MODEL STUDY</b>		
	<b>A. INTRODUCTION</b>	<b>187</b>
	<b>B. SCENARIO 1 OUTPUT</b>	<b>187</b>
	<b>C. SCENARIO 2 OUTPUT</b>	<b>190</b>
	<b>LIST OF ACRONYMS</b>	<b>195</b>
	<b>LIST OF REFERENCES</b>	<b>199</b>
	<b>INITIAL DISTRIBUTION LIST</b>	<b>207</b>

## LIST OF FIGURES

Figure 1.	Target Engagement Process.....	5
Figure 2.	Open Architecture Warfare System Domain Model (OAWSDM).....	7
Figure 3.	FORCENet and relationship to the Global Information Grid.....	26
Figure 4.	OODA Loop Model.....	37
Figure 5.	OODA, DCE, and JDL Data Fusion Model.....	40
Figure 6.	The Vee Model for the SEDP (Blanchard and Fabrycky 2006).....	43
Figure 7.	Architecture Analysis Vee Diagram.....	44
Figure 8.	Time Critical Target Architecture Flow Context Diagram.....	62
Figure 9.	Functional Flow Block Diagram for Observe.....	64
Figure 10.	Functional Flow Block Diagram for Orient.....	65
Figure 11.	Functional Flow Block Diagram for Decide.....	66
Figure 12.	Functional Flow Block Diagram for Act.....	67
Figure 13.	Operational View (OV-1) for TCT scenarios.....	70
Figure 14.	Simplified Concept of Model.....	71
Figure 15.	Time-based MOP formulation for FIAC scenarios.....	73
Figure 16.	Process Flow for the Main Functional Modules of the OATCTEPM.....	82
Figure 17.	C.I. for Baseline Results of MOEs in Scenarios 1.....	92
Figure 18.	C.I. for Baseline Results of MOEs in Scenarios 2.....	92
Figure 19.	Baseline Results of Time-Based MOPs in Scenario 1.....	94
Figure 20.	Baseline Results of Time-Based MOPs in Scenario 2.....	94
Figure 21.	C.I. for Idealized Results of MOEs in Scenario 1.....	95
Figure 22.	C.I. for Idealized Results of MOEs in Scenario 2.....	96
Figure 23.	Scenario 1 C <sup>3</sup> Time Based MOP Improvement.....	98
Figure 24.	Scenario 1 MOE Improvement.....	99
Figure 25.	Scenario 2 C <sup>3</sup> Time Based MOP Improvement.....	100
Figure 26.	Scenario 2 MOE Improvement.....	100
Figure 27.	Map of Mandeb Straight and Gulf of Aden.....	110
Figure 28.	Map of the Gulf of Oman and the Persian Gulf.....	111
Figure 29.	Red Cell Attack Plan.....	118
Figure 30.	Map of the Strait of Hormuz and Persian Gulf Area.....	120
Figure 31.	Search / Detect (S/D) Function.....	151
Figure 32.	Data / Information Services (DIS) Function.....	152
Figure 33.	Data / Information Services (DIS) Function Continued.....	153
Figure 34.	Planning, Assessment, and Decision (PAD) Function.....	154
Figure 35.	Planning, Assessment, and Decision (PAD) Function Continued.....	156
Figure 36.	Planning, Assessment, and Decision (PAD) Function Continued.....	157
Figure 37.	Weapon / Asset Services (W/AS).....	158
Figure 38.	Mission Execution (ME) Function for Gun Weapon System (GWS).....	159
Figure 39.	Mission Execution (ME) Function for Close-In Weapon System (CIWS).....	160
Figure 40.	Mission Execution (ME) Function for Precision Attack Missile (PAM).....	161
Figure 41.	Mission Execution (ME) Function for Armed Helicopter (Helo).....	162
Figure 42.	Input Analyzer Firm Track Times for Scenario 1.....	163
Figure 43.	Input Analyzer Validate Target Times for Scenario 1.....	164

Figure 44.	Input Analyzer Identify Target Times for Scenario 1.....	165
Figure 45.	Input Analyzer Threat Evaluation Times for Scenario 1.....	166
Figure 46.	Input Analyzer Target Priority Times for Scenario 1.....	167
Figure 47.	Input Analyzer Mission Evaluation Times for Scenario 1.....	168
Figure 48.	Input Analyzer Weapon Assignment Times for Scenario 1.....	169
Figure 49.	Input Analyzer Plan Approval Times for Scenario 1.....	170
Figure 50.	Input Analyzer Clearance to Fire Times for Scenario 1.....	171
Figure 51.	Input Analyzer Direct Engagement Times for Scenario 1.....	172
Figure 52.	Input Analyzer Firm Track Times for Scenario 2.....	173
Figure 53.	Input Analyzer Validate Target Times for Scenario 2.....	174
Figure 54.	Input Analyzer Identify Target Times for Scenario 2.....	175
Figure 55.	Input Analyzer Threat Evaluation Times for Scenario 2.....	176
Figure 56.	Input Analyzer Target Priority Times for Scenario 2.....	177
Figure 57.	Input Analyzer Mission Evaluation Times for Scenario 2.....	178
Figure 58.	Input Analyzer Weapon Assignment Times for Scenario 2.....	179
Figure 59.	Input Analyzer Plan Approval Times for Scenario 2.....	180
Figure 60.	Input Analyzer Clearance to Fire Times for Scenario 2.....	181
Figure 61.	Input Analyzer Direct Engagement Times for Scenario 2.....	182
Figure 62.	Average Number of Leakers per Improved Model.....	188
Figure 63.	Average Number of Targets per Improved Model.....	188
Figure 64.	Average C <sup>3</sup> Time per Improved Model.....	189
Figure 65.	Average Probability of Raid Annihilation per Improved Model.....	189
Figure 66.	PAN Results for Scenario 1.....	190
Figure 67.	Average Number of Leakers per Improved Model.....	191
Figure 68.	Average Number of Targets per Improved Model.....	191
Figure 69.	Average C <sup>3</sup> Time per Improved Model.....	192
Figure 70.	Average Probability of Raid Annihilation per Improved Model.....	192
Figure 71.	PAN Results for Scenario 2.....	193

## LIST OF TABLES

Table 1.	Desired Inputs and Outputs of the OAWSDM .....	59
Table 2.	Scope and Bounds Analysis.....	61
Table 3.	Assumptions Derived from the Model Rules of Engagement .....	77
Table 4.	Threat and Ship Assumptions Common to Both Scenarios.....	78
Table 5.	Scenario 1 Specific Assumptions.....	79
Table 6.	Scenario 2 Specific Assumptions.....	79
Table 7.	Assumptions for Weapon Systems Used in the OATCTEPM.....	80
Table 8.	Baseline Results for MOEs.....	91
Table 9.	Idealized Results for MOEs .....	94
Table 10.	Comparison of Idealized and Baseline Results for Scenario 1 and 2 .....	96
Table 11.	MOEs for the Idealized and Base Models .....	97
Table 12.	Range of Values Considered Improvements in MOEs.....	97
Table 13.	Summary of Improved Results for Scenario 1 and Scenario 2.....	101
Table 14.	Comparison of Improved Results to Idealized and Baseline Results .....	102
Table 15.	Performance Changes from Baseline Model to Improved Model .....	103
Table 16.	Number of Leakers to Engaged Targets and $C^3$ Times.....	104
Table 17.	Summary of Threats.....	114
Table 18.	Scenario 1 Target Information .....	119
Table 19.	Scenario 2 Target Information .....	123
Table 20.	Create Basic Process Block .....	143
Table 21.	Process – Basic Process Blocks .....	145
Table 22.	Assign – Basic Process Blocks .....	147
Table 23.	Decide – Basic Process Blocks .....	149
Table 24.	Record – Basic Process Blocks.....	150
Table 25.	Dispose – Basic Process Blocks .....	150
Table 26.	Radar Model Assumptions.....	183
Table 27.	Ranges (m) for a RCS of $1 m^2$ .....	185
Table 28.	Radar Range (m) as a Function of RCS ( $m^2$ ) for given $P_D$ .....	186



THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

The authors of this paper would like extend their thanks, first and foremost to our families who have supported our hard work and long hours, who have endured endless interruptions and telephone calls from classmates and who have been forced to pick up additional work around the house because we were consumed by school work.

We would like to thank Professor (Lt. Col, USMC) Serg Posadas for assisting us with our model. We appreciate the time you took to review our model and help us better navigate the Arena software.

We would also like to thank Tony Cece for his graphical arts assistance. He was directly responsible for transforming our clumsy power point and stick figures into the functional analysis and scenario graphics found in this paper.

Finally, we would like to thank Professors Mike Green and Clifford Whitcomb for their efforts as our Academic Advisors and guidance throughout this capstone project.

THIS PAGE INTENTIONALLY LEFT BLANK

## **EXECUTIVE SUMMARY**

The purpose of this study is to evaluate the Open Architecture Warfare System Domain Model (OAWSDM) against surface time critical targets with a primary focus on Command, Control, and Communication (C3) processes. In addition, to the concepts of Open Architecture this project explores FORCEnet and various technological applications to improve the time required to engage small boat attacks.

Beginning with the OAWSDM, a functional analysis was conducted to better understand the component functions in the architecture. These functions were then synthesized into the Open Architecture Time Critical Target Engagement Process Model (OATCTEPM) created in the Arena® software package. This model represents the notional engagement cycle of a Navy cruiser from the time the threat is detected until it is neutralized. Two scenarios were developed to exercise the system. The first scenario is a surprise assault from a number of small personal watercraft. The second scenario is a saturation assault in which approximately fifty crafts of varying sizes attack. Results from these scenarios were analyzed for system bottlenecks and process critical paths. Using this data, recommended improvements to data flow and decision making were implemented and the scenarios rerun.

The study concludes that, with respect to time critical targets, the time required to process the embedded C3 functions is excessive given the limited engagement window presented by TCT. Processes that required human interaction showed the longest delays and impacted the effectiveness of the OAWSDM against time critical targets. Future research in the C3 element should focus on reducing the time required to execute those sub-elements requiring human interaction through the implementation of automated decision support systems.

# I. INTRODUCTION

## A. PROBLEM STATEMENT

Over the last twenty years the mission of the US Navy has evolved considerably. Consequently, as the cold-war era moved to the war on terrorism, traditional naval battle-group warfare has given way to a more network-centric based architecture, which can range from a single-platform combating close-in targets, to coordinated global information warfare. In response, naval leadership has steered its emphasis toward a theoretical model, known as the Open Architecture Warfare System Domain Model (OAWSDM) to address the multitude of changing, and new, mission requirements for the US Navy.

As part of this new era of terrorism, the enemy seeks to use unconventional methods and surprise to inflict maximum damage. Therefore this paper examined the OAWSDM, as presented, to determine its effectiveness against time critical targets. To test this architecture, a detailed model based on the OAWSDM was developed and evaluated to determine its effectiveness. Specific focus was applied to the Command, Control, and Communication (C<sup>3</sup>) portion of the architecture and alternatives were explored in an effort to shorten the kill chain.

In order to evaluate the OAWSDM, two scenarios presented were developed to serve as inputs for the Open Architecture Time Critical Targeting Engagement Process Model (OATCTEPM) (constructed using the Arena® software package), as it has been interpreted by the authors of this paper. These scenarios represent attacks by potential adversaries and terrorist organizations in the regions where they are staged. Both scenarios involve Fast In-shore Attack Craft (FIAC) designed to disable or destroy a US Naval High-Value Unit (HVU). These are further discussed later in the paper and technical details of these scenarios are presented in Appendix I.

## **B. BACKGROUND**

To fully understand the problems presented by a TCT, there are several key topics that must be defined and understood. These topics encompass time critical targets, kill chains and types of target kill and are meant to familiarize the reader with these topics prior to proceeding through the rest of the paper. The OAWSDM is also discussed in this section to provide background information on the functional model.

### **1. Time Critical Targets**

In order to understand the problems presented by a time critical target, some fundamental questions first must be addressed on what is meant by a Time Critical Target (TCT) and how it is different from a typical target. Specifically, the following questions are answered:

1. What is a TCT?
2. Why is a TCT important?
3. How is a TCT typically prosecuted?
4. What deficiencies exist in targeting a TCT?

#### ***What is a time critical target?***

A time critical target, as the name implies, "...is one with a limited window of vulnerability or engagement opportunity during which it must be found, located, identified, targeted, and engaged" (Perry and others 2002). The firing solution for this type of target must flow through the targeting process quickly in order to achieve a target kill. Once acquired, a TCT requires an immediate response. The difficulty in targeting a TCT lies in the fact that all targeting phases must act with a limited amount of time.

#### ***Why is a time critical target important?***

In the late 1990s, the Government Accountability Office (GAO), along with the service doctrine commands identified the need for engagement of a TCT.

Enemies have realized that techniques such as hiding, deception, and constant movement have been very effective against the United States and have exploited these tactics with some success. One recent example of a TCT attack was that perpetrated on the USS COLE, which occurred on October 12, 2000. That morning, the ship was approached on the port side by a small craft with an explosive device onboard. It detonated, killing seventeen sailors and leaving a 35 by 36 foot hole in the side of the destroyer. The Judge Advocate General Manual (JAGMAN) investigation of the USS COLE bombing found that "the Commanding Officer of COLE did not have the specific intelligence, focused training, appropriate equipment or on-scene security support to effectively prevent or deter such a determined, preplanned assault on his ship" going on to recommend significant changes in Navy procedures. (National Commission on Terrorist Attacks 2004)

A second example of a TCT in modern warfare is that of valuable enemy assets that must be eliminated when the opportunity arises. These could take the form of enemy leadership or highly mobile weapons. "In Operation Desert Storm, Scud missile transporter-erector-launcher (TEL) vehicles constantly eluded coalition efforts to find them as they launched 40 missiles into Israel. Even though [General] Charles Horner, joint force air and space component commander (JFACC), prioritized the destruction of Scud TELs to a high level and dedicated more than 4,700 sorties to the effort, postwar intelligence showed no proof that a single Scud was destroyed." (Marzolf 2004) Missed opportunities to capture enemy leadership have been publicized in the news over and over again. When the US began the effort to ensure the newly formed government of Afghanistan would succeed, called Operation Anaconda, by initiating a push to capture or kill the remaining Taliban and Al Qaeda members still hiding in that country, many managed to escape into neighboring Pakistan. Those who eluded capture include Osama Bin Laden, who still remains free to this day, in part because of the inefficiency of the Time Critical Targeting process. (Lambeth 2005).

### ***How is a time critical target typically prosecuted?***

A TCT is subjected to the same targeting phases as other targets, but the process must be completed in a much smaller time period. The general process for prosecuting any target involves locating, identifying, tracking, attacking, and evaluating. Due to the small amount of time to prosecute a TCT, lost opportunities become common. Unfortunately this allows the TCT to appear, complete its mission, and disappear. The engagement process is further detailed as well as the use of soft and hard kills.

### ***What deficiencies exist in targeting a time critical target?***

The Office of Naval Research (ONR) identified Time Critical Targets as a future threat for which defensive and offensive capabilities must be established. The ONR report went on to state that the enemy "...will be mobile and moving, they will do their best to hide in clutter, and they will be uncomfortably close to friends and neutrals." (Office of Naval Research 2001) Problems with engaging TCTs include "...a lack of necessary information and time constraints." (Marzolf 2004) In order to engage TCTs successfully, there must be a seamless flow of information between assets within the battlespace, allowing the war fighters to have a heightened level of awareness. It is conceivable that if the USS COLE had this heightened awareness level and had obtained information about a possible small boat attack that the outcome of this event would have been much different. Open Architecture and FORCEnet are intended to be key enablers for the development of solutions that provide this necessary, seamless flow of information between assets in the battlespace.

## **2. Target Engagement Process**

One of the many goals of OA implementation is to shorten the time-line associated with a combat system's Detect, Control, and Engage (DCE) functions. This sequence of events is known in the vernacular as the "kill chain". The kill chain is analogized with the well-known "OODA-Loop" model (Observe, Orient, Decide, and Act) and is the fundamental underlying process undertaken subconsciously by humans in almost any endeavor requiring action. The steps are compared in figure 1.



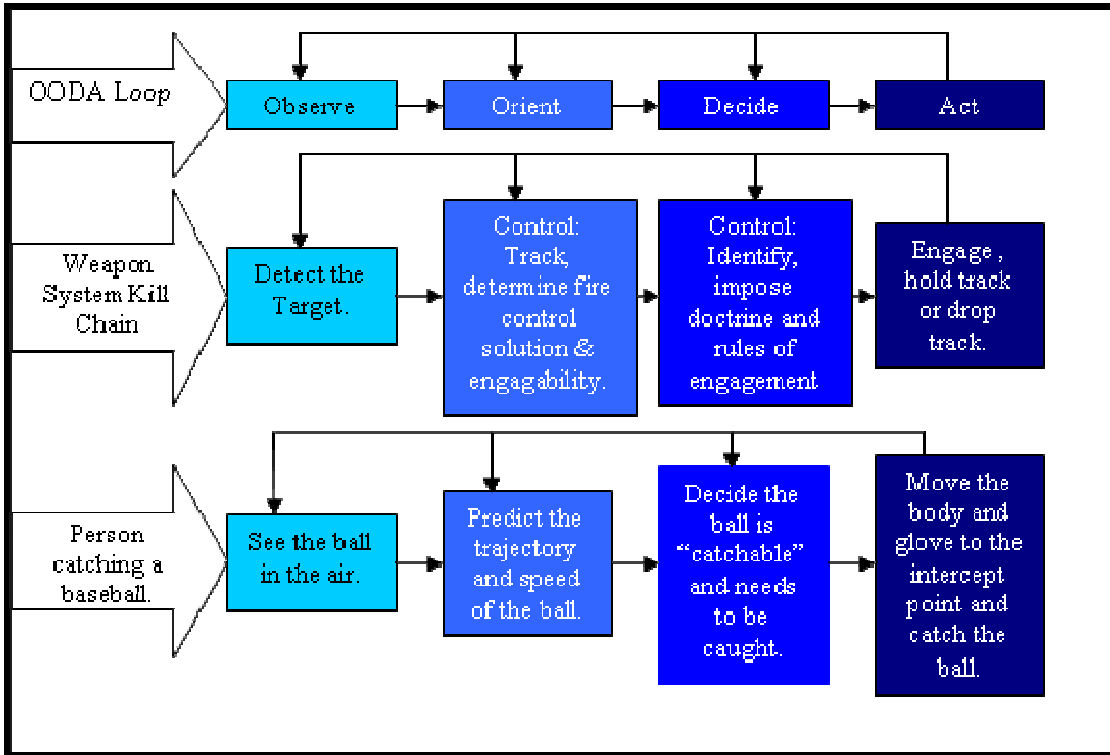


Figure 1. Target Engagement Process

*This comparison demonstrates that the Kill Chain is fundamentally based on the same basic process as the OODA Loop or a basic human decision loop.*

It is logical to assert here, that a shorter kill chain supports the concepts of intercepting an inbound target farther away from own ship, freeing up assets to support other engagements in the queue (or re-engagement of a target, in the event of a miss).

### 3. Target Kill

There are varying levels of kill assessments for different types of targets and weapons. Naveh (2001) defined the hard kill as the actual physical contact between the interceptor (whole, or fragments) and the target, causing its destruction versus a soft kill, which is brought about by preventing the target from completing its mission through the use of electronic countermeasures (jamming). Other types of “kills” include mission and

mobility kill, which are closely related and refer to incapacitating the target to a level that renders it ineffective.

For the purposes of this paper, the term “target kill” refers to the complete destruction of the targets of interest through direct contact by the interceptor. Additionally, there is no observed difference among the definitions for a hard kill, mission or mobility kill. This approach was used to facilitate the behavior of the model and eliminate confusion in this area.

#### **4. Open Architecture Warfare System Domain Model**

The concepts of Open Architecture (OA), FORCEnet, and others are defined and discussed in detail in the next section of this paper; however, a short introduction to the OAWSDM is given here, as this key concept serves as the backbone of this report. The OAWSDM, depicted in figure 2, has been published in the FORCEnet Implementation Strategy (NRC 2005), as well as many other reports and papers.

The strategy serves to demonstrate the framework for a loosely-coupled, service-oriented combat system architecture, which is important to realizing the goals of network-centric operations. The second section of this paper describes the interrelationships between the OAWSDM, FORCEnet and the Sea Power 21 vision in more detail. A true instantiation of this framework does not exist today; however, there are some services such as Inertial Navigation Systems (INS) and Precise Time and Time Interval (PTTI) (based on Global Positioning System (GPS) networks), which are enabling technologies in the form of achieving target correlation among separated platforms and achieving common track pictures.

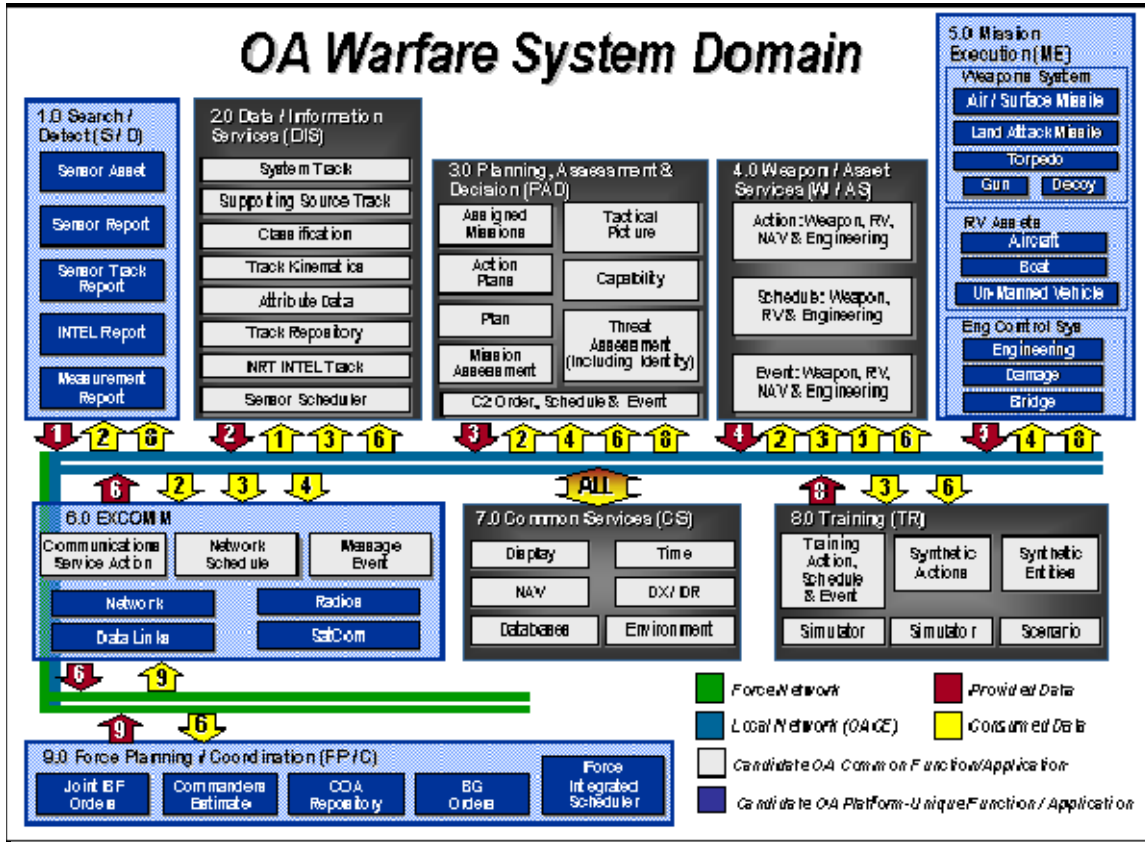


Figure 2. Open Architecture Warfare System Domain Model (OAWSDM)

*This paper serves to evaluate the OAWSDM in its handling of time critical targets. The model was developed to address the implementation of OA on Navy ships. (Deerin and others 2006)*

The service-oriented nature of this architecture enables the cross-utilization of resources among the current service-specific air, subsurface, surface, and land warfare domains. It is hypothesized here that the OAWSDM, while capable of supporting many functions across all warfare domains, is not sufficient for addressing certain forms of time critical targets (TCTs) in the surface warfare domain.

## **C. RESEARCH OBJECTIVES**

The objective of this research paper is to document the evaluation of the Open Architecture Warfare System Domain Model as a foundation for future systems that must engage time critical targets. This includes whether the OAWSDM is valid in these engagements and if there are any improvements that can be made to more effectively deal with a TCT. While the OAWSDM involves the target engagement sequence from initial detection to putting ordnance on target, this research focuses on the command, control, and communication functions within the architecture, holding both the detection and weapon capabilities as constant across all analyses. Given this overall objective, a research methodology is defined in support of this objective. This methodology is delineated below and explored in the rest of this paper.

## **D. SITUATION ASSESSMENT**

From the objective, all the relevant areas were researched, from operational doctrines such as Future Naval Fires to technologies that would help implement and improve this time critical engagement such as FORCEnet and automated decision aids. The next section offers a historical perspective on the need for this research.

### **1. The Past**

In recent history, experiences in the Persian Gulf (1991 and 2003-present) and Kosovo (1995-1998) revealed a limited ability to rapidly identify and strike time critical targets. In the Gulf War, for example, Air Force and Navy pilots were frustrated in attempts to destroy mobile Scud launchers before the vehicles fired their missiles. US aircraft had an extremely small window of opportunity to destroy the missiles on the ground. The time it took to locate the launchers exceeded the time it took the Iraqis to shoot and relocate (Hebert 2003). The time needed to effectively attack these mobile targets is much shorter than the established 30 to 72 hour targeting cycle needed to attack most ground targets (Wiggins 2001). Even more so than the semi-stationary Scud

launcher in clear skies, emerging targets are a challenge at night and even more of a challenge when there is significant weather (Hebert 2003).

At this time, it was noted that all the systems involved in the sensor to shooter process do not operate effectively together. The many systems needed to identify and strike targets are separately owned and operated by each of the military services as well as other Department of Defense (DOD) and intelligence community agencies. During these operations, over 100 command, control, communications, intelligence, surveillance, and reconnaissance systems were needed to identify and strike a target. These systems had limited ability to interoperate both technically (such as incompatible data formats) and operationally (legacy sensors tend to work in classic stovepipes that do not share data outside of the domain of the host system (Rushton 2004)). Given this reality, these systems simply cannot easily and quickly exchange the information to combat time critical targets (Wiggins 2001).

The Joint Forces Commander was faced with integrating more than 400 different mission and software applications resulting in over 100 different operational architecture efforts. The DOD's Director for Interoperability estimated that there were \$36 billion worth of systems that the services planned to buy that would not be able to operate together effectively. The Joint Interoperability Test Command (JITC), whose mission it is to test pieces of equipment that pertain to multiple branches of the armed services or other agencies, does not have the facilities needed to test the interactions between all weapons systems and information systems. Due to this factor, organizations have not always complied with the interoperability testing and certification process. At this time, the Joint Requirements Oversight Council (JROC) was also not focused on evaluating systems from a joint war fighting perspective. DOD still lacks a joint service concept of operations to defeat time critical targets and, as a result, each military service plans and acquires systems to meet requirements under its own concept of operations. The only acceptable solution decided upon was that duplicative and disparate systems would not be allowed to go forward (Wiggins 2001).

## **2. Present**

While much has improved in the past decade, there is still much work ahead. During Operation Enduring Freedom in Afghanistan, the Air Tasking Order (ATO) has been decreased from 72 to 24 hours, and 80 percent of the targets destroyed were passed to pilots after they had left the carrier deck showing a definite improvement since operations in the early and mid nineties (NRC 2005). The Navy delivered four times the tonnage of goods and equipment for Operation Iraqi Freedom in four months than it delivered for Desert Storm during a total of seven months of operations (Barkenhausen 2004).

A maritime information environment called FORCEnet is under development, which is an extension of the Global Information Grid (GIG). FORCEnet requires a seamless and timely flow of data to be transformed into executable information. Consequently, it is also meant to provide the knowledge-building protocols through the tactical, operational, and strategic levels of warfare. This connectivity that allows real-time weapons systems must be in the same IP based technology as the operational system, though, necessitating a more joint design methodology and thorough joint testing.

Modern systems like the AEGIS Weapon System and the Ship Self Defense System currently have archaic, monolithic, and proprietary software conditions that need to be transformed into modern applications that conform to open commercial standards so the FORCEnet vision can be met (Rushton 2004). OA enables a new approach in acquiring and managing reusable software components while taking advantage of standards-based computing technologies from the Commercial Off the Shelf (COTS) marketplace. Most current combat and weapon systems are considered either Category 1 or 2 OA compliant, which are system designs that are precursors to true modular (decoupled) hardware and software condition. Category 4 is a maturation of the Open Architecture environment to allow cross platform use of common applications such as in an identical word processing application running on LINUX, Windows, Apple, or other computer operating systems. (Rushton 2004)

The Open Architecture Computing Environment (OACE) planned to provide:

- A flexible foundation for rapidly introducing new warfighting capabilities into the combat system to pace the threat
- Interoperability across diverse joint battle management command & control systems
- A system design that fosters affordable development and life-cycle maintenance
- A system design that reduces upgrade cycle time and time-to-deployment for new features
- An architecture that allows technology refresh despite rapid COTS obsolescence
- Improvements in Human Systems Integration (Rushton 2004).

The OAWSDM was primarily defined by:

- Identifying Navy war-fighting functionality across platforms and systems that may include commonality of function, processing, design, interface, and/or data/information exchange; and
- Further identify those systems, functions, or interfaces that are unique to particular Navy platforms. The OACE must be capable of executing the performance requirements for the warfighting capabilities in the proposed OAWSDM (Rushton 2004).

Even with all these enhancements, many current systems incorporate design features based on the DOD-led computing technologies of the 1980s. Consequently, weapon system enhancements have caused adjunct relationships in handling sensor data and the elements of the common tactical data picture. The net result has been to establish a challenging correlation problem across multiple track databases. Interoperability across the battle force is more precise than before but less coherent, as the various mechanisms for reporting track objects failed to coalesce into a common picture. With command support from ISR, distributed, and collaborative planning tools not fully integrated, crews are forced to manually correlate and transfer information between weapon systems. (Rushton 2004)

In “The Critical Network Centric Warfare Enabler”, Rushton states that in order to further evolve this system for the better, the user must be preeminent in defining what information is needed. In order to use the limited available bandwidth efficiently, the information transmission and retrieval scheme must only transmit information that the warrior specifically needs or requests. The identification, shipping instructions, and retrieval options must be sufficiently flexible to meet the warrior’s rapidly changing mission requirements. Network Centric capabilities are essential to meeting the requirements of the littoral and inland battlespace in which maritime forces must operate for the foreseeable future.

Today, the DOD no longer leads or even significantly influences developments in information technology. The commercial, non-DoD, market place that drives the pace and character of information technology has embraced OA. Key tenets of the GIG and FORCEnet, such as web based command and control, information dissemination management, and modern human systems integration depend on OA in COTS based products. (Rushton 2004)

### **3. Future**

The desired future state is one of total connectivity. It is the difference between disparate ships being involved in a larger-scale operation and a single battle group or fleet, using their combined sensing abilities to have extensive battlespace awareness, being able to call to action an optimized combination of offensive and defensive capabilities from all involved platforms to achieve mission success. It will be a network enabled foundation that allows the collaborative use of distributed warfare assets for time critical operations where the best shooter is selected from a set of geographically distributed firing units to improve the chances of intercepting targets and improve the economy of weapon resources. Earlier launch decisions will be possible when sensors are intelligently tasked based on shared knowledge of the battlespace. Sensors and weapons will not have to be paired for engagements. This will lead to the effective kinematical range of weapons being expanded and additional operational capabilities such as forward



pass and off-board engagement support for guidance relay and target illumination will be available. Complex threat environments, in which sophisticated or significant numbers of aerospace targets exist, will use automated collaborative fire control or integrated fire control. (Young 2005)

Fire-control systems will utilize a decentralized architecture with smart nodes that communicate and collaborate over a network. Information is shared among the distributed units and each unit will develop a shared picture of the battlespace. From the shared picture, each unit will determine the best use of the Force's resources and task local resources. This will allow common functions to be used across the Force and a force-wide perspective to be used in managing resources. (Young 2005)

According to Rushton, future systems designers will have an operational imperative to ensure that the fundamental tenets of joint interoperability are realized in order to achieve a robust network centric warfare capability. The GIG will provide the enabling foundation for Network Centric Warfare (NCW), information superiority, decision superiority, and full spectrum dominance. This will lead to dramatically improved information positions, in the form of common operational pictures that will provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power. The ability to achieve shared situational awareness and knowledge among all elements of a joint force, in conjunction with allied and coalition partners, is viewed as a cornerstone of transformation to achieve future warfighting capabilities. Success in exploiting the GIG in NCW depends in large part on how well it achieves interoperability and force-wide information sharing through the implementation of FORCEnet (Rushton 2004).

One of the key elements essential to the success of future war-fighters is a highly responsive, high-capacity GIG that allows them to integrate and synchronize their capabilities within the multitude of fluid, rapidly changing military operational

environments that must respond to ever-changing missions. Accurate, timely, secure, and assured information will allow commanders and their staffs to gain and apply superior knowledge and understanding of the battlespace. This will manifest in the ability to collaboratively formulate and disseminate plans and orders, synchronize forces, exert effective control over the battlespace, sustain a high velocity of action, and help achieve full-spectrum dominance over the enemy (Rushton 2004).

This information synchronization will enable the future war-fighters' ability to operate with reduced forces at high operational tempos where dynamic planning and redirection of assets is the norm. Delivery of information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets to joint commanders, their forces, and the President and SECDEF within specified time frames will be possible. This will lead to the war-fighters' ability to obtain and use combat and administrative support information from national, allied, coalition, and other widely dispersed assets. Overall, collection, processing, storage, distribution, and display of information horizontally and vertically throughout organizational structures across the battlespace will occur (Rushton 2004).

This timeline can be summarized around a few major points that should be remembered as this study is further discussed.

- Legacy combat systems have historically been developed and operated in a stove-pipe environment.
- Recent attempts by the JROC to force a paradigm shift to a network centric, interoperable battle group have not been completely successful and have led to challenging correlation problems in the endeavor to create a common air picture.
- The tenets of FORCEnet provide a conceptual framework for new system development, and OA provides the enabling technologies to realize this concept.
- The future will hold extensive battle space awareness for the entire joint force, as well as the capabilities to operate as a fully integrated, offensive or defensive, unit.

## **E. APPROACH AND METHODOLOGY**

The approach followed through the study is discussed in the following items. These steps form a narrowing approach to the problem, beginning with a familiarization of current doctrine and research in the areas pertinent to the objective. From this, along with the target OAWSDM, a scope and bounds analysis and input/output study was conducted and the findings provided the needed information to construct a context diagram. From that context diagram, a functional flow is developed. Based on the analysis of the engagement process, enough information was gained to begin the construction of a simulation model, which is used to study a theoretical design based on the components of the OAWSDM. This design is then exercised with scenarios designed to represent valid time critical targets of a small boat nature. By changing assumed parameters in the model pertaining to human input into the system, the  $C^3$  times, the relationship between decision making efficiency and overall mission effectiveness is shown. Conclusions and future work recommendations are finally discussed for this study. The specific steps are listed below and further explained:

- Problem Definition and Enabling Technology
  - Initial Problem Definition (Section I)
  - Literature Search (Section II)
  - OAWSDM Decomposition & Analysis (Section III. B.)
  - Input-Output Analysis (Section III. C.)
  - Scope and Bounds Analysis (Section III. D.)
- Functional Analysis & Allocation (Section III. E.)
  - Context Diagram
  - Functional Flow
- Scenario Development
  - Operational View (Section IV. B.)
  - Metrics Definition (Section IV. C.)
  - OATCTEP Model Scenario Definition (Section IV. D.)
  - OATCTEP Model & Scenario Assumptions (Section IV. E.)
- Synthesize Model Blocks & Subsystems

- Radar Model Design (Section IV. F.)
- System Model Design (Section IV. G.)
- Run Scenarios
  - OATCTEPM Simulation Results Analysis & Evaluation (Section V.)

### **1. Research Current Naval Doctrine**

The purpose of this step is to outline current Naval Doctrine related to this effort. This includes FORCEnet, Future Naval Fires, Open Architecture, and SeaPower 21. It is important to understand the framework in which all of the succeeding research will fit into and also to ensure that any recommendations that are generated from this research also abide by current and future Naval vision.

### **2. Identify Important Enablers**

Once the framework is defined, the literature search addresses all areas relevant to the primary objective. Initial searches include current threats, target engagement, existing time critical target models, and research performed on the OAWSDM. Once this is accomplished, technologies which may improve the response to time critical targets are identified and explored. Specifically, the areas of expeditionary pervasive sensing, automated decision aides, system learning and adaptation, and fuzzy logic are important enablers for increased ability to engage TCTs.

### **3. Decompose and Analyze the OAWSDM**

The Open Architecture Warfare System Domain Model is decomposed so that a detailed analysis of its ability to successfully prosecute a time critical target could be measured. This begins with defining the general inputs and outputs, as well as its scope and bounds and constructing a context diagram. These functions are then mapped to a process flow, transforming the OAWSDM into a process model, which can then be simulated and analyzed.

#### **4. Develop a TCT Engagement Model**

This model will simulate various engagements with predefined targets and measure the effectiveness of a typical system, within the construct of the OAWSDM, in being able to engage those targets. A baseline model is created which is then altered in an effort to improve the response of the system based on the initial findings. This model is understandably a simplification of a highly complex system, and as such, all assumptions are documented during its creation.

#### **5. Develop Time Critical Targeting Scenarios**

Once the model input requirements are defined, scenarios are developed which represent realistic time critical engagements for the system. These scenarios exercise different aspects of the architecture and seek to define the system performance as much as possible in the scope of the research.

#### **6. Develop Measures of Effectiveness**

Upon completion of the scenarios and baseline model, measures of effectiveness (MOEs) are defined in order to objectively evaluate the performance of the system. These MOEs represent key characteristics of system effectiveness in the scenarios. The MOEs are used to gauge success and failure of the simulation and in comparing the baseline with any suggested upgrades.

#### **7. Obtain and Analyze Baseline Results**

Using the time critical target scenarios and the baseline configuration of the model, a statistically significant number of simulation iterations are run. These results are analyzed for trends and compared to the predefined measures of effectiveness. Based on these results, key areas for improvement are identified. These improvements can be either structural or numerical in nature. The structural improvements are derived from areas in which parallel or otherwise reduced processing can occur to speed up TCT engagements. Numerical improvements involve reducing individual input time parameters based on applicable research concerning technological improvement.

## **8. Incorporate Model Improvements and Rerun**

Using improvements suggested by the analysis performed on the baseline model results, incorporate improvements as possible. The effect of these improvements can then be analyzed for their statistical significance in improved effectiveness.

## **9. Document Results and Recommendations**

The final step of the research methodology is to fully document the above work, and with the results of the baseline and improved models, to provide recommendations on how to effectively use the OAWSDM architecture to implement systems that can combat time critical targets.

## **F. SCOPE**

The methodology used to analyze the effectiveness of a system based on the OAWSDM in prosecuting a surface based Naval TCT. The simulation presented herein is based on a single fictional cruiser engaging all incoming targets. The simulation takes place in a busy shipping lane in a potentially hostile area. Simulation results assume clear skies and calm seas. The simulation does not take into account machinery breakdown, soft kill effects, or target probability of hitting the ship. The simulation was constructed using two scenarios, one representing a quick engagement with fewer targets and one representing a saturation attack by many targets. Other scenarios may show different results. All target and ship parameters are rough estimates and are only meant to be representative enough to compare system performance across scenarios and with proposed improvements.

## **G. OUTPUTS**

The significant output is to show the effect of the C<sup>3</sup> functions on the overall effectiveness level for the OAWSDM in combating a TCT. Proposed improvements to the existing architecture are given and probable improvements through the use of such technology are presented. The design for the simulation used for this study is presented

throughout the paper including actual model flow, assumptions, and parameters. Detailed data on the scenarios used is provided as well.

## **H. ORGANIZATION OF THE PAPER**

Section II provides the results of a detailed literature search on topics used during the development of this thesis. Section III contains a thorough explanation of the methodology used to develop the OATCTEPM from the OAWSDM, the OODA Loop, and other sources found during the literature search. Section IV introduces the scenarios developed to run in the OATCTEPM, the measures of effectiveness used to analyze the results, the overall design of the OATCTEPM, and the assumptions made during the development of these. Section V presents the results of the scenario simulations and analysis of alternative technologies that improve the response to small boat TCTs in the OAFDM. Section VI contains conclusions and final recommendations, including those for future research.

The paper also contains four appendices, including a detailed description of the two scenarios used in this paper, a walkthrough of the simulation model, an explanation of the radar model calculations and a detailed explanation of the improved model study. Following the appendices, acronyms and references used in this paper are presented.

THIS PAGE INTENTIONALLY LEFT BLANK



## **II. LITERATURE SEARCH**

In order to fully understand the research objective, a thorough literature search was conducted, producing two results. The first result was a foundation on which the group based all assumptions, constraints, scope, bounds, and scenarios. Secondly, it provided a better understanding of stakeholder concerns and established the building blocks for the analysis and conclusions provided later in this paper. Furthermore, the problems presented by this research are neither new, nor unique, to the US Navy. Every attempt was made to not only thoroughly understand and document DoD and Navy requirements, but also to obtain lessons learned from current and previous work to solve similar problems. Key topics reviewed in this section are Open Architecture, FORCEnet, Time Critical Targets, Future Naval Fires, Expeditionary Pervasive Sensing, Service Oriented Architecture, and the OODA Loop and Target Engagement Processes.

### **A. OPEN ARCHITECTURE**

The Navy's implementation of Open Architecture evolved in response to the Department of Defense (DoD) requirement to implement Modular Open Systems. In May of 2003, the DoD released DoD Directive (DoDD) 5000.1, which stated that "Acquisition programs shall be managed through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs. A modular, open-systems approach shall be employed, where feasible." (DoDD 5000.1 2003) This concept is further explained in Chapter 4.4.1 of the DoD Acquisition Guidebook. It defines an open system as a "...system that employs modular design tenets, uses widely supported and consensus-based standards for its key interfaces, and is subject to validation and verification tests to ensure the openness of its key interfaces." (Defense Acquisition Guidebook 2006) It further defines an open systems design as

*A design approach for developing an affordable and adaptable open system. It derives inputs from both the technical management processes and technical processes undertaken within the systems engineering and other life-cycle processes, and in turn impacts these processes. The open systems design strategy should be implemented as part of the program's overall technical approach and must become an integral part of the program's SEP. (Defense Acquisition Guidebook 2006)*

In order to facilitate the implementation of an open systems approach, in section 2.3.15 of the Defense Acquisition Guidebook five Modular Open System Approach (MOSA) principles are established:

- Establish an Enabling Environment
- Employ Modular Design
- Design Key Interfaces
- Use Open Standards and
- Certify Conformance.

DoD also created the Open Systems Joint Task Force (OSJTF) which has published further guidance on the implementation of MOSA. This information can be found in the Program Managers Guide. (PMG 2004)

In response to the DoD Open Systems requirement, the Department of the Navy established Open Architecture in its first memorandum on the subject, *Naval Open Architecture Scope and Responsibilities*, in August of 2004. It amplified and expanded "...upon the policy, guidance and direction necessary for the successful implementation of the Navy's Open Architecture (OA) Strategy" (Young 2004). It was followed later in the month of August by two documents defining the Open Architecture Computing Environment. These documents, Open Architecture (OA) Computing Environment Design Guidance Version 1.0 and Open Architecture (OA) Computing Environment Design Technologies and Standards Version 1.0, established specific technical requirements and guidance necessary for the implementation of OA. In December of

2005, the Navy showed further commitment to OA implementation by releasing another memorandum from the Deputy Chief of Naval Operations entitled “Requirement for Open Architecture (OA) Implementation” (OACEDG 2004). As the memorandum stated, the Navy must “...shorten the kill chain across the family of systems...” and “...shorten the time and cost it takes to deliver capability improvements.” Since this memo the Navy has also released the Naval Open Architecture Contract Guidebook and the Open Architecture Assessment Model (OAAM) to assist program managers in integrating OA within their programs. (Edwards 2005)

Further information on Open Architecture can be found on the Defense Acquisition University’s web site (DAU 2007). According to this site, Open Architecture is defined as, “A multi-faceted strategy providing a framework for developing joint, interoperable systems that adapt and exploit open system design principles and architectures.” The Open Architecture framework consists of a set of principles, processes and best practices that address the following:

- “Provide more opportunities for competition
- Optimize total system performance
- Are easily developed and upgraded
- Minimize total ownership costs
- Rapidly field affordable, interoperable systems
- Employ non-proprietary standards for internal interface
- Enable component reuse.”

## **B. FORCENET**

Using Open Architecture, the United States Navy (USN) is currently pursuing a real-time, situational awareness concept called FORCEnet to aid in decision making capabilities and distributing combative power where needed. FORCEnet is defined in the FORCEnet Implementation Strategy as

*...the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed, combat force that is scalable across all levels of conflict from seabed to space and sea to land.*  
(Mayo and Nathman 2003)

FORCENet is intended to leverage several computing and network technologies to help the Navy realize the Net-Centric concept of warfare and information exchange. “FORCENet will help create a unified battlespace by providing near-instantaneous collection, analysis, and dissemination of information coupled to advanced computer-driven decision aids to joint force commanders” (Mayo and Nathman 2003). FORCENet may also provide the advantage of information superiority to increase responsiveness and survivability by allowing forces to disperse while focusing offensive and defensive firepower from afar. FORCENet is meant to provide the information that enables knowledge-based operations, delivering greater power, protection, and operational independence than ever before possible to joint force commanders.

Implementing the concept of FORCENet depends upon development of network architecture, such as the Global Information Grid (GIG), which is comprised of standard joint protocols, common data packages, seamless interoperability, and enhanced security. US Navy assets, as well as joint services, agencies, and allied nations could feed that network.

According to the Naval Warfare Development Command (NWDC) in Newport, Rhode Island, “...FORCENet will focus its efforts on integrating existing networks, sensors, and command and control systems” (Mayo and Nathman 2003). In the future, the system evolves into a fully netted force that allows commanders to engage the battlefield with increased awareness and quicker reaction time. It also provides real-time enhanced collaborative planning among joint and coalition forces. With greater sharing of time sensitive information and knowledge of threats, friendly forces experience increased survivability and effectiveness. FORCENet has the following intended impacts:

- Connected warriors, sensors, networks, command and control, platforms, and weapons
- Accelerated speed and accuracy of decision
- Integrated knowledge to dominate the battlespace

These impacts are some of the key benefits to implementing FORCEnet. The future capabilities required of FORCEnet include but are not limited to:

- Expeditionary, multi-tiered, sensor and weapons grids
- Distributed, collaborative command and control
- Dynamic, multi-path and survivable networks
- Adaptive / automated decision aids
- Human-centric integration

By implementing Open Architecture into FORCEnet many benefits will be realized. In utilizing a Modular Open Systems Approach (MOSA) through open architecture, FORCEnet will experience superior availability, supportability, reliability, and maintainability. This is achieved by making the system scalable and modular. With multiple inputs into the system a greater redundancy will be present which in turn enhances availability by allowing for graceful degradation. By employing an open architectural framework, the interoperability of the system greatly increases. For more than twelve years now the Navy and the DoD have been working to develop a Single Integrated Air Picture (SIAP) and have yet been able to build one. This is primarily due to the lack of standard interfaces which in turn has inhibited systems' interoperability. For proper data fusion, FORCEnet needs to establish and implement standards along with information architectures that lead to deterministic outcomes. (Mayo and Nathman 2003)

An advantage to further developing the FORCEnet concept using Open Architecture is that it allows for an incremental development. This means that older subsystems can be replaced and newer technologies can be inserted in phases since it would not be possible to update every element simultaneously. The information architecture for FORCEnet is thought of as a boundary between layers of functionality

that is held constant and allows developments to progress independently on all sides of the boundary.

*FORCENet is faced by many challenges such as interoperability problems, old architectures that are difficult to change or adapt, expensive and time-consuming refreshes, and high cost of acquisition and support. These challenges are the main drivers to the open architecture initiative of the Navy and DoD. In respect to Open Architecture, the FORCENet community is especially interested in the topic of Open Architecture Computing Environment (OACE) where attention has been drawn to functional partitioning and interface control. This is what is required for FORCENet but currently lacking in the architecture and standards documentation. (NRC 2005)*

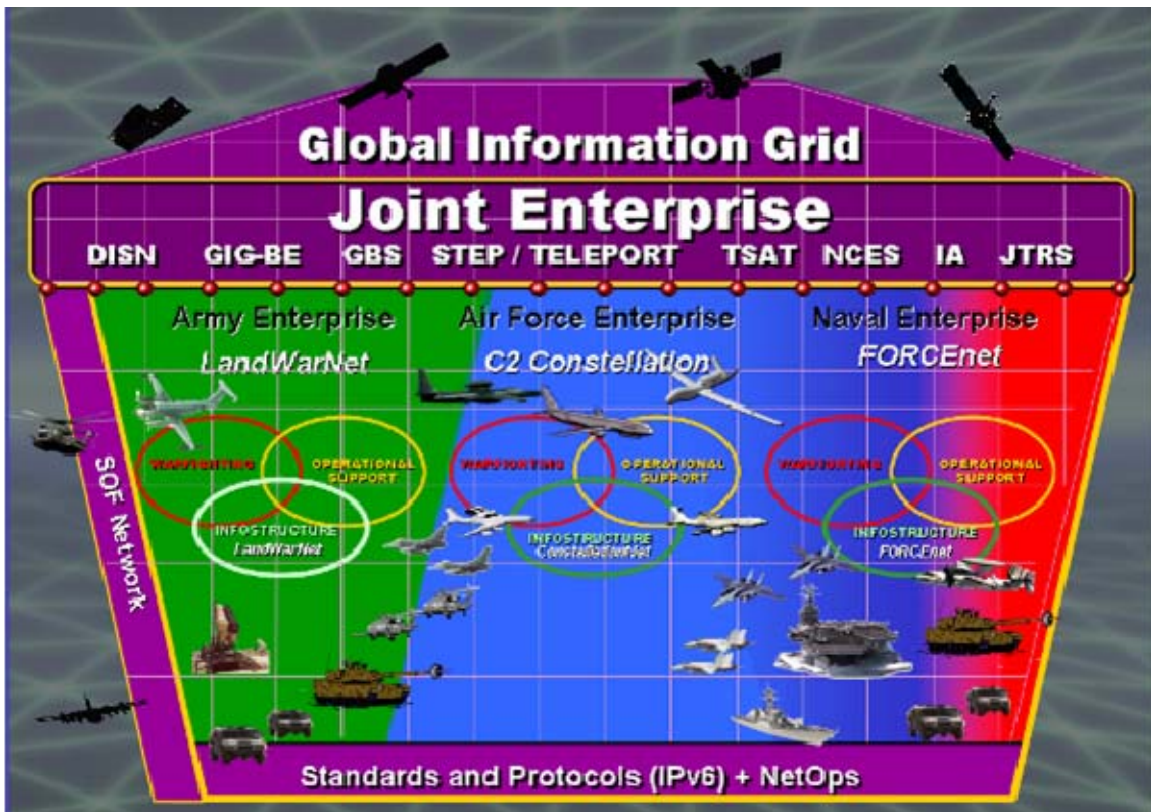


Figure 3. FORCENet and relationship to the Global Information Grid

*This figure shows the relationship between the next generation Army, Air Force, and Navy architectures and, in turn, their relationship to the Global Information Grid. (Bell 2004)*

It should be noted that the functionality of FORCEnet is a subset to battle force functionality in that it contributes to the battle management, battlespace dominance, and sustaining control over the battlespace. “The definition of interfaces between FORCEnet and other systems will continue to be an ongoing process.” (NRC 2005)

### **C. TIME CRITICAL TARGETING**

The concept of Time Critical Targeting is central to the issue under investigation. The targeting process must take on the ability to effectively obtain detection information, process that information, and utilize it to place ordnance on target.

Research in the area of Time Critical Targeting was conducted in an inside-out pattern, starting with the identification of the need to improve the prosecution of these fleeting targets from within all military communities (a joint observation), followed by component perspectives; ground troops, naval platforms, and air platforms. These three perspectives are both unique and very similar, at the same time.

#### **1. DoD Joint Perspective**

In a letter from the Government Accountability Office (GAO) to Congressman Jerry Lewis, Chairman of the Defense Appropriations Subcommittee, these perspectives were addressed with several examples. It highlighted DoD studies that point out a variety of reasons that “sensor to shooter” timelines are ineffective against TCTs. This weakness is well-known and exploited by the enemy. The primary reason behind this shortcoming is stated to be a lack of interoperability between the various systems employed by the various services. This document also explored reasons that previous efforts to bridge this gap have failed, “...because the services were unwilling to forego their unique requirements in favor of requirements that would benefit the department as a whole.” (Wiggins 2001) Additional reasons were also given.

A publication called *The Joint Targeting Process and Procedures For Targeting Time-Critical Targets* was produced in 1997 and was "...prepared under the direction of the Commander, US Army Training and Doctrine Command (TRADOC); Commanding General, Marine Corps Combat Development Command (MCCDC); Commander, Naval Doctrine Command (NDC); and Commander, Air Combat Command (ACC)," and established Tactics, Techniques, and Procedures (TTP) for addressing time critical targets. Although this is a 10-year old publication, the tenets for the joint targeting process remain valid and current: joint battlespace control, coordination measures, "grid box", and "bull's eye" techniques, interconnecting battle management (C2) systems. The impact that time has had on this concept is that the enabling technology has improved over the last 10 years and the goal is becoming more achievable. (USAF 1996)

## **2. Service Component Perspectives**

### *Air Force Efforts*

*The Air Force is developing a new family of systems to attack time-critical targets that are expected to reduce attack times. For example, the time-critical targeting cell initiative will provide the air component commander's air operations center an ability to detect and direct forces to attack targets quickly. The theater battle management core system is expected to merge several legacy systems such as its Air Tasking Order [(ATO)] system, which controls employment of fixed wing aircraft in the battle area with new capabilities, to reduce the timelines to attack time-critical targets. (Wiggins 2001)*

Several critical points were made in a presentation by Brig Gen Jim Morehouse, Director of C2 DCS and Air & Space Operations. Among them it was pointed out that the amount of time allowable for prosecution of time critical targets could be as low as single-digit minutes. Secondly, it was highlighted that the prosecution of these target isn't just dropping bombs (kinetic), but it could also be in the form of information operations, or even humanitarian relief. (Morehouse 2002)



Two approaches to TCT have been proposed, *Reactive* and *Preemptive* (Marzolf 2004). The preemptive (or predictive) revolves around utilizing intelligence to predict the locations of time critical threats and the employment of loitering weapons platforms to strike targets in a more timely manner.

### ***Navy Efforts***

*The Navy is developing a new series of systems for its time-critical strike future naval capability program, such as the Real Time Execution Decision Support (REDS) Initiative. The Navy is also working on a network-centric warfare concept that will network Navy sensors, command centers, and its long-range weapons to attack a broader range of targets (including those in the deep battle area) more effectively. This concept includes a vast array of procurement and research and development weapon systems, ships, aircraft, and command and control, communications, intelligence and reconnaissance programs. The Navy is considering the need for new command and control ships to provide the Navy with the capability to control deployed joint forces while stationed off shore. (Wiggins 2001)*

The Office of Naval Research (ONR) is “...developing technologies that enable strides against targets in compressed vulnerability windows in all joint operations, in any environment, under all conditions.” (Office of Naval Research 2001) A multitude of initiatives by the ONR are discussed relative to Time Critical Strike. A Time Critical Strike Future Naval Capabilities IPT was established to manage these future initiatives.

### ***Army Efforts***

*The Army is continuing to fund its Battlefield Digitization initiative, which is designed to improve the flow of battlefield information within the Army’s fighting organization structure. The Army is also developing a transformation strategy, which is designed to ensure that the Army could respond to a broad range of*

*operations. The strategy centers on developing a combat force that is expected to be lighter, but just as powerful and survivable as today's heavy force. This new force will be planned around Future Combat systems. These systems will provide the capability to attack critical targets much deeper in the battle area before they become a direct threat. (Wiggins 2001)*

### **3. Private Industry Perspectives**

Solutions and perspectives from private industry were also explored, such as the “Imagine...and act” presentation by G. Gardner, VP, Government and Homeland Security Solution, Oracle Corporation, which explored potentially viable architectures that utilize modern information technology and business processes, enabled by future technologies such as the Global Information Grid (GIG), to shorten the kill chain. (Gardner 2005)

### **4. Additional Views**

The Defense Advanced Research Projects Agency (DARPA) Special Projects Office (SPO) is fully engaged with the pursuit of networked targeting-based solutions for TCTs. Their efforts include research in the areas of Affordable Moving Surface Target Engagement (AMSTE) and Advanced Tactical Targeting Technology (AT3). Both of these programs are geared toward closing the gaps and tightening the coupling between the sensors and shooters. In September of 2005, DARPA SPO successfully demonstrated Tactical Targeting Network Technology (TTNT) in tactical aircraft. This demonstration is also discussed in the Expeditionary Pervasive Sensing (EPS) / Networked Sensors portion of this chapter; however, it warrants mention here as well, due to its enormous contribution toward the prosecution of TCTs. This is a testament to how closely knitted these concepts are to each other. The extent of material available regarding time critical targets and improving time-critical strike capabilities is enormous. The focus of these studies relates to a common theme, which can be expressed (in Air Force terms) as the “Kill Chain.”

## **D. FUTURE NAVAL FIRES**

The Future Naval Fires concept is being developed in support of SEA STRIKE, which is “a broadened concept for naval power projection that leverages enhanced C4ISR, precision, stealth, and endurance to increase operational tempo, reach, and effectiveness.” (Naval Power 21 2002) SEA STRIKE is one fundamental concept of the Navy’s Concept of Operation (CONOP) of SEA POWER 21. This CONOP was developed to guide the US Navy in aligning and accelerating its progress in offensive power, defensive assurance, and operational independence around the globe.

SEA STRIKE operations describe how the 21st-century Navy plans to exert direct, decisive, and sustained influence in joint campaigns. Persistent intelligence, surveillance, and reconnaissance; time sensitive strike; ship-to-objective maneuver; information operations; and covert strike to deliver devastating power and accuracy in future campaigns are all a part of these developing operations. This FNF concept is built around four primary pillars:

### **1. First Pillar**

The first pillar of the FNF concept is Simultaneous Operations. Traditional naval operations involved sequential phasing of battle. Focuses were on “rolling back enemy capabilities, force build-ups followed by offensive action.” (NWDC 2007) The FNF concept is developed for non-linear battlefields and involves conducting parallel operations across the strategic, operational and tactical levels of war on a non-linear battlefield.

### **2. Second Pillar**

The second pillar of FNF requires setting up a Fully Netted Digital Fires Network. All available fires across the battlespace will be linked in an automated process, which will enable massed fires in unison or specific patterns. This added capability could be an additional option to be deployed against Time Critical Targets.

### **3. Third Pillar**

The third pillar of FNF involves possessing a capability for Organic Tactical Sensing. Sensor to weapon connectivity is supported by a fully integrated sensors network. The Expeditionary Pervasive Sensing concept, which includes capabilities starting with space based sensors and continuing all the way to sensors on the sea floor, will be used to develop the fully integrated network. Expeditionary Pervasive Sensing (EPS) is composed of multiple levels and sensors at the area and theatre stage. Platforms will include both manned and unmanned systems/sensors using an Integrated Fire Control (IFC) system. EPS is further discussed in section E.

### **4. Fourth pillar**

The fourth and final pillar of the FNF concept is to possess the Required Supporting Capabilities. This pillar will basically focus on the enhancement of expeditionary organizational capabilities, war fighter training, and sustainment. Logisticians will need to be highly trained and highly valued to fully support the success of the FNF concept.

As naval weapons systems advance, the FNF capabilities also advance. When naval fires are required, “the joint task force commander will have a variety of naval weapons to choose from, including accurate stand-off munitions delivered from aircraft, gun-fired precision-guided munitions, and sophisticated ballistic and cruise missiles launched from surface warships and submarines.” (Rudderow 2002) Submarines, surface warships, and aircraft carriers with long-range options in deploying missiles or attack aircraft will all be a part of the Navy’s overall SEA STRIKE capabilities, as well as the Future Naval Fires concept.

## **E. NETTED SENSORS AND EXPEDITIONARY PERVASIVE SENSING**

### **1. Evolution of Network Centric Concepts**

The evolution of Network Centric Concepts can be best described by the below excerpt from the Tactical Digital Information Links website, authored by J. Pike.

*The concept of a sensor network is nothing new to the US Navy. The need for situational awareness for decision makers and the desire to have disparate forces operate in a coherent manner prompted the development of several technologies, which have come to be known as Tactical Digital Information Links (TADILs). This family consists of several network formats, such as Link 4A, Link-11, Link-16, and Link-22. Link-16 is the DoD's primary tactical data link for command, control, and intelligence; providing critical joint interpretability and situation awareness information. Link-16 uses a Time Demand Multiple Access (TDMA) architecture and the "J" message format standard. The "J" series of message standards are designated as the Department of Defense's primary tactical data link, according to the Joint Tactical Data Link Management Plan (JTDLMP). (Pike 2000)*

A disadvantage of the existing TADILs is the inherent latency, which can be measured in seconds in some cases. This latency is not a correctable parameter, based primarily on the fact that the TADIL information is collected and filtered into a target positioning track prior to transmission. The time that is required to do this precludes using the data for any functions that would require a high, consistent update rate. However, TADILs are very effective at distributing pertinent information and providing situational awareness to key decision makers, enabling timely Force-level control over a battle group or joint force.

The Cooperative Engagement Capability (CEC) was the next evolution in improving network centric operations among sea-borne platforms. This system offers

several advantages over the TADIL systems. CEC not only offers the same improved situational awareness advantage, but actually increases the effective battle space of surface combatants. The enabler for this capability is based on a much higher speed network and minimum front-end processing. Raw radar information is shared among Cooperating Units (CUs) and is used in conjunction with each platform's organic sensors (if present) to form composite tracks, which are of higher fidelity than a track produced by any single platform. In the case of remote engagements, bandwidth management schemes are employed to ensure required data rates are achieved to support said engagements. In the larger scheme of things, the Defense Industry Daily stated that, "CEC is a critical hinge of the U.S. Navy's Sea Shield and FORCENet doctrines under SeaPower 21..." which is in-line with the Stakeholder guidance provided in the SOW for this development effort. Additional resources used to investigate CEC are included in the bibliography.

## **2. Beyond the Status Quo**

While the Cooperative Engagement Capability is considered a huge leap in the direction of network centric warfare, it only addresses a small portion of the Sea Power 21 vision. To more completely fulfill this aspect of DoD's transformation, the netted sensor concept must expand to allow for a much greater number of individual sensors, as well as suites of sensors. There also must be a departure from the single star-network topology employed by CEC to a network of networks architecture, which will foster a multi-tiered command and control (C<sup>2</sup>) scheme based on roles and capabilities of the sensors and/or their respective platforms. The concept of a network of networks supports the incorporation of a multitude of sensors, to include space-based, air, surface, and sub-surface.

The DoD thrust for Commercial Off The Shelf (COTS) requirements has served to steer development efforts toward existing standards such as the utilization of Internet Protocol (IP) data formats for implementing and managing data networks. A substantial amount of research based on Information Assurance (IA) has been supported by the

National Security Agency (NSA) and is referred to as the GIG vision. The scope of this vision, "...will be a net-centric system operating in a global context to provide processing, storage, management, and transport of information to support all DoD, national security, and related Intelligence Community missions and functions-strategic, operational, tactical, and business-in war, in crisis, and in peace." (NSA 2007)

Currently, there are several major initiatives relating to the Global Information Grid listed in Aviation Daily (Adams 2005) as follows:

- "Information Assurance (IA)
- Horizontal Fusion, network centric demonstrations
- Transformational Communications, sitcom
- Family of beyond line-of-sight terminals (FAB-T), wideband sitcom
- Transformational Satellite (TSAT), for high-volume communications
- Teleports, links between terrestrial and satellite communications
- GIG-Bandwidth Expansion (GIG-BE), for ground-laid optical fiber."

DARPA successfully demonstrated the Tactical Targeting Network Technology (TTNT) in 2005. The system utilized "...internet protocol-based, high-speed, dynamic, ad hoc data-link network designed to enable tactical aircraft to quickly target moving and time-critical targets." (Adams 2005) The work conducted by DARPA supported the use of low-latency internet-protocol applications for transferring still images, stream video, cursor on target, as well as several others.

### **3. Applicability to Time Critical Targeting**

The concept of EPS is important to time critical targets because it can improve the detection of time critical threats. However, for EPS to be effective, it must be a part of a network that meets the real time requirements of such targets.

## **F. SERVICE ORIENTED ARCHITECTURE**

Service Oriented Architecture (SOA) is a method of building and processing computer resources around services that are consumed rather than data objects. It is a formal computing architecture standard managed by the Organization for the Advancement of Structured Information Standards (OASIS). OASIS formally defines SOA as a "...paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains" (MacKenzie and others 2006). An example service that might be used in the OAWSDM would be Get Ships Heading. This service would be accessible to other programs and would provide ship's heading when called upon. More information about significant entities and the relationships that might exist between them in a service oriented environment can be found in the Reference Model for Service Oriented Architecture at the committee website (MacKenzie and others 2006).

## **G. TARGET ENGAGEMENT AND THE OODA MODEL**

During the Korean and Vietnam War eras, Colonel John Boyd of the United States Air Force developed a model that he used during aerial combat. The model contained processes Boyd considered necessary to win both in aerial combat and at war in general. His model was comprised of four functions: Observe, Orient, Decide, and Act, which form an iterative loop known as the OODA Loop. The OODA Loop conceived by Col. Boyd is depicted in figure 4 (Ullman 2007).



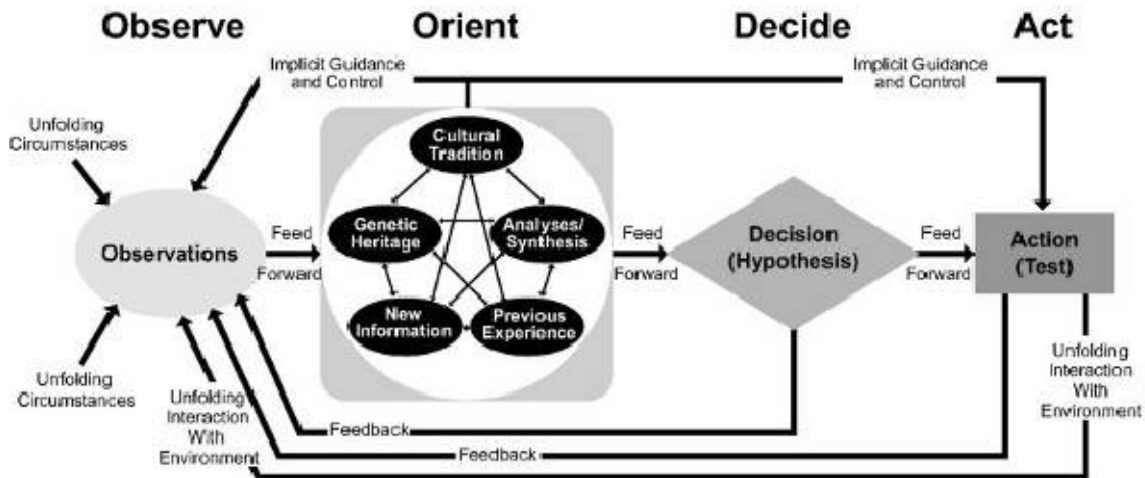


Figure 4. OODA Loop Model

*The OODA Loop, as developed by Colonel John Boyd, showing the Observe, Orient, Decide, and Act components of the loop. The OODA loop is used in conjunction with the OAWSDM in this paper to model the engagement process for time critical targets. (Ullman 2007)*

Data is first collected through the use of sensor systems and human intelligence (HUMINT) observations. Observation information is almost always incomplete, uncertain, and evolving originating from multiple different sources. Observations of developing conditions have implied filtering that is based on the problem at hand (Ullman 2007). These observations are the raw information which decisions and actions are based upon. Before a decision is made orientation occurs and for the information to be oriented, the raw observed data must first be processed. For a decision to be made, the decision maker desires a certain level of confidence in the amount and accuracy of the information collected. There is a paradox in that one may never have all the information they require. The filtering of information is typically fashioned from past experience, background, and varying techniques. When Colonel Boyd developed the OODA Loop, it was intended for a single decision maker (i.e. a fighter pilot in combat). Since then, this model has been applied to many platforms and organizations both demonstrating success and failure. In organizations there are multiple decision makers whom each present their own past experience and techniques which vary. If the variety is too great then comprises are made, bad decisions made, or no decision at all due to more analysis of data being sought after. In a time critical situation, it becomes imperative that the information

provided for the decision making process is as complete and clear as possible to facilitate better and faster decisions.

It is important to note that the OODA model is an iterative loop. With each iteration, the process becomes refined through learning that occurs from the reaction to each decision and action. This refinement allows for more efficient decision making as time goes on.

The observations presented to the system come from multiple sources. There are two problems posed during observation. First, the observed data and information is ever changing, incomplete, inconsistent, uncertain, and dependent on the observation system or person. Second, the collected information from multiple sources can vary. This variation introduces a degree of uncertainty. If one of the sensors presents correct information, the system must determine which information is correct (Ullman 2007). This could be especially problematic when observing time critical targets. The more sensors that detect a target, the more resources and time that will be required to correlate or “fuse” that data into an accurate track.

The primary purpose of orientation is to make sense of the observations. If the information is modeled for formal analysis, the decision maker is able to interpret the information more effectively. Unfortunately, much of the information cannot be modeled easily. It is very important that the information is managed to match the decision maker’s requirements (Ullman 2007). The decision maker must be confident that the amount of information is sufficient and the information itself is valid. The orientation of information is dependent on the viewpoint of who is interpreting them (Ullman 2007). The uncertainty of the information is the main driver for the OODA Loop failing to perform as desired. Decision makers are unconformable with this uncertainty and fear the repercussions of making a bad decision. In the time critical engagement process, information regarding tracks should be presented in such a way as to facilitate quick

decision making while minimizing the likelihood of errors. There should be an understanding that this is not an easy task and there are no fail proof systems.

Alternative courses of action are developed as a result of orientation. Once a decision is made the reaction is observed and oriented in response. Decision making is an iterative process of “repeatedly deciding what to do next – observe more information, do further orientation, or take action” (Ullman 2007). One technique used to improve orientation is the prioritization of information. At any given time there are multiple situations that must be dealt with, by prioritizing them the decision maker can better make good decisions to act upon. Because of the uncertainty of the observations, the ability to manage both qualitative and quantitative information is a must. Lastly, to further improve the orientation, alternative actions and possible outcomes are developed during the orientation process. This allows the decision maker to consider multiple courses of action and the likely response.

There are techniques that can manage the deliberation of the information for decision making. The focusing of sensors on a particular area of interest can allow for more data and information to be gathered and presented to the decision makers. The decision makers must also determine how much time to devote to data collection and analysis of information due to the time sensitive nature of the targets of interest. Finally, separating the easy, or obvious, efforts from the difficult does facilitate the decision making process and allows for more time to be devoted to the more unknown targets. The orientation of information is fused together to aid in the decision making process. This fused information could be presented in the form of a Single Integrated Air or Ground Picture (SIAP/SIGP) displaying all the target information from the multiple sensors and platforms. (Ullman 2007)

Decision making is the most important process of the OODA loop. Not making a decision puts the OODA loop into an endless Observe – Orient loop. This is unacceptable because the information being collected is time sensitive. The key takeaway from decision making to improve the OODA loop is to learn from past experiences and

decisions. It is here where the Open Architecture Warfare System Domain Model (OAWSD), discussed earlier, can be improved also. Both models must refine this process to become more efficient.

The act process must be consistent with the decisions that were made. If the actions were not carried out properly then the loop is broken because appropriate feedback cannot be reiterated into the model. Ullman points out to “associate the actions taken with specific OODA loops, or tasks.” Actions are actually carried out in each of the processes within the OODA loop.

Luessen demonstrates that there is an inherent relationship between the OODA loop and engagement models such as the Detect Control Engage (DCE) Model and the Joint Directors of Laboratories (JDL) Data Fusion Model as shown below.

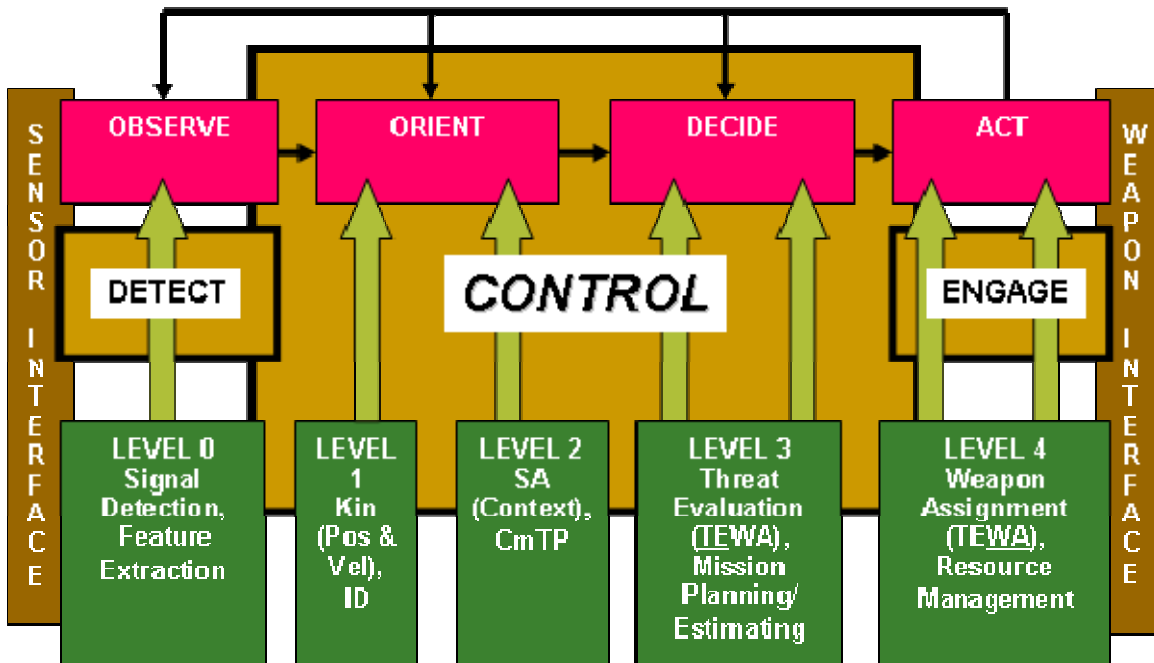


Figure 5. OODA, DCE, and JDL Data Fusion Model

*The above figure was created to show the relationship between three of the process models used to describe target engagements. The pink blocks show the OODA model, the tan blocks show the Detect Control Engage (DCE) model and the green blocks indicate components of the JDL Data Fusion Model (Luessen 2003).*

This figure demonstrates how the OODA, DCE and JDL phases relate. It illustrates the idea that “control” extends into all aspects of the three models. With respect to the engagement of time critical targets, figure 5 illustrates the many functions encapsulated in the C<sup>3</sup> portion of the cycle. Because of its broad coverage, combined with the complexity of including the many aspects of the detect and engage model, the C<sup>3</sup> functions were selected as the focal point for this research project.

## **H. SUMMARY OF LITERATURE SEARCH**

The literature search was necessary to gain a better understanding of topics important to this research such as Open Architecture, FORCEnet, Time Critical Targets, Future Naval Fires, Expeditionary Pervasive Sensing, Service Oriented Architecture, and Target Engagement Processes. Open Architecture is a DoD requirement to enforce modular system design. For the simulation, this led to a modular design that enabled easier changes between the scenarios used as well as the baseline, improved and ideal models for each. FORCEnet works to optimize information flow to achieve a distributed, collaborative command and control infrastructure. These efficiencies in the C<sup>3</sup> portions of the target engagement cycle were used to estimate segments of the simulated process. Current enemy capabilities require developments in support of Time Critical Targeting, to prosecute fast moving, maneuverable targets with a limited window of opportunity. Systems used against TCTs require faster, more efficient processing and a general understanding of this and other needs presented by this threat are necessary for the simulation in this study. Future Naval Fires is the doctrine guiding the development of new strike systems by the Navy. It focuses on improving C4ISR and combines simultaneous operations, a fully netted digital fires network, organic tactical sensing, and the required supporting capabilities to achieve this. Expeditionary Pervasive Sensing is one of the pillars of FNF and is focused on increasing the detection capability which, although not the focus of this study, would be another area of future research in its effect on mission effectiveness. Service Oriented Architecture focuses on bandwidth management, allowing the decision maker to pull relevant information instead of bombarding irrelevant information along with the relevant and requiring the sorting of the

two which slows the overall decision making process. Finally, Target Engagement Processes were studied in order to find a process to merge with the hierarchical structure of the OAWDSM, leading to the simulation used. The OODA Loop was the process used throughout this study, having a long history and simple implementation. Each of these topics led to the process and assumptions presented in this study.

### III. ANALYSIS OF THE OAWSDM

#### A. SYSTEMS ENGINEERING DESIGN PROCESS

This study uses a systematic and iterative approach, governed by a mix of Systems Engineering Design Processes (SEDP). Significant influence, for the process used in this study, comes from Benjamin Blanchard and Wolter Fabrycky's book, *Systems Engineering and Analysis*, 4th Ed. This is the Vee Model for the Systems Engineering Design Process and is shown in figure 6.

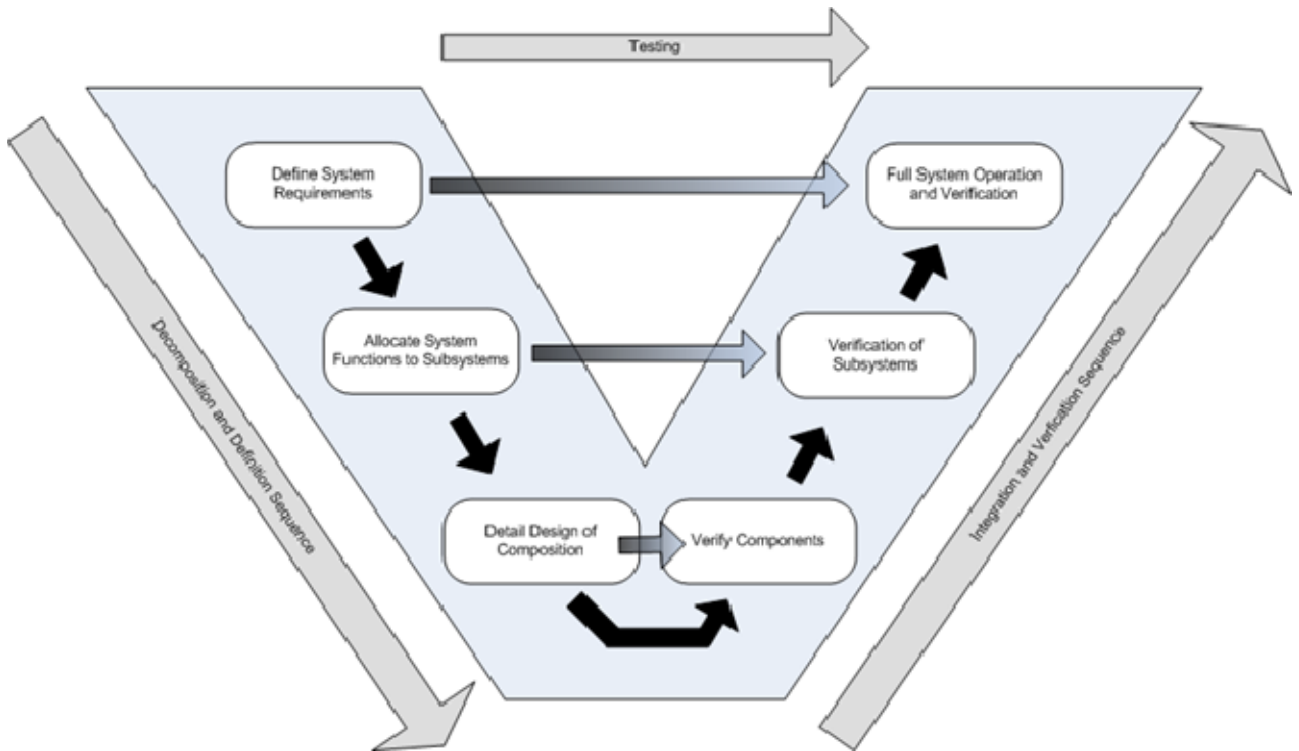


Figure 6. The Vee Model for the SEDP (Blanchard and Fabrycky 2006)

*The Vee Model as presented by Blanchard and Fabrycky shows the flow of the initial problem decomposition and subsequent synthesis of a design solution.*

In the Vee Model, the SEDP progresses from an initial definition of system requirements to an allocation of system functions to subsystems of the proposed design.

Detail design work is then performed which leads to verification testing of those segments. These small segments are rolled into subsystems, again verified, and eventually to a full fledged system that undergoes a final verification. The horizontal arrows indicate the source of the verification testing, where each stage of the design is verified in its representation of the detail design, subsystem design, or system requirements, respectively. Again, this model is meant to describe the design of a system and not the analysis of an architecture, but with some adaptation, it will provide the basis of the methodology of this study. Figure 7 shows the adaptation of the previous SEDP for use in this study.

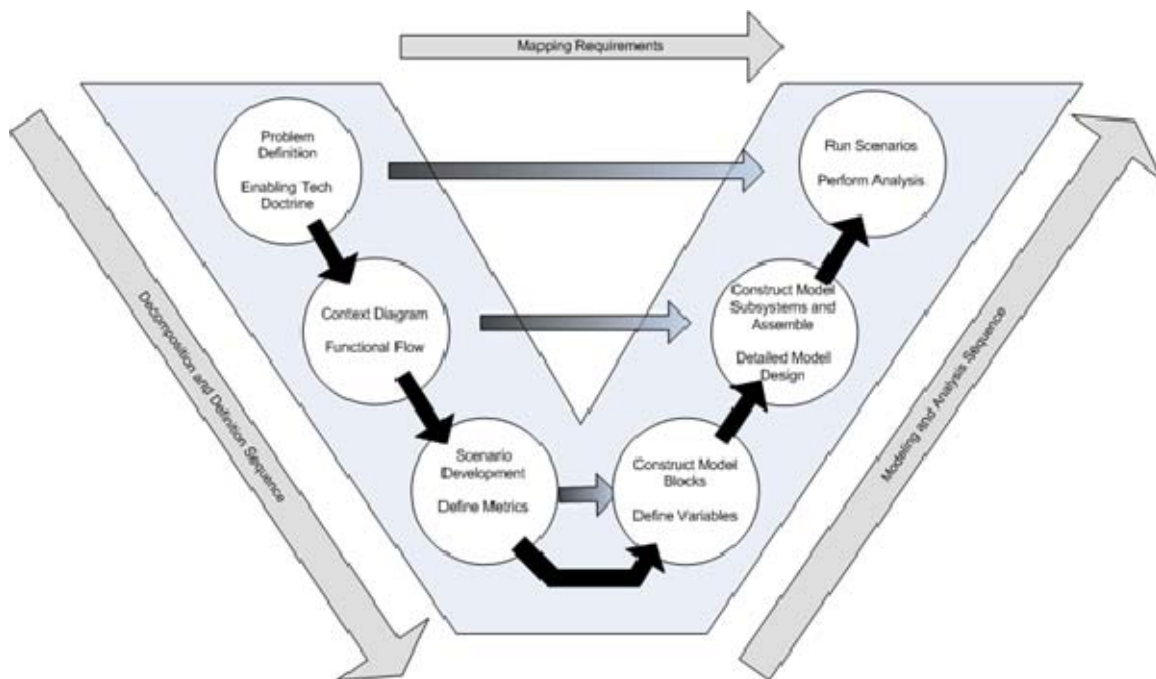


Figure 7. Architecture Analysis Vee Diagram

*This Vee diagram has been adapted for architecture analysis, in which a system is not necessarily being designed as the end product, but in which a representative system must still be created to test the overall framework it is meant to be designed from.*

For this purpose, the construction of the system is a step along the way and while the system does not need to be ideal, resulting from alternative generation and value systems analysis, it does need to be representative of systems that are designed around



the architecture being studied. In order to ensure this, the architecture is broken into its component functions which are ordered and further decomposed so that a simulation model can be accurately constructed. The problem definition will lead to this and then to developing representative scenarios and bringing further definition to the system model. This is then built up into model subsystems, tested against the functional decomposition, and finally assembled into a working model that can utilize the scenarios to provide simulation results, which are then analyzed. Specifically, the steps taken are as follows:

- Problem Definition and Enabling Technology
  - Initial Problem Definition (Section I)
  - Literature Search (Section II)
  - OAWSDM Decomposition & Analysis (Section III. B.)
  - Input-Output Analysis (Section III. C.)
  - Scope and Bounds Analysis (Section III. D.)
- Functional Analysis & Allocation (Section III. E.)
  - Context Diagram
  - Functional Flow
- Scenario Development
  - Operational View (Section IV. B.)
  - Metrics Definition (Section IV. C.)
  - OATCTEP Model Scenario Definition (Section IV. D.)
  - OATCTEP Model & Scenario Assumptions (Section IV. E.)
- Synthesize Model Blocks & Subsystems
  - Radar Model Design (Section IV. F.)
  - System Model Design (Section IV. G.)
- Run Scenarios
  - OATCTEPM Simulation Results Analysis & Evaluation (Section V.)

## B. OPEN ARCHITECTURE WEAPONS SYSTEM DOMAIN MODEL DECOMPOSITION

The OAWSD model as depicted in figure 2 is comprised of nine primary functions:

- 1.0 Search/Detect
- 2.0 Data/Information Systems
- 3.0 Planning, Assessment, and Decision
- 4.0 Weapon/Asset Services
- 5.0 Mission Execution
- 6.0 External Communication
- 7.0 Common Services
- 8.0 Training
- 9.0 Force Planning/Communication

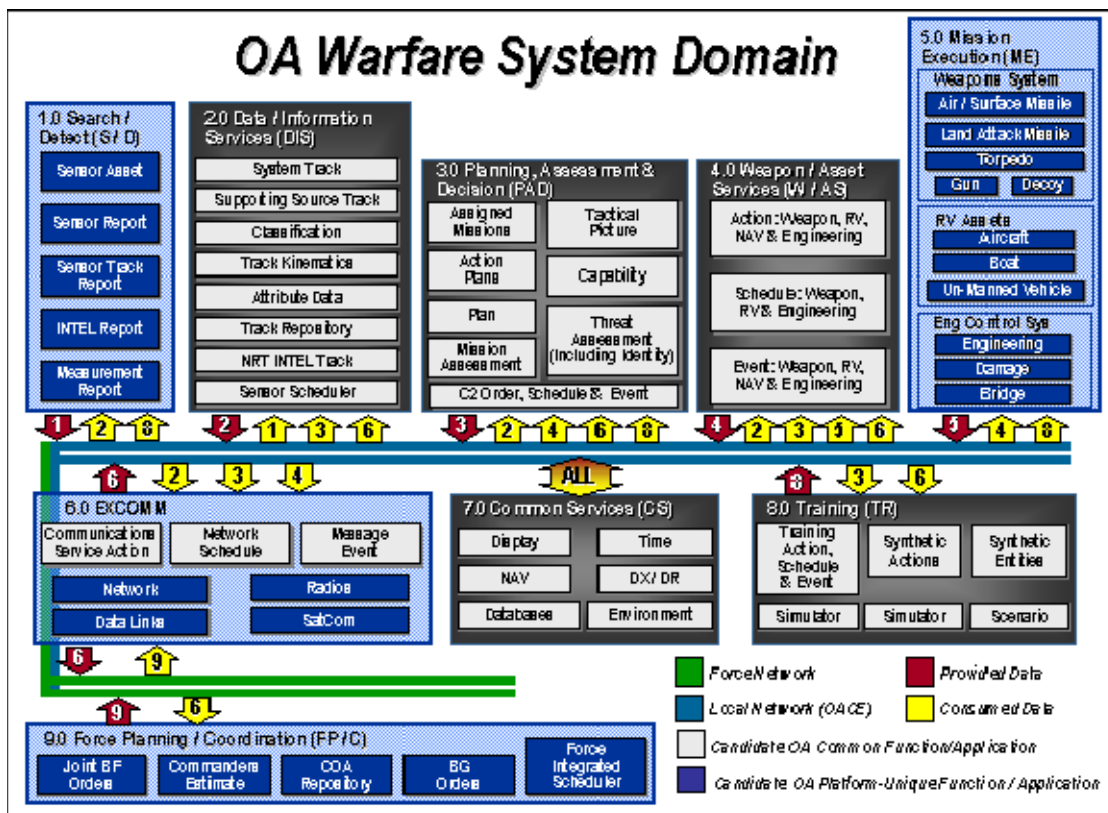


Figure 2, The OA Warfare System Domain Model, Repeated for Clarity

## **1. Search / Detect (S/D)**

The search/detect partition includes the systematic surveillance by sensors of a defined area, and the observation (detection) of an object or entity of possible interest. These sensors include but are not limited to radars, electronic warfare support (ES) sensors, intelligence gathering sensors, electro-optical (EO) or infrared (IR) sources, acoustic sources, and identification friend-or-foe (IFF).

The S/D functional component utilizes local sensors to detect contacts. Sensor track positional reports and intelligence (INTEL) reports are distributed over the LAN for other users. S/D will accept track cues from other remote units and task local sensors to search and detect for possible threats.

The Search / Detect function consists of the following components:

- 1.1 Sensor Assets are the physical input mechanisms to the system. They detect targets and send data to the system tracker. These assets include different radar systems, sonar, EO/IR sensors, electronic intelligence (ELINT), and any other type of detection equipment.
- 1.2 Sensor Reports contain current operational status updates of the netted sensors.
- 1.3 Sensor Track Reports provide target telemetry, such as relative location (range), radial velocity, and elevation, or depth to the system tracker.
- 1.4 INTEL Reports are provided to decision makers to aid in placement of ordinance and locations of high profile targets of interest.
- 1.5 Measurement Reports are used by maintenance technicians for assistance in troubleshooting and repair activities of sensor systems.

The outputs of the Search / Detect (S/D) function state what sensor assets are available, provide reports on sensors including detections, track reports from sensors including positions, and report on INTEL and measurement reports.

Data is also shared between other functions in the OAWSD model. The output data from Search / Detect (S/D) function is provided to the 2.0 Data / Information Services (DIS) and 7.0 Common Services (CS) functions via the local OACE network LAN. The Search / Detect (S/D) function inputs data from 2.0 Data / Information Services (DIS), 7.0 Common Services (CS), and the 8.0 Training (TR) functions via the local OACE network LAN.

## **2. Data / Information Services (DIS)**

Data/Information Services (DIS) is the repository for all track data and non-kinematic information, and is responsible for sensor coordination. The DIS functional component will maintain all time critical system track data for real time (RT) and near real time (NRT) tracks, including kinematics, identification, class, Link-Track Number, and primary and secondary source information. DIS will distribute time critical track data over LAN for other users.

The DIS function is comprised of the following sub functions and applications:

- 2.1 System Track is a correlation of sensor tracks into a single integrated display that is presented to the user.
- 2.2 Supporting Source Tracks are used if the primary sensor fails or is off-line then the next best track quality is provided from an additional sensor.
- 2.3 Classifications of tracks are labeled as either surface, airborne, or undersea targets. Tracks are also identified as either threat, friendly, or unknown.
- 2.4 Track Kinematics are those that describe the motion of the track, information presented as velocity, heading, altitude (if applicable) relative to user.
- 2.5 Attribute Data function associates the data to a specific sensor, weapon system, or platform.

- 2.6 Track Repository is the storage of track information in the form of a history log used to playback in either training scenarios or investigation of an incident.
- 2.7 NRT INTEL Tracks provide INTEL information to commanders and decision makers. These are used to build a trend of threat movement and capabilities.
- 2.8 Sensor Scheduler is used lay out the plan of operations and preventative maintenance of the sensor subsystems.

The DIS function outputs system and supporting source tracks. The function also provides the classification of the threat, kinematics of the track, attribute data, and NRT INTEL track data. The function also acts as the scheduler for the sensors in the system.

The Data / Information Services (DIS) function also provides data to other functions while utilizing data from various functions. The data provided by the DIS function is used by the 1.0 Search / Detect (S/D), 3.0 Planning, Assessment & Decision (PAD), 4.0 Weapon / Asset Services (W/AS), 6.0 EXCOMM, and the 7.0 Common Services (CS) functions via the local OACE network LAN. The DIS function also makes use of data from the 1.0 Search / Detect (S/D), 3.0 Planning, Assessment & Decision (PAD), 6.0 EXCOMM, and the 7.0 Common Services (CS) functions via the local OACE network LAN.

### **3. Planning, Assessment & Decision (PAD)**

The PAD directs and coordinates execution of the following warfare areas: Anti-Air Warfare (AAW), Strike Warfare (STW), Anti-Surface Warfare (ASUW), Anti-Submarine Warfare (ASW), Amphibious Warfare (AMW), Mine Warfare (MW), Naval Special Warfare (NSW), and Command and Control Warfare (C2W). The PAD functional component directs execution of all of the various warfare areas, perform threat assessments, and accept Command and Control orders.

The PAD function consists of the following sub functions and applications:

- 3.1 Assigned Missions contain the lists and details of current, upcoming, and previously designated missions.
- 3.2 Tactical Picture provides a current layout of the battle space to local force commanders and decision makers.
- 3.3 Action Plans are the details of upcoming missions and actions.
- 3.4 Capability is the current competence of system due to limitations or availability of various sensors and weapon systems.
- 3.5 Plan is a list of events and tasks to be accomplished.
- 3.6 Mission Assessment is the analysis of completed and in-progress missions that is analyzed and used for future mission planning.
- 3.7 Threat Assessment (Including Identity) includes the level of potential threat to mission and allied forces. The assessment also identifies specifically what the threat is and its capabilities.
- 3.8 Command & Control (C2) Order, Schedule & Event function programs the tasks to C2 operators according to a hierarchal scheme.

The PAD function provides the mission assignment and tactical picture of the battlespace to the user. The PAD function also supplies plans of action, assessment of mission, identity of threat, and the assessment of threat. In addition to these the function also provides C2 order, schedule, and event.

The function supplies data via the local OACE network LAN to the 1.0 Search / Detect (S/D), 4.0 Weapon / Asset Services (W/AS), 6.0 EXCOMM, 7.0 Common Services (CS), and the 8.0 Training (TR) functions. Data is provided to the PAD function via the local OACE network LAN from the 1.0 Search / Detect (S/D), 4.0 Weapon / Asset Services (W/AS), 6.0 EXCOMM, 7.0 Common Services (CS), and the 8.0 Training (TR) functions.

#### **4. Weapon / Asset Services (W/AS)**

W/AS is the controlling function for all shipboard and shipboard-controlled assets within Mission Execution, and the coordination function for other BF W/AS-enabled assets. W/AS in general develops and schedules all actions to be taken. W/AS directs weapons assets, remote vehicle assets, and ship's Hull, Mechanical & Electrical (HM&E) assets.

Controls and coordinates all shipboard and shipboard controlled assets included in the mission execution block. Also provides weapon, remotely controlled vehicle (RV), navigation (NAV), and engineering to the system.

The W/AS function is made up of the following sub functions and applications for weapons, remotely controlled vehicles (RV), navigation (NAV), and engineering systems:

- 4.1 The Action function controls the actions of assets such as radiate, safe, fire, etc.
- 4.2 The Schedule application controls the schedule of weapon systems and assets such as when preventative maintenance and overhaul occurs.
- 4.3 The Event utility provides status report for the weapon systems, navigation, remote controlled vehicles, and engineering assets to system.

The function supplies data via the local OACE network LAN to the 3.0 Planning, Assessment & Decision (PAD), 5.0 Mission Execution (ME), 6.0 EXCOMM, and the 7.0 Common Services (CS) functions. Data is provided to the W/AS function via the local OACE network LAN from the 2.0 Data / Information Services (DIS), 3.0 Planning, Assessment & Decision (PAD), 6.0 EXCOMM, and the 7.0 Common Services (CS) functions.

## **5. Mission Execution (ME)**

The ME function is comprised of the specific ship and RV execution assets, including weapons, RV assets, and other ship assets. The Weapon assets include missiles (air/surface/land), guns, torpedoes, decoys/electronic attack, etc. The RV assets include controlled aircraft, boats, and unmanned vehicles. The Ship assets include engineering, damage control, and the integrated bridge. The function maintains all weapons, remote vehicle, ship and communications assets.

The Mission Execution function is made up of three primary OA platform-unique function/applications with sub-functions and assets.

- 5.1 Weapons Systems are used to place ordinance upon designate threats.
  - 5.1.1 Air/Surface Missiles are launched from land, sea, or subsurface platforms.
  - 5.1.2 Land Attack Missiles are fired from land, sea, air, or subsurface platforms.
  - 5.1.3 Torpedoes are deployed from air, sea, or subsurface platforms.
  - 5.1.4 Guns are fired from sea, air or land systems.
  - 5.1.5 Decoys are countermeasures used for evasive actions or to draw out threats from seclusion. Decoys are available in a multitude of forms and capable of being deployed from all platforms.
- 5.2 Remote Controlled Vehicle (RV) Assets are used for reconnaissance, placement of ordinance, and the acquisition and transmission of INTEL.
  - 5.2.1 Aircraft are used to fly over areas of interest and photograph potential targets. The aircraft is also capable to carrying a limited amount of ammunition.
  - 5.2.2 Boats are used for reconnaissance and the gathering of INTEL.
  - 5.2.3 An Un-Manned Vehicle such as a robot is used to investigate possible threats like improvised explosive devices (IED) and other missions where deemed useful.
- 5.3 Engine Control System directs the operation of propulsion for the platforms.



- 5.3.1 The Engineering component includes propulsion and life support systems.
- 5.3.2 The Damage function provides status resulting from damage due to enemy fire, friendly fire, weather, system failure, and navigation hazards
- 5.3.3 The Bridge is the central control center where the status and the control of the engineering systems are located.

## **6. External Communication (EXCOMM)**

This partition represents the link between the combat system and the various data and information sources available both within and external to the force. The External Communication (EXCOMM) function is a conduit responsible for sending and receiving track data, planning information, Intelligence (INTEL), etc., to and from other units in the battle force (BF), battle group (BG), or entities external to the BF/BG. It represents the link between the combat system and the various data sources within and external to Battle Force; responsible for sending/receiving track data, mission plans, intelligence to and from other units in the Battle Force.

The EXCOMM function consists of three OA common functions including the Common Services Action, Network Schedule, and Message Event functions. The EXCOMM also contains four OA platform-unique components such as Network, Radios, Sat COM, and Data Links.

- 6.1 Communications Service Action is an OA common function that enables communication between decision makers and war fighters.
- 6.2 Network Schedule is the OA common function that allocates time to systems and users for communication in order to manage bandwidth.
- 6.3 Message Events are an OA common function that provides users, commanders, and decision makers the status of system assets.

- 6.4 Network is an OA platform-unique application that provides means for simultaneous communications between multiple users rather than point-to-point.
- 6.5 Data Links is the OA platform-unique application that allows for data and information to be shared, or transferred, between weapons systems, sensors, and other system assets.
- 6.6 Radios are the OA platform-unique systems allow communication between war fighters the battlespace or local operational theatre.
- 6.7 Sat COM is the OA platform-unique system that provides communication between war fighter and decision makers around the world via satellites.

The outputs of the EXCOMM function include track data, planning information as well as INTEL. Data from the EXCOMM function is distributed to the 1.0 Data / Information Services (DIS), 3.0 Planning, Assessment & Decision (PAD), 4.0 Weapon / Asset Services (W/AS), 7.0 Common Services (CS), 8.0 Training (TR) functions through the local OACE network LAN. Data is also provided to the 9.0 Force Planning / Coordination (FP/C) function on the Force Network. Data is received from the 1.0 Data / Information Services (DIS), 3.0 Planning, Assessment & Decision (PAD), 4.0 Weapon / Asset Services (W/AS), 7.0 Common Services (CS) functions through the local OACE network LAN. Data is also provided to the EXCOMM function from the 9.0 Force Planning / Coordination (FP/C) function via the Force Network.

## **7. Common Services (CS)**

The Common Services (CS) Partition consists of the following: Databases, Display, Time, Data Extraction/Data Reduction (DX/DR), Environment, Navigation (NAV), and Utilities. These represent those services within and across the combat system, unit, and BF that are common.

This function represents all services within the Combat level, Unit or Battle Force Level that are common to the system. The function is comprised of six OA common function/applications.

- 7.1 Displays provide users with real-time tactical display of targets and system status.
- 7.2 The Navigation (NAV) function aides the user with position, velocity, heading, and bearing information integrated with targets, land masses, weather, depth, and if applicable, altitude.
- 7.3 Databases contain information used to build scenarios for prediction of events such as weather conditions, collision avoidance, etc.
- 7.4 The Time function provides the system with synchronous timing for assets, war fighters and decision makers.
- 7.5 Data Extraction / Data Reduction (DX/DR) function is used for in-depth data analysis of specific areas of interest. This tool provides analysts and engineers a better look at why a fault or event has occurred within a system or subsystem.
- 7.6 The Environment application factors in environmental conditions and potential impacts to system and war fighters.

Outputs for the function involve display, navigation (NAV), database, and environmental information as well as time and data extraction & reduction. Data is provided to and received from all functions in the OAWSD.

## **8. Training (TR)**

This partition provides for scenario generation, exercise control from own ship and remote stations afloat and ashore, and training playback and analysis tools to assess the battle readiness of the force, unit, and individual. The scope of training addresses total ship mission training requirements for the tactical system team/operator, maintenance technician, damage control team/operator, etc., as well as training within a BF context.

The TR Partition provides for the planning, conduct, assessment, and management of readiness information for training. It represents an embedded force training capability available pier-side and underway for training (a) the battle force, (b) ships from a total ship perspective, (c) individual own-ship teams, and (d) the individual operators. It will support individual operator training through interactive lesson-based training, as well as supporting training of operator teams and sub-teams within a single platform, and multi-platform training through interactive scenario-based training.

The Training (TR) function is made up of three main OA common function / applications and three applications that are used in the main functions.

8.1 The Training Action, Schedule & Event function controls when, where, and with what resources the war fighters use to simulate battle conditions.

8.1.1 A Simulator is used to replicate the actions, schedules, and events used in the training system.

8.2 Synthetic Actions are provided to the war fighter and commander for use in the training system.

8.2.1 A Simulator is used to synthesize the actions the war fighter and commander is to enact upon.

8.3 Synthetic Entities are used to provide the system with synthetic test targets to practice using the weapon system, communication, and sensor controls.

8.3.1 The Scenario function supplies user with various situations to be used for training purposes.

The main output of the training function is an assessment of battle readiness. Data from the Training function is supplied to the 1.0 Search / Detect (S/D), 3.0 Planning, Assessment & Decision (PAD), 5.0 Mission Execution (ME) and 7.0 Common Services (CS) functions through the local OACE network LAN. The Training (TR) function receives data from the 3.0 Planning, Assessment & Decision (PAD) and the 6.0 EXCOMM functions on the local OACE network LAN.

## **9. Force Planning / Coordination (FP/C)**

FP/C enables the coordination of and collaboration among own-ship and Battle Force (BF) assets to perform a particular mission. This function performs coordination between warfare areas as well as coordination / de-confliction within a warfare area (e.g. STW using missiles, manned aircraft, or guns). This function also generates, assigns, manages, and implements force orders for all defined mission areas. It assesses the plan and performs rapid re-planning as necessary. FP/C also allocates specific assets to operations or missions, and provides initial mission conduct guidance to assets

The Force Planning / Coordination function provides mission coordination at the Battle Force level; processes Force Orders; assesses the mission plan and provides re-planning as needed.

This function includes six OA platform-unique function/applications.

- 9.1 Joint Battle Force (BF) Orders are provided to the joint war fighters with actions to be accomplished.
- 9.2 The Commanders Estimate provides the decision makers with an estimation of battlespace size, threat conditions and assessment.
- 9.3 The Common Operating Area (COA) Repository retains historical information to be used for evaluation, analysis, and future decision making.
- 9.4 The Battle Group (BG) Orders supplies participants in the Battle Group with orders for the current mission.
- 9.5 The Force Integrated Schedule is a plan of actions for local, joint and coalition forces.

The function outputs the coordination between warfare areas and de-confliction within warfare area. Force orders for all defined mission areas are provided as output from the function. The FP/C function also produces planning and re-planning and

allocation of specific assets to operations or missions. The initial mission conduct guidance to assets and assessment of mission plan is also presented by the function.

Data is provided to and received from the 6.0 EXCOMM function on the Force Network and the 7.0 Common Services (CS) function on the local OACE network LAN.

## **10. OAWSDM Analysis**

After decomposing the OAWSDM, it is interesting to note several key issues that will be relevant to the functional decomposition and evaluation of the model. First, the system provides some limitations on which functions can communicate with one another. For example, the Search/Detect function has two way communications with only the Data/Information Services function. There are systems which may want to rely on unprocessed, raw data from the sensors in order to function. The lack of direct connectivity between the sensing function and the communications function also precludes sharing of raw data outside of the system. Second, the system provides no health monitoring, diagnostic/prognostic function or interface status. While this is not the focus of this study, being aware of the system degradation due to hardware or software failure can directly impact the availability and effectiveness of the detect, control, and engagement process. It is understood that a system built within the OAWSDM may include elements not explicitly shown in the model such as built in test, but by not including it in the model, the possibility exists that a system constructed within this architecture will lack that capability. While these observations do not contribute to the development of the model in this study, they should be considered in the development of an improved OAWSDM-based system.

## **C. INPUT – OUTPUT ANALYSIS**

To clarify the problem space, an Input-Output analysis was conducted. Since the OAWSDM is complex and designed to perform multiple functions, it is important to understand the desired inputs and outputs in relation to the specific surface TCT problem

at hand. The Input-Output analysis represented the system architecture collecting raw data and processing it as it completes its mission of intercepting time critical targets.

Three inputs were defined: awareness, planning and availability data. Awareness data consists of sensory information provided by both organic and remote sensors used to detect incoming TCT threats. Planning data, which includes the battle group configuration and rules of engagement, provide the basis upon which TCT engagement plans are determined. Finally, availability data defines what sense, control and engage assets are available to employ against the TCT. Two primary outputs were defined: ordnance on target, which refers to the actual desired output of a TCT kill and target data, which refers to data sent to other platforms. These inputs and outputs are used to construct an OAWSDM TCT context diagram.

Inputs	Awareness Data Organic Sense Remote Sense Planning Data Battle Group Configuration Rules of Engagement Availability Data
Outputs	Ordnance on Target Target Data

Table 1. Desired Inputs and Outputs of the OAWSDM

**D. SCOPE AND BOUNDS ANALYSIS**

The Scope and Bounds Analysis is meant to provide a framework within which to analyze the problem space. In order to scope the problem, the identifiable needs are laid out. These are the concrete things that the resultant model of the architecture, must

provide. For the time critical targeting problem, certain scopes and bounds were needed to limit the problem to a manageable study. These are detailed in table 2.

Process	Bounds	Scope
OATCTEPM	The OATCTEPM will model the detect-control-engagement process as bounded below. The model is designed for use with two scenarios involving surface TCTs. The model is limited to a single ship's engagement during a single scenario that can then be analyzed in multiple replicates.	Uses notional versions of weapon systems used on a modern cruiser type ship and employs technology readily useable in 2007. Created using Arena software package. Uncertainty is modeled using uniform or normal distributions around a notional average value for a process.
Model Analysis	The analysis of the model created to study the OAWSDM will focus on the C <sup>3</sup> portion of the Detect, Control, and Engage paradigm. The model will be run using scenarios developed for surface based TCTs.	Determine the overall effectiveness of the OAWSDM with respect to TCTs. Create a model that would allow analysis of an integrated combat system, which adheres to this architecture.
Detect-Control-Engagement Process	Engagement begins at target detection, with the Detection Process. At this point, target is unknown until classification is performed. It ends with either the target reaching keepout range or a target hard kill.	Engagement takes place aboard a single cruiser type vessel. If target reaches keepout range, it is declared a leaker and no battle damage assessment is made. Target is either destroyed or is not hit; there is no soft kill or disabling.
Detection	Detection process will begin at initial target detection as the maximum detection range is breached by incoming enemy vessel. It ends at handoff to ship control systems	Detection process and capability are constant throughout analysis. Detection capability is based on common scientific principles employed in the design and implementation of all surface search radar systems.
Control	The control process consists of the command, control and communication process and is bounded by the interfaces between functions defined in the OAWSDM.	The C <sup>3</sup> function lies between the Detect and Engage functions and includes many activities that require human interaction. These activities are bounded by specific functions - Validate Target, Identify Target, Threat Evaluation, Assign Target Priority, Mission



		Evaluation, Weapon Assignment, and Plan Approval. These functions map directly to the OAWSDM.
Engage	The engage process begins with weapon assignment and runs to the completion of the overall process, the kill evaluation.	Engagement processes and capabilities are constant parameters throughout the analysis.

Table 2. Scope and Bounds Analysis

## E. FUNCTIONAL ANALYSIS

The functional analysis conducted in this study leverages on the information collected in the problem definition phase. This phase begins with the construction of an Architecture Flow Context Diagram (AFCD). The figure below illustrates the system in its environment of terminators (Hatley, Hruschka, and Pirbhai, 2000). This context diagram serves as the foundation for the development of the functional flow diagrams.

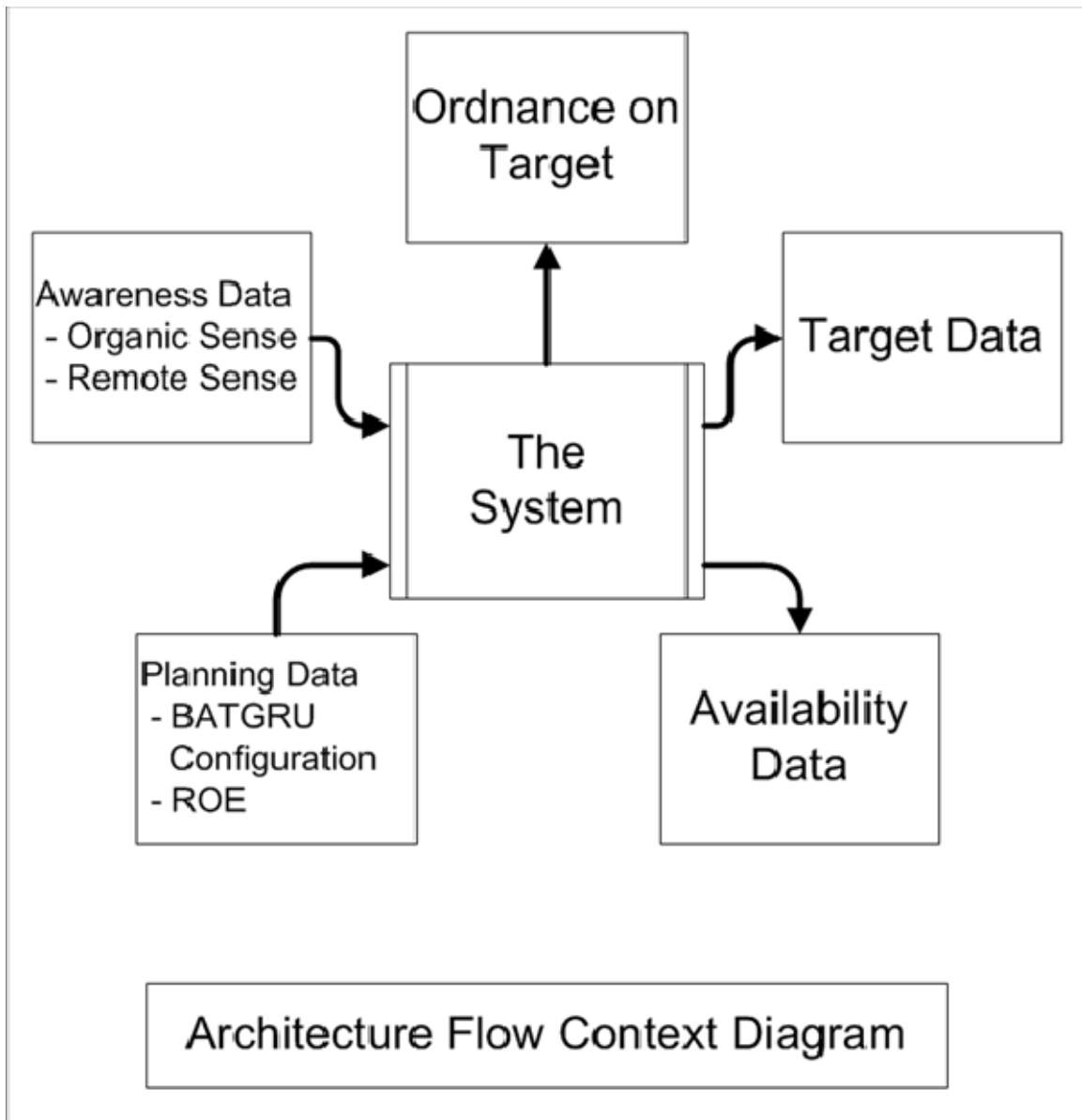


Figure 8. Time Critical Target Architecture Flow Context Diagram

Additional processes influenced the development of the functional flow, such as the DCE and JDL model pictured in figure 5, using the OODA Loop as a foundation. The fusion of these paradigms with the context diagram above, serve as the basis for the functional flow analysis. This analysis is necessary to transform the OAWSDM architecture into a form that can be readily used to create a process simulation using the Arena software package. The OATCTEPM that results is used to analyze the effectiveness of the OAWSDM against time critical targets.

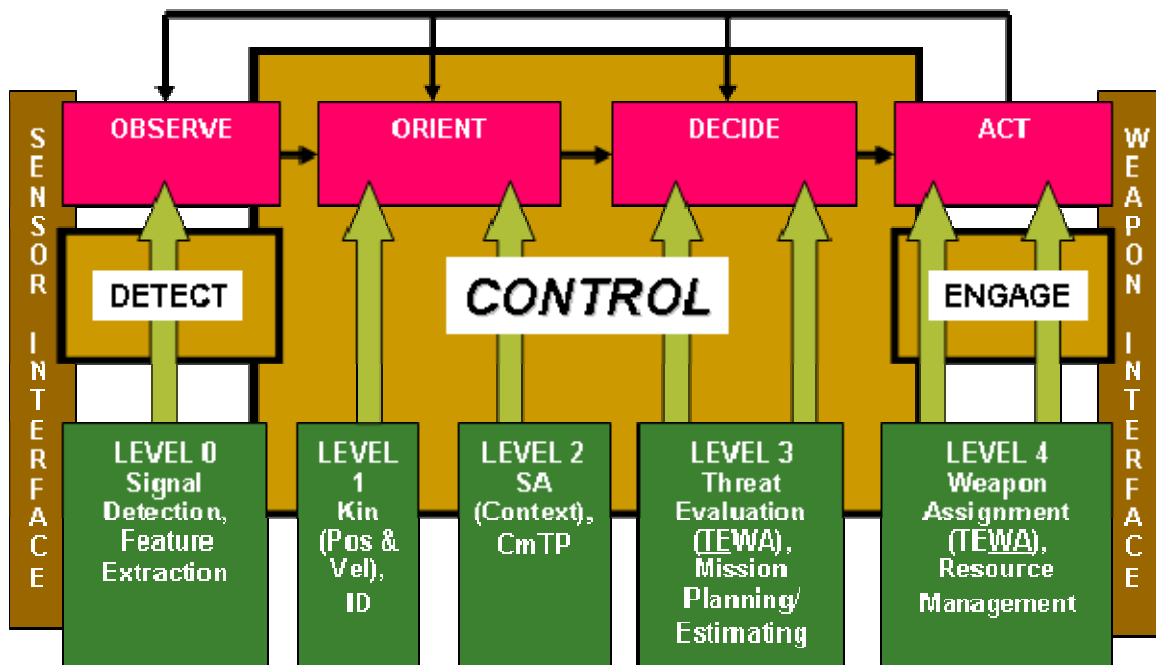


Figure 5, OODA, DCE, and JDL Data Fusion Model Repeated for Clarity

(Luessen, 2003)

### 1. Function Flow Analysis

Once this basic context is defined, a functional flow block diagram is constructed for each segment of the process. This process view illustrates the functions in the order in which they occur as well as how data moves through the system defined by the OAWSDM. These diagrams then provide the basis for the OATCTEPM as it is constructed in Arena. This model, as described in section IV of this paper, provided a

detailed analysis of the OAWSDM effectiveness against time critical targeting scenarios as defined in Appendix I.

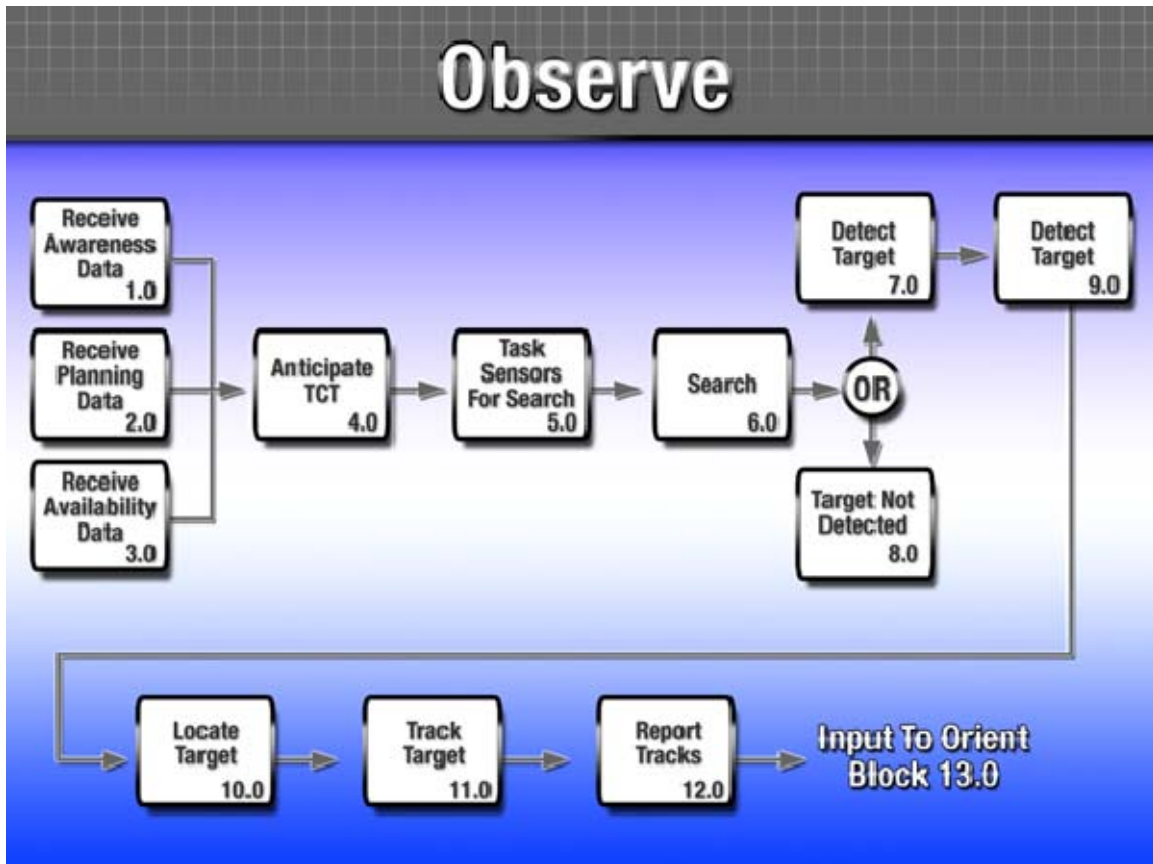


Figure 9. Functional Flow Block Diagram for Observe

*This is the functional flow for the Observe function. Beginning with the receipt of initial data, sensors are tasked to acquire further detail so that a target can be located and classified. This process terminates at either the non-detection of the target or the detection and subsequent tracking of the target.*

# Orient

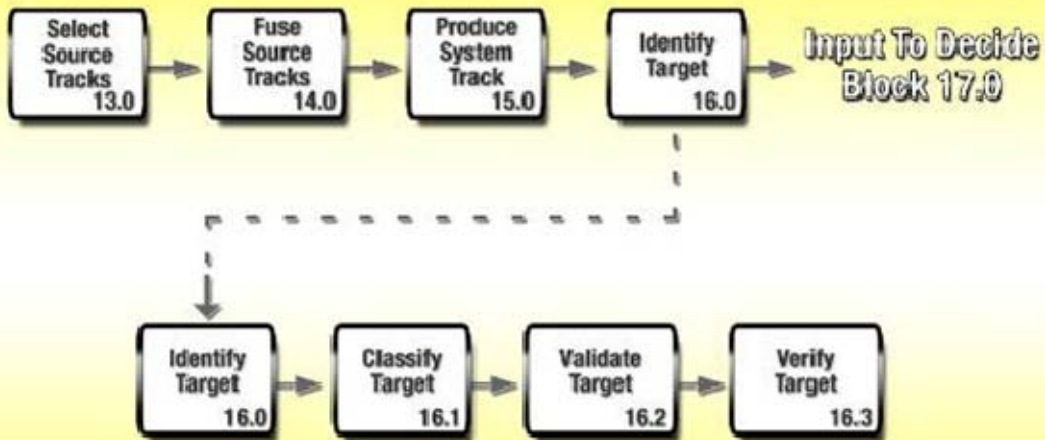


Figure 10. Functional Flow Block Diagram for Orient

*This is the functional flow for the Orient function. Beginning with the receipt of tracks from the Observe function, data is fused from multiple sensor sources leading to classification of the target and subsequent verification.*

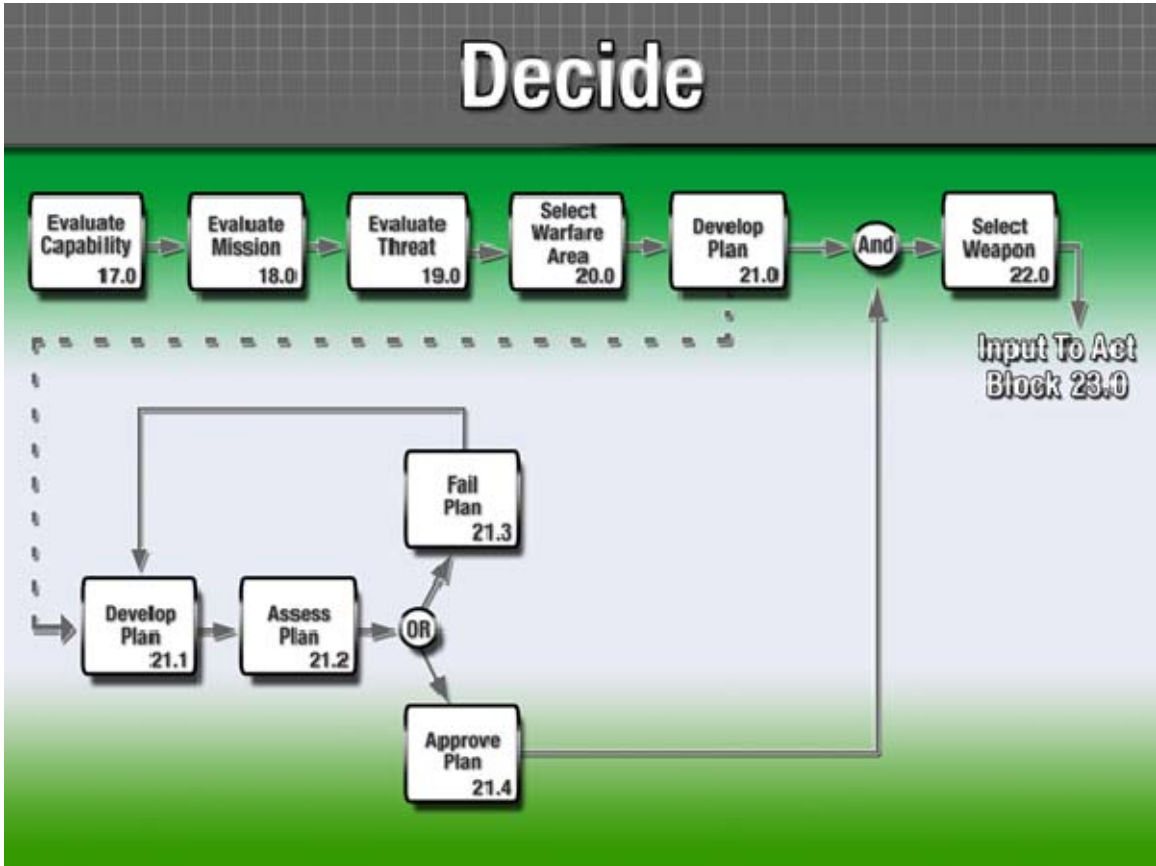


Figure 11. Functional Flow Block Diagram for Decide

*This is the functional flow for the Decide function. Beginning with the verified target from the Orient function, ship capabilities are evaluated based on the target and necessary planning is conducted for interception of the target. This process terminates with the selection of a weapon system to begin the engagement with.*

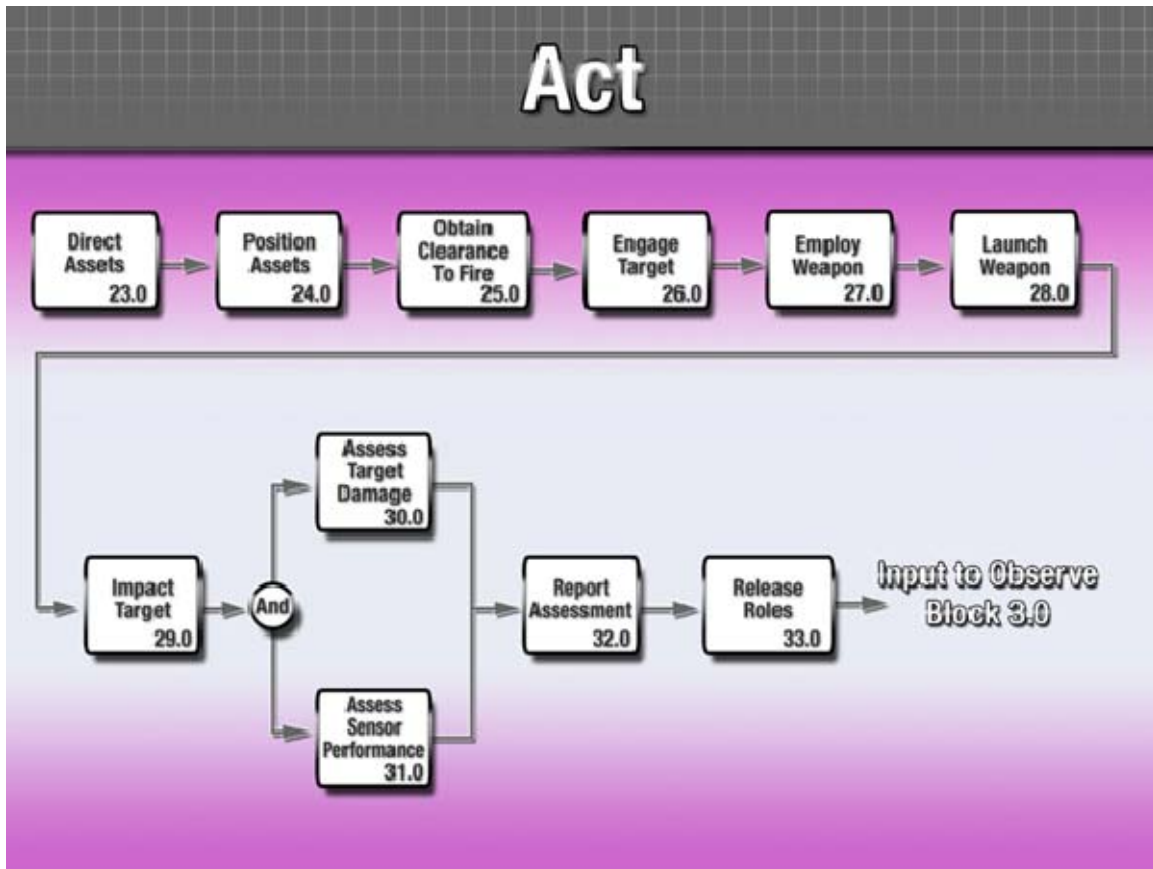


Figure 12. Functional Flow Block Diagram for Act

*This is the functional flow for the Act function. Beginning with the weapons selection in the Decide function, ship assets are directed to intercept the target. Weapons are launched and a kill assessment is made, resulting in further engagements as necessary.*

The functional analysis performed provides the foundation needed to construct a simulation model of a TCT engagement framed by the OAWSDM architecture. This framework is used to show a notional process that was transformed into the OATCTEPM, as described in Appendix II. This simulation allows the system flow to be instrumented so that measurements can be recorded and analyzed.

THIS PAGE INTENTIONALLY LEFT BLANK



## **IV. MODEL DESIGN**

### **A. MODELING GOALS**

Based on the functional analysis, a model was developed in Arena to fully represent the functionality of the OAWSDM during the time critical engagements described in Appendix I. This model, the OATCTEPM, was developed to provide simulated results similar enough to a possible future implementation of the OAWSDM that a comparison could be performed with an improved version of the simulated system. The OAWSDM was used as a basis for development of the OATCTEPM created in Arena. Research concerning time-critical targeting, as presented in the Literature Search section of this paper, was also used in the development of the model to ensure the focus remains on the unique issues posed by time-critical targets.

All of the functional blocks within the OAWSDM have been represented in the OATCTEPM with exception of 8.0 Training. The other eight functional blocks of the OAWSDM are: 1.0 Search/Detect, 2.0 Data/Information Services, 3.0 Planning, Assessment, and Decision, 4.0 Weapon/Asset Services, 5.0 Mission Execution, 6.0 External Communications, 7.0 Common Services, and 9.0 Force Planning/Coordination. Each of the model blocks within the OATCTEPM has been mapped into one of these 8 functional blocks of the OAWSDM. A full explanation of each model block along with process flow diagrams of the model is contained in Appendix II and shows the categorization of each model block into the functional blocks of the OAWSDM.

### **B. OPERATIONAL VIEW**

In order to better understand the totality of the scenarios presented for evaluation of the OAWSDM, an operational view, known as an OV-1, was developed (DODAF 2007). This OV-1 shows the cruiser as the focal point of the scenario. In this representation of the second scenario detailed in Appendix I, it is surrounded by a number of different threats, all radially inbound. The cruiser is effectively on its own for

the immediate confrontation, although a similar ship is in the region and can be signaled for assistance after the initial assault. The cruiser possesses two attack helicopters which are used to help combat the incoming threats.

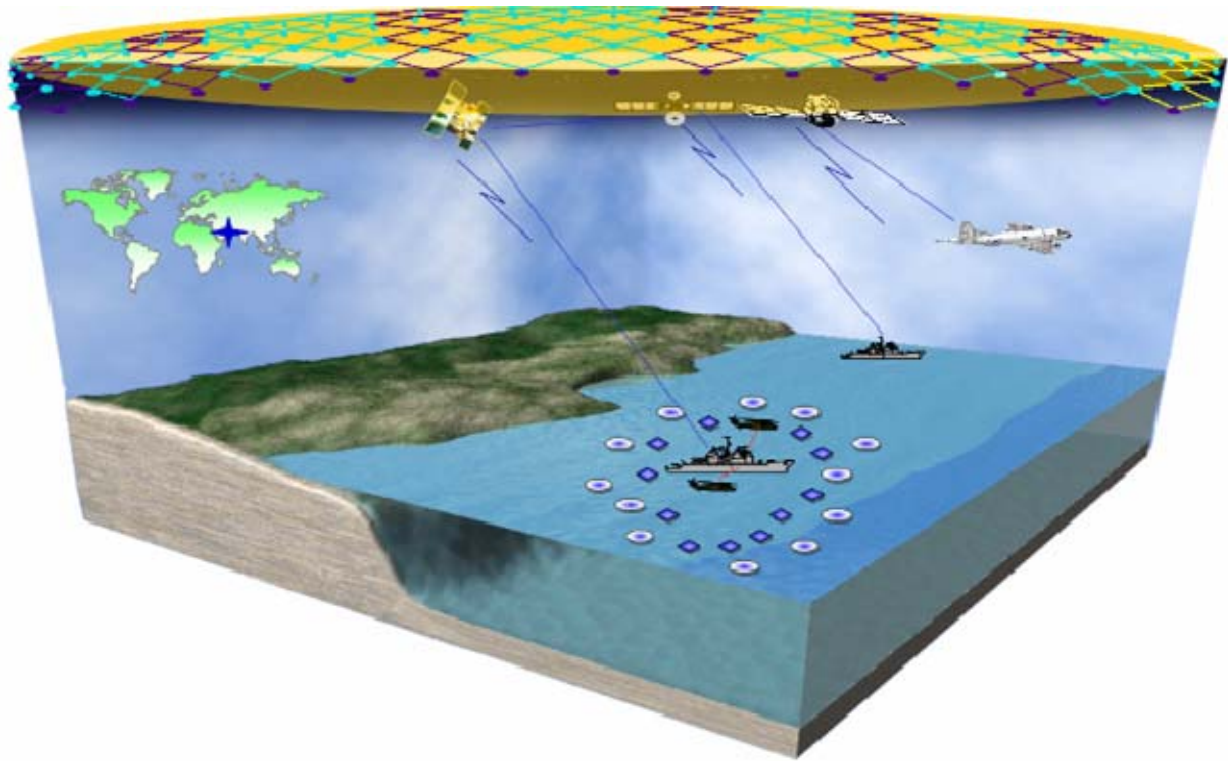


Figure 13. Operational View (OV-1) for TCT scenarios

*The above OV-1 represents the second scenario presented in Appendix I. It shows a saturation attack against a lone cruiser by a large number of FIACs.*

## C. METRICS DEFINITION

### 1. Introduction

In order to conduct a meaningful evaluation of the OAWSDM, an instantiation was developed and is the basis for the model presented in this project. This is based on the projected development of the system and combined with the OODA target engagement model. The simulation model is complex; therefore figure 14 is offered as a starting point to present a more simplified view in the form of the Detect – Control – Engage paradigm

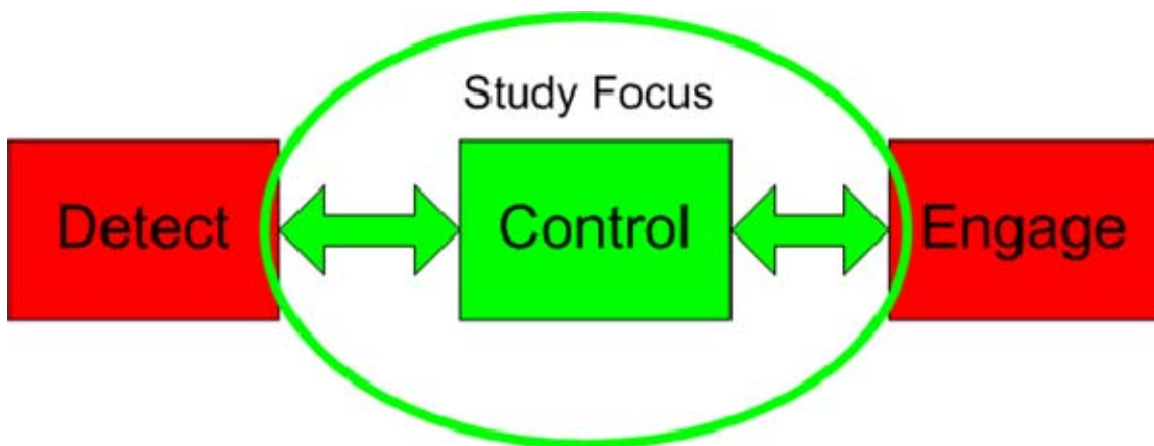


Figure 14. Simplified Concept of Model

*The yellow (highlighted) section of the figure indicates the area of interest for the analysis effort – it is the Command, Control and Communications (C<sup>3</sup>) conduit.*

The development of Measures of Performance (MOPs) and Measures of Effectiveness (MOEs) is dependent on the situation being studied. Due to the complexity of the model used in this study, the performance qualities of the system are classified into more narrow groups, which contain quantities that have some *common denominator* (Cohen, Lapid, and Gur 2000) against which the effectiveness of the OAWSDM can be evaluated. The following sections describe the development of these evaluation measures.

## 2. Baseline Model MOPs

Upon creation of the OATCTEPM, the first step in analyzing its effectiveness was to run a baseline case for each scenario. These results were used to examine the first set of Measures of Performance. These MOPs are listed below:

Time Segment	Description	Functional Flow Designation
Validate Target Time	Validate target time is the time needed from firm track to target validation.	16.2 Validate Target
Identify Target Time	Identify target time is the time required from validation of the target to identifying the target.	16.0 Identify Target
Threat Evaluation Time	Threat evaluation time is the time consumed between identifying target and threat evaluation of the target.	19.0 Evaluate Threat
Assign Target Priority Time	Assign target priority time is the time required once threat evaluation is final to the completion of assigning the target a priority.	16.1 Classify Target
Mission Evaluation Time	Mission evaluation time is the time needed to evaluate the mission as a go or no go and starts directly after the target is assigned a priority and ends after the mission evaluation is complete.	18.0 Evaluate Mission
Weapon Assignment Time	Weapon assignment time is the time required to assign a weapon to a target and starts once mission evaluation is completed and only if the mission is evaluated as a mission go.	22.0 Select Weapon
Plan Approval Time	Plan approval time is the time required to review weapon assignments made by the platform and to acquire approval by the leader of the platform.	21.0 Develop Plan

### Individual Component Times

After the data was collected, the MOPs were used to determine which segments of the overall engagement process would yield the most benefit from possible improvement.

### 3. Total C3I Time MOP

A sum of the data associated with the MOPs listed in table 3 is used to compare the baseline model performance to that of any improved concepts. The C<sup>3</sup>I time, in seconds (s), is defined as the time from the initiation of the “Firm Track” process block to the completion of the “Direct Engagement to Weapon” process block in the OATCTEPM:

$$\text{Total C}^3\text{I} = \text{Validate Target} + \text{Identify Target} + \text{Threat Evaluation} + \text{Assign Target Priority} + \text{Mission Evaluation} + \text{Weapon Assignment} + \text{Plan Approval}$$

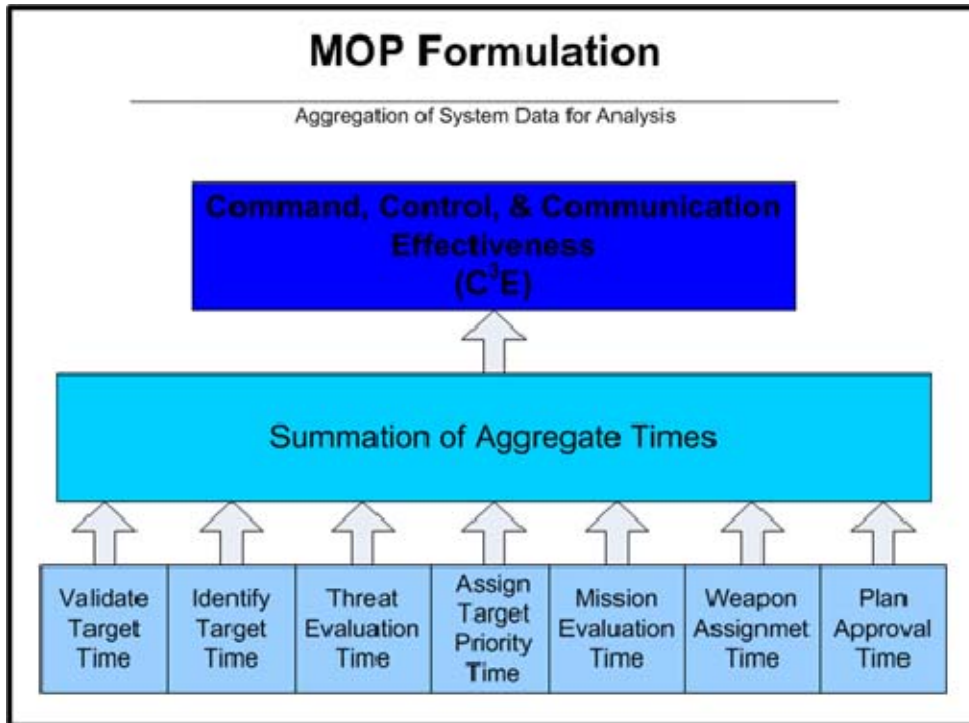


Figure 15. Time-based MOP formulation for FIAC scenarios

*The above figure describes the formulation of the Measures of Performance used for the analysis of the simulation.*

#### 4. Measures of Effectiveness

The primary measure of effectiveness for the scenarios is the probability of a target making it past the defending ship's defenses, known herein as the probability of a leaker. Mathematically, this is shown in the below equation, where the probability of a leaker,  $P_L$ , is defined as the number of targets not intercepted in a given scenario divided by the total number of targets:

$$P_L = \frac{\text{Failures}}{\text{Total}} = \frac{\text{Number of Targets Not Intercepted in a Trial}}{\text{Total Number of Targets in the Trial}}$$

From this, another MOE can be defined as the complement to the probability of leakers, the probability of raid annihilation,  $P_{RA}$ . The probability of raid annihilation is defined in the below equation, where it is merely

$$P_{RA} = 1 - P_L$$

This represents the probability of intercepting all the incoming targets in a given scenario.

The model results are comprised of numerous individual runs and as such, the MOEs are presented as averages of those runs. Hence, it is also desirable to not only examine the average of the runs but to examine the distribution as well. For this purpose, a third MOE was defined: probability of success,  $P_{SUC}$ . This MOE is defined as the number of trials where there are no leakers (and hence raid annihilation was achieved) divided by the total number of trials:

$$P_{SUC} = \frac{\text{Successes}}{\text{Total}} = \frac{\text{Number of Trials without a Leaker}}{\text{Total Number of Trials}}$$

While a low probability of leakers leads to a high probability of raid annihilation, this MOE shows how often raid annihilation is, indeed, achieved.

## **5. MOE and MOP Comparison**

As a final step, the C<sup>3</sup>I time and the MOEs defined in the previous subsection will be compared graphically. This analysis will plot the C<sup>3</sup>I time as an independent variable and the probability of raid annihilation and success as the dependant variables. By performing this analysis, some relationship can be developed to assist in the identification of the MOEs vary as a function of the C<sup>3</sup>I time.

## **6. Use of MOEs in the OATCTEPM**

The OATCTEPM is designed to record the data required to evaluate the MOEs. The MOEs will demonstrate the effectiveness of the OAWSDM for each of the time-critical targeting scenarios and suggest what level of improvement may be necessary to yield the desired state. The data recorded by the Arena model consists of the following:

- Total number of kills
- Total time from detect to completion (whether target kill or target within keepout range)
- Number of kills by each weapon (Gun Weapons System, Close In Weapons System, Precision Attack Missile, and Harpoon)
- Number of targets within keepout range.

The statistics for each of these pieces of data are kept and recorded throughout the simulation runs. The results of the data recording are used to calculate the MOEs.

## **D. MODEL SCENARIO DEFINITION**

Two different TCT scenarios are developed to provide the context to run the OATCTEPM and evaluate the OAWSDM against small boat attacks. The parameters of the model change according to the specific scenario being run through the model. The two scenarios and all details of the scenarios are described in Appendix I. Some of parameters that are defined in each scenario are target type, target speed, target range, and target identification parameters.

The first scenario described in Appendix I is an attack by a group of Type-I fast inshore attack craft (FIAC). A Type I FIAC is a two-man personal watercraft armed with a rocket propelled grenade (RPG) launcher and/or a large blast bomb. The Type-I FIAC has an effective weapon range of 0.5 km. There will be four groups of two personal watercraft attacking the cruiser, each starting at a range of 3 km and traveling inbound with a velocity of 40 km/h. Two armed helicopters carrying eight Hellfire missiles each have been deployed before the start of the scenario but will not be part of this engagement.

The second scenario described in Appendix I is a FIAC saturation attack. The attack will consist of twenty Type-I FIAC, twenty Type-II FIAC, and ten Type-III FIAC. Type-II FIAC represents an Iranian Boghammar craft with a weapon range of 9 km. Type-III FIAC represents a C-14 Cat-class catamaran missile boat with a weapon range of 15 km.

## **E. MODEL AND SCENARIO ASSUMPTIONS**

### **1. Rules of Engagement**

Rules of Engagement (ROE) provide the basis of acceptable engagement practices for naval ships to ensure that operations remain in agreement with national objectives and policy. In “Naval Rules of Engagement: Management Tools for Crisis”, ROEs are described as standing orders that, “...specify under what circumstances force may be used to achieve political and military objectives” (Hayes 1989). Due to the ROEs, the timeliness of utilized force can dramatically impact a ship’s ability to respond in a time-critical situation. It is not the intent of this study to conduct a detailed examination of naval ROEs and their impact on the TCT engagement; however the ROEs can play a crucial role they can play in the successful engagement of a TCT. For the purposes of this study, it is assumed that a ship’s ROE allow it to engage threats from small enemy boats described within the scenarios and support the command and control and engagement as represented in the OATCTEPM.



## 2. ROE Based Assumptions

Following is a brief description of ROE related assumptions used in the scenarios and model:

<b>Rules of Engagement Assumptions</b>
Intelligence supports that a small-boat attack is highly likely and rules of engagement have been clearly defined allowing ships to engage threatening targets
All in-bound surface targets traveling greater than 35 knots are considered a threat
In-bound threats are tracked and engaged prior to reaching the defined keep out range for the target
Outbound entities are considered non-threatening
The ship has the capability to identify a target and distinguish its type (I, II or III as defined in the scenario description) based on the target's radar cross section, speed and behavior
All nations who operate surface vessels in the area have been warned that directly approaching a US vessel at high speeds without prior authorization and identification validation results in engagement and destruction of the inbound vessel
The ship is operating in condition modified Zebra and transitions to Zebra upon detection of a threatening in-bound target
Based on threats, all US naval vessels closely monitor local traffic within a 100 km radius and are looking for any patterns of behavior that may indicate organization or potential attack including but not limited to trailing, running parallel courses, slowly approaching the vessel, loitering
Friendly forces are actively monitoring local communications chatter

Table 3. Assumptions Derived from the Model Rules of Engagement

## 3. Scenario Assumptions

In the development of the two scenarios used in this research, assumptions were defined for the types of targets and the defending ship's capabilities. The assumptions are

detailed, beginning with those that are common to both scenarios examined. Scenario specific assumptions follow, along with assumptions specific to the weapons systems employed in the scenarios.

<b>General Scenario Assumptions</b>			
Platform is a single CG(X)			
All initial detections utilize a modern surface radar system			
Target Assumptions			
	size (height in feet)	speed (knots)	weapon range (km)
Type I	small (3')	40	0.5
Type II	medium (10')	40	9
Type III	large (25')	50	15
All targets are considered small, medium, or large			
Each target type has only one weapon range			
Once the target reaches its weapon range, the target is considered a leaker and is recorded as a failure for the CG(X)			
Based on the general makeup of the area of operation 65% of entities are friendly, 10% are hostile, 25% are unknown			
For specific scenarios, all targets are considered to be hostile			
Unknown targets are repeatedly interrogated until identity is resolved			
No unknown vessels are engaged			
Targets are assigned priority according to target type and distance from keep out range			
A higher priority is assigned to targets if they are within 1 km of own ship			
Mission evaluation may send target away from CG(X) and to another platform but the scenarios assume that mission evaluation always results in a mission go			
Weapon assignment normally occurs according to target range, but weapon assignment is specific to each scenario as discussed in previous section			
Approval of plan occurs 95% of the time and disapproval occurs 5% of the time and then requires re-approval with another delay added in			
Obtaining clearance to fire occurs 95% of the time and is delayed until clearance to fire is obtained the other 5% of the time			

Table 4. Threat and Ship Assumptions Common to Both Scenarios

#### 4. Scenario 1 Specific Assumptions

In order to collect all the information needed to support the OATCTEPM, a number of assumptions are necessary for the mechanics of each scenario. Below these assumptions pertaining to scenario 1 are listed.

<b>Scenario 1 Assumptions</b>
The environmental conditions are ideal to support detection and engagement of the oncoming attack and the sea state is 0-1
Eight two-man Type-I targets (personal watercraft), armed with 1 (each) Rocket-Propelled Grenades (RPGs) and packed with high explosives which can be detonated by the driver, or remotely from a stand-off position by an observer, attack the High Value Unit (HVU) simultaneously from four different directions
Keep-out range for the Type-I targets is 500 meters
Inside 500 meters the targets can inflict a soft kill by damaging array faces, etc., with
It is the intention of the Red Force to breach the hull with explosives and inflict a hard
A total of four helicopter flight crews are embarked on USS VULNERABLE for the
The ship has only two helicopters armed with 8 AGM-114 Hellfire missiles
The helicopters are 100% operational ready and remain so throughout the given scenario
All shipboard systems are fully operational and do not fail throughout the given scenario

Table 5. Scenario 1 Specific Assumptions

#### Scenario 2 Specific Assumptions

Table 6 lists the additional assumptions needed to implement scenario 2.

<b>Scenario 2 Assumptions</b>
The environmental conditions are ideal to support detection and engagement of the oncoming attack and the sea state is 0-1
It is the intention of the red force to breach the hull with explosives or an anti-ship missile and inflict a hard kill (sink the ship)
A total of four helicopter flight crews are embarked on USS VULNERABLE for the transit from the Mediterranean to the Battlegroup
The ship has only two helicopters armed with 8 AGM-114 Hellfire missiles
The helicopters are 100% operational ready and remain so throughout the given scenario
All shipboard systems are fully operational and do not fail throughout the given scenario

Table 6. Scenario 2 Specific Assumptions

## 5. Overall Model Assumptions

In addition to scenario assumptions and those related to the rules of engagement for the protagonist of this simulation, a number of assumptions were necessary to create the OATCTEPM itself. The below assumptions are necessary to fully understand the model and for interpreting results produced by the model.

<b>Weapon System Assumptions</b>				
Initial engagement is directed to weapon based on initial weapon assignment				
Engagement can be routed to another weapon depending on round availability and target range				
Reaction time for each weapon system is accounted for				
Time of flight for each weapon system is accounted for				
Armed Helicopter positioning time is accounted for if applicable				
Other weapons may be assigned differently depending on scenario				
	Gun Weapon System (GWS)	Precision Attack Missile (PAM)	Close-In Weapon System (CIWS)	Armed Helicopter
Number of Systems	2	4 PAMS per VLS (2 VLS)	2 each with 50 bursts	2 helicopters
Firing Doctrine	Shoot three-look-shoot three	Shoot-look-shoot	Shoot burst-look-shoot burst	Shoot-look-shoot
Probability of Kill ( $P_{KA}$ )	0.85/salvo	0.95	0.90	0.95
Amount of Total Ammunition	400 rounds	36 PAMs	300 bursts	16 AGM-114 Hellfire missiles
Reload Capability	no reload	multiple	2 reloads each of 50 bursts (delay required)	unavailable due to ship firing continuously during scenarios
Send to Other Weapon System	GWS to CIWS	PAM to GWS		
A delay is added in for loading gun rounds so the maximum firing rate for the gun is lower than the usual 15-20 rounds per minute				

Table 7. Assumptions for Weapon Systems Used in the OATCTEPM

## **F. RADAR MODEL DESIGN**

The intent of the radar model is to simulate a modern surface search sensor. It provides the OATCEPM with associated ranges given the probability of detection ( $P_D$ ) and radar cross section (RCS) of the target. Furthermore, it plays a key role in the Search and Detect portion of the OATCTEPM by providing these ranges as inputs to the model as needed. The calculations and resulting detection tables can be found in Appendix III of this paper.

## **G. OATCTEPM SIMULATION MODEL DESIGN**

The design of the OATCTEPM in the Arena software package was developed through the use of the functional flow block diagrams that were formulated from a combination of an initial analysis of the OAWSDM, the OODA loop, and research into time critical target requirements. A thorough analysis of the model was completed to ensure the OAWSDM is represented well throughout the OATCTEPM. Each block contained within the model was analyzed and categorized into one of the eight functional blocks of the OAWSDM used in this simulation (the Learn function is not included). The detailed design of the OATCTEPM is presented in Appendix II.

The main functions of the model are shown in figure 16 to help summarize the flow of the model:

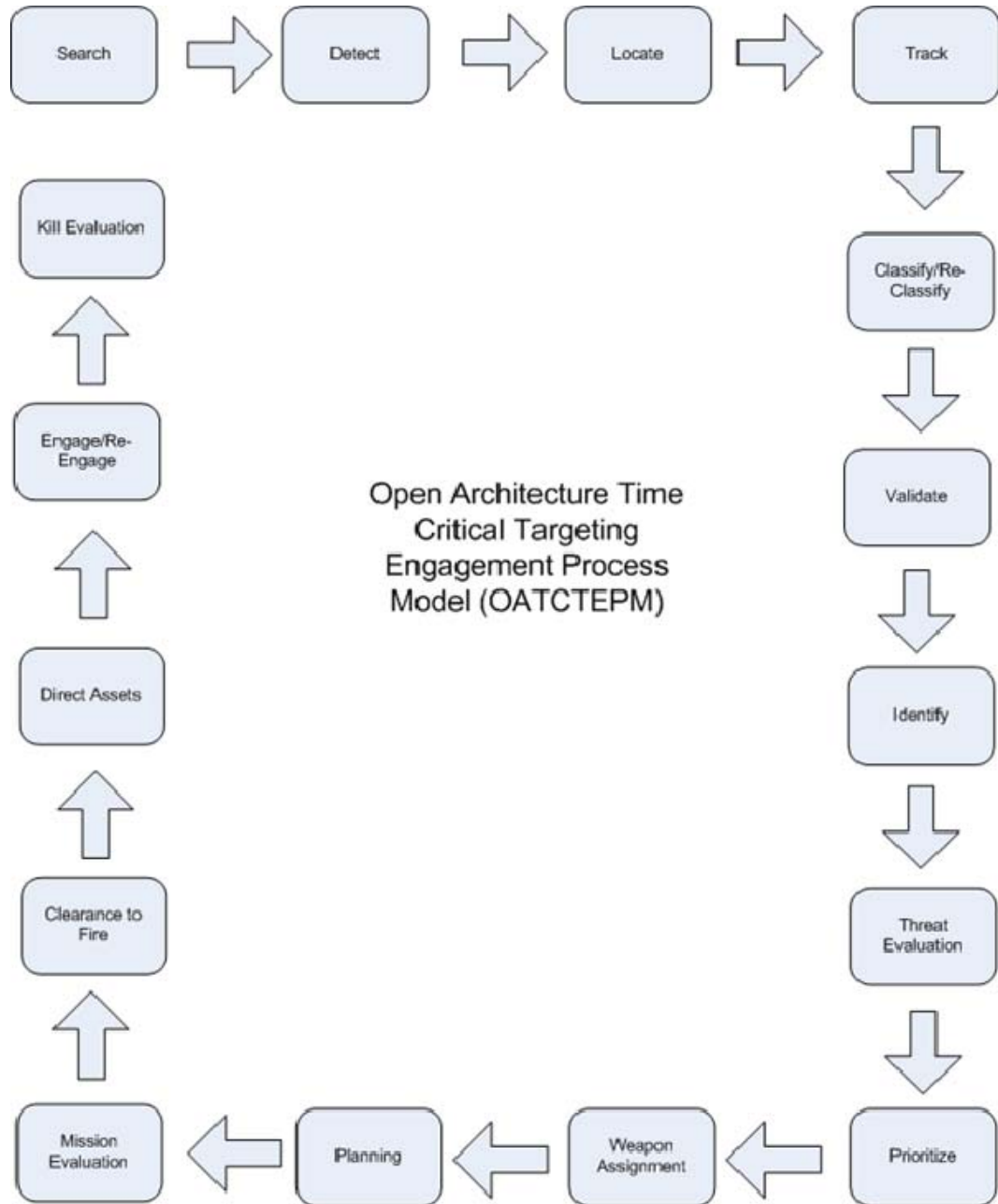


Figure 16. Process Flow for the Main Functional Modules of the OATCTEPM

*The OATCTEPM was developed to evaluate the OAWSDM. The figure shows a top level view of the functional flow of the model.*

## **H. LIMITATIONS**

In order to maintain the normal posture of a cruiser in the threat area, the OATCTEPM was not originally developed specific to an individual scenario. For example, not all targets were meant to be hostile. Furthermore, only a representative number of targets within the threat area were allocated to attack at varying times. In order to properly test the model, groups of targets were created to arrive at different times. However, this model is not currently designed to engage all created scenarios in a single instance and as such, small changes were made to further adapt it for each of the scenarios.

THIS PAGE LEFT INTENTIONALLY BLANK



## **V. RESULTS AND ANALYSIS**

Using the scenarios presented in Appendix I and the OATCTEPM was run. These results include a base case with values chosen to represent a baseline system. This was then changed to an idealized model in which full automation could be achieved, zeroing out all command and control function times. Finally, a number of incremental improvements on the baseline, ranging from five to thirty percent improvement on human decision times were studied. This section presents these results and is organized into five parts. The first part outlines the measures of performance and effectiveness used to evaluate the model results. The second part provides the results for the base model. The third part provides the results from the idealized model which are used to establish the ideal values. The output from the base model will be used to set the baseline from which areas of improvement can be determined. The baseline also provides the thresholds that must be exceeded for a success to be declared. The fourth part provides a comparison of the baseline and idealized models. The final part provides results from the improved model and a comprehensive analysis of each improvement to the model with the interaction of the time based MOEs and the performance based MOEs. The results and analysis are performed using data files generated by each model using Arena's Output Analyzer.

### **A. DISCUSSION OF MOPS AND MOES USED TO ANALYZE RESULTS**

Within each of the model results the data is separated by scenario 1 and 2 and is organized for comparison according to the MOPs and MOEs. The MOPs and MOEs utilized for the comparison of results are:

Time-Based Measures of Performance:

1. Validate Target Time
2. Identify Target Time
3. Threat Evaluation Time
4. Target Priority Time
5. Mission Evaluation Time
6. Weapon Assignment Time

## 7. Plan Approval Time

Measures of Effectiveness:

8. Probability of Leaker
9. Probability of Raid Annihilation
10. Probability of Success

### 1. Discussion of Time-Based MOPs

The purpose of this section is to discuss the seven different MOPs and the different variables that affect these MOPs. This discussion will allow us to target the control times for improvement and will give a better understanding of the factors affecting the performance of the model.

#### *Validate Target Time*

This value represents the time span from firm track to target validation. Within that time period, target classification takes place. Target classification will require human interaction and the use of different sensors to classify the target. Electro-optical and infrared sensors will be used to assist in this task.

The first pass of target validation includes a classification of the target as friendly, unknown, or hostile. If the track is classified as friendly, the track is disregarded for the purpose of the model. An unknown target is sent through the classification process until it is classified as hostile or friendly. The unknown target accumulates delays for each classification of unknown until it is classified as hostile or friendly. If the target is classified as hostile, a final second pass delay is added. The classification of a hostile target is assumed to be correct and is validated and a first pass delay is initiated, then the target is validated.

The most room for improvement is realized in the classification of the target as unknown. If target classification could improve on the first pass, the overall target validation time could easily be improved by not accumulating more delays from the classification of an unknown target. This may be a difficult area to improve due to the unknown or indeterminable intention of a suspect and the risk of committing a type-II error.

### ***Identify Target Time***

Identify target time is the time required from validation of the target to identifying the target. Within this time period, the target is identified as a small target, medium target, or large target. This target identification is based on the target's radar cross section and is easily translated into small, medium, or large. If an electro-optical or infrared sensor is used, human interaction occurs and results in a slightly longer delay for target identification.

Identifying the target based on its radar cross section should not impose a very large delay in the overall process. Room for improvement in target identification most likely does not exist and, if improved, will not improve the overall results by much due to the small amount of time needed to complete this task.

### ***Threat Evaluation Time***

Threat evaluation time is the time consumed between identifying target and threat evaluation of the target. Threat evaluation is the process of evaluating the threat and recognizing the weapon range of the target. The acquisition of the target's weapon range provides us with the target's keep out range. The target's keep out range informs us of the type of threat we are dealing with and allows us to assign priorities later.

Threat evaluation will use current intelligence and databases to assign a weapon range to that particular target according to its attributes. Access to this information is automated and does not involve much human interaction. The time needed to perform these tasks may be improved through improved threat evaluation techniques and may prove to be beneficial to the overall time needed to execute a target.

### ***Assign Target Priority Time***

Assign target priority time is the time required once threat evaluation is final to the completion of assigning the target a priority. Assigning priority to a target is based on the target's current range compared to the target's keep out range as assessed in threat evaluation. A target priority of 1, 2, or 3 is assigned to the target with 1 being the highest priority and 3 being the lowest priority.

Assigning a target priority is an automatic task with the result determined by the current range of the target compared to the target's determined keep out range. The task of assigning a target a priority does not involve much time at all and improvements would only lead to small improvements in overall performance. Small improvements in multiple locations of the model could lead to a significant increase in performance.

### ***Mission Evaluation Time***

Mission evaluation time is the time needed to evaluate the mission as a go or no go and starts directly after the target is assigned a priority and ends after the mission evaluation is complete. Mission evaluation involves some human interaction within and outside the platform along with automatic interaction within and outside the platform. The mission may be evaluated as a no go and outside assistance is requested by the platform. The two scenarios presented to the platform result in a mission go result for mission evaluation 95 percent of the time. If the platform were saturated with more targets than presented in scenario 2, the platform would require outside assistance more than 5 percent of the time to successfully execute the raid of targets.

Mission evaluation could be rather quick depending on the situation. The human interaction required within the platform and outside the platform lead to the belief that there could be room for improvement in the mission evaluation function of the model.

### ***Weapon Assignment Time***

Weapon assignment time is the time required to assign a weapon to a target and starts once mission evaluation is completed and only if the mission is evaluated as a mission go. Weapon assignment time is complete once a weapon is assigned to a target. The assignment of the weapon can change during the engagement portion of the model depending on availability and other factors.

Four weapons are used for engagement in the two scenarios. These four weapons are the Gun Weapons System (GWS), Close-In Weapons System (CIWS), Precision Attack Missile (PAM), and Armed Helicopter. Since the platform is a CG-XX, the overall combat system includes a forward and aft Gun Mount, a forward and aft CIWS Mount, a forward and aft PAM launcher, and two armed helicopters armed with Hellfire missiles.

The assignment of one of the four types of weapons depends on the target type and the target range. The assignment of the weapon is an automatic function that uses logic to assign the weapon. Human action is not required to complete this function; therefore, time to complete this function is not a problem.

### ***Plan Approval Time***

Plan approval time is the time required to review weapon assignments made by the platform and to acquire approval by the leader of the platform. Plan approval time starts after the completion of weapon assignment and continues until the

plan to execute the target is approved. If the plan is not approved for the target, another weapon assignment is made and the plan is reviewed. After the plan is approved, which happens to be 95 percent of the time for these scenarios, clearance to fire must be obtained as a final check to fire the weapon at the target.

Plan approval is the function that takes the most amount of time for the platform to execute. Plan approval requires more human interaction than any of the other functions contained within the model. For these reasons, plan approval should be a focus for improvement if at all possible.

## 2. Discussion of MOEs

The purpose of this section is to discuss the three different MOEs and the different variables that affect these MOEs. This discussion will allow us to understand the factors affecting the performance of the model.

### *Probability of Leaker*

Probability of Leaker is the average number of leakers observed within each trial. The statistic is defined within the model by the following expression:

$$P_L = \frac{\text{Failures}}{\text{Total}} = \frac{\text{Number of Targets} - (\text{GWS Kills} + \text{CIWS Kills} + \text{PAM Kills} + \text{Armed Helo Kills})}{\text{Number of Targets}}$$

### *Probability of Raid Annihilation*

Probability of Raid Annihilation is equal to one minus the Probability of Leaker. The statistic is defined within the model by the following expression:

$$P_{RA} = 1 - P_L = 1 - \frac{\text{Number of Targets} - (\text{GWS Kills} + \text{CIWS Kills} + \text{PAM Kills} + \text{Armed Helo Kills})}{\text{Number of Targets}}$$

### ***Probability of Success***

Probability of Success is the actual number of trials run through the model that resulted in zero leakers being observed. This MOE differs from Probability of Raid Annihilation since it is not based on the average output of each model taken over the entire run. It is based on the actual quantity of leakers observed in each trial conducted. The statistic is defined within the model by the following expression:

$$P_{suc} = \frac{Successes}{Total} = \frac{\text{Number of Trials without a Leaker}}{\text{Total Number of Trials}}$$

### **B. BASELINE MODEL**

The baseline model analyzes the time critical targeting engagement process for both scenario 1 and 2 given the generalized implementation of the OAWSDM discussed previously in this paper. It uses uniform distributions based on average time frames required to complete each C<sup>3</sup> function. Each of these delays allows the model to output baseline results for both the time-based MOPs and MOEs.

<b>Model Results (500 reps)</b>	<b>Baseline Times</b>	
	Scenario 1	Scenario 2
Probability of Leaker	9.8%	13%
Probability of Raid Annihilation	90.2%	87%
Probability of Success	48%	0.4%

Table 8. Baseline Results for MOEs

Table 8 summarizes the average values displayed within the 95 percent confidence intervals for the MOEs illustrated in figures 17 and 18. The probability of success for scenario 1 is 48 percent. A total of two hundred sixty repetitions out of five hundred conducted allow a minimum of one leaker with the maximum observed of eight. The probability of leaker is 9.8 percent and the probability of raid annihilation is 90.2 percent for any given trial in scenario 1. Only two trials out of five hundred trials in

scenario 2 did not allow a leaker so the probability of success for scenario 2 is 0.4 percent. The maximum number of leakers observed was twenty-one. The probability of a leaker is 13 percent and the probability of raid annihilation is 87 percent for any given trial in scenario 2.

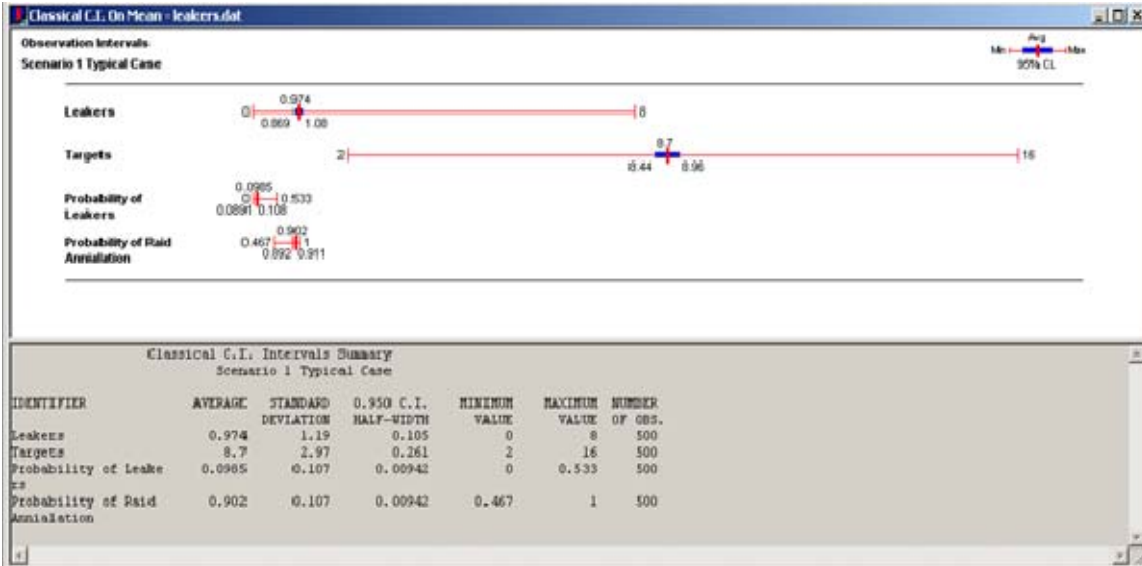


Figure 17. C.I. for Baseline Results of MOEs in Scenarios 1.

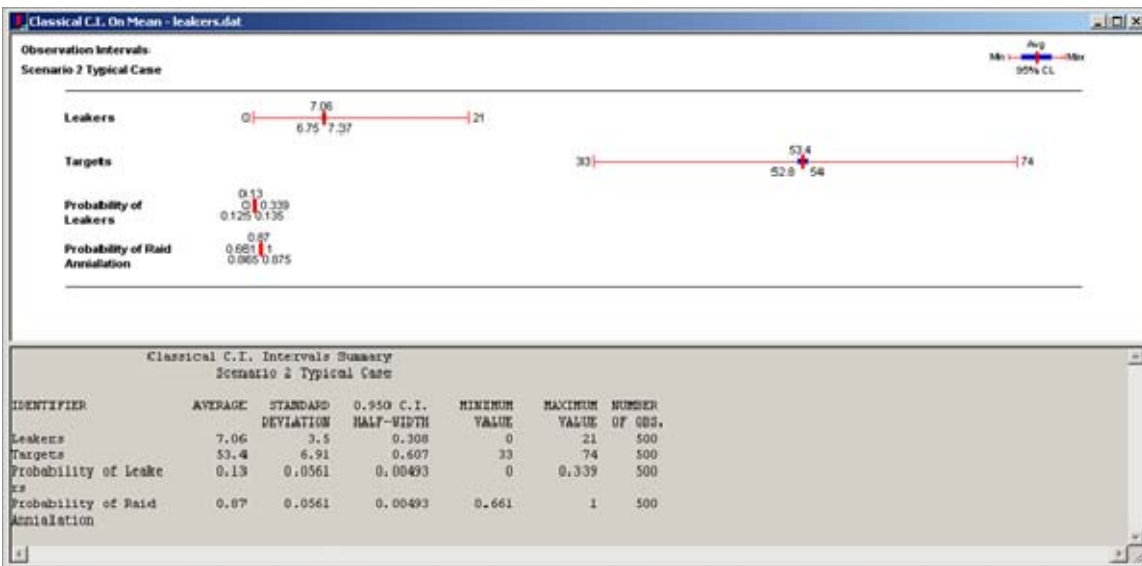


Figure 18. C.I. for Baseline Results of MOEs in Scenarios 2.



The Pareto charts showing the relative ranking of the time-based MOPs are displayed in figures 19 and 20. The efforts to improve the model are focused on reducing the overall time consumed by the previously identified C<sup>3</sup> functions. Below, these functions are organized by their respective contribution to the C<sup>3</sup> delay:

1. Plan Approval
2. Mission Evaluation
3. Threat Evaluation
4. Validate Target
5. Target Priority
6. Identify Target
7. Weapon Assignment

Plan Approval requires a minimum of three times more time to complete than any other of the C<sup>3</sup> functions due to the extensive human interaction that occurs in this function. In fact, all of the functions that take a longer amount of time to perform are the functions that include human action to complete. These functions will be focused on in the improved model and decisions will be made in regards to which functions to improve. The results provide a starting point for both the idealized model and the improved model to compare to.

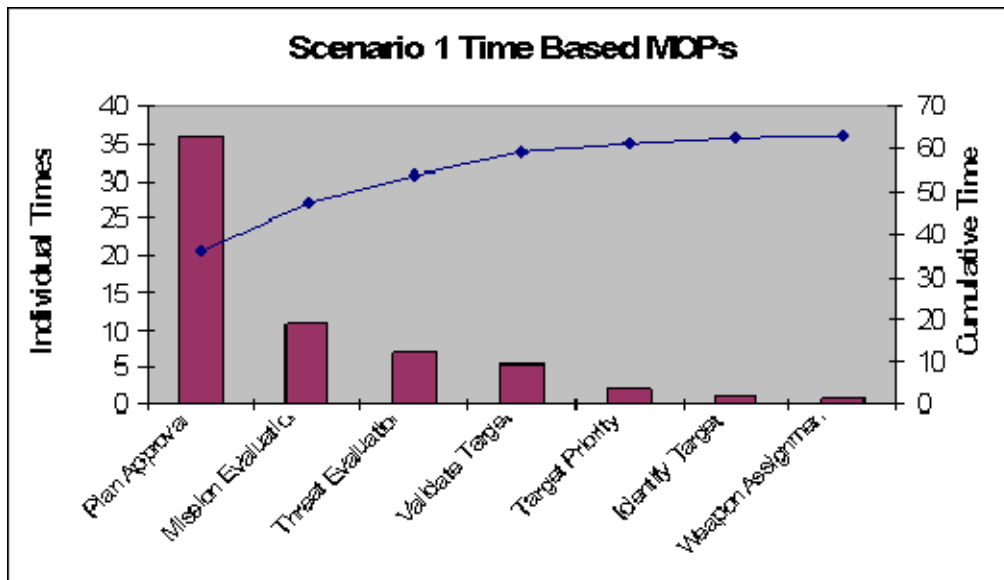


Figure 19. Baseline Results of Time-Based MOPs in Scenario 1

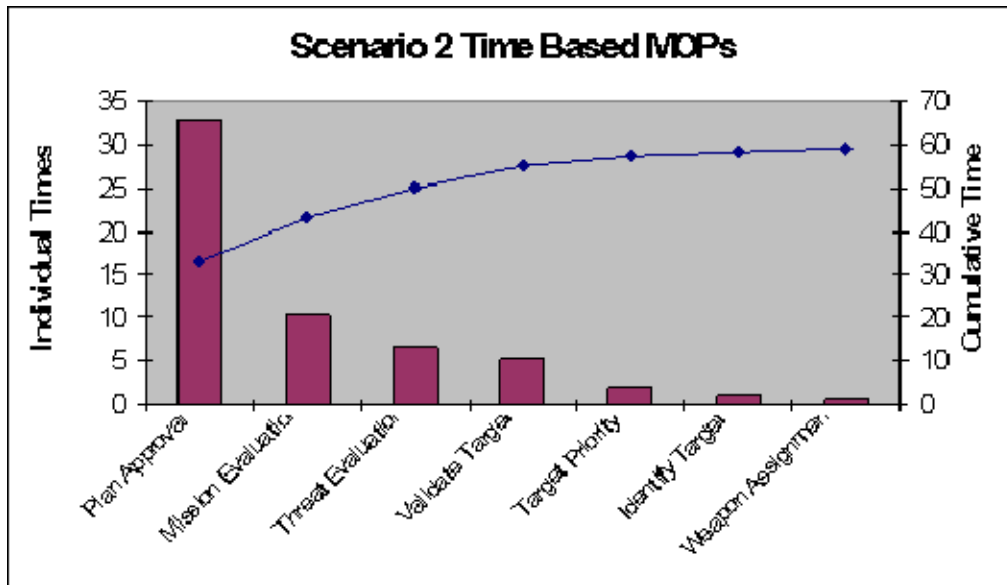


Figure 20. Baseline Results of Time-Based MOPs in Scenario 2

### C. IDEALIZED MODEL

The idealized model is a variation on the base model with all of the Command, Control and Communication ( $C^3$ ) times set to zero. By setting all of the time-based MOPs to zero, idealized results are obtained. These idealized results provide performance results of the OAWSDM if the  $C^3$  actions took no time to perform. Generating a set of idealized results identified a delta between it and the base model.

Model Results (500 reps)	Idealized Times	
	Scenario 1	Scenario 2
Probability of Leaker	4.7%	4.9%
Probability of Raid Annihilation	95.3%	95.1%
Probability of Success	64.2%	8.2%

Table 9. Idealized Results for MOEs

Table 9, above, summarizes the average values displayed within the 95 percent confidence intervals for the MOEs illustrated in figures 21 and 22. The probability of success for scenario 1 is 64.2 percent. A total of three hundred twenty-one repetitions out of five hundred conducted allow a minimum of one leaker with the maximum of five being observed. The probability of leaker is 4.7 percent and the probability of raid annihilation is 95.3 percent for any given trial in scenario 1. Only forty-one of the five hundred trials in scenario 2 did not allow a leaker so the probability of success for scenario 2 is 8.2 percent. The maximum number of leakers observed was thirteen. The probability of leaker is 4.9 percent and the probability of raid annihilation is 95.1 percent for any given trial in scenario 2. The performance results for the idealized model establish the ideal standard for scenarios 1 and 2 without implementing changes to sensor or combat capability. The results for the idealized model are significantly more than the performance and set an upper limit for possible improvements.

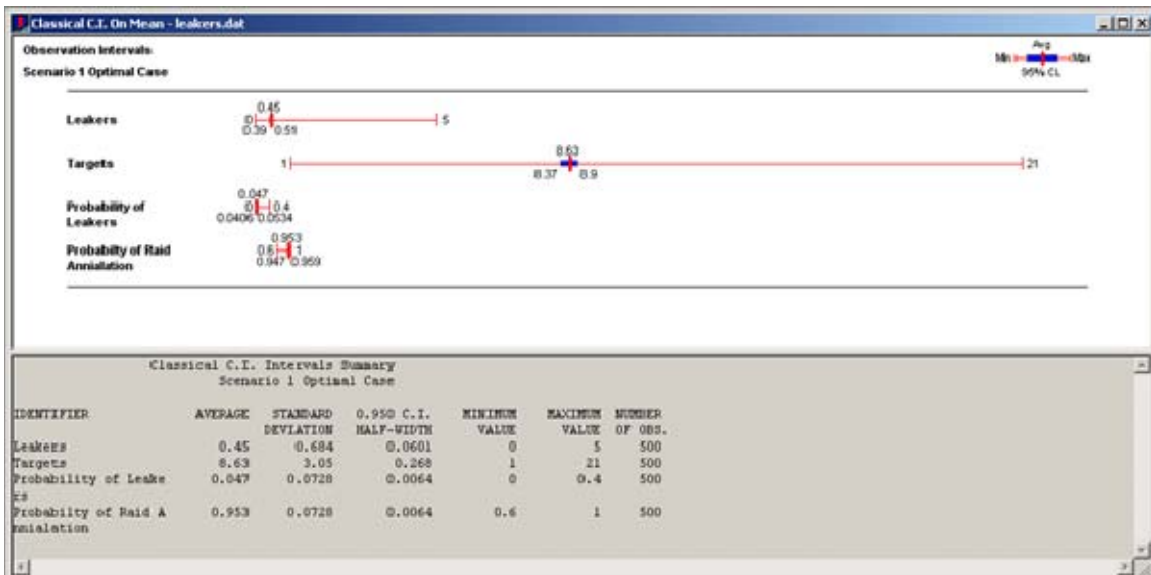


Figure 21. C.I. for Idealized Results of MOEs in Scenario 1.

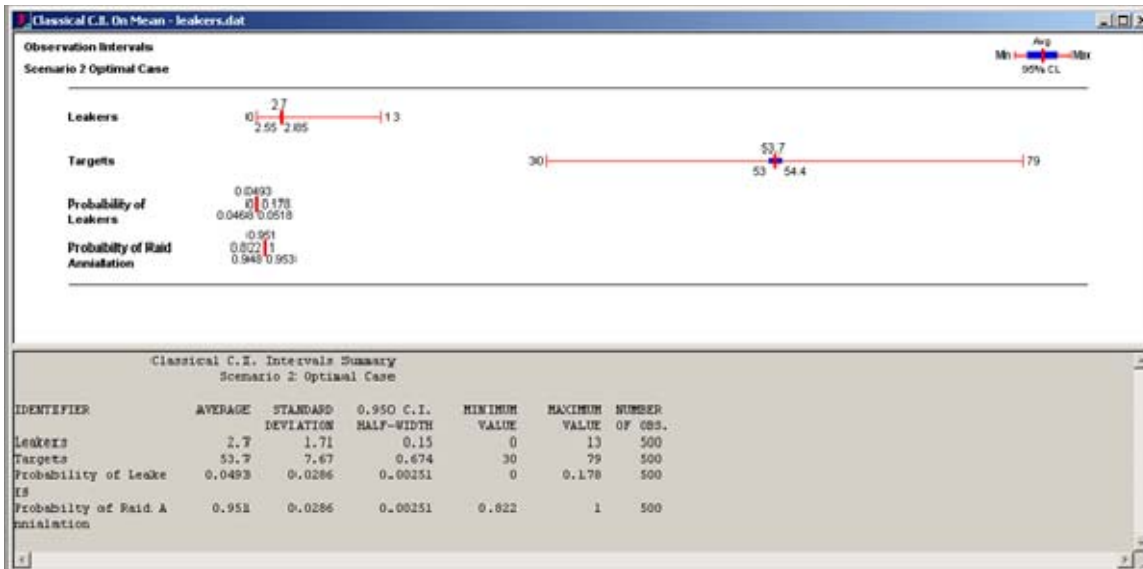


Figure 22. C.I. for Idealized Results of MOEs in Scenario 2.

#### D. COMPARISON OF BASELINE AND IDEALIZED MODELS

When comparing the MOEs and time-based MOPs for the idealized model and the base model, as shown in table 10, the baseline results indicate that room for improvement exists.

Model Results (100 reps)	Scenario 1		Scenario 2	
	Idealized	Baseline	Idealized	Baseline
Probability of Leaker	4.7%	9.8%	4.9%	13%
Probability of Raid Annihilation	95.3%	90.2%	95.1%	87%
Probability of Success	64.2%	48%	8.2%	0.4%

Table 10. Comparison of Idealized and Baseline Results for Scenario 1 and 2

Table 11 summarizes the MOPs for the idealized and base models. Any MOP value resulting in an improvement from the baseline value, as shown in table 12, will be considered a success in the improved model.

MOEs for Improved Model	Scenario 1		Scenario 2	
	Idealized	Baseline	Idealized	Baseline
Probability of Leaker	4.7%	9.8%	4.9%	13%
Probability of Raid Annihilation	95.3%	90.2%	95.1%	87%
Probability of Success	64.2%	48%	8.2%	0.4%
Validate Target Time	0 s	5.31 s	0 s	5.38 s
Identify Target Time	0 s	1.07 s	0 s	1.13 s
Threat Evaluation Time	0 s	6.87 s	0 s	6.56 s
Target Priority Time	0 s	2.08 s	0 s	2.01 s
Mission Evaluation Time	0 s	10.9 s	0 s	10.3 s
Weapon Assignment Time	0 s	0.79 s	0 s	0.79 s
Plan Approval Time	0 s	36.1 s	0 s	32.8 s

Table 11. MOEs for the Idealized and Base Models

MOEs for Improved Model	Scenario 1	Scenario 2
	Success	Success
Probability of Leaker	< 9.8%	< 13%
Probability of Raid Annihilation	> 90.2%	> 87%
Probability of Success	> 48%	> 0.4%
Validate Target Time	< 5.31 s	< 5.38 s
Identify Target Time	< 1.07 s	< 1.13 s
Threat Evaluation Time	< 6.87 s	< 6.56 s
Target Priority Time	< 2.08 s	< 2.01 s
Mission Evaluation Time	< 10.9 s	< 10.3 s
Weapon Assignment Time	< 0.79 s	< 0.79 s
Plan Approval Time	< 36.1 s	< 32.8 s

Table 12. Range of Values Considered Improvements in MOEs

## E. ANALYSIS OF IMPROVED MODEL

The focus of improvement for the OAWSDM is to decrease the time required to complete command, control, and communications functions with human involvement. Planning is the function in the OAWSDM that takes the most amount of time to complete due to the human decision making that must take place to approve the plan to execute targets. Evaluating the mission and validating a target are the other functions that involve a large amount of human interaction.

The areas of decision aide tools and automation were investigated to determine what percentage of improvement could be realistically gained in the C<sup>3</sup> functions that are heavily dependant on human interaction. Appendix 4 contains the results of the testing of the various improved models. The improved model was re-run six separate times with Plan Approval, Mission Evaluation and Threat Evaluation times being reduced 5 percent each pass up to a total of 30 percent reduction. The detailed results of each pass can be found in Appendix 4. Synopses of the results are displayed below.

The time based MOPs, for scenario 1, are displayed in figure 23. A steady reduction trend in C<sup>3</sup> time can be observed from the base case (63.84 seconds) to the 30 percent improvement case (46.86 seconds). The MOEs, in figure 24, show a steady improvement trend in Probability of Raid Annihilation from the base case (89.5%) to the 30 percent improvement case (94.3%).

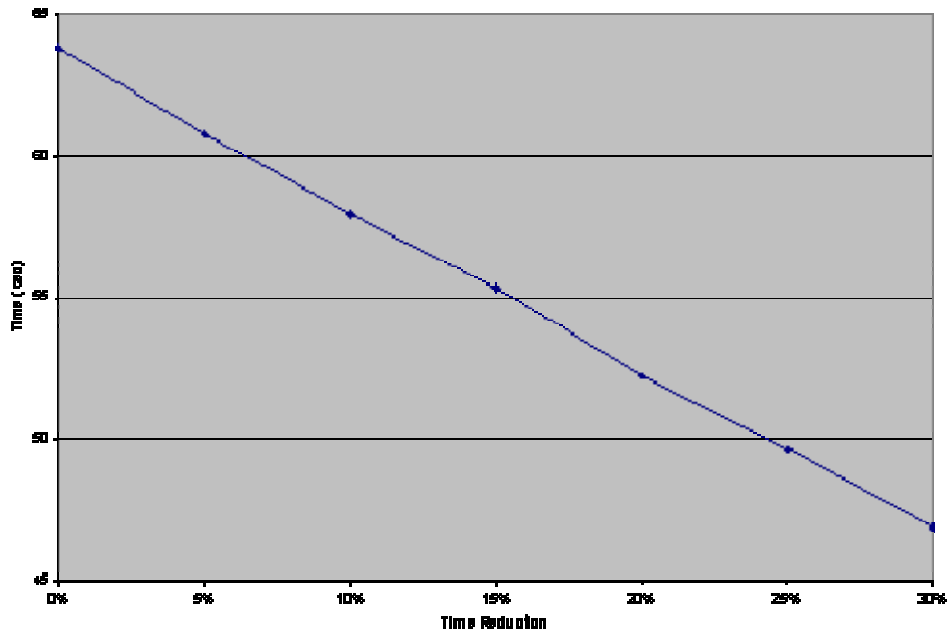


Figure 23. Scenario 1 C<sup>3</sup> Time Based MOP Improvement

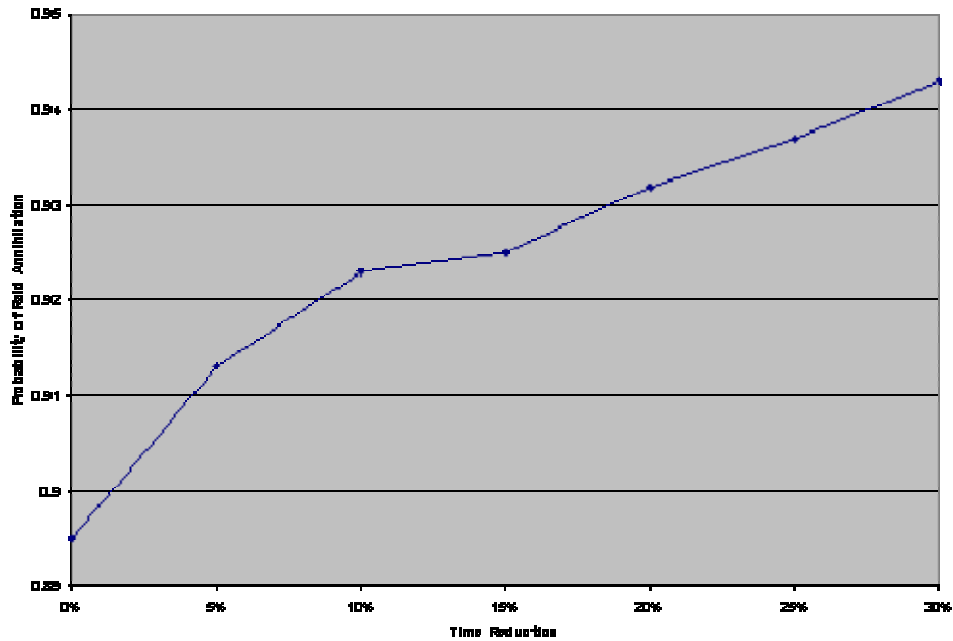


Figure 24. Scenario 1 MOE Improvement

The time based MOPs, for scenario 2, are displayed in figure 25. A steady reduction trend in  $C^3$  time can be observed from the base case (59.25 seconds) to the 30 percent improvement case (44.32 seconds). The MOEs, in figure 26, show a steady improvement trend in Probability of Raid Annihilation from the base case (86.7%) to the 30 percent improvement case (93.4%).

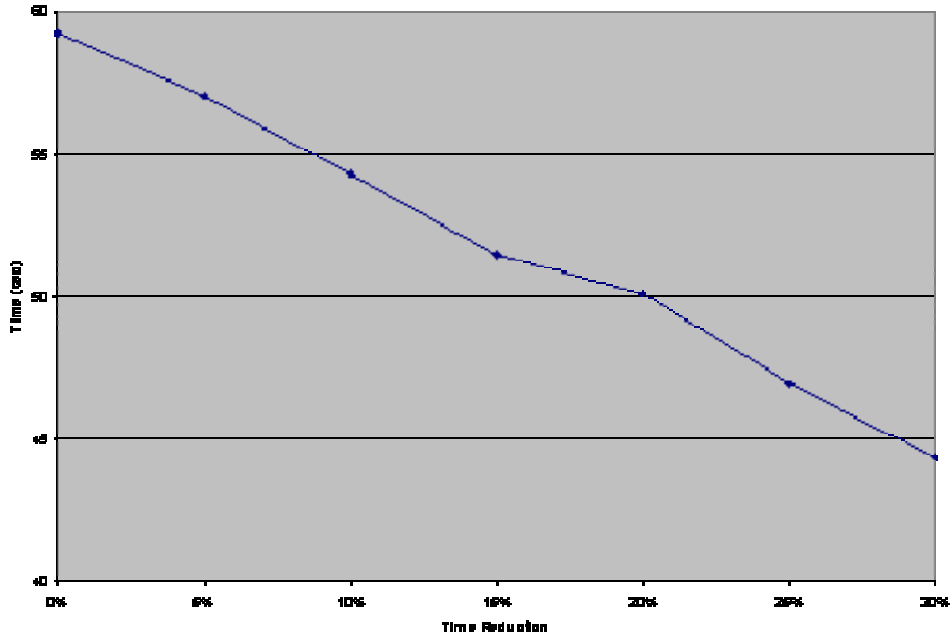


Figure 25. Scenario 2 C<sup>3</sup> Time Based MOP Improvement

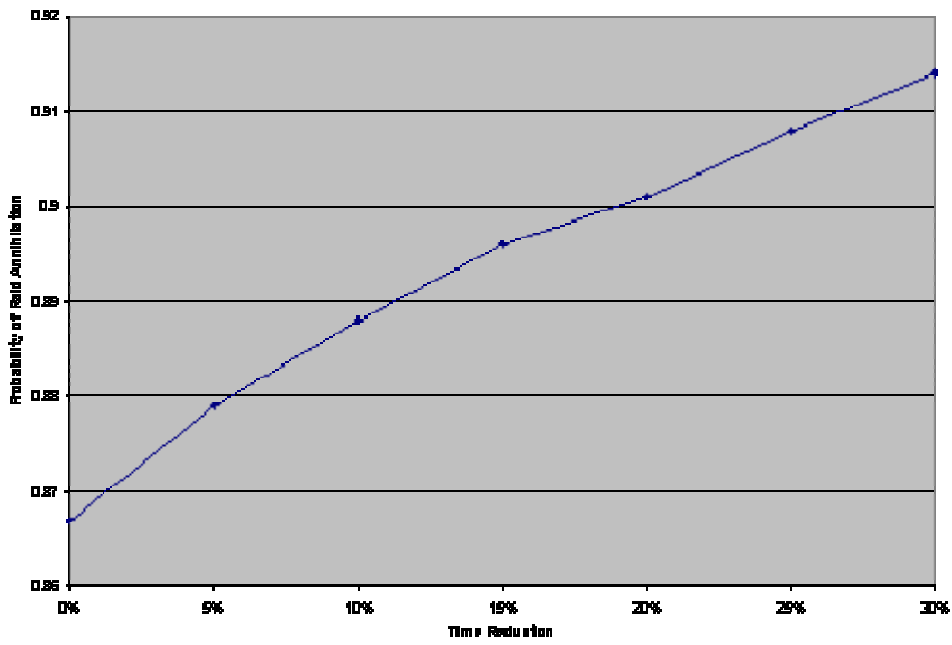


Figure 26. Scenario 2 MOE Improvement



**F. RESULTS OF IMPROVED MODEL**

Based on the analysis performed, the final version of the improved model was configured with a 30 percent reduction in the key human interaction portions of C<sup>3</sup> time. This section details the results of the improved model when compared with the base and idealized model.

From table 13, the probability of success for scenario 1 using improved command and control times is 62 percent. One hundred ninety repetitions out of five hundred conducted allow a minimum of one leaker with the maximum observed of six. The probability of leaker is 5.7 percent and the probability of raid annihilation is 94.3 percent for any given trial in scenario 1. Only eight trials out of five hundred trials in scenario 2 did not allow a leaker so the probability of success for scenario 2 is 1.6 percent. The maximum number of leakers observed was eighteen. The probability of leaker is 8.6 percent and the probability of raid annihilation is 91.4 percent for any given trial in scenario 2. The performance results for the improved model are less than the idealized performance but illustrate improvement in comparison to the baseline model.

Improved Model Results (500 reps)	Improved Times	
	Scenario 1	Scenario 2
Probability of Leaker	5.7%	8.6%
Probability of Raid Annihilation	94.3%	91.4%
Probability of Success	62%	1.6%

Table 13. Summary of Improved Results for Scenario 1 and Scenario 2

The focus of improvement is to decrease the operator dependent times within the C<sup>3</sup> portion of the model. A comparison of the results from the idealized, baseline and improved models for the primary and secondary MOEs is listed in table 14. Applying the criteria for successful improvement from table 12, which simply specifies that each MOE for the Baseline system represent the threshold upon which the Improved system is

compared for each scenario, 1's Identify Target Time, Threat Evaluation Time, Target Priority Time and Weapon Assignment Time did not meet or exceed the required thresholds. In scenario 2, Threat Evaluation Time and Target Priority Time did not meet or exceed the required thresholds for success.

MOEs for Improved Model	Scenario 1			Scenario 2		
	Idealized	Baseline	Improved	Idealized	Baseline	Improved
Probability of Leaker	4.7%	9.8%	5.7%	4.9%	13%	8.6%
Probability of Raid Annihilation	95.3%	90.2%	94.3%	95.1%	87%	91.4%
Probability of Success	64.2%	48%	62%	8.2%	0.4%	1.6%
Validate Target Time	0 s	5.31 s	3.72 s	0 s	5.38 s	3.65 s
Identify Target Time	0 s	1.07 s	1.09 s	0 s	1.13 s	1.08 s
Threat Evaluation Time	0 s	6.87 s	7.00 s	0 s	6.56 s	6.81 s
Target Priority Time	0 s	2.08 s	2.09 s	0 s	2.01 s	2.02 s
Mission Evaluation Time	0 s	10.9 s	7.55 s	0 s	10.3 s	7.2 s
Weapon Assignment Time	0 s	0.79 s	0.80 s	0 s	0.79 s	0.78 s
Plan Approval Time	0 s	36.1 s	24.7 s	0 s	32.8 s	22.5 s

Table 14. Comparison of Improved Results to Idealized and Baseline Results

Table 15 illustrates the effect on performance resulting from the uniform reduction of  $C^3$  times by 20% within the improved model. The average decrease in  $C^3$  times, after 500 trials, for scenario 1 was 17.2 percent. The decrease in operator action delays resulted in a 41.9 percent reduction in Probability of Leakers which improves Probability of Raid Annihilation by 4.55 percent and Probability of Success by 29.17 percent. A decrease of 14.9 percent was observed in  $C^3$  times for scenario 2. The decrease in operator action delays resulted in a 33.9 percent reduction in Probability of Leakers which improves Probability of Raid Annihilation by 5.1 percent and Probability of Success by 300 percent.

MOEs for Improved Model	Scenario 1			Scenario 2		
	Baseline	Improved	$\Delta$ Perf.	Baseline	Improved	$\Delta$ Perf.
Probability of Leaker	9.8%	5.7%	58.16%	13%	8.6%	66.15%
Probability of Raid Annihilation	90.2%	94.3%	4.55%	87%	91.4%	5.06%
Probability of Success	48%	62%	29.17%	0.4%	1.6%	300.00%
Validate Target Time	5.31 s	3.72 s	70.06%	5.38 s	3.65 s	67.84%
Identify Target Time	1.07 s	1.09 s	-1.87%	1.13 s	1.08 s	95.58%
Threat Evaluation Time	6.87 s	7.00 s	-1.89%	6.56 s	6.81 s	-3.81%
Target Priority Time	2.08 s	2.09 s	-0.48%	2.01 s	2.02 s	-0.50%
Mission Evaluation Time	10.9 s	7.55 s	69.27%	10.3 s	7.2 s	69.90%
Weapon Assignment Time	0.79 s	0.80 s	-1.27%	0.79 s	0.78 s	98.73%
Plan Approval Time	36.1 s	24.7 s	68.42%	32.8 s	22.5 s	68.60%
Total C <sup>3</sup> Time	63.12 s	52.28 s	82.83%	58.97 s	50.17 s	85.08%

Table 15. Performance Changes from Baseline Model to Improved Model

The performance increases for both scenarios are effectively the same. The large increase in Probability of Success for scenario 2 is the result of the limited number of trials that observed zero leakers. The baseline and improved models produced a total of two and eight trials respectively where zero leakers were observed. In comparison, scenario 1 produced 240 and 310 trials respectively where zero leakers were observed.

Table 16 illustrates the relationship between the number of leakers, the number of engaged targets in the system and C<sup>3</sup> times. The number of leakers within each scenario is the basis for calculating Probability of Leakers, Probability of Raid Annihilation and Probability of Success.

Scenario	Model	Leakers	Engaged Targets	C <sup>3</sup> Time
1	Baseline	0	7.247	62.840
		1	8.503	63.103
		2	10.627	63.261
		3	11.839	64.523
	Improved	0	7.686	46.358
		1	9.639	47.805
		2	10.828	45.197
		3	13.450	49.690
2	Baseline	0	44.000	58.850
		1	43.750	67.300
		2	49.000	57.600
		3	49.405	58.771
	Improved	0	47.625	45.838
		1	48.771	43.763
		2	49.156	44.222
		3	50.543	44.612

Table 16. Number of Leakers to Engaged Targets and C<sup>3</sup> Times

For both scenarios the Probability of Raid Annihilation is decreased as the C<sup>3</sup> times are increased. The more time a target remains within the C<sup>3</sup> portion of the model the fewer number of targets that can successfully be engaged without a leaker. Each target that enters the model has a finite time, based on individual kinematics, within which it can be engaged and destroyed or neutralized. Increases in the amount of time a target is required to pass through the C<sup>3</sup> portion of the model reduces the time available to enter the engagement queue and be processed by the specific weapon. The smaller the engagement time the less likely the model will be able to re-engage a target that was not destroyed or neutralized. The baseline and improved models, for scenario 1, can only support a maximum of seven targets before the likelihood of a leaker will appear. For scenario 2, the baseline model can support a maximum of 44 targets and the improved model can support up to 47 targets before a leaker would likely appear.

## VI. CONCLUSION

### A. STUDY CONCLUSIONS

After examining the OAWSDM in its current state to determine its capability to combat the surface TCT threat, with emphasis on the C<sup>3</sup> portion of the open architecture, this study concludes the following.

- Processes that required human interaction showed the longest delays and impacted the effectiveness of the OAWSDM against time critical targets.
- Two key areas represented the longest delays:
  - Plan Approval Time, which averaged over 30 seconds in the baseline model, was the time required to review weapons assignments and acquire command approval to engage the TCT.
  - Mission Evaluation Time, which averaged over 10 seconds in the baseline model, was the time needed to evaluate the mission as a go or no go.
- Both delay times involved human-in-the-loop decision making.

While the OAWSDM may not present any technical open architecture or network flaws in its design, it fails to factor in the role of humans into the decision making process. In doing so, it overlooks a key factor in the effectiveness of the architecture against surface TCT engagements. When processes requiring decision making were incrementally improved, the P<sub>RA</sub> correspondingly increased. Therefore, future efforts to improve the effectiveness of combat system implementations based on the OAWSDM should focus on processes that decrease the amount of time required for human decision making.

### B. FUTURE WORK

As the threat of surface TCT grows, the overall C<sup>3</sup> function must adopt abilities to support larger and faster number of engagements. As previously concluded, the common thread between these long delay times is some level of human involvement in the decision making process. In order to achieve the reduced times described in this study's

improved model, investing in technology such as automated decision aids and improving human systems integration are needed.

The overarching process behind these changes has direct ties to the overall decision making capabilities of the involved parties. A recent study, Tactical Decision Making Under Stress, indicated a potential for improvement by implementing a Decision Support System (DSS). The DSS allowed Navy tactical decision making to be enhanced by integrating and organizing current pertinent situational information into a useable display. The study concluded, “Displays that are consistent with these naturalistic decision-making strategies provide the most useful support to commanders, facilitating the rapid development of an accurate assessment of the situation” (Hutchins, Kelly, Moore, Morrison 1997). Accordingly, a unique system that maintains a mode of situational awareness and has the ability to assist with specific decisions would help improve human-in-the-loop decision making.

Therefore, incorporating automated decision aids into the command and control process is suggested for further research. The motivation behind this path is clearly defined by the fact that when engaging TCTs individuals are being inundated with mass amounts of information, which directly results in slower processing capabilities. In order to combat this inevitable problem, an autonomous system or automated decision support tool would allow the user a freedom to carefully make a decision and maintain a clear understanding of the current state.

## **APPENDICES**

THIS PAGE INTENTIONALLY LEFT BLANK



## **APPENDIX I: SCENARIOS FOR TIME CRITICAL TARGETING (TCT) SIMULATION**

The two scenarios being presented are intended to serve as input for the Open Architecture Time Critical Targeting Engagement Process Model (OATCTEPM), constructed using Arena® software. These scenarios provide representative attacks by potential adversaries and terrorist organizations in the regions where they are staged. The scenarios involve Fast In-shore Attack Craft (FIAC) designed to disable or destroy a US Naval High-Value Unit (HVU).

### **GEO-POLITICAL SITUATION**

Political tensions between the United Nations (UN) and Iran have escalated and have led to a political stand-off over their uranium enrichment activities. The Iranian government has long been suspected of harboring terrorists and financially supporting their activities. Recent intelligence reports have indicated Iran intends to supply terrorist organizations with weapons-grade materials and support for manufacturing of Weapons of Mass Destruction (WMD). The Naval assets mentioned in these scenarios are not real and represent future capabilities.

In response to the UN accusations, the Iranian Leadership has ordered the arrest of all remaining UN inspectors after setting an unrealistic deadline for their departure from the country. The UN Security Council issued an ultimatum to release the inspectors or face potential aggressive action by UN forces. In response to the UN ultimatum, the US and Allied forces have committed resources to the Persian Gulf and Arabian Sea as a show of force. In support of these efforts, the USS INVINCIBLE (CG(X)), currently located in the Mediterranean Sea, has been ordered to relieve other forces in the area. To reach the Joint Task Force (JTF), the USS INVINCIBLE will transit the Suez Canal, steam through the Red Sea, then transit the Mandeb Strait (also known as Bab el Mandeb) into the Gulf of Aden (see figure 27).



Figure 27. Map of Mandeb Strait and Gulf of Aden

*The Mandeb Strait connects the Red Sea to the Gulf of Aden. The area of the attack in the first scenario is indicated by the red explosion. (Wikipedia Contributors, Yemen)*

A second ship, the USS DEFENDER (CG-X) is on a Northerly heading from the Indian Ocean toward the Gulf of Oman, where it will transit the Strait of Hormuz, and enter the Persian Gulf (see figure 28, below).

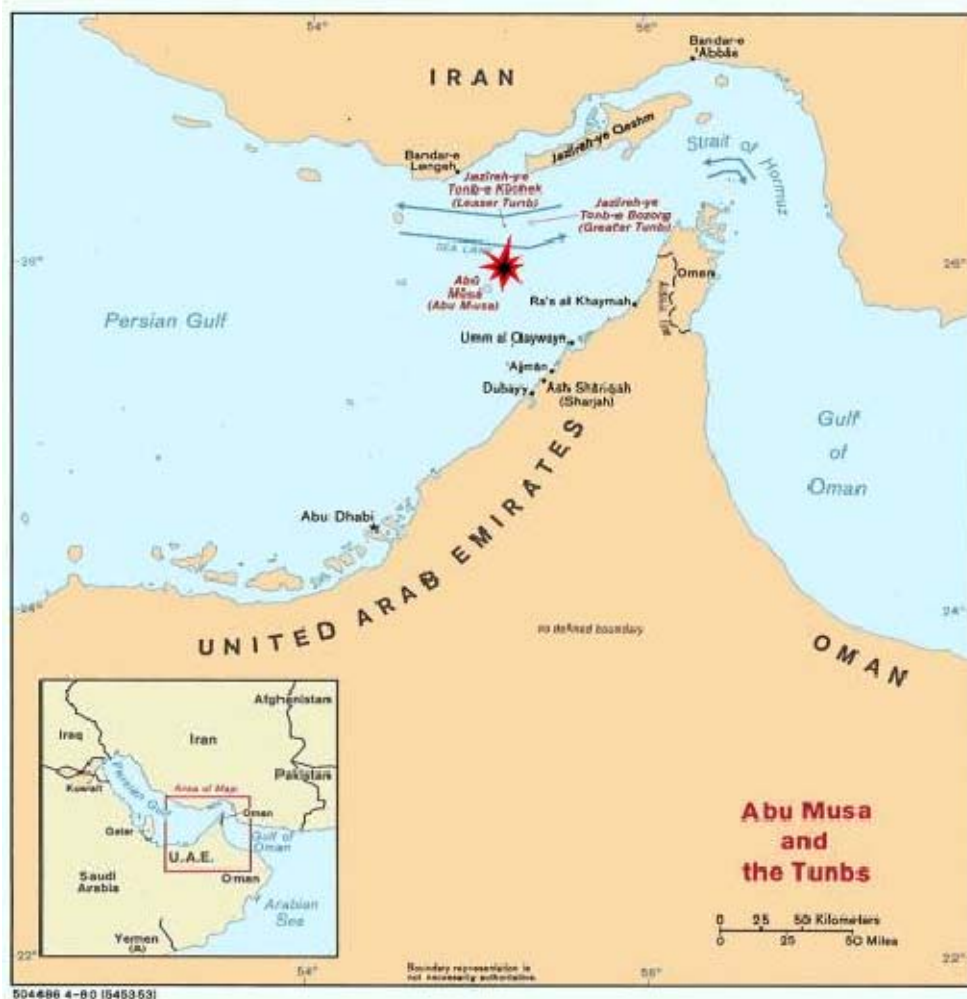



Figure 28. Map of the Gulf of Oman and the Persian Gulf

*The Strait of Hormuz connects the Arabian Sea to the Persian Gulf. The area of the attack in the second scenario is indicated by the red explosion. (Strait of Hormuz map from: Global Security Organization.hormuz\_80.gif 2005)*

Intelligence reports have been provided to the fleet operating in this region. Specific threats have been identified and are summarized in table 17:

FIAC Threat Type	Description
<p data-bbox="256 373 363 411" style="text-align: center;"><b>Type I</b></p> <p data-bbox="99 489 521 1125">Two-man personal watercraft with Rocket Propelled Grenade (RPG) weapons and/or a large blast bomb used in a suicide attack. Credited with a firing range of 500 meters, at which point the enemy is assessed as a “leaker”, who has achieved their mission objectives by inflicting damage on the target vessel. (Galligan, Galdorisi and Marland 2005)</p>	<p data-bbox="792 373 1247 411" style="text-align: center;"><b>Typical Personal Watercraft</b></p> <div data-bbox="712 489 1325 890" style="text-align: center;">  </div> <p data-bbox="561 968 1479 1108" style="text-align: center;">This Air Force photo from the Defense Visual Information Center (Hannan 2002) depicts Coast Guard personnel acting as terrorists armed with RPG in exercise Northern Exposure 2002.</p> <p data-bbox="545 1186 1398 1388"> <b>Avg. Speed:</b> 40 knots  <b>Armament:</b> Rocket Propelled Grenade (RPG) Launcher  <b>Effective Range:</b> 500 Meters  <b>Estimated RCS:</b> 3 dBm<sup>2</sup> </p> <p data-bbox="545 1465 1458 1549"><b>Additional Info:</b> This threat can be deployed from other sea-borne vessels, or launched from the beach.</p>

## Type II

Medium sized “Boghammar” class boat with an unguided multiple launch bombardment rocket, or a larger anti-tank guided weapon with a launch range of 9 km, at which point it then becomes a “leaker”. (Galligan, Galdorisi and Marland 2005)

## Iranian Boghammar Craft



This is 1992 and it is an Iranian Boghammar brought back to Coronado after being sunk during Operation Earnest Will. Special Boat Unit-13 had two and they were used as “aggressor boats” against the fleet in exercises. (Boghammar Photo: <http://www.warboats.org/SBU13.htm>)

**Speed:** 40 knots

**Armament:** 107mm Rocket Launcher

**Effective Range:** 9 km

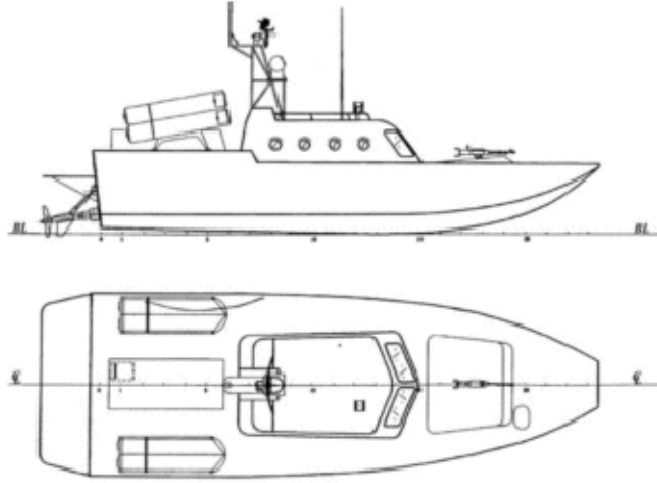
**Estimated RCS:** 6 dBm<sup>2</sup>

**Additional Info:** “Iranian manufactured rockets launchers include the Haseb, an Iranian 12 tube 107 mm MRL that is a variant of a Chinese 107 mm rocket...” (Globalsecurity.org 2007)

### Type III

Small Fast Patrol Boat (FPB) typified by C-14 Cat-class Catamaran Missile Boat, with smaller anti-ship missile and degree of sensor and Command and Control (C2) fit. Weapon ranges of out to 15 km for the ASM exist. Once the boat crosses the 15 km point, it will become a “leaker”.

### C-14 Cat-class Catamaran Missile Boat



C-14 Photo: <http://www.globalsecurity.org/military/world/china/pcfg-cat-pics.htm>

- Speed:** 50 knots
- Armament:** C-701 Anti Ship Missile
- Effective Range:** 15 km (~8 miles)
- Estimated RCS:** 10 dBm<sup>2</sup>

**Additional Info:** “The C-701 light-weight anti-ship missile measures 2.5 meters long, less than half that of the Yingji-801. The diameter of the subsonic anti-ship short-range missile is also much smaller. It has a range of **15 kilometers** and a cruising speed of Mach 0.8. It uses television guidance control and its anti-jamming capability is comparable to that of the US Maverick missile. However, the C-701 can be launched from ships and planes, unlike the air-to-surface Maverick. “ (Globalsecurity.org 2007)  
“The C-701 anti-ship missile was first exhibited at China's Second International Aviation and Aerospace Show held in Zhuhai late 1998. Initially only a version launched from a helicopter was revealed. But at the end of 1998, China announced that a version launched from a building was under development. It would be in service in 2002.” (Globalsecurity 2007)

Table 17. Summary of Threats

**Note:** All estimated RCS values were derived from information contained in “Table 10.4 Generalized Maritime RCS values – Radar Technology Encyclopedia” of John Briggs’ book *Target Detection by Marine Radar*.

## **SCENARIO #1 - ATTACK BY A GROUP OF TYPE-1 FAST INSHORE ATTACK CRAFT (FIAC)**

Type-I (2-man personal watercraft) FIAC will be the only attacking craft for this scenario.

### **Tactical Situation (TACSIT)**

The USS INVINCIBLE (CG-X) has transitioned the narrowest portion of the Mandeb Straight and is making 15 knots on a Southerly heading. The USS INVINCIBLE represents the most sophisticated vessel in the US Navy's inventory. Consequently, it is considered a high priority target and would demoralize the Blue forces with a defeat. The Mandeb Straight represents one of the busiest shipping lanes in the world.

### **Assumptions**

- The environmental conditions are ideal to support detection and engagement of the oncoming attack and the sea state is calm.
- Approximately eight 2-man Type-1 (personal watercraft), armed with 1 (each) Rocket-Propelled Grenades (RPGs) and packed with high explosives which can be detonated by the driver, or remotely from a stand-off position by an observer, will attack the High Value Unit (HVU) simultaneously from various directions.
- Keep-out range for the Type-1 targets is 500 meters. Inside 500 meters the targets can inflict mission kill by damaging array faces, etc., with shrapnel (Galligan, Galdorisi and Marland 2005).
- It is the intention of the red force to breach the hull with explosives and inflict a hard kill (sink the ship).

- Intelligence has established a high threat level based on previous FIAC attacks in this area; however, if the FIAC breach the 500 meter keep-out range, a mission kill is assured.
- A total of two helicopters and four flight crews are embarked on USS INVINCIBLE for this scenario.
- Both helicopters are armed with Hellfire missiles. It is also assumed that the helicopters are 100% operational ready and will remain so throughout the given scenario.
- All shipboard systems will be fully operational and will not fail throughout the given scenario.

### **Blue Force Posture**

The Fleet Commander has ordered all Naval vessels underway in this area to maintain the appropriate alert level for independent steaming. Currently, USS INVINCIBLE is steaming independently in a high-traffic area, with two armed airborne helicopters providing support around own ship.

### **Red Force Posture**

The red force consists of a cell of terrorists, who have planned to execute an attack on a U.S. HVU on very short notice. Red Force intelligence has reported the USS INVINCIBLE transitioning the Red Sea, headed south. The red cell has outfitted eight personal watercraft with High Explosives (HE) and two suicide terrorists each. The second terrorist on each personal watercraft is armed with an RPG-7 launcher. Four civilian vessels have been employed to piggy-back the personal watercraft in pairs to strategic locations to execute and ambush-type attack. When the attack commences, all eight targets will be inbound simultaneously at a range of 3 km and an average speed of 40 knots.

The Red Cell has decided to attack the USS INVINCIBLE after she transitions the Mandeb Strait and enters the Gulf of Aden.



## **The Attack**

The red cell has deployed one of the fishing vessels (Piggyback-1) in the Red Sea. This vessel is the cell coordinator and has spotted the USS INVINCIBLE. (Note: A-xx is denoting “Attack, minus xx time.”) Figure 29 below can be referenced for a description of the attack.

**A-12 hours:** Piggyback-1 follows INVINCIBLE at a safe distance South, through the Mandeb Straight. USS INVINCIBLE has two helicopters airborne, enforcing the 1000 meter keep-out range.

**A-6 hours:** Piggyback #1 updates the red forces of USS INVINCIBLE’s location and issues the order for Piggyback 2 through 4 to assume their pre-determined positions. The order also provides the position of USS INVINCIBLE that will trigger the attack.

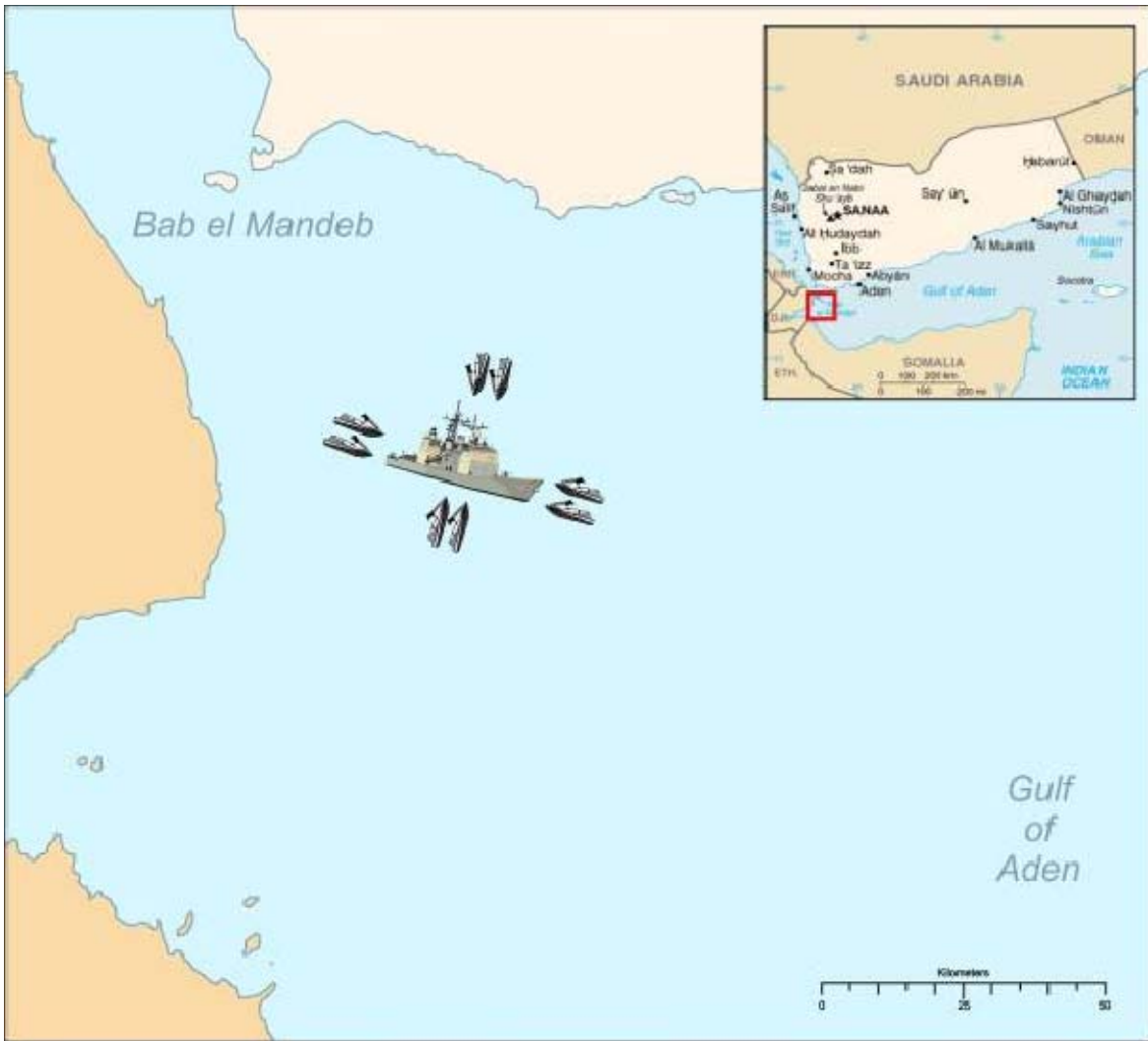


Figure 29. Red Cell Attack Plan

*This figure shows the approximate position of all forces involved in scenario 1. The engagement takes place in the Bab el Mandeb with eight hostile personal watercrafts positioned around the cruiser.*

**A-2 hours:** All red cell forces are in attack positions and holding (with the exception of Piggyback-1 who is following at matched speed of 20 knots, range 3 km).

**A-30 minutes:** Piggyback-1 increases speed closes on USS INVINCIBLE. The Tactical Action Officer (TAO) is alerted to the fishing vessel which is closing in on the ship and will breach the 1,000 meter keep-out zone in approximately 3 minutes 15 seconds.

**A-0 minutes:** USS INVINCIBLE reaches the trip-point and all four Piggyback platforms deploy personal watercraft, which immediately head directly toward own ship, averaging 40 knots. The position, range and other kinematical information of each target is provided in table 18.

Target	Average Pop-Up Range	Relative Bearing to Own Ship	Average Speed
1	3,000 Meters	45.0 Degrees	40 Knots
2	3,000 Meters	45.0 Degrees	40 Knots
3	3,000 Meters	135.0 Degrees	40 Knots
4	3,000 Meters	135.0 Degrees	40 Knots
5	3,000 Meters	225.0 Degrees	40 Knots
6	3,000 Meters	225.0 Degrees	40 Knots
7	3,000 Meters	315.0 Degrees	40 Knots
8	3,000 Meters	315.0 Degrees	40 Knots

Table 18. Scenario 1 Target Information

## **SCENARIO #2 - FIAC SATURATION ATTACK**

### **TACSIT:**

USS DEFENDER is steaming toward the Persian Gulf. Intelligence reports that a terrorist cell, which is believed to be supported by the Iranian government, planned and executed an attack on USS INVINCIBLE earlier the same day. All ships in the area are alerted and additional ISR assets are tasked to support areas of potential attack within and around the Persian Gulf and the Strait of Hormuz (see figure 30).

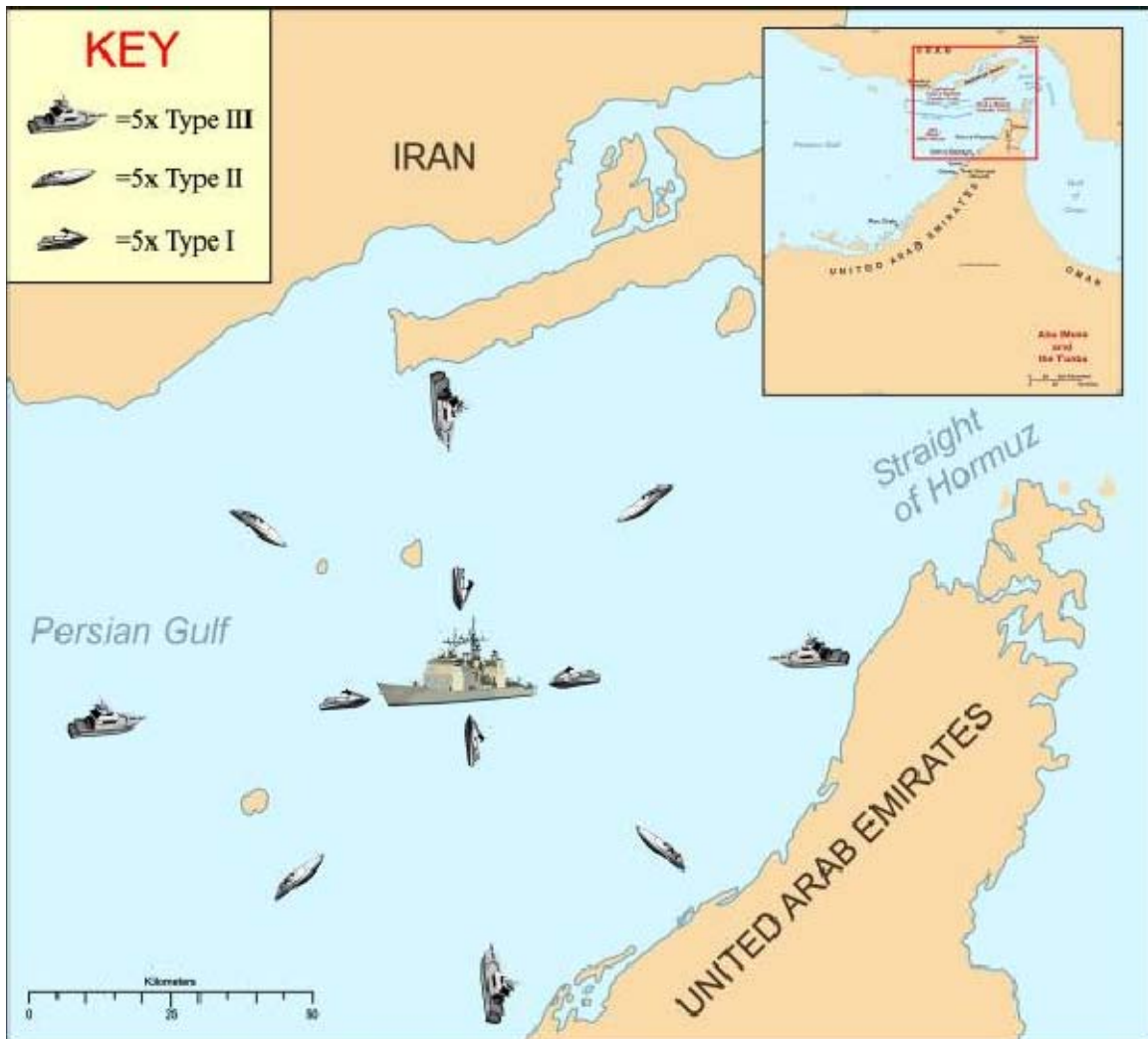


Figure 30. Map of the Strait of Hormuz and Persian Gulf Area

*The relative arrangement of forces for scenario 2 is shown in this figure. The engagement takes place in the Persian Gulf near the Strait of Hormuz. (Strait of Hormuz map from: Global Security Organization.hormuz\_80.gif, 2005)*

The Persian Gulf is a busy body of water that routinely contains shipping and fishing vessels, as well as small recreational craft. While Iran borders the Persian Gulf, there are also several neutral and non-hostile countries that do as well. In light of the earlier attack on the USS INVINCIBLE, coalition forces have issued multiple warnings to local countries and broadcast routine messages warning vessels to avoid approaching Coalition Naval vessels, or they will be fired upon. To prevent firing on non-hostile boats, requests

have been made to all local friendly and neutral countries to warn their population to avoid areas where coalition forces are operating and to not directly approach any Coalition vessels.

**Assumptions:**

- The environmental conditions are ideal to support detection and engagement of the oncoming attack and the sea state is calm.
- Current rules of engagement for the coalition forces are to monitor local traffic 50 km radius and look for any patterns of behavior that may indicate organization or potential attack including but not limited to trailing, running parallel courses, slowly approaching the vessel, loitering.
- Coalition forces are also monitoring radio and local communications chatter including cell phone and satellite phone communication.
- It is the intention of the red force to breach the hull with explosives or an anti-ship missile and inflict a hard kill (sink the ship).
- Intelligence has established a high threat level based on previous FIAC attacks in this area; however, if the FIAC breach their respective keep-out range, a soft kill is assured.
- A total of two helicopters and two flight crews are embarked on USS DEFENDER for this scenario.
- Both helicopters are armed with Hellfire missiles. It is also assumed that the helicopters are 100% operational ready and will remain so throughout the given scenario.
- All shipboard systems will be fully operational and will not fail throughout the given scenario.

The USS DEFENDER is at a high state of alert and is connected to a joint tactical cooperative engagement network, which includes sensor data from other ships as well as patrolling helicopter and UAV assets.

**Red Force Posture:**

After the attack on the USS INVINCIBLE in the Mandeb Strait, enemy forces have decided to mount a second, coordinated attack using about 50 small boats of various types. The incoming boats will consist of approximately 20 Type I, 20 Type II, and 10 Type III FIAC. The red force intends to attack from multiple bearings. The attack will occur around mid day.

**The Attack**

**A-4 Minutes:** Intelligence notes increased chatter among boat traffic surrounding coalition forces. Intelligence also intercepts a short satellite phone message with the words “commence” and “attack” in the message.

**A-3 Minutes:** Red forces begin their approach from multiple bearings.

**A-0 Minutes:** USS DEFENDER goes to general quarters and immediately begins focusing on non-cargo suspect targets. Remaining helicopter is launched, for a total of two helicopters armed with Hellfire missiles, which are patrolling around the ship. Example position, range and other kinematical information of each target is provided in table 19:

<b>Target</b>	<b>Approximate Range</b>	<b>Relative Bearing to Own Ship</b>	<b>Average Speed</b>
1-5 (Type-III)	50 Kilometers	90.0 Degrees	50 Knots
6-10 (Type-III)	50 Kilometers	270.0 Degrees	50 Knots
11-15 (Type-II)	45 Kilometers	45.0 Degrees	40 Knots
16-20 (Type-II)	45 Kilometers	135.0 Degrees	40 Knots
21-25 (Type-II)	45 Kilometers	225.0 Degrees	40 Knots
26-30 (Type-II)	45 Kilometers	315.0 Degrees	40 Knots
31-35 (Type-I)	3000 Meters	0.0 Degrees	40 Knots
36-40 (Type-I)	3000 Meters	90.0 Degrees	40 Knots
41-45 (Type-I)	3000 Meters	180.0 Degrees	40 Knots
46-50 (Type-I)	3000 Meters	270.0 Degrees	40 Knots

Table 19. Scenario 2 Target Information

THIS PAGE INTENTIONALLY LEFT BLANK



## **APPENDIX II: DETAILED DISCUSSION OF OATCTEPM DESIGN**

Detailed model parameters are shown in table 20 through table 25 below the detailed discussion of the model. Please refer to that table for model parameters. The detailed discussion of each model block follows below.

### **1.0 SEARCH/DETECT (S/D)**

The S/D functions of the OATCTEPM are further broken down into Sensor Asset, Sensor Report, Sensor Track Report, INTEL Report, and Measurement Report. The model blocks created in ARENA that represent the S/D block of the OATCTEPM are shown below with a description:

Search: Creates the target and provides a delay for the search of the target.

#### Assumptions

1. This block does not affect MOEs because the time will not be measured until target is detected.
2. Parameters for this block will vary depending on scenario. A variable has been created in ARENA that allows the user to enter the total number of targets that change based on scenario number.
3. For scenario 1, the total number of targets is 65. Out of the 65 targets entered, on average, 8 small targets will be considered hostile.
4. For scenario 2, the total number of targets is 400. On average, 20 small targets will be considered hostile, 20 medium targets will be considered hostile, and 10 large targets will be considered hostile. Out of the 400 targets, 50 will be considered hostile and scheduled for engagement.

Detect: Assigns target range and detection time.

#### Assumptions:

1. For scenario 1, the Detect\_Range assignment will be “3”.
2. For scenario 2, the Detect\_Range assignment will be “discrete (0.4,3,0.8,45,1,50)”.

Locate: Decision block that divides the targets into large RCS, medium RCS, and small RCS based on the detection range of the target.

Large RCS: Assigns target type large RCS, assigns target profile of either incoming or outbound, and assigns a speed to the target.

Assumptions:

1. Speed of large target will be 0.02572 kilometers per second or approximately 50 knots.

Medium RCS: Assigns target type medium RCS, assigns target profile of either incoming or outbound, and assigns a speed to the target.

Assumptions:

1. Speed of medium target will be 0.02058 kilometers per second or approximately 40 knots.

Small RCS: Assigns target type small RCS, assigns target profile of either incoming or outbound, and assigns a speed to the target.

Assumptions:

1. Speed of small target will be 0.02058 kilometers per second or approximately 40 knots.

## **2.0 DATA/INFORMATION SERVICES (DIS)**

The DIS functions of the OATCTEPM are broken down into the following functions: System Track, Supporting Source Track, Classification, Track Kinematics, Attribute Data, Track Repository, NRT Intel Track, and Sensor Scheduler. The model blocks

created in ARENA that represent DIS functions are shown below with a description of the block and its function:

Transition to Track: Decision block that leads to dropped track if target is outbound.

Disregard Track if Outbound: Disregard track if target is outbound.

Assumptions:

1. Assume that all tracks that are outbound will remain outbound and all tracks that are inbound will remain inbound.

Firm Track?: Decision block that leads to firm track if target is within range and delay if target is not within range.

Assumptions:

1. Assume that there will be no delay for firm track for all small targets. All small targets are well within range for tracking purposes and will immediately be transitioned to firm track.

Awaiting Firm Track: Decision block that leads to delay based on target RCS.

Large RCS Delay: Provides delay until firm track has been established for large RCS targets.

Medium RCS Delay: Provides delay until firm track has been established for Medium RCS targets.

Firm Track Time: Assigns firm track time and firm track range.

Classify Target: Decision block that leads to classification of the target as hostile, unknown, or friendly for first pass classification.

Assumptions:

1. Fifteen percent of targets are considered hostile in the operating area.

2. Twenty percent of targets are considered unknown in the operating area.
3. The final sixty-five percent of targets in the operating area are considered friendly.
4. These numbers were estimated from people who have been deployed in the operating area.

Hostile First Pass: Assigns the target as hostile.

Unknown First Pass: Assigns the target as unknown.

Friendly First Pass: Assigns the target as friendly.

Disregard Track First Pass: If target is assigned friendly, track is disregarded.

Reclassify Target: Decision block that reclassifies unknown targets as hostile, unknown, or friendly.

Hostile Second Pass: Assigns the previously unknown target as hostile.

Friendly Second Pass: Assigns the previously unknown target as friendly.

Disregard Track Second Pass: If target is assigned friendly, track is disregarded.

Validate Target: Validates classification of target.

### **3.0 PLANNING, ASSESSMENT, AND DECISION (PAD)**

The PAD functions of the OATCTEPM are broken down into the following functions: Assigned Missions, Tactical Picture, Action Plans, Capability, Plan, Threat Assessment

(including Identity) and C2 Order, Schedule, and Event. The model blocks created in ARENA that represent PAD functions are shown below with a description of the block:

Identify Target: Decision block that identifies each target as small, medium, or large.

Type 1 Target Small: Assigns target type 1 small to target.

Type 2 Target Medium: Assigns target type 2 medium to target.

Type 3 Target Large: Assigns target type 3 large to target.

Threat Evaluation: Decision block that sends target to assign block depending on target type.

Target Type 1 Weapon Range: Assigns target weapon range of 500 meters to all small targets.

Target Type 2 Weapon Range: Assigns target weapon range of 9 kilometers to all medium targets.

Target Type 3 Weapon Range: Assigns target weapon range of 15 kilometers to all large targets.

Assign Target Priority: Assigns a priority to each target depending on keepout range and current range of target.

Assumptions:

1. All targets within 4 kilometers of their keepout range will be assigned a priority of 1.
2. All targets within 8 kilometers but greater than 4 kilometers will be assigned a priority of 2.
3. Any targets at a range greater than 8 kilometers will be assigned a priority of 3.
4. Target priorities range from 1 to 3.

5. Target priorities can change as they make their way through the control and engagement portions of the model.

Assign Priority 1 for Target Type 1: Assigns a priority of 1 to small targets.

Assign Priority 2 for Target Type 1: Assigns a priority of 2 to small targets.

Assign Priority 3 for Target Type 1: Assigns a priority of 3 to small targets.

Assign Priority 1 for Target Type 2: Assigns a priority of 1 to medium targets.

Assign Priority 2 for Target Type 2: Assigns a priority of 2 to medium targets.

Assign Priority 1 for Target Type 3: Assigns a priority of 1 to large targets.

Assign Priority 2 for Target Type 3: Assigns a priority of 2 to large targets.

Mission Evaluation: Decision block that evaluates the mission as “go” or “no go.” If mission is evaluated as “go”, the target continues through the model. If mission is evaluated as “no go”, the mission is sent to another platform for engagement or other options.

Assumptions:

1. Ninety-five percent of all missions are assigned “go” for the scenarios presented.
2. A cruiser should be able to approve at least ninety-five percent of the missions presented to it if the missions meet the scenario (scenario 1 or 2) guidelines presented to this model.

Send to other: Target is sent to another platform for engagement or other options.

Mission Go: Mission is evaluated as “go” and assigned “go” for continuation.

Weapon Assignment: Decision block that assigns a weapon according to target type and target range.

Assumptions:

1. Weapons are assigned according to specific scenario. Certain weapons are chosen for scenario 1 based on parameters presented in scenario 1 and certain weapons are chosen for scenario 2 based on parameters presented in scenario 2.
2. CIWS and GWS are assigned to targets in scenario 1.
3. CIWS, GWS, PAM, and Armed Helo are assigned targets in scenario 2.
4. Small arms have not been assigned in this model. If a ship was being overwhelmed by small boats, small arms would most likely be utilized and would give the ship a slightly better chance of defending itself.
5. Since the keepout range for small targets was assigned as 500 meters, small arms were not implemented into the model.

Assign GWS: Assigns GWS as engaging weapon for target.

Assign CIWS: Assigns CIWS as engaging weapon for target.

Assign PAM: Assigns PAM as engaging weapon for target.

Assign Armed Helo: Assigns Armed Helo as engaging weapon for target.

Target Within Keepout Range: Ends target movement through model due to target reaching its keepout range. When a target reaches this point, a failure is recorded.

Range Update for Engagement: Calculates target range for engagement and evaluation.

Assign Higher Priority?: Decision block that assigns a higher priority for immediate execution of target if it is within 1 kilometer of its keepout range.

Assumptions:

1. Targets approaching their own keepout range are assigned a higher priority, but maintain a lower priority than targets that are reengaged by the system.

Assign High Priority: Actual assignment of a higher priority occurs in this block. A higher priority target will move ahead in the engagement queue to the front of the queue for immediate engagement.

#### **4.0 WEAPON / ASSET SERVICES (W/AS)**

The W/AS functions of the OATCTEPM are broken down into the following functions: Action: Weapon, RV, NAV, and Engineering, Schedule: Weapon, RV, NAV, and Engineering, Event: Weapon, RV, NAV, and Engineering. The model blocks created in ARENA that represent W/AS services are shown below with a description of the block:

Assumptions:

1. GWS rounds will always be available because the scenarios being executed will never use the maximum number of GWS rounds available on the ship.
2. CIWS rounds will always be available because the scenarios being executed will never use the maximum number of GWS rounds available on the ship.
3. There are a maximum number of rounds (24 missiles) available for PAM.
4. There are a maximum number of rounds (16 Hellfire missiles, 8 each Armed Helo) available for Armed Helo.

Direct Engagement to Weapon: Decision block that sends target to a particular engagement queue based on assignments made to target in previous sections of the model.

PAM Available?: Decision block that checks to see if the PAM system is available for target engagement. If the system is available, the target is sent to the engagement queue for PAM. If it is not available, the target is sent to GWS for engagement.



Armed Helo Rounds Available?: Decision block that checks to see if Hellfire Missiles are available for target engagement. If Hellfire are available, the target is sent to the engagement queue for Armed Helo. If Hellfire are not available, the target is sent to PAM for engagement.

## **5.0 MISSION EXECUTION (ME)**

The ME functions of the OATCTEPM are broken down into the following functions: Air/Surface Missile, Land Attack Missile, Torpedo, Gun, Decoy, Aircraft, Boat, Un-Manned Vehicle, Engineering, Damage, and Bridge. The model blocks created in ARENA that represent ME services are shown below with a description of the block:

Assumptions:

1. Reaction, flight, cycle, and kill evaluation times have been estimated, but errors in these estimates may exist.
2. Probability of kill numbers have been estimated for each of the weapon systems and the accuracy of these numbers is unknown.
3. Re-engagement of a target happens immediately after the first engagement and a target moves ahead in the queue for re-engagement.

GWS Reaction Time: Reaction time for GWS engagement.

GWS Cycle: GWS engagement queue for targets.

Assumptions:

1. The firing doctrine for GWS is shoot three-look-shoot three.

GWS Time of Flight: GWS time of flight based on target range.

GWS Kill Evaluation Delay: Time needed for GWS kill evaluation. The Optical Sighting System (OSS is an EO/IR system) is used for kill evaluation in the GWS.

GWS Range Update for Kill Evaluation: Updates target range for kill evaluation decision block.

GWS Range Evaluation: Decision block that checks target range and makes sure target is not within keepout range before target kill.

Target within Keepout Range GWS: Records targets that have reached their respective keepout range.

GWS Kill Evaluation: Decision block that decides whether a target engaged by GWS has been killed. If target was not killed, a higher priority is assigned to the target so the target moves to the front of the engagement queue for re-engagement.

Assumptions:

1. Re-engaging a target that was not killed with previous rounds saves time. This is why a higher priority has been assigned for re-engagement.

GWS Kill: Ends model and records target as a kill.

Assign Higher Priority for GWS ReEngage: A higher priority is assigned to engage the target immediately.

GWS Range Evaluation for ReEngage: Evaluates range of target to make sure target is not within keepout range before re-engagement.

Target Within Keepout Range for ReEngage GWS: Target has reached its respective keepout range before re-engagement occurred.

CIWS Reaction Time: Reaction time for CIWS engagement.

CIWS Cycle: CIWS engagement queue for targets.

Assumptions:

1. Firing doctrine for CIWS is shoot burst-look-shoot burst.

CIWS Time of Flight: CIWS time of flight based on target range.

CIWS Kill Evaluation Delay: Time needed for CIWS kill evaluation.

CIWS Range Evaluation: Decision block that checks target range and makes sure target is not within keepout range before target kill.

Target within Keepout Range CIWS: Records targets that have reached their respective keepout range.

CIWS Kill Evaluation: Decision block that decides whether a target engaged by CIWS has been killed. If target was not killed, a higher priority is assigned to the target so the target moves to the front of the engagement queue for re-engagement.

CIWS Kill: Ends model and records target as a kill.

Assign Higher Priority for CIWS ReEngage: A higher priority is assigned to engage the target immediately.

Target Within Keepout Range for ReEngage CIWS: Target has reached its respective keepout range before re-engagement occurred.

CIWS Range Evaluation for ReEngage: Evaluates range of target to make sure target is not within keepout range before re-engagement.

PAM Reaction Time: Reaction time for PAM engagement.

PAM Cycle: Engagement queue for PAM weapon.

Assumptions:

1. Firing doctrine for PAM is shoot one-look-shoot one.

PAM Time of Flight: Time of flight for PAM based on target range.

PAM Kill Evaluation Delay: Delay for kill evaluation by PAM weapon system.

PAM Range Evaluation: Update to target range for range evaluation of target.

Target within Keepout Range PAM: Target has reached its respective keepout range.

PAM Kill Evaluation: Kill evaluation delay for PAM.

PAM Kill: Target kill recorded for PAM and end of model for target.

Assign Higher Priority for PAM ReEngage: A higher priority is assigned to target for immediate re-engagement of target by PAM.

PAM Range Evaluation for ReEngage: Evaluates target range before re-engagement to check to see if target has reached its respective keepout range.

Target within Keepout Range for ReEngage PAM: Records number of targets that have reached their keepout range.

Delay for GWS Range: If target is sent to GWS from PAM weapon system, a delay is executed until target reaches GWS max range for engagement.

Armed Helo Reaction Time: Reaction time for Armed Helo engagement.

Armed Helo RePosition: Reposition time for Armed Helo to reach target.

Assumptions:

1. Armed Helo Reposition time is based on the speed of the helicopter and the range to the targets.

Armed Helo Cycle: Engagement queue for Armed Helo.

Assumptions:

1. Firing doctrine for Armed Helo is shoot one-look-shoot one.

Armed Helo Time of Flight: Time of flight for hellfire missile.

Armed Helo Kill Evaluation Delay: Delay for kill evaluation through Armed Helo pilots.

Armed Helo Range Evaluation: Evaluates target range.

Target within Keepout Range Armed Helo: Checks to see if target has reached its respective keepout range.

Armed Helo Kill Evaluation: Decision block that decides if target has been killed by Hellfire missile.

Armed Helo Kill: Records target kill by Armed Helo and ends model for target.

Assign Higher Priority for Armed Helo ReEngage: A higher priority is assigned to target for immediate re-engagement.

Target within Keepout Range for ReEngage Armed Helo: Target reaches keepout range.

## 6.0 EXTERNAL COMMUNICATIONS (EXCOMM)

The EXCOMM functions of the OATCTEPM are broken down into the following functions: Communications Service Action, Network Schedule, Message Event, Network, Data Links, Radios, and SatCom. The model blocks created in ARENA that represent EXCOMM services are shown below with a description of the block:

Assumptions:

1. All delay times are estimates.

Search Delay: Delay for search of target.

Detection Delay: Delay for target detection.

Locate Delay: Delay for locate of target.

Firm Track Delay: Delay for establishing firm track of target.

First Pass Delay: First pass delay for target classification.

Second Pass Delay: Second pass delay for target classification.

Re Classify Delay for Unknown: A delay is executed if classification of target continues to be unknown.

Identify Delay: Delay for finalizing target identity.

Threat Evaluation Delay: Delay for threat evaluation.

Target Priority Delay: Delay for assigning target priorities.

Mission Evaluation Delay: Delay for evaluation of mission.

Weapon Assign Delay: Delay for weapon assignment.

Plan Approval Delay: Delay for approval of plan for execution of targets.

Delay for Waiting: Delay for waiting for approval of plan.

Clearance to Fire Delay: Delay for waiting for clearance to fire to be obtained.

Update Priority Delay: Delay for updating the priority of a target to higher priority based on target range.

## **7.0 COMMON SERVICES (CS)**

The CS functions of the OATCTEPM are broken down into the following functions: Display, Time, NAV, DX/DR, Databases, and Environment. The model blocks created in ARENA that represent EXCOMM services are shown below with a description of the block:

Assumptions:

1. A failure by a weapon system does not mean that the failure is caused by the weapon system. The failure could have been contributed to the target not being detected far enough in range to allow the weapon system to engage the target in time or there may be other circumstances that contributed to a failure by the cruiser.

Locate Range Update: Update to target range at time of target locate function of model.

Range Update for Priority: Update to target range at time of target priority function of model.

Range Update for Plan: Update to target range for planning purposes of the model.

Range Update for Engagement: Update to target range for engagement of the target. A higher priority is assigned to target if this range update shows that the target is within 1 kilometer of its respective keepout range.

GWS Range Update for Kill Evaluation: Target range is updated for kill evaluation.

CIWS Range Update for Kill Evaluation: Target range is updated for kill evaluation.

PAM Range Update for Kill Evaluation: Target range is updated for kill evaluation.

Armed Helo Range Update for Kill Evaluation: Target range is updated for kill evaluation.

Record Targets within Keepout Range: Records number of targets within keepout range.

Record Failures GWS: Failures by GWS, which means the number of targets that have reached keepout range when assigned to GWS.

Record GWS Kills: Number of kills logged by GWS.

Record Failures GWS for ReEngage: Number of failures by GWS after first engagement of target. These failures will only occur after an unsuccessful GWS engagement of the target.

Record Failures CIWS: Number of failures by CIWS or number of targets that have reached their respective keepout range when assigned to CIWS.



Record CIWS Kills: Number of kills by CIWS.

Record Failures CIWS for ReEngage: Number of failures by CIWS after first engagement of target.

Record Failures PAM: Number of failures by PAM weapon system or number of targets allowed by PAM to reach their respective keepout range.

Record PAM Kills: Number of targets killed by PAM weapon system.

Record Failures PAM for ReEngage: Number of failures by PAM after first engagement of a target.

Record Failures Armed Helo: Number of failures by Armed Helo.

Record Armed Helo Kills: Number of targets killed by Armed Helo.

Record Failures Armed Helo for ReEngage: Number of failures or number of targets allowed to reach keepout range by Armed Helo after first engagement of target.

Record GWS Salvos: Record total number of GWS salvos. Each GWS salvo consists of 3 rounds fired directly at the target.

Record CIWS Bursts: Number of CIWS bursts fired at targets.

Record PAM Fired: Record total number of PAM fired at targets.

Record Hellfire Fired: Record total number of Hellfire fired at targets.

## **8.0 TRAINING (TR)**

The TR functions of the OATCTEPM are broken down into the following functions: Training Action, Schedule, and Event, Synthetic Actions, Synthetic Entities, Simulator, Scenario. There are no model blocks created in ARENA that represent TR functions.

Assumptions:

1. All training functions within the OA model will remain as described in the OA model.
2. Model blocks for Training do not fit into the ARENA model and have been left out. This does not mean that they should be removed from the OA model.
3. The scenarios being run through the model are actual scenarios at war-time and training is assumed to have been completed prior to the actual scenarios.

## **9.0 FORCE PLANNING / COORDINATION (FP/C)**

The FP/C functions of the OATCTEPM are broken down into the following functions: Joint BF Orders, Commanders Estimate, COA Repository, BG Orders, and Force Integrated Scheduler. The model blocks created in ARENA that represent FP/C functions are shown below with a description of the block:

Send to other: Mission evaluation concludes that more force is needed to complete mission.

Plan Approval: Decision block that either approves or rejects plan to execute targets. If plan is not approved, the target must go back through the planning stage.

Obtain Clearance to Fire: Decision block that gives clearance to fire on targets. If clearance to fire is not obtained, a delay for waiting to obtain clearance to fire is executed until clearance to fire has been approved.

## OATCTEPM PROCESS VARIABLES

The following tables show the parameters of the different types of process blocks stored in the Arena model. Each table signifies a different kind of block including: Create, Process, Assign, Decide, Record, and Dispose.

Create - Basic Process							
Name	Entity	Type	Value	Units	Entities per Arrival	Max Arrivals	First Creation
Search	Target	Constant	0	Seconds	Total Number of Targets	1	0

Table 20. Create Basic Process Block

Process - Basic Process											
Name	Type	Action	Priority	Resources	Delay Type	Units	Allocation	Min	Value	Max	Expression
Search Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	5	10	15	1
Detection Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	1	1	1
Locate Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.1	1	1	1
Large RCS Delay	Standard	Delay	Medium(2)	0 Rows	Expression	Seconds	Value Added	0.5	2	1.5	$((\text{Locate\_Range} - 33.7)/\text{Locate\_Speed})$
Medium RCS Delay	Standard	Delay	Medium(2)	0 Rows	Expression	Seconds	Value Added	0.5	2	1.5	$((\text{Locate\_Range} - 28.3)/\text{Locate\_Speed})$
Firm Track Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.1	1	0.3	1

Re Classify Delay for Unknown	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	0	1	1
First Pass Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	1	0	3	1
Second Pass Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	2	0	5	1
Validate Target	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	2	0	3	1
Identify Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.1	0	2	1
Threat Evaluation Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	3	0	10	1
Target Priority Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	1	0	3	1
Mission Evaluation Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	5	0	15	1
Weapon Assign Delay GWS Scenario 2	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	0	1	1
Plan Approval Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	15	0	45	1
Clearance to Fire Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	3	0	10	1
Delay for Waiting	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	3	0	15	1
Update Priority Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.1	0	0.2	1
GWS Cycle	Standard	Seize Delay Release	Medium(2)	1 Row	Uniform	Seconds	Value Added	9	1	12	1
GWS Time of Flight	Standard	Delay	Medium(2)	0 Rows	Expression	Seconds	Value Added	0.5	1	1.5	Target_Range_Engage*2.5+7
GWS Kill Evaluation Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	1	1	5	1
GWS Reaction Time	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	10	1	15	1
CIWS Cycle	Standard	Seize Delay Release	Medium(2)	1 Row	Uniform	Seconds	Value Added	5	1	10	1
CIWS Time of Flight	Standard	Delay	Medium(2)	0 Rows	Expression	Seconds	Value Added	0.5	1	1.5	Target_Range_Engage*1.5
CIWS Kill Evaluation Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	5	1	10	1
CIWS Reaction Time	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	10	1	15	1
PAM Cycle	Standard	Seize Delay Release	Medium(2)	1 Row	Uniform	Seconds	Value Added	3	1	10	1
PAM Time of Flight	Standard	Delay	Medium(2)	0 Rows	Expression	Seconds	Value Added	0.5	1	1.5	Target_Range_Engage*3
PAM Kill Evaluation Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	3	1	5	1
PAM Reaction Time	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	30	1	60	1
Armed Helo Cycle	Standard	Seize Delay Release	Medium(2)	1 Row	Uniform	Seconds	Value Added	1	1	3	1

Armed Helo RePosition Scenario 1	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	5	1	10	Target_Range_Direct*5
Armed Helo Kill Evaluation Delay	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	1	1	3	1
Armed Helo Time of Flight	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	1	1	3	Target_Range_Direct*5
Armed Helo Reaction Time	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	5	1	20	1
Armed Helo RePosition Scenario 2	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	15	1	30	Target_Range_Direct*5
Weapon Assign Delay CIWS Scenario 2	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	0	1	1
Weapon Assign Delay PAM Scenario 2	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	0	1	1
Weapon Assign Delay Armed Helo Scenario 2	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	0	1	1
Weapon Assign Delay CIWS Scenario 1	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	0	1	1
Weapon Assign Delay GWS Scenario 1	Standard	Delay	Medium(2)	0 Rows	Uniform	Seconds	Value Added	0.5	0	1	1
For GWS Kills	Standard	Delay	Medium(2)	0 Rows	Constant	Seconds	Value Added	0.5	0	1.5	1
For CIWS Kills	Standard	Delay	Medium(2)	0 Rows	Constant	Seconds	Value Added	0.5	0	1.5	1
For PAM Kills	Standard	Delay	Medium(2)	0 Rows	Constant	Seconds	Value Added	0.5	0	1.5	1
For Armed Helo Kills	Standard	Delay	Medium(2)	0 Rows	Constant	Seconds	Value Added	0.5	0	1.5	1
Delay for GWS Range	Standard	Delay	Medium(2)	0 Rows	Expression	Seconds	Value Added	0.5	2	1.5	((Target_Range_ReEngage - 15)/Locate_Speed)
PAM ReEngage Available	Standard	Delay	Medium(2)	0 Rows	Constant	Seconds	Value Added	0.5	0	1.5	1
Armed Helo ReEngage Available	Standard	Delay	Medium(2)	0 Rows	Constant	Seconds	Value Added	0.5	0	1.5	1

Table 21. Process – Basic Process Blocks

<b>Assign – Basic Process</b>	
<b>Name</b>	<b>Assignment</b>
Detect	2
Small RCS	3
Medium RCS	3
Large RCS	3
Locate Range Update	1
Firm Track Time	2
Hostile First Pass	1
Unknown First Pass	1
Friendly First Pass	1
Hostile Second Pass	1
Friendly Second Pass	1
Type 1 Target Small	3
Type 2 Target Medium	3
Type 3 Target Large	3
Target Type 1 Weapon Range	1
Target Type 2 Weapon Range	1
Target Type 3 Weapon Range	1
Range Update for Priority	1
Assign Priority 1 for Target Type 1	1
Assign Priority 2 for Target Type 1	1
Assign Priority 3 for Target Type 1	1
Assign Priority 1 for Target Type 2	1
Assign Priority 2 for Target Type 2	1
Assign Priority 3 for Target Type 2	1
Assign Priority 1 for Target Type 3	1
Assign Priority 2 for Target Type 3	1
Assign Priority 3 for Target Type 3	1
Mission Go	1
Range Update for Plan	1
Assign GWS	1
Assign CIWS	1
Assign PAM	1
Assign Armed Helo	1
Range Update for Engagement	1
Assign High Priority	1
GWS Range Update for Kill Evaluation	1
Assign Higher Priority for GWS ReEngage	2
CIWS Range Update for Kill Evaluation	1
Assign Higher Priority for CIWS ReEngage	2
PAM Range Update for Kill Evaluation	1
Assign Higher Priority for PAM ReEngage	2

Armed Helo Range Update for Kill Evaluation	1
Assign Higher Priority for Armed Helo ReEngage	2
Assign CIWS Scenario 1	1
Assign GWS Scenario 1	1
Validate Target Time	1
Identify Target Time	1
Threat Evaluation Time	1
Target Priority Time	1
Mission Evaluation Time	1
Weapon Assignment Time	1
Clearance to Fire Time	1
Direct Engagement Time	1
Plan Approval Time	1

Table 22. Assign – Basic Process Blocks

Decide - Basic Process							
Name	Type	% True	If	Variable Name	Attribute Name	Is	Value
Locate	N-way by Condition	50	Entity Type	Variable 1	Attribute 1	>=	1
Transition to Track	2-way by Condition	50	Attribute	Variable 1	Locate_Profile	==	0
Firm Track?	2-way by Condition	50	Attribute	Variable 1	Locate_RCS_Type	==	1
Awaiting Firm Track	2-way by Condition	50	Attribute	Variable 1	Locate_RCS_Type	==	2
Classify Target	N-way by Chance	50	Entity Type	Variable 1	Attribute 1	>=	1
Re Classify Target	N-way by Chance	50	Entity Type	Variable 1	Attribute 1	>=	1
Identify Target	N-way by Condition	50	Entity Type	Variable 1	Attribute 1	>=	1
Threat Evaluation	N-way by Condition	50	Entity Type	Variable 1	Attribute 1	>=	1
Assign Target Priority	N-way by Condition	50	Entity Type	Variable 1	Attribute 1	>=	1
Mission Evaluation	2-way by Chance	95	Entity Type	Variable 1	Attribute 1	>=	1
Weapon Assignment Scenario 1	2-way by Condition	50	Attribute	Variable 1	Detect_Range	==	3 && (Weapon Assign Delay CIWS Scenario 1.NumberIn < 5)
Target Type Count	N-way by Condition	50	Entity Type	Variable 1	Attribute 1	>=	1
Plan Approval	2-way by Chance	95	Entity Type	Variable 1	Attribute 1	>=	1
Obtain Clearance to Fire	2-way by Chance	85	Entity Type	Variable 1	Attribute 1	>=	1
Range Evaluation	2-way by Condition	50	Attribute	Variable 1	Target_Range_Engage	>	Target_Weapon_Range
Assign Higher Priority?	2-way by Condition	50	Attribute	Variable 1	Target_Range_Engage	<=	Target_Weapon_Range+1
Direct Engagement to Weapon	N-way by Condition	50	Entity Type	Variable 1	Attribute 1	>=	1
GWS Range Evaluation	2-way by Condition	50	Attribute	Variable 1	Target_Range_GWS_Eval	>	Target_Weapon_Range
GWS Kill Evaluation	2-way by Chance	80	Entity Type	Variable 1	Attribute 1	>=	1
CIWS Kill Evaluation	2-way by Chance	85	Entity Type	Variable 1	Attribute 1	>=	1
CIWS Range Evaluation	2-way by Condition	50	Attribute	Variable 1	Target_Range_CIWS_Eval	>	Target_Weapon_Range
PAM Kill Evaluation	2-way by Chance	90	Entity Type	Variable 1	Attribute 1	>=	1
PAM Range Evaluation	2-way by Condition	50	Attribute	Variable 1	Target_Range_PAM_Eval	>	Target_Weapon_Range



Armed Helo Kill Evaluation	2-way by Chance	95	Entity Type	Variable 1	Attribute 1	>=	1
Armed Helo Range Evaluation	2-way by Condition	50	Attribute	Variable 1	Target_Range_ArmedHelo_Eval	>	Target_Weapon_Range
Scenario Position Time for Helo	2-way by Condition	50	Variable	Scenario	Attribute 1	==	1
Scenario 1 or Scenario 2?	2-way by Condition	50	Variable	Scenario	Attribute 1	==	1
Weapon Assignment Scenario 2	N-way by Condition	50	Entity Type	Variable 1	Attribute 1	>=	1
PAM Available for ReEngage?	2-way by Condition	50	Expression	Variable 1	Attribute 1	>=	(PAM Reaction Time.NumberIn + PAM ReEngage Available.NumberIn) < 24
PAM Available for Engage?	2-way by Condition	50	Expression	Variable 1	Attribute 1	>=	(PAM Reaction Time.NumberIn + PAM ReEngage Available.NumberIn) < 24
Armed Helo Available for Engage?	2-way by Condition	50	Expression	Variable 1	Attribute 1	>=	(Armed Helo Reaction Time.NumberIn + Armed Helo ReEngage Available.NumberIn) < 16
Armed Helo Available for ReEngage?	2-way by Condition	50	Expression	Variable 1	Attribute 1	>=	(Armed Helo Reaction Time.NumberIn + Armed Helo ReEngage Available.NumberIn) < 16

Table 23. Decide – Basic Process Blocks

<b>Record - Basic Process</b>			
<b>Name</b>	<b>Type</b>	<b>Value</b>	<b>Counter Name</b>
Record Number of Targets	Count	1	Record Number of Targets
Record Number of Large Targets	Count	1	Record Number of Large Targets
Record Number of Small Targets	Count	1	Record Number of Small Targets
Record Number of Medium Targets	Count	1	Record Number of Medium Targets
Record Targets within Keepout Range	Count	1	Record Targets within Keepout Range
Record GWS Salvos	Count	1	Record GWS Salvos
Record Failures GWS	Count	1	Record Failures GWS
Record GWS Kills	Count	1	Record GWS Kills
Record Failures CIWS	Count	1	Record Failures CIWS
Record CIWS Kills	Count	1	Record CIWS Kills
Record CIWS Bursts	Count	1	Record CIWS Bursts
Record Failures PAM	Count	1	Record Failures PAM
Record PAM Kills	Count	1	Record PAM Kills
Record PAM Fired	Count	1	Record PAM Fired
Record Failures Armed Helo	Count	1	Record Failures Armed Helo
Record Armed Helo Kills	Count	1	Record Armed Helo Kills
Record Armed Helo Fired	Count	1	Record Armed Helo Fired

Table 24. Record – Basic Process Blocks

<b>Dispose - Basic Process</b>
<b>Name</b>
Disregard Track if Outbound
Disregard Track First Pass
Disregard Track Second Pass
Send to other
Target within Keepout Range
Target within Keepout Range GWS
GWS Kill
Target within Keepout Range CIWS
CIWS Kill
Target within Keepout Range PAM
PAM Kill
Target within Keepout Range Armed Helo
Armed Helo Kill

Table 25. Dispose – Basic Process Blocks

## OATCTEPM ENGAGEMENT FLOW

This section of figures describes the process flow within the OATCTEPM. Because of its complexity, it has been broken into many figures to fully detail the model. The blocks shown are all explained in detail earlier in this appendix.

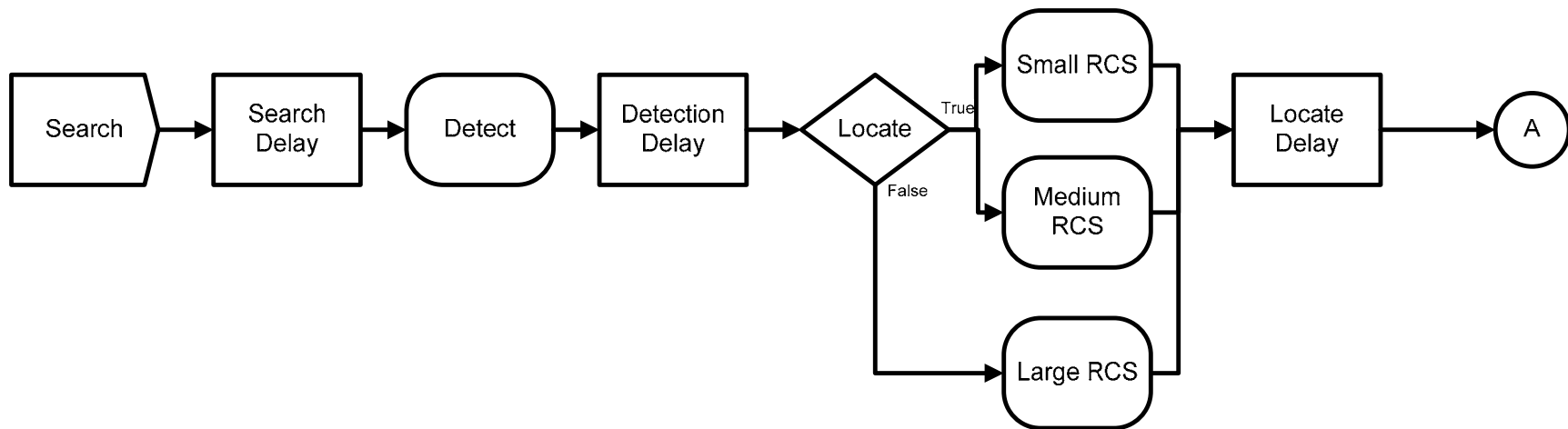


Figure 31. Search / Detect (S/D) Function

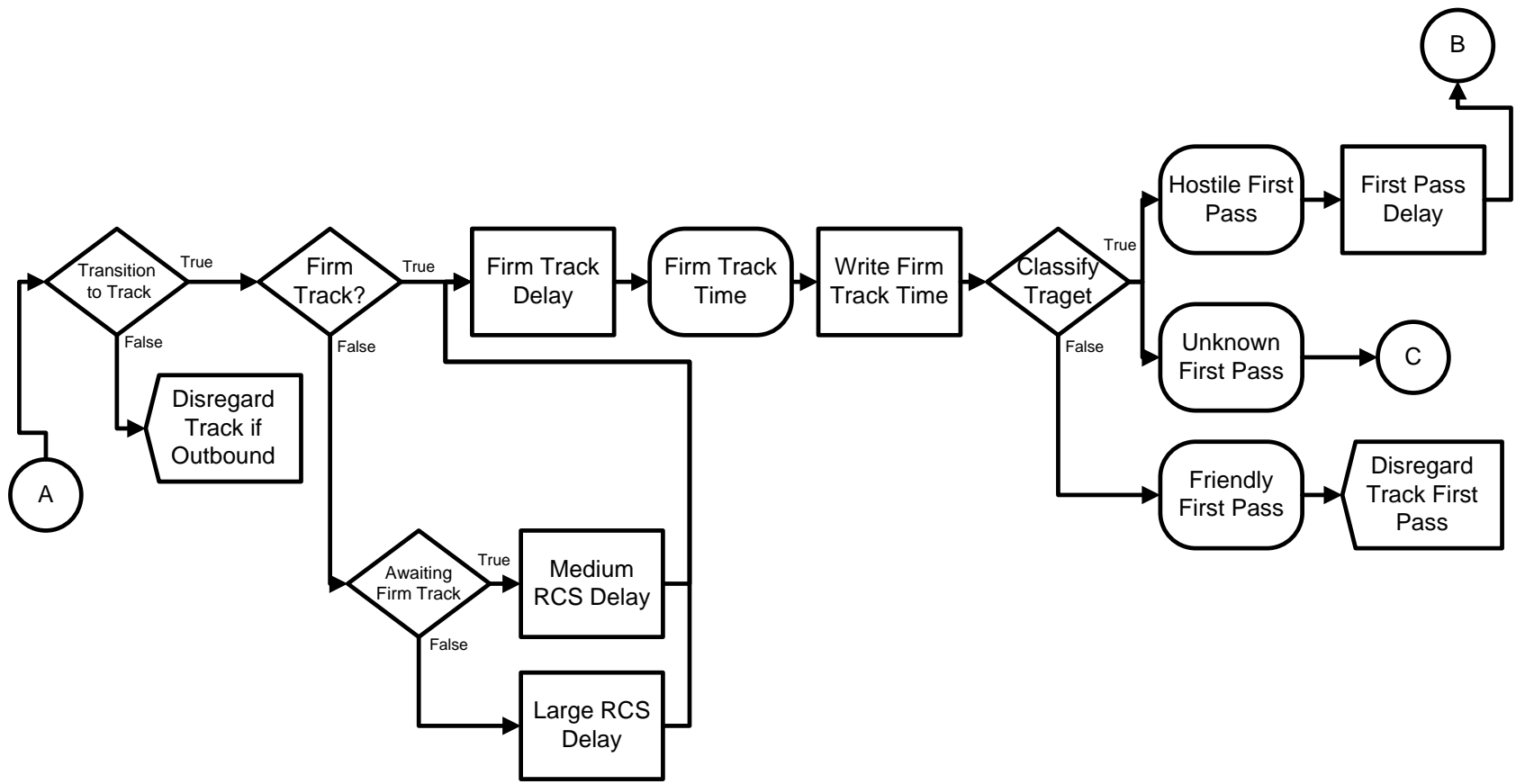


Figure 32. Data / Information Services (DIS) Function

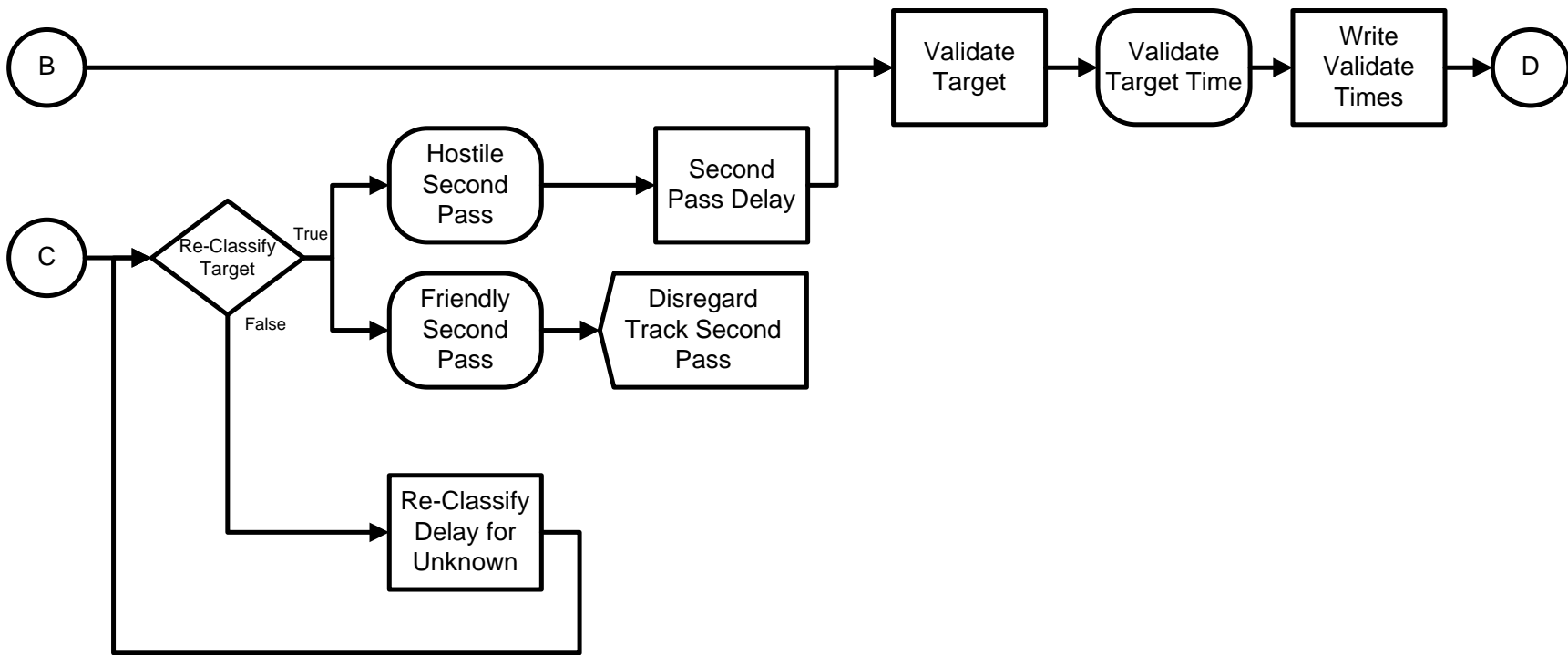


Figure 33. Data / Information Services (DIS) Function Continued

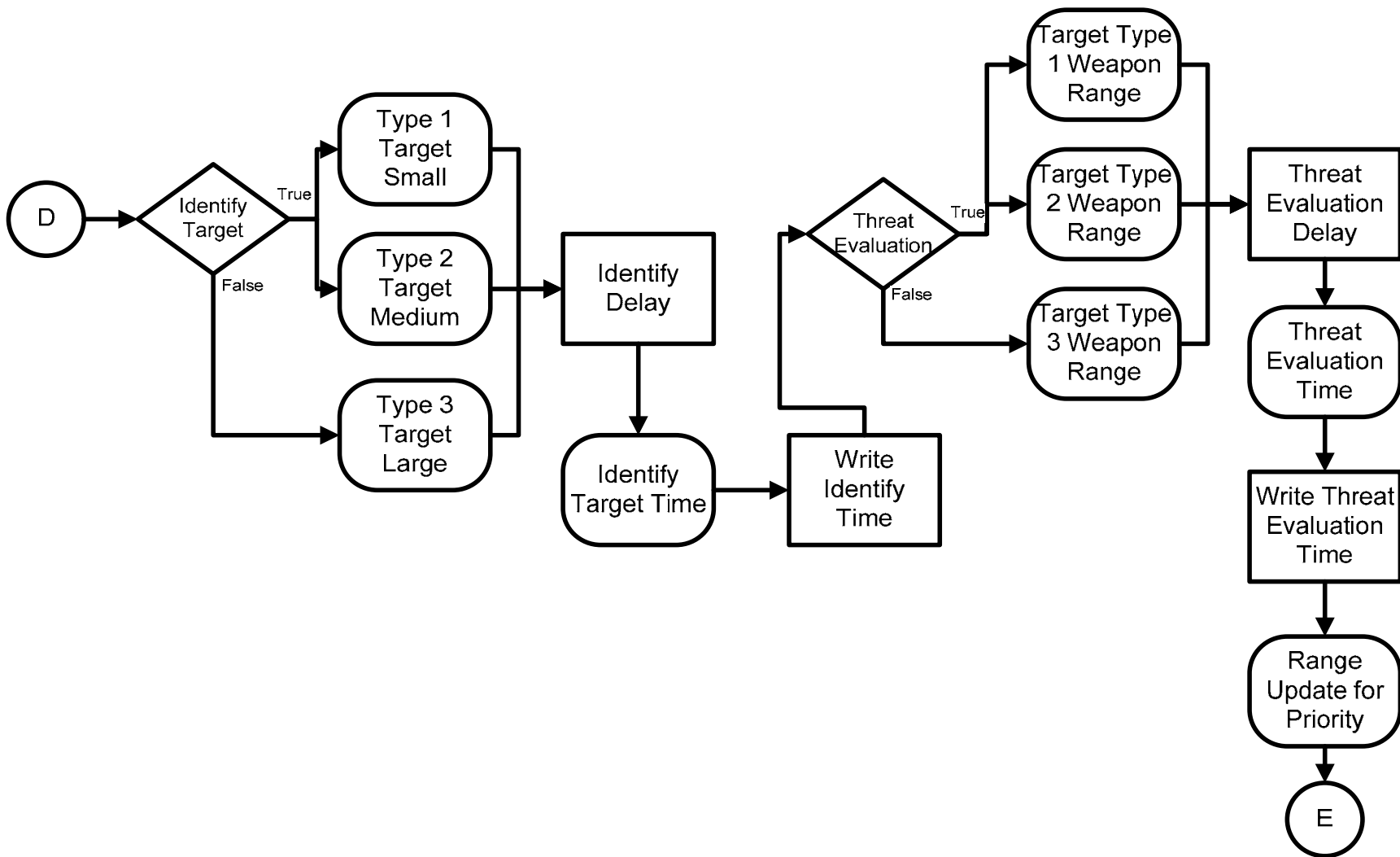
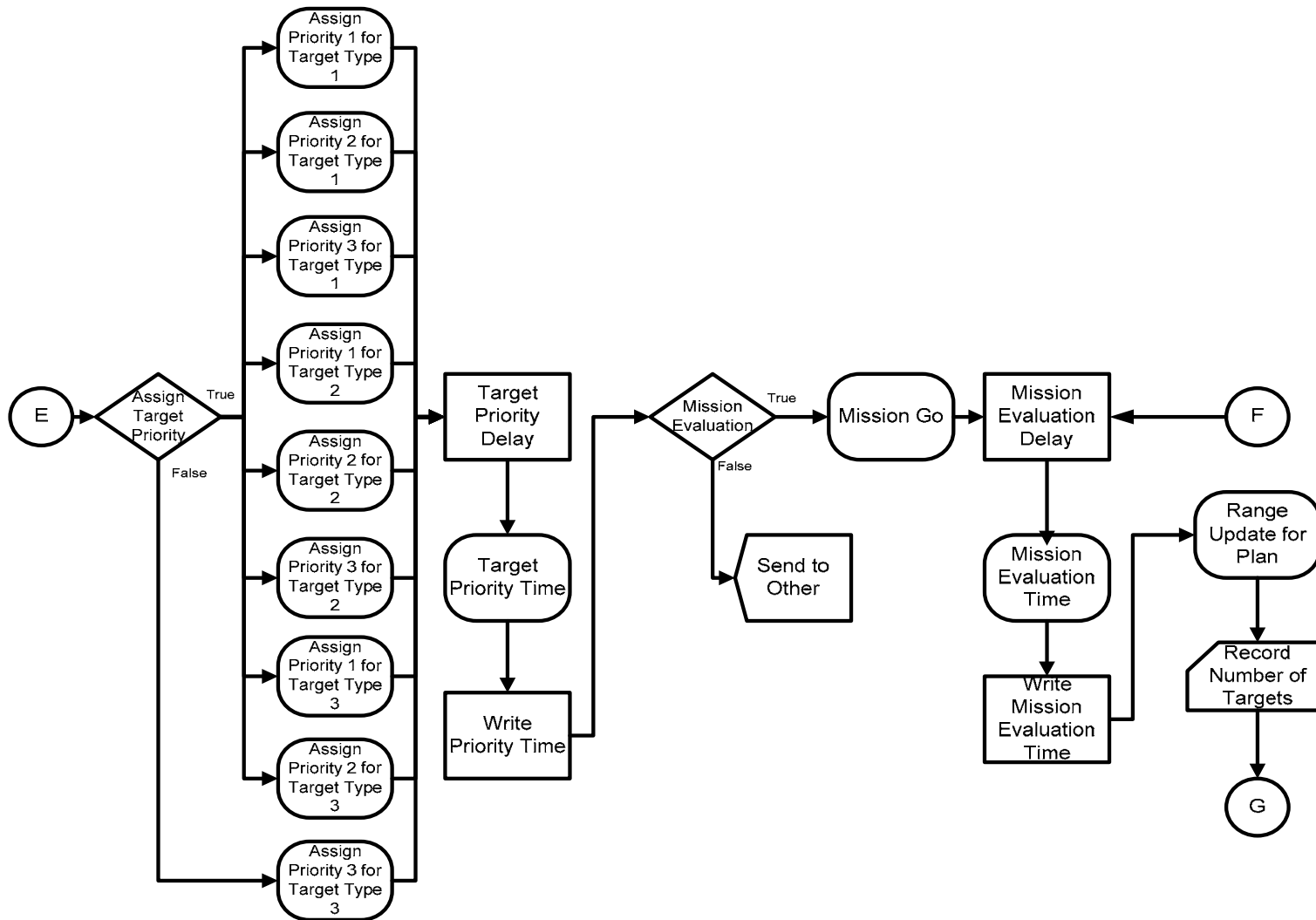


Figure 34. Planning, Assessment, and Decision (PAD) Function



Planning, Assessment, and Decision (PAD) Function Continued

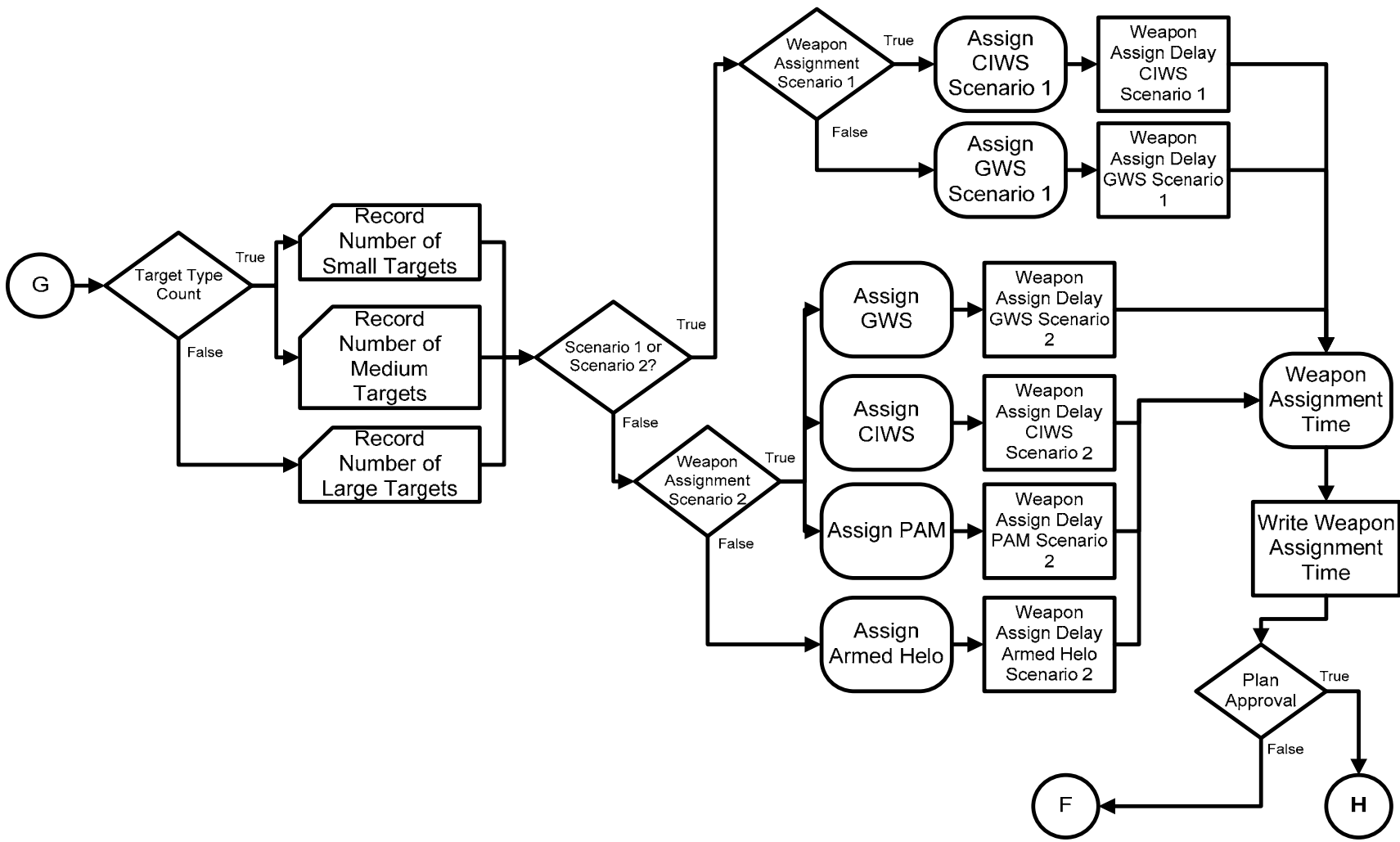


Figure 35. Planning, Assessment, and Decision (PAD) Function Continued



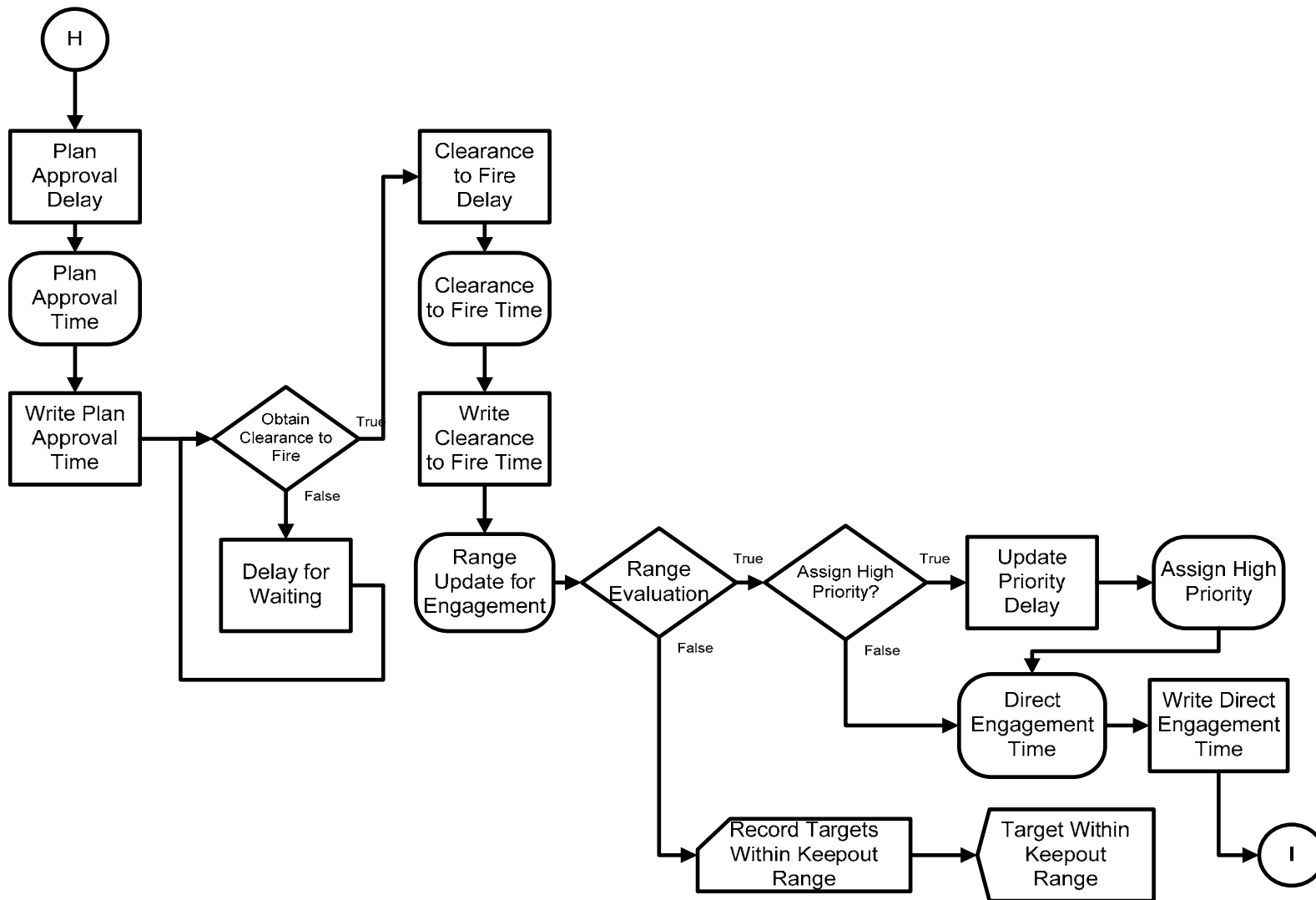


Figure 36. Planning, Assessment, and Decision (PAD) Function Continued

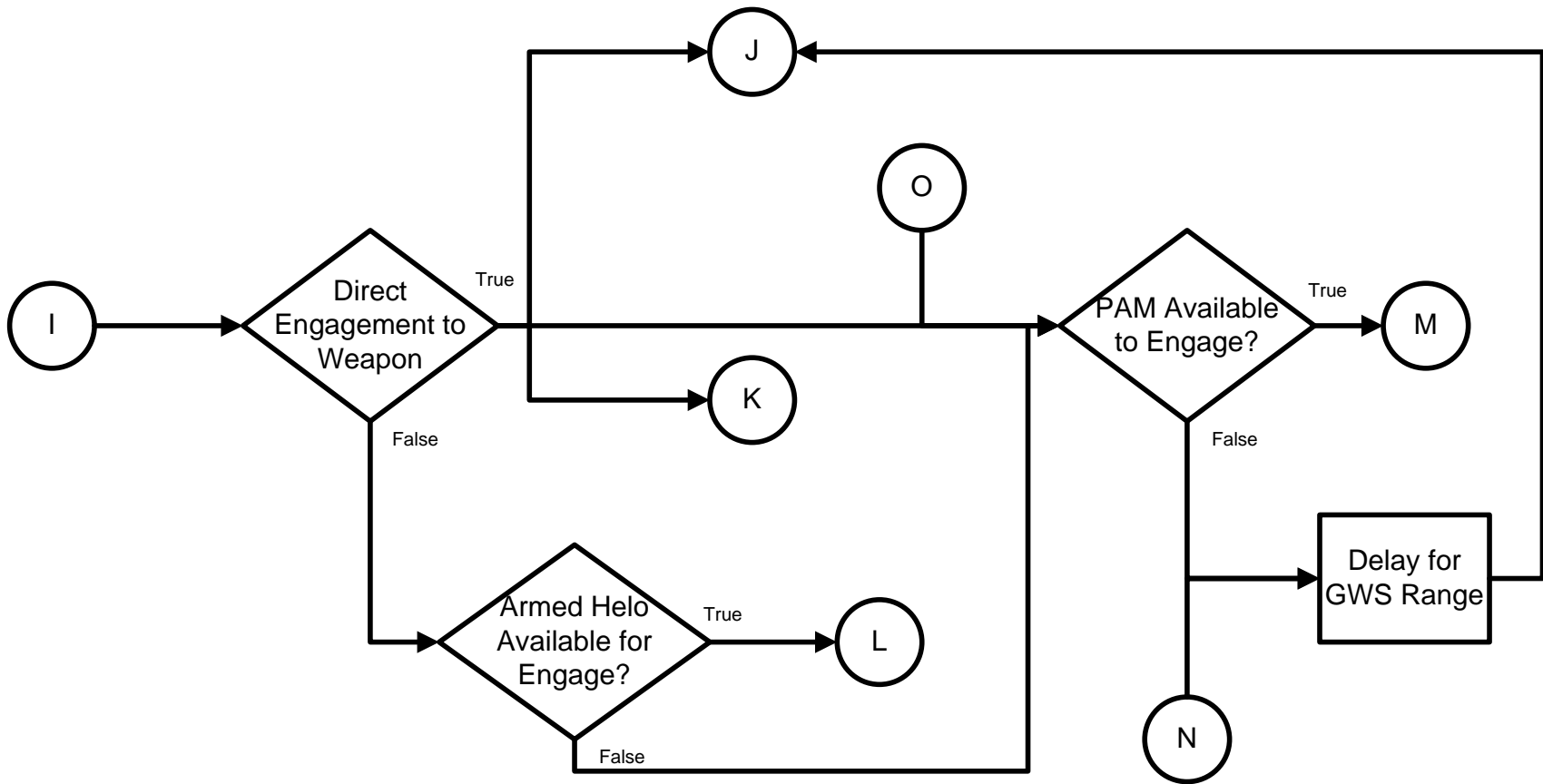


Figure 37. Weapon / Asset Services (W/AS)

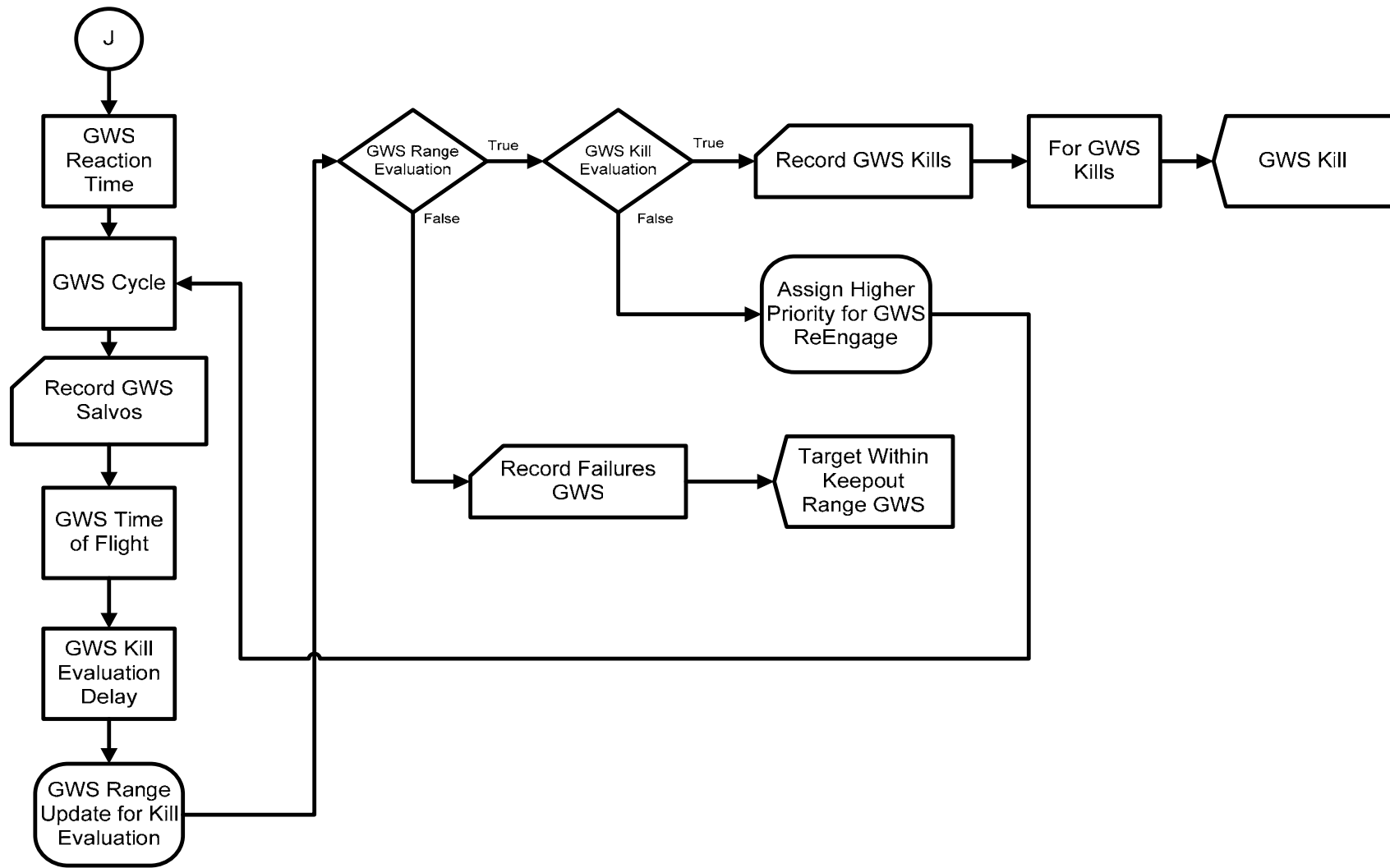


Figure 38. Mission Execution (ME) Function for Gun Weapon System (GWS)

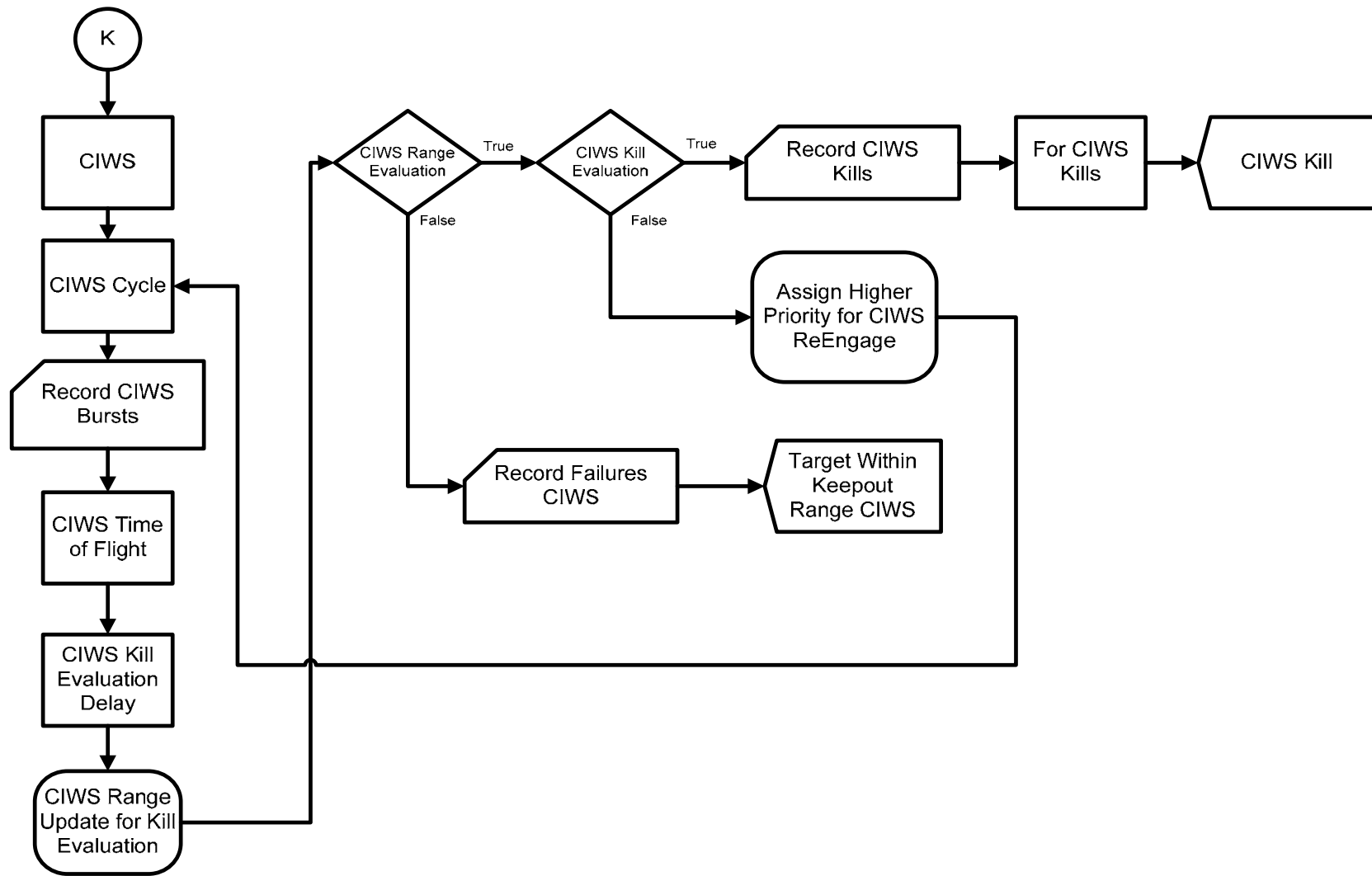


Figure 39. Mission Execution (ME) Function for Close-In Weapon System (CIWS)

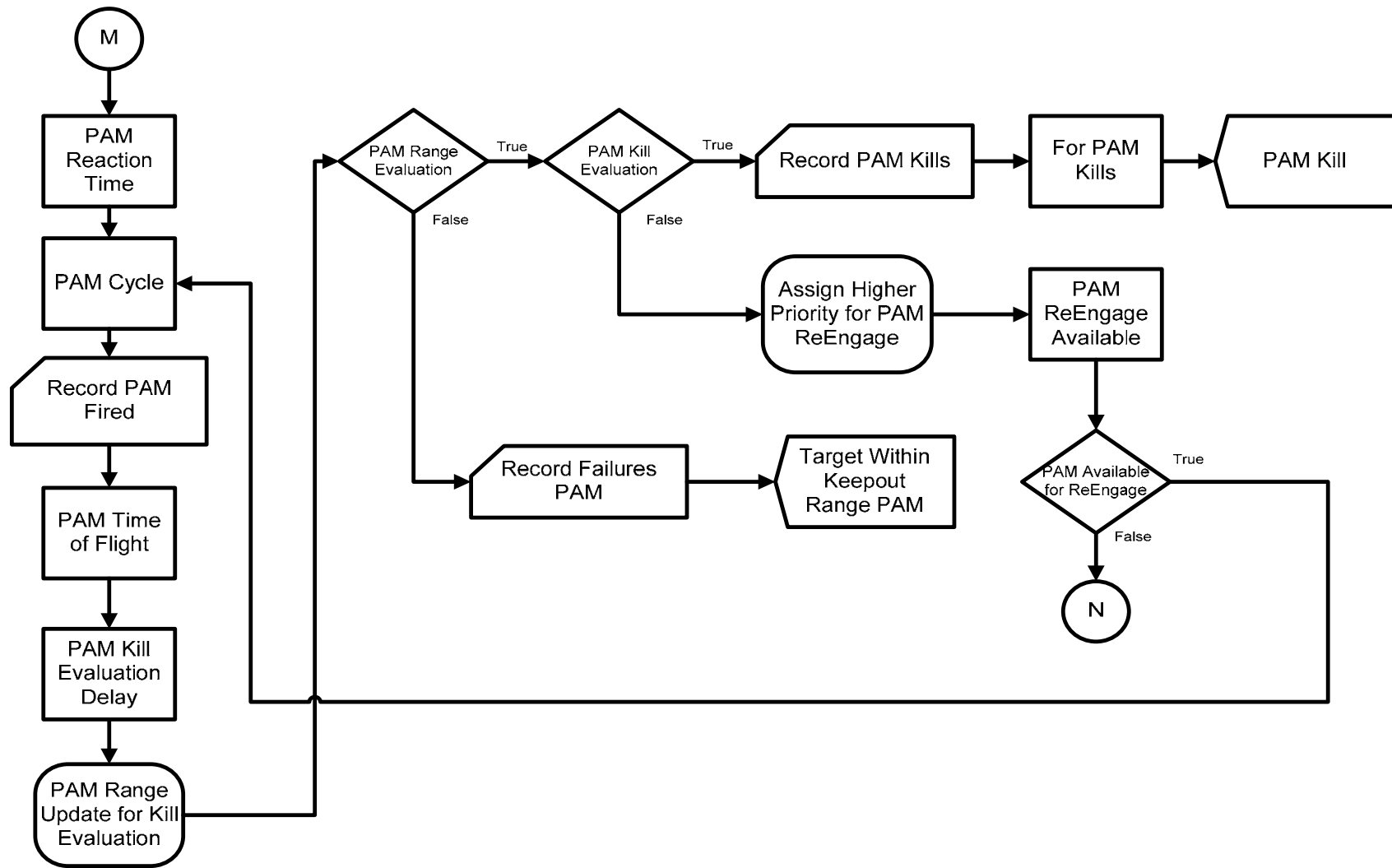


Figure 40. Mission Execution (ME) Function for Precision Attack Missile (PAM)

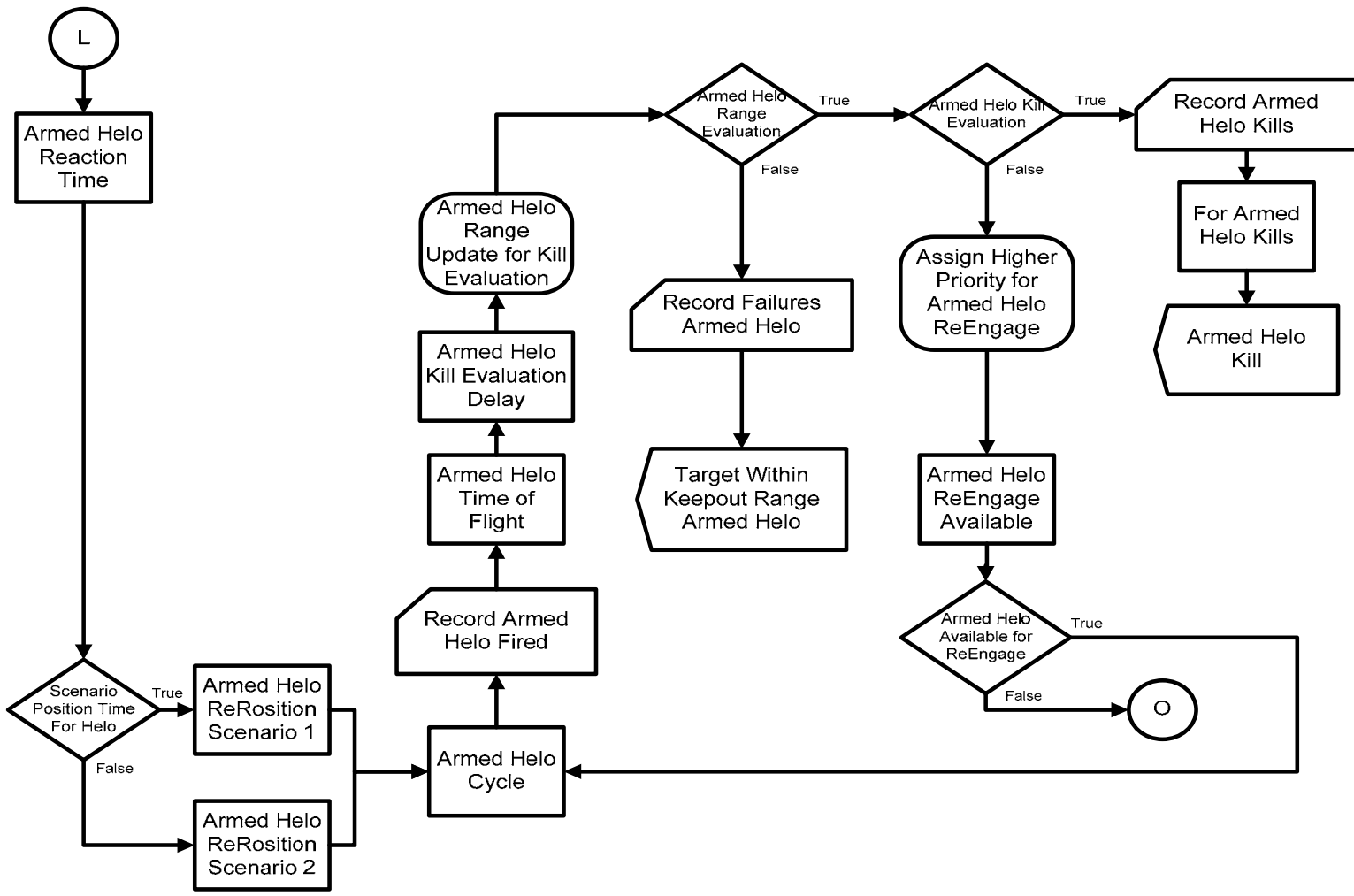


Figure 41. Mission Execution (ME) Function for Armed Helicopter (Helo)

## OATCTEPM PROCESS VARIABLE INPUT DISTRIBUTIONS

The following figures show the actual distributions generated by the Arena software as inputs to the data presented in section V. This is presented for completeness of detail concerning the model used and the method for generating the results discussed.

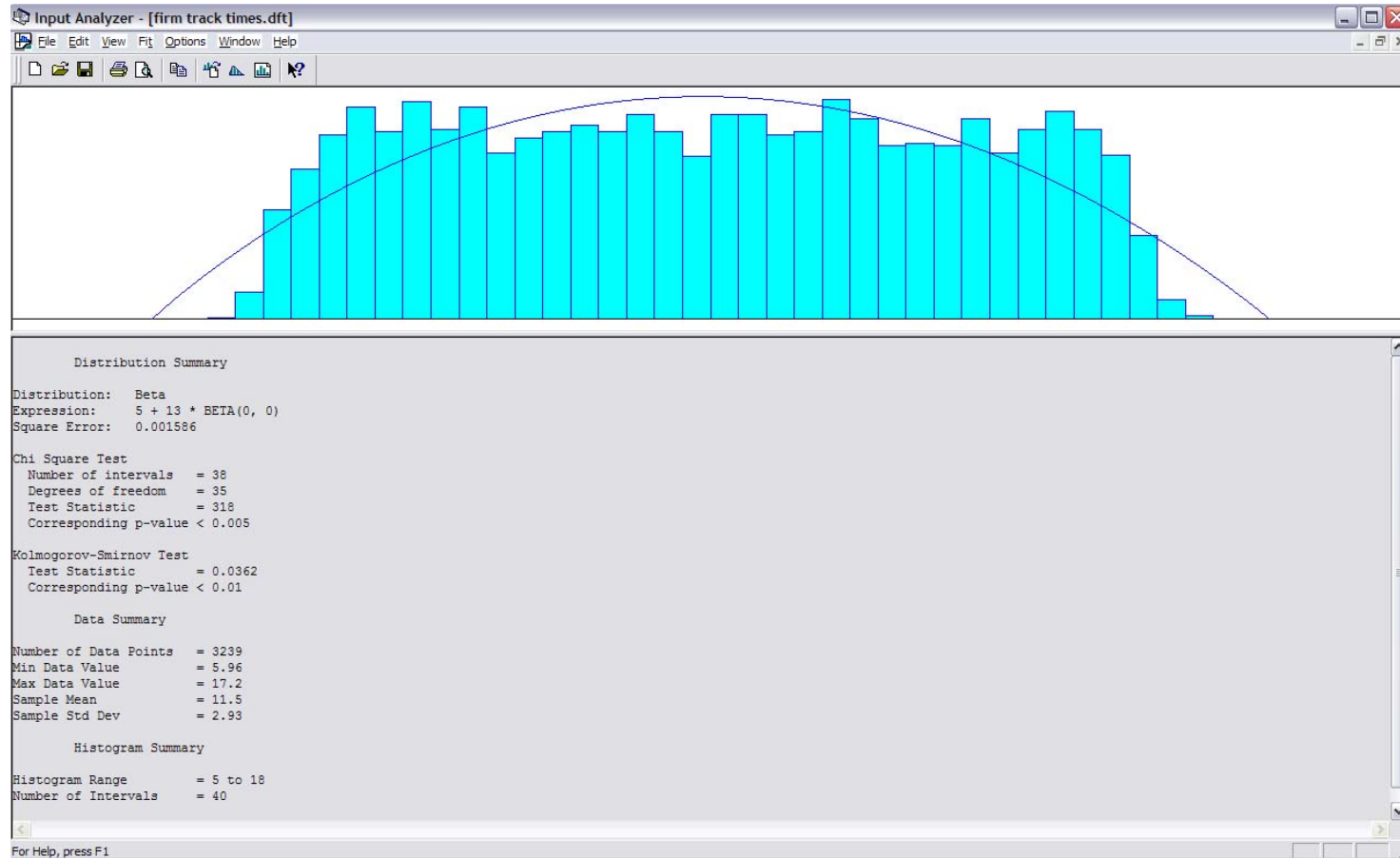


Figure 42. Input Analyzer Firm Track Times for Scenario 1

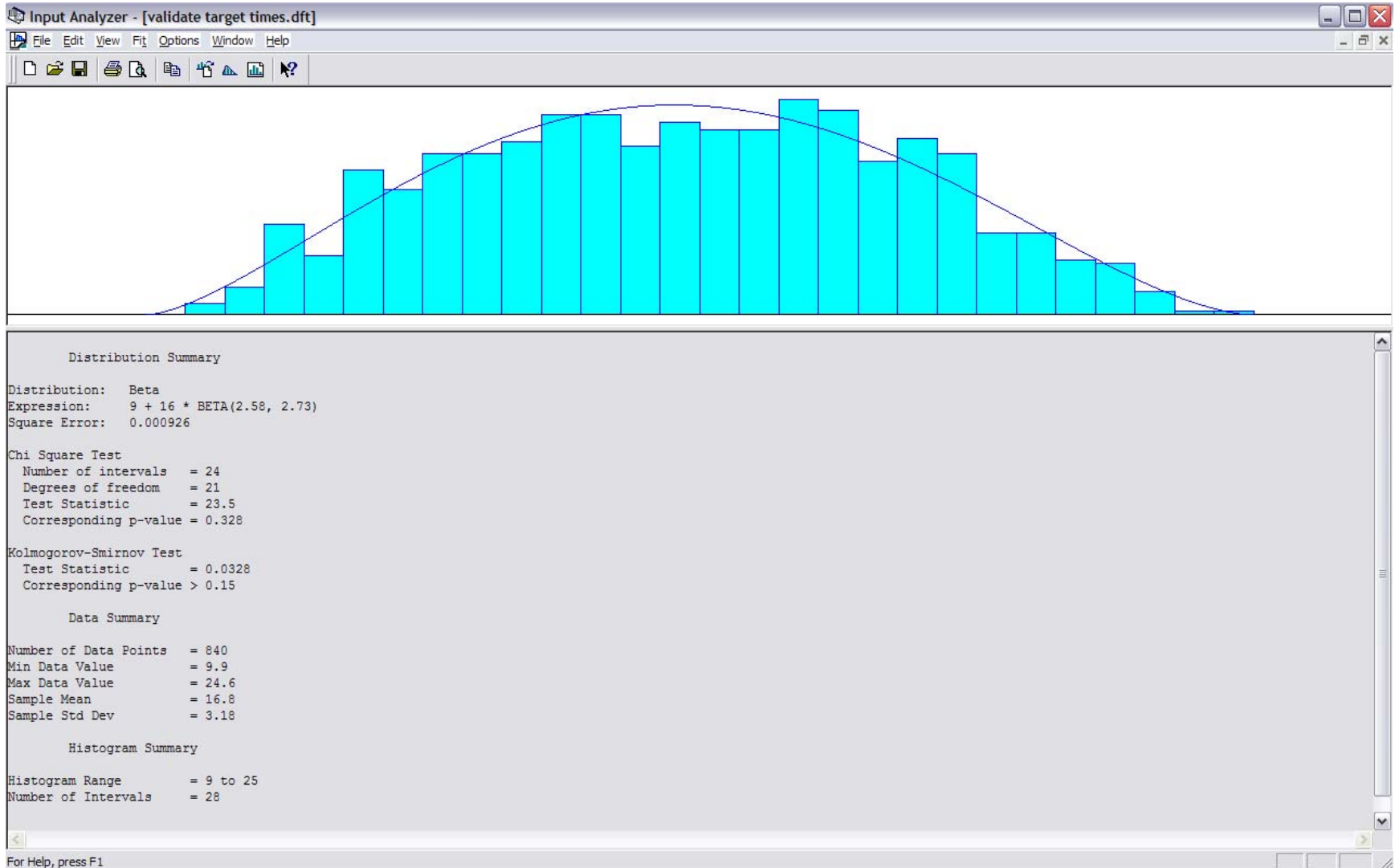


Figure 43. Input Analyzer Validate Target Times for Scenario 1



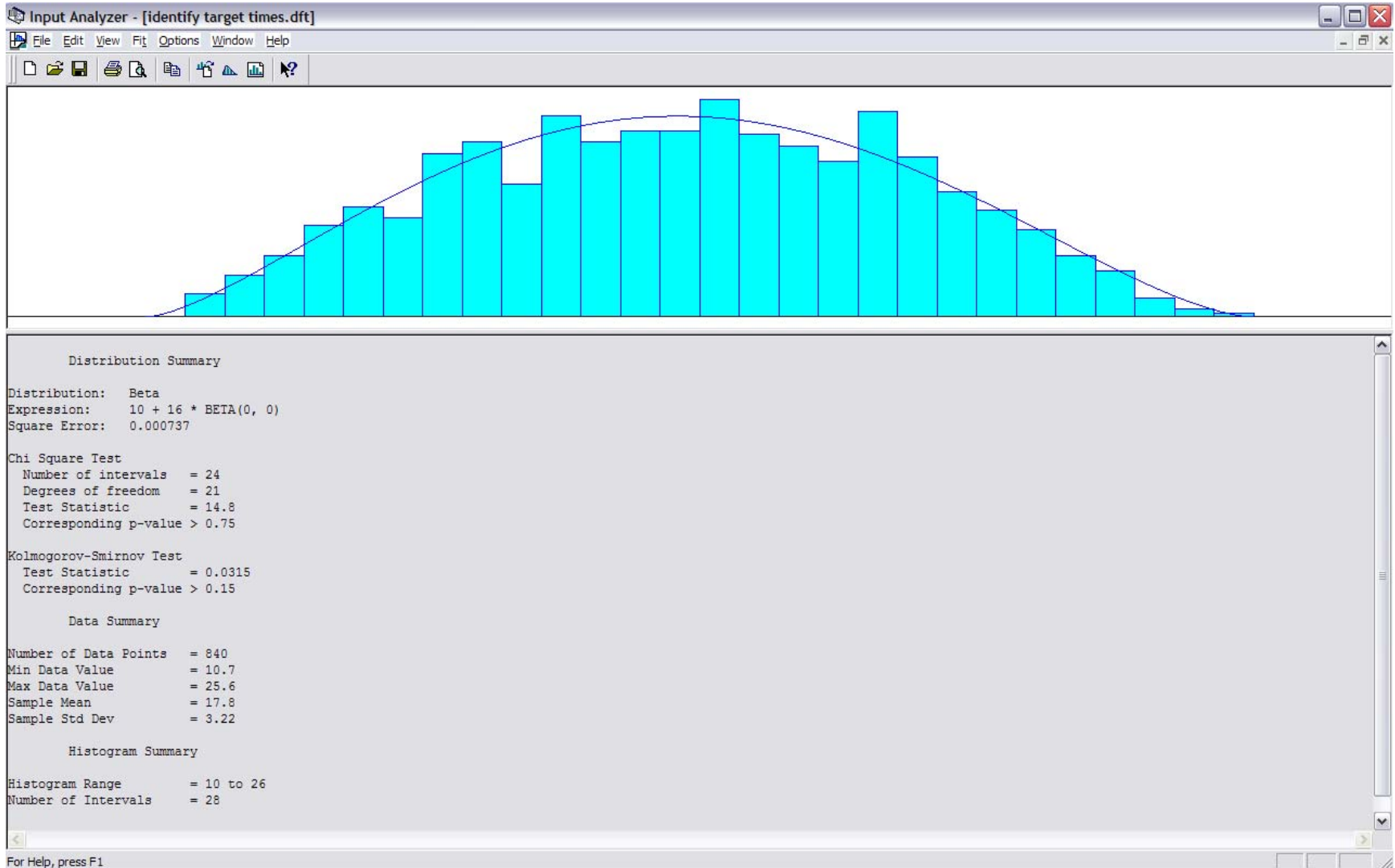


Figure 44. Input Analyzer Identify Target Times for Scenario 1

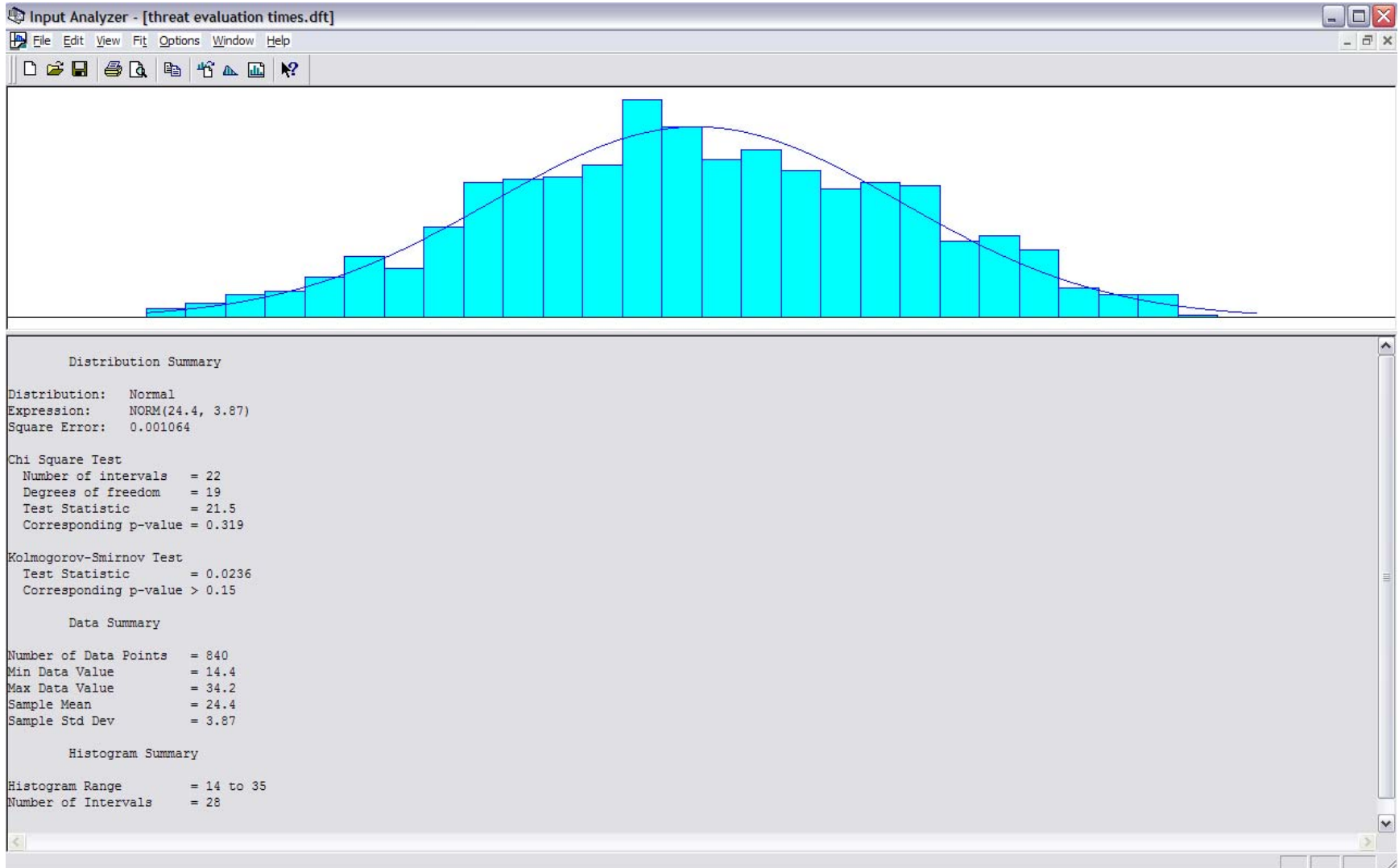


Figure 45. Input Analyzer Threat Evaluation Times for Scenario 1

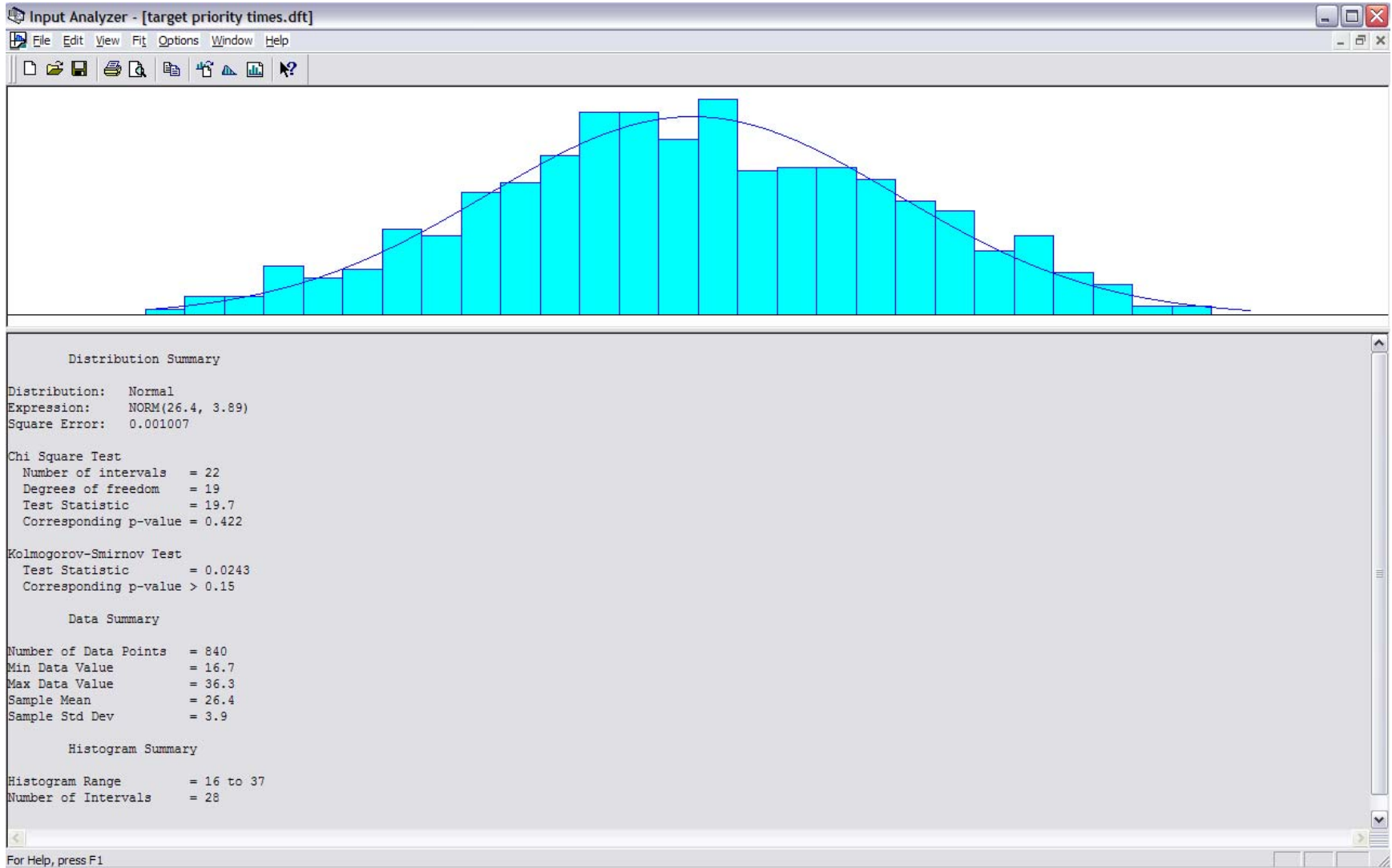


Figure 46. Input Analyzer Target Priority Times for Scenario 1

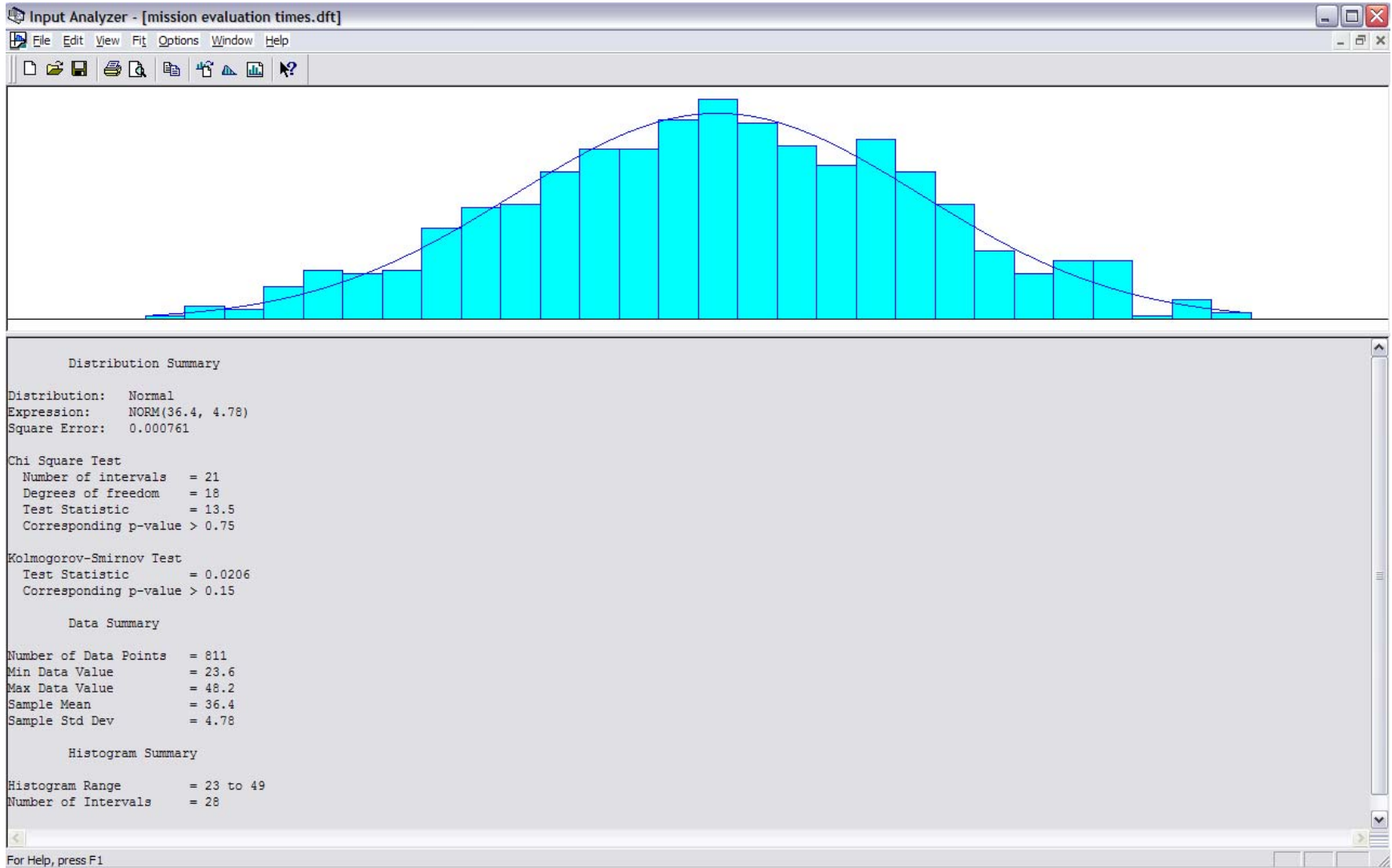


Figure 47. Input Analyzer Mission Evaluation Times for Scenario 1

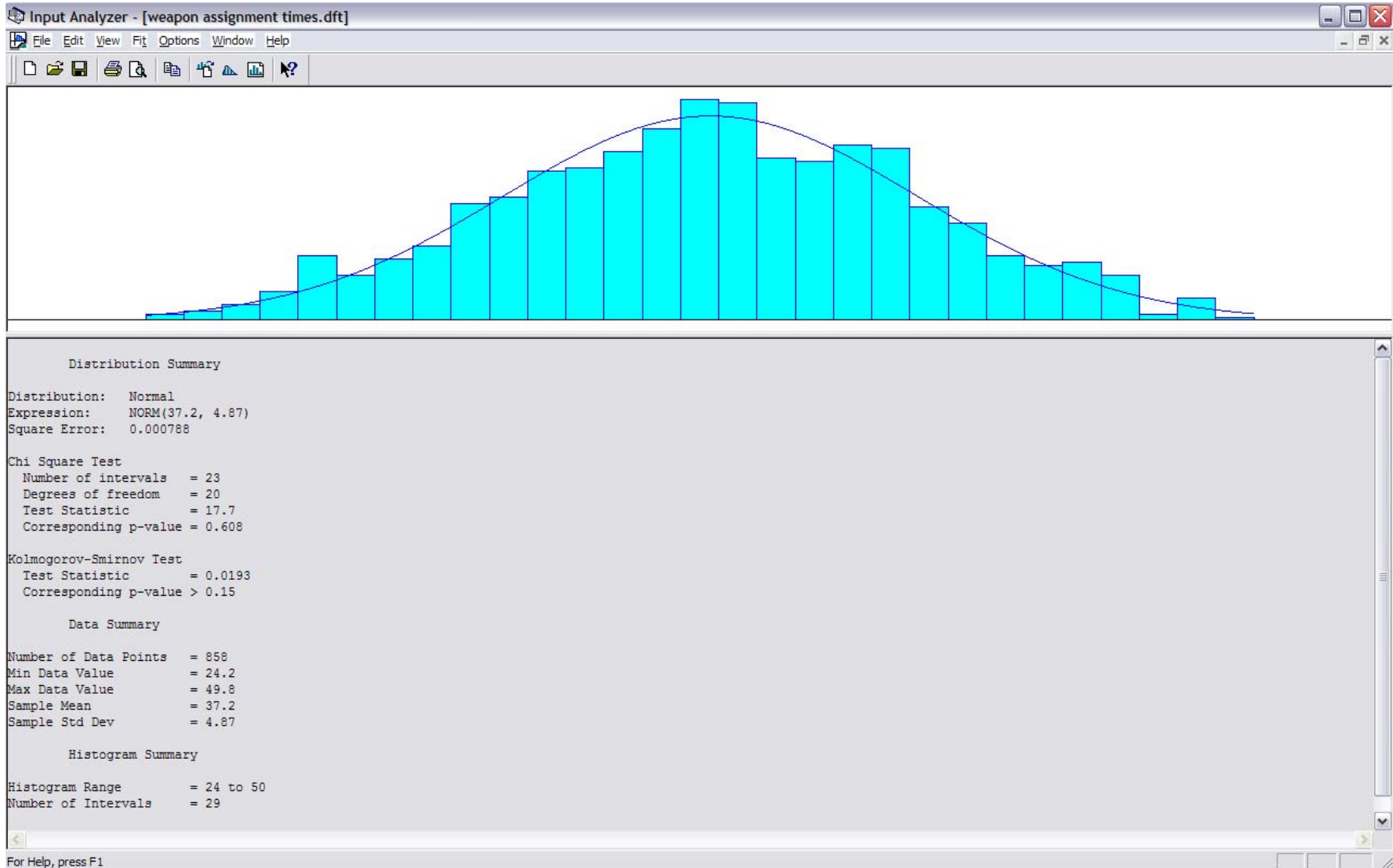


Figure 48. Input Analyzer Weapon Assignment Times for Scenario 1

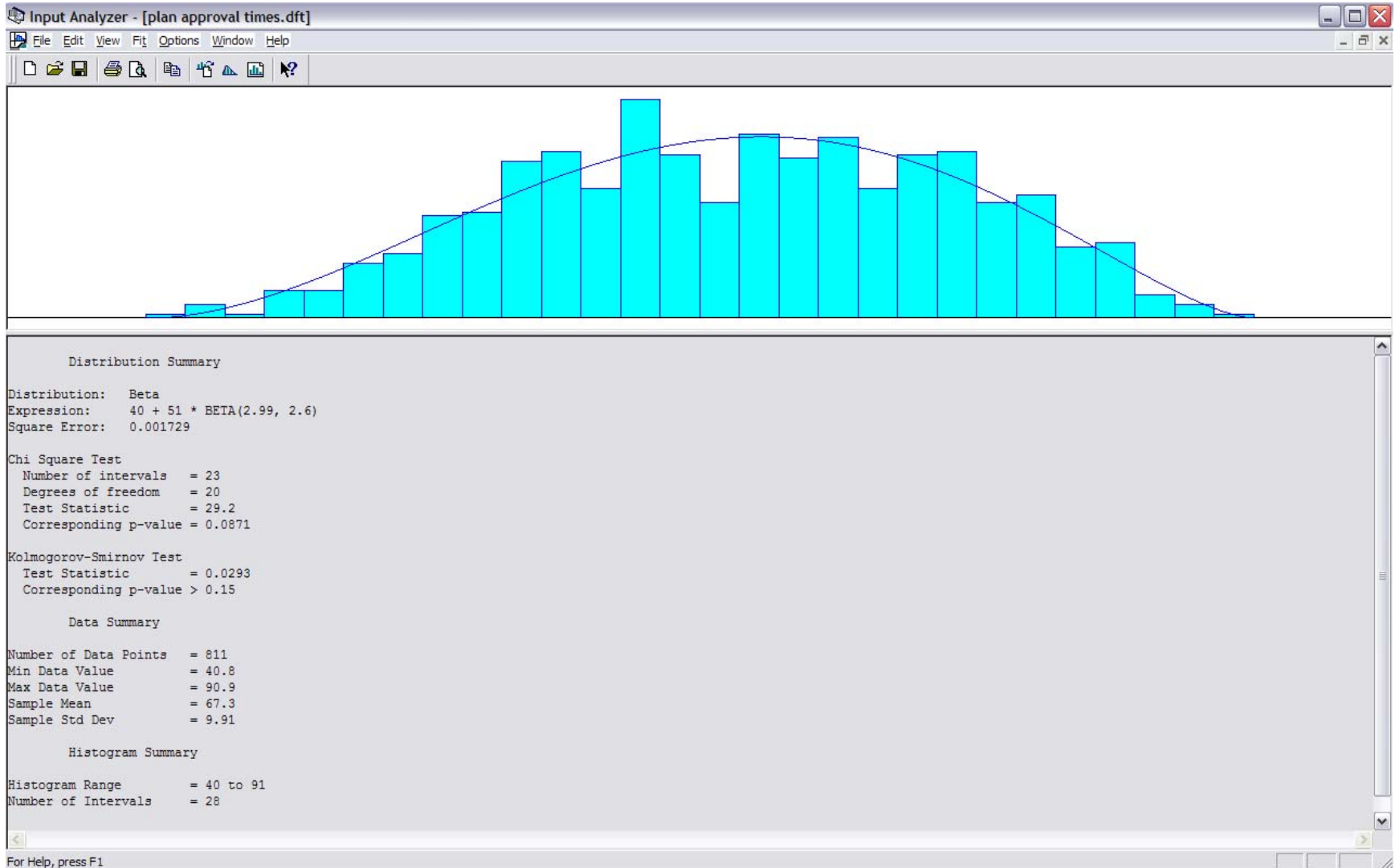


Figure 49. Input Analyzer Plan Approval Times for Scenario 1

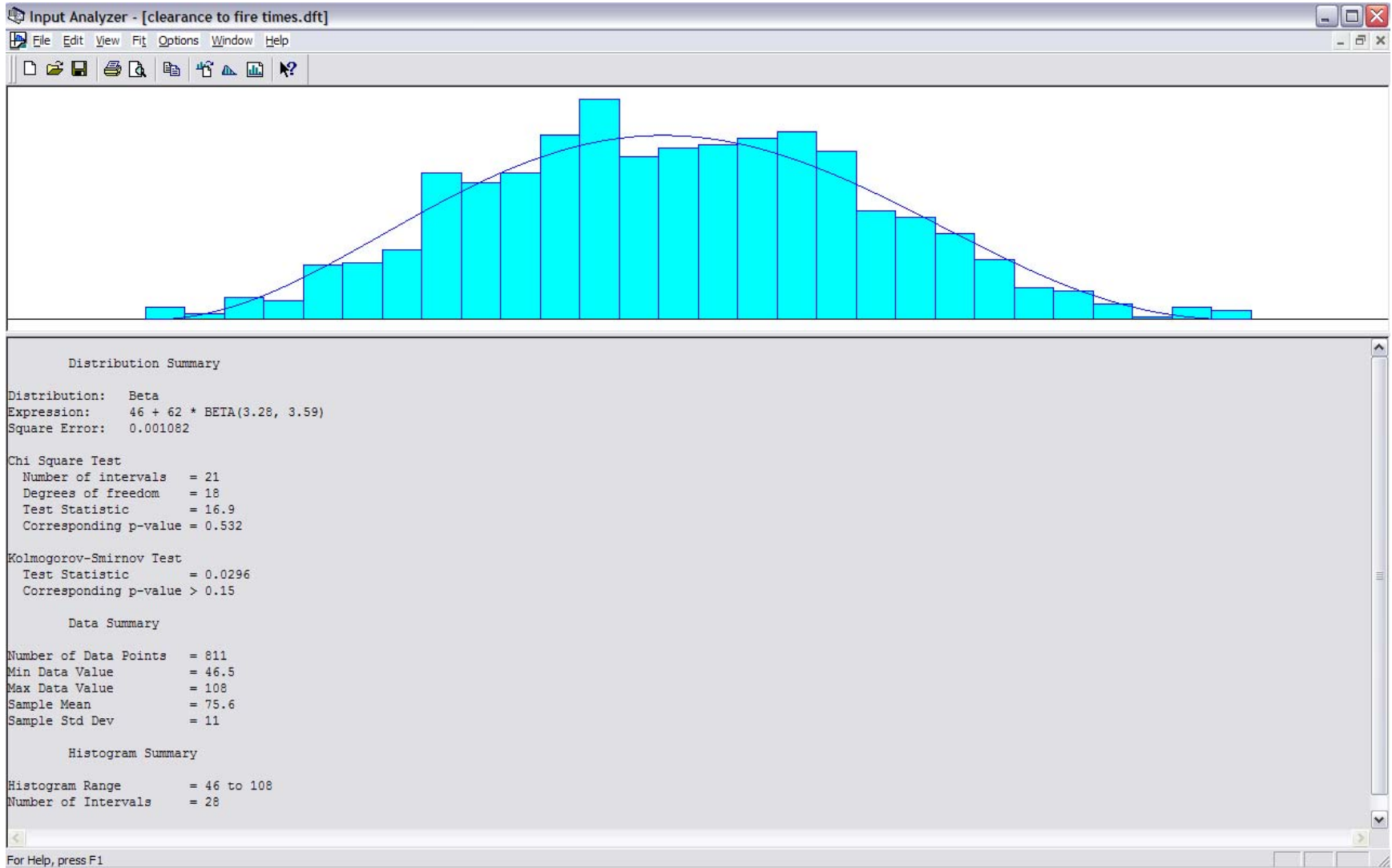


Figure 50. Input Analyzer Clearance to Fire Times for Scenario 1

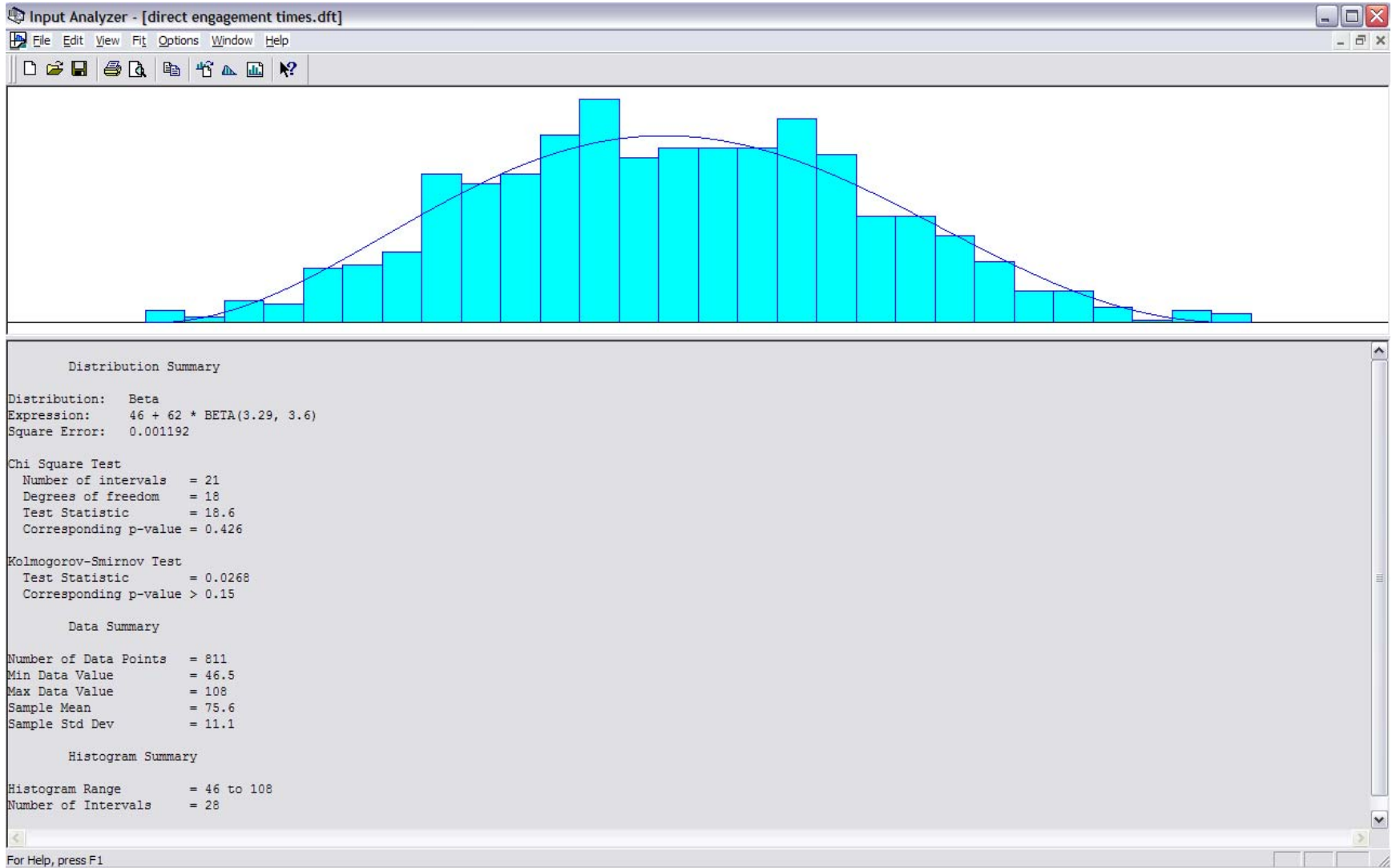


Figure 51. Input Analyzer Direct Engagement Times for Scenario 1



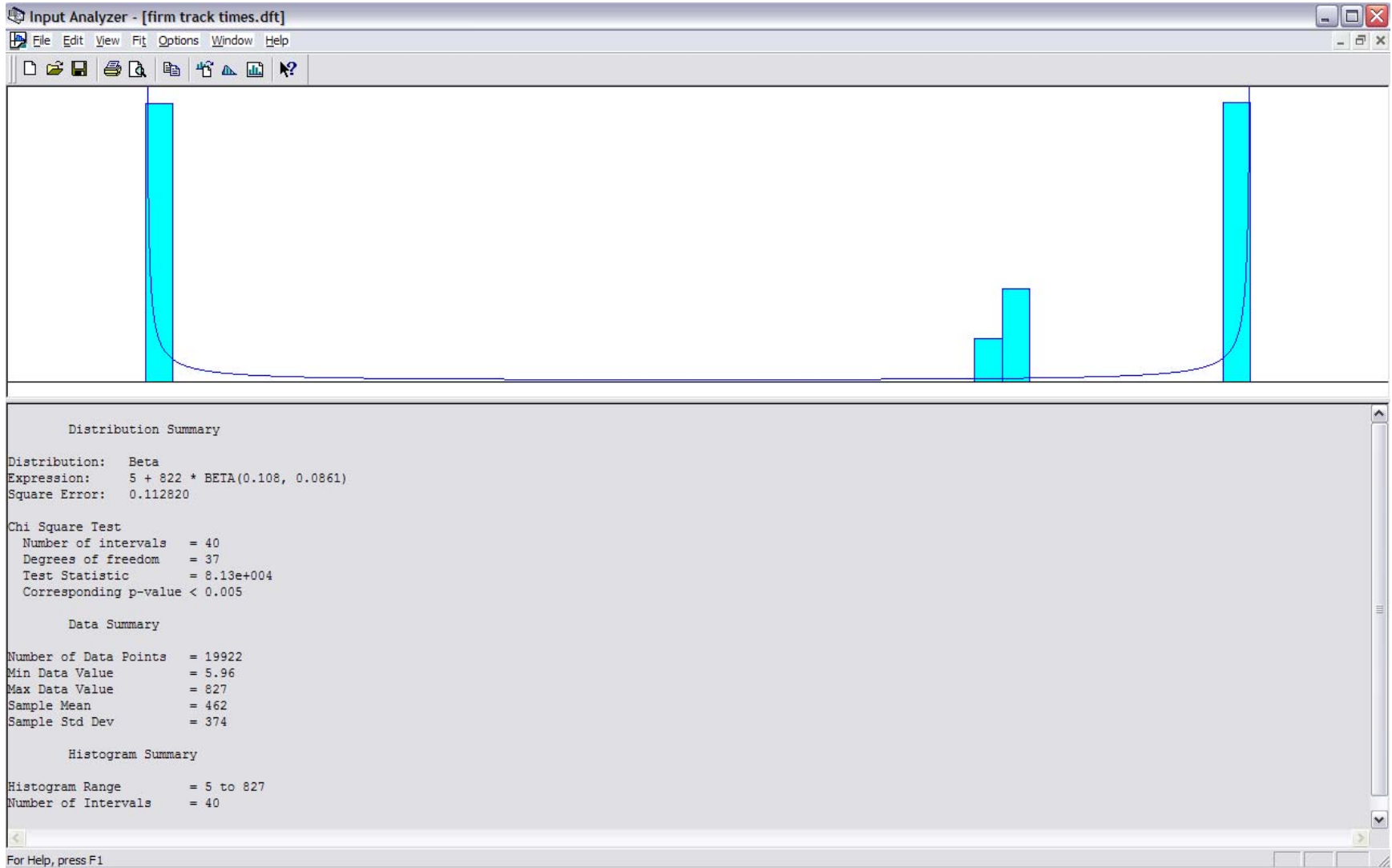


Figure 52. Input Analyzer Firm Track Times for Scenario 2

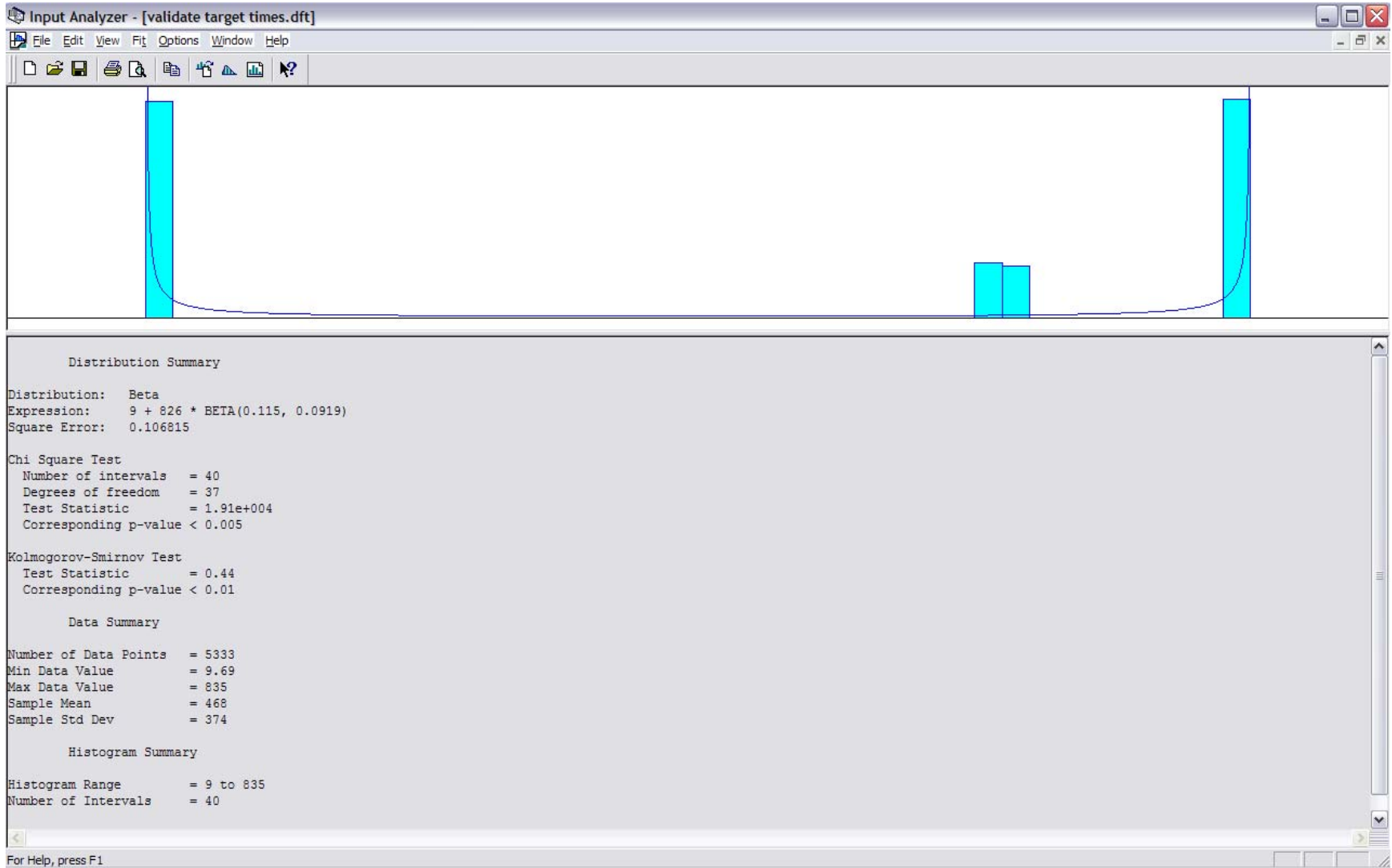


Figure 53. Input Analyzer Validate Target Times for Scenario 2

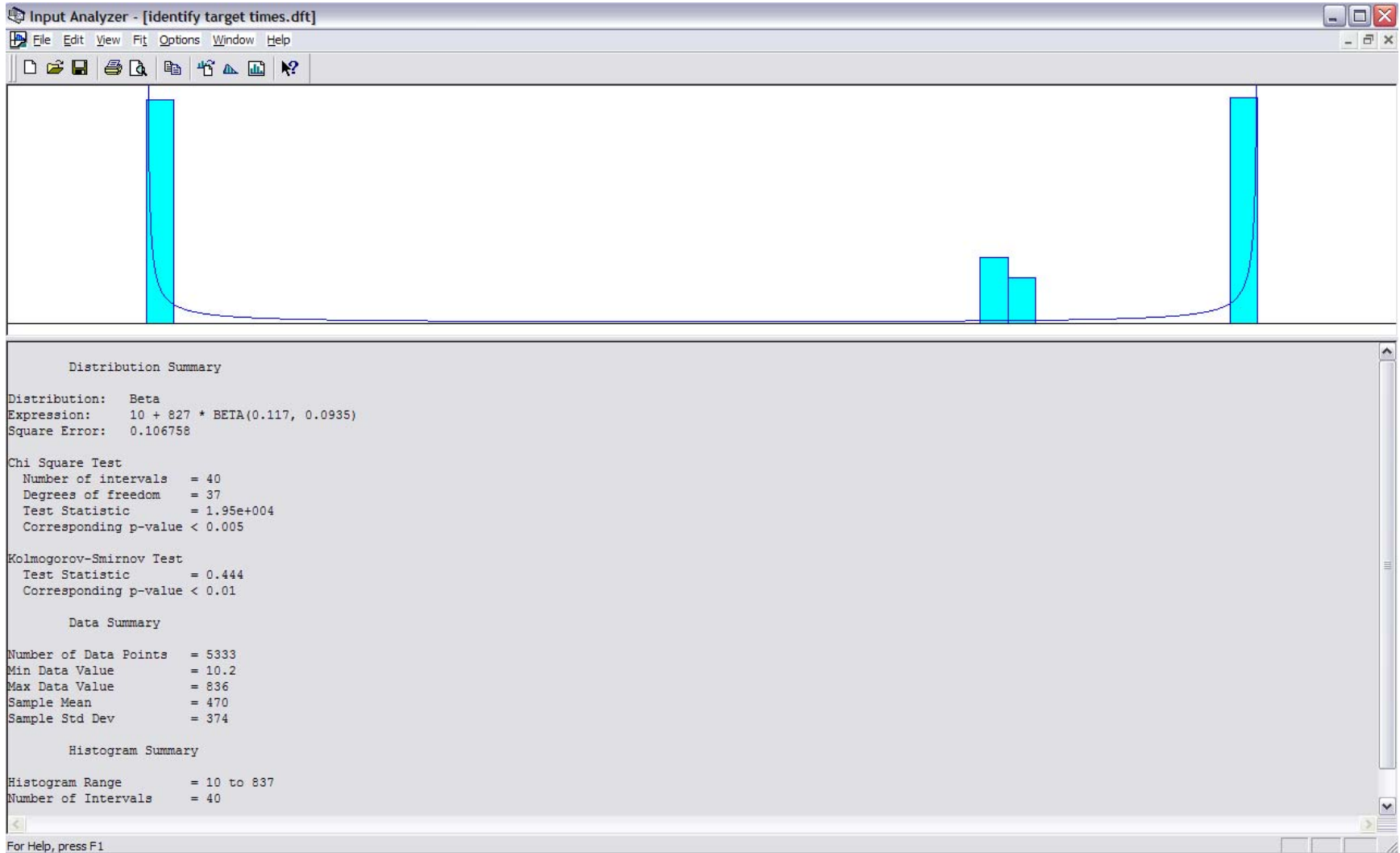


Figure 54. Input Analyzer Identify Target Times for Scenario 2



Figure 55. Input Analyzer Threat Evaluation Times for Scenario 2

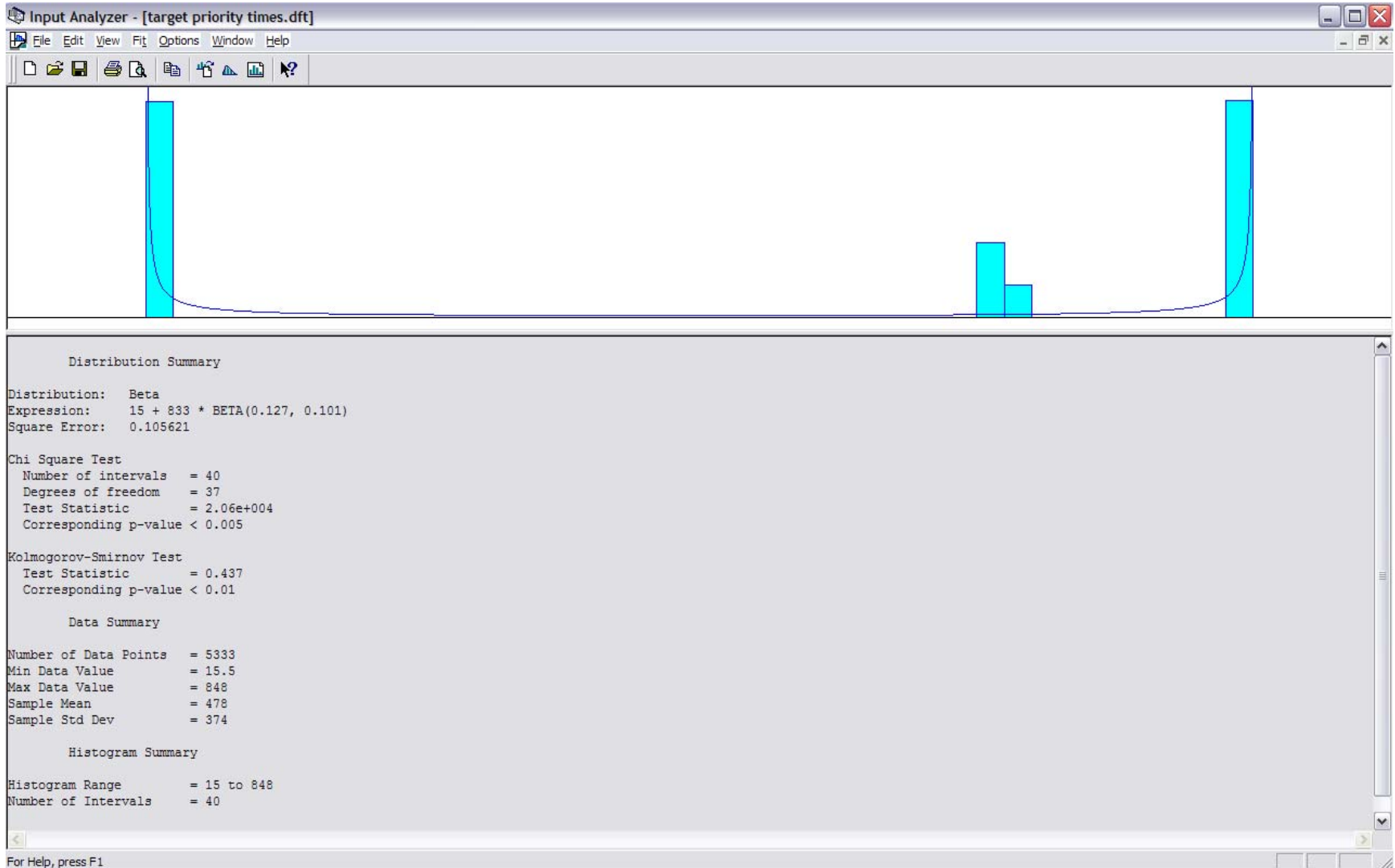


Figure 56. Input Analyzer Target Priority Times for Scenario 2

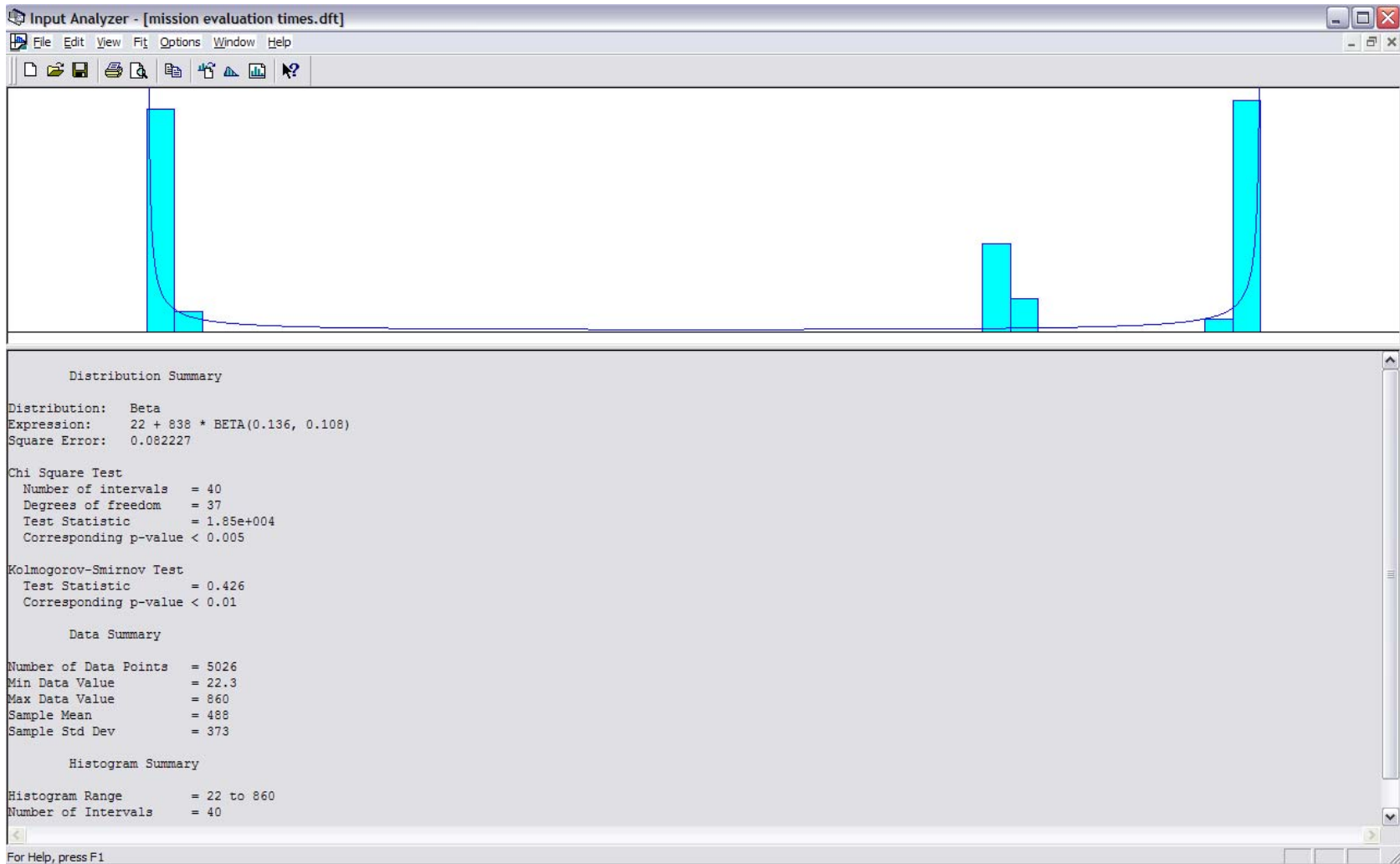


Figure 57. Input Analyzer Mission Evaluation Times for Scenario 2

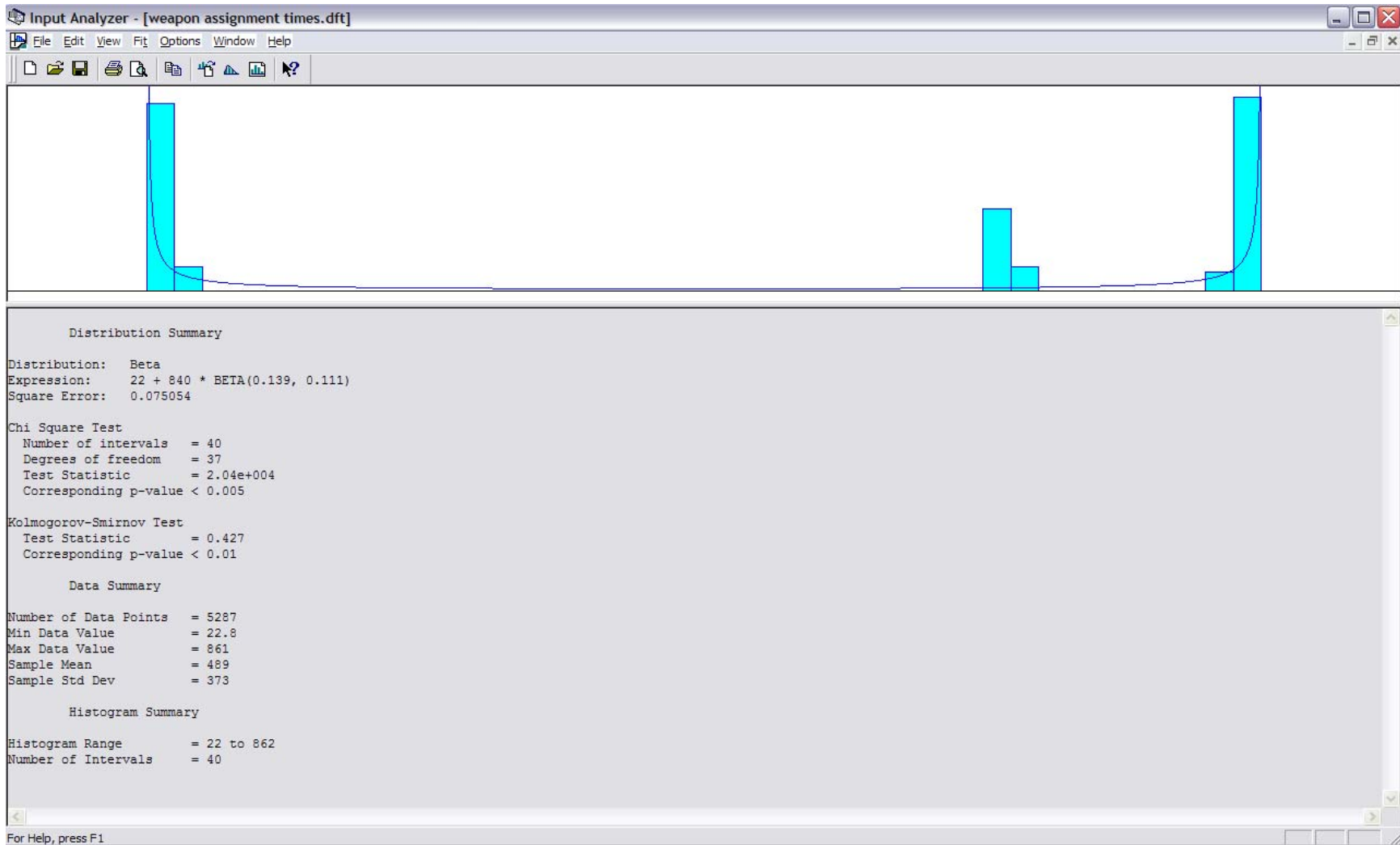


Figure 58. Input Analyzer Weapon Assignment Times for Scenario 2

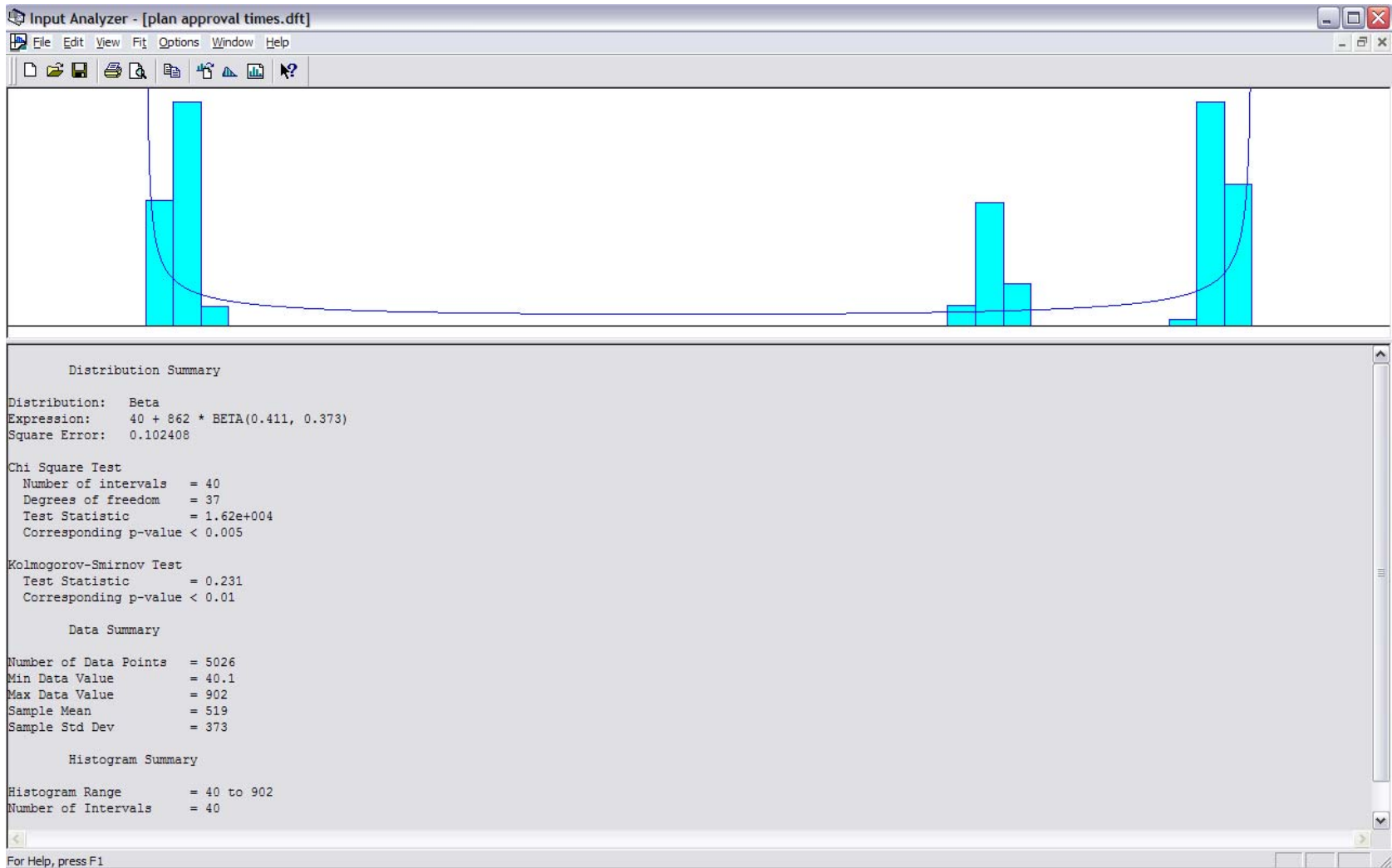


Figure 59. Input Analyzer Plan Approval Times for Scenario 2



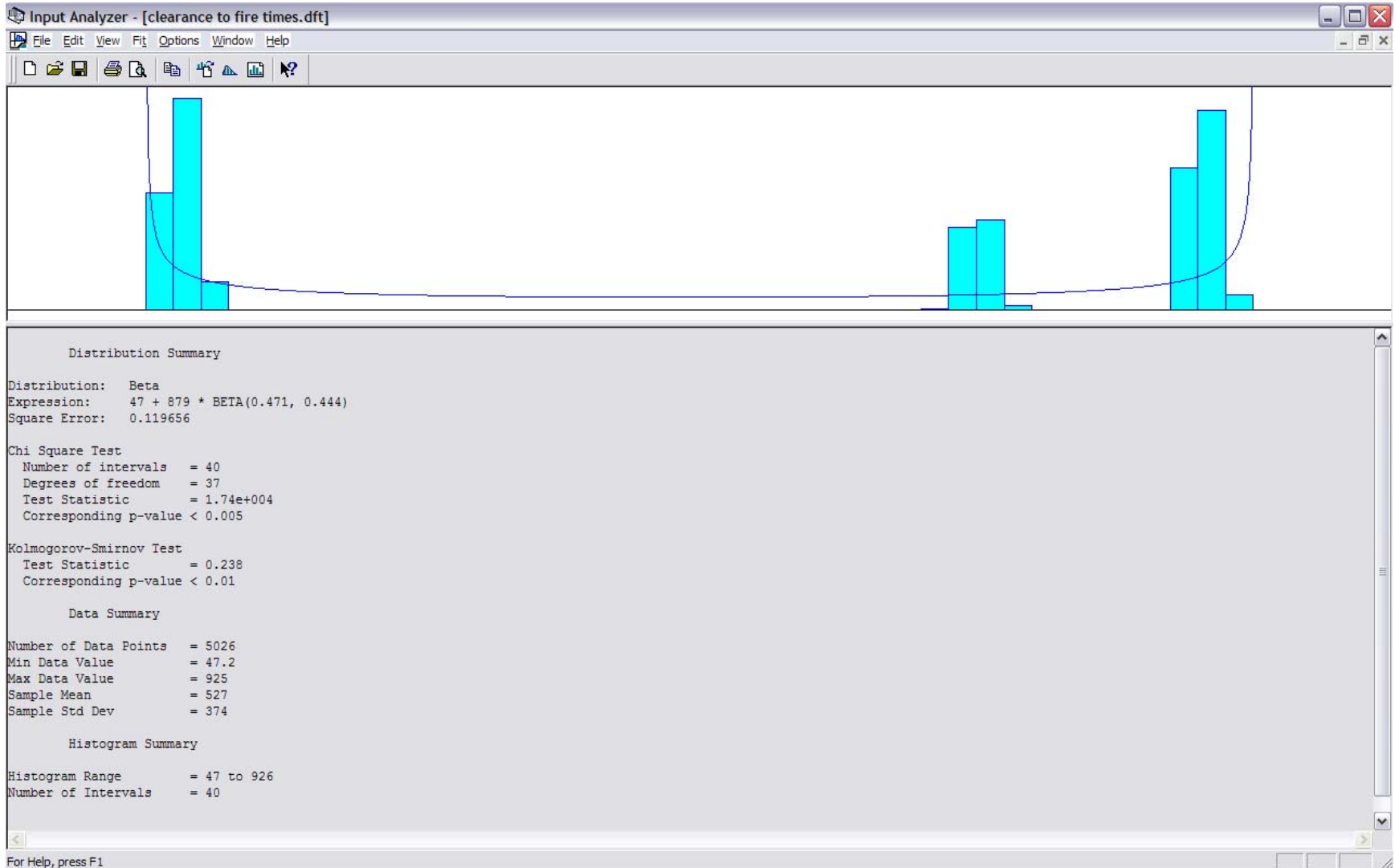


Figure 60. Input Analyzer Clearance to Fire Times for Scenario 2

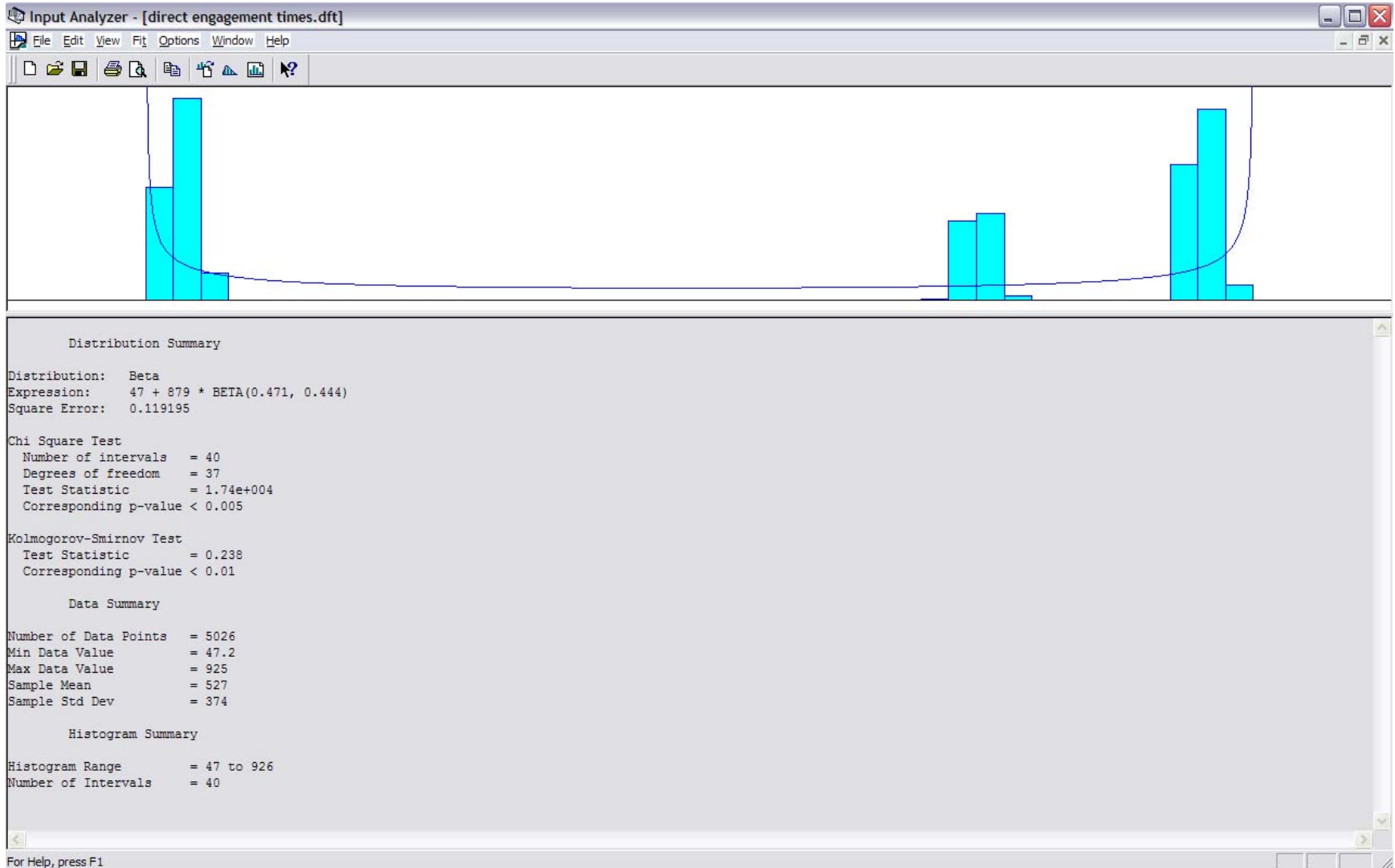


Figure 61. Input Analyzer Direct Engagement Times for Scenario 2

## APPENDIX III: RADAR MODEL DETAILED EXPLANATION OF CALCULATIONS

### PURPOSE OF THE RADAR MODEL

The intent of the radar model is to simulate a modern surface search sensor. It provides the OA model associated ranges given the probability of detection ( $P_D$ ) and radar cross section (RCS). Furthermore, it plays a pinnacle role in the Search and Detect portion of the OATCTEPM.

### RADAR MODEL ASSUMPTIONS

The assumptions applied to the creation of this model are listed below in table 26.

1	Assume all ideal environmental conditions
2	Assume no electronic interferences
3	Assume no radar losses
4	Assume all targets with a RCS greater than one to be considered a firm track which equates to a $P_D$ equal to ninety percent at a range of 21.96 NM. This is determined from the following calculation: $R_{NM} = 1.23(\sqrt{h_{RADAR}} + \sqrt{h_{TARGET}}) = 1.23*(\sqrt{133 \text{ ft}} + \sqrt{40 \text{ ft}}) = 21.96 \text{ NM}$

Table 26. Radar Model Assumptions

## DESIGN OF THE RADAR MODEL

This basic model has been designed using a range relationship taken from *Principles of Naval Weapons Systems* (Payne 2006). The relationship allows for a target range to be determined if the target's RCS is known and a previous RCS with range can be provided. The algebraic form of this equation, EQ(1), can be viewed below and the variables are defined as follows:

- $R_1$  is the known range of a target
- $R_2$  is the unknown range
- $\sigma_1$  is the known RCS of a target
- $\sigma_2$  is the known RCS of a target with unknown range

$$R_2 = \sqrt[4]{\frac{\sigma_2}{\sigma_1}} * R_1 \quad \text{EQ(1)}$$

In order to facilitate the efforts of this model, ranges for a particular RCS had to be created with a specific set of signal to noise ratios (S/N). The S/Ns required were extracted from a set of Rice curves printed in *Radar Principles for the Non-Specialist* (Toomay 1998). These S/Ns were chosen for a set of  $P_D$  s being used for this model along with a value for a probability of false alarm ( $P_{FA}$ ) of  $10^{-6}$ . In addition, the required RCS and known range information was found in *The Naval Institute Guide to World Naval Weapon Systems* (Friedman 2006). These values were then substituted into EQ(2) to calculate a set of ranges for a series of cross sections. The baseline values used for this model are for a RCS of  $1 m^2$  and maximum range of detection, which is associated to a  $P_D$  equal to fifty percent, of forty thousand yards. Furthermore, a description of variables from EQ(2) is provided below:

- $R_{RCS=1}$  is the range to be determined
- $R_1$  is the known range of a target
- $S / N_{P_D}$  is the signal to noise ratio for the probability of detection for  $R_1$

- $S / N_{P_{D2}}$  is the signal to noise ratio for the probability of detection for  $R_{RCS=1}$

$$R_{RCS=1} = (10^{(LOG(R_1) + (S/N_{PD1} - S/N_{PD2}/40))}) \quad \text{EQ(2)}$$

After plugging the values into the EQ(2) and performing a set of calculations, a series of ranges were computed. These ranges for a RCS of  $1 m^2$  were created for a set of  $P_D$  s that began at .50 and incrementally increased by a value of .05 to a maximum of .90. The results of this equation are listed in table 27, Ranges (m) for a RCS of  $1 m^2$ .

Pd	S/N	Range (m)
90	13.5	32225.3
85	13	33166.3
80	12.8	33647.1
75	12.5	34134.8
70	12.3	34530
65	12	35131.5
60	11.8	35538.3
55	11.5	36157.4
50	11.3	36576.1

Table 27. Ranges (m) for a RCS of  $1 m^2$

The results presented in table 27 were then substituted back into EQ(1) and used to determine ranges for targets of known RCSs. These RCSs that were determined by this method hold values of  $.1 m^2$  and  $.5 m^2$  and can be viewed in table 28 Radar Range (m) as a Function of RCS ( $m^2$ ) for given  $P_D$ .

$P_D$	RCS = $.1 m^2$	RCS = $.5 m^2$	RCS = $1 m^2$
.9	15238.41	27098.15	32225.3
.85	15683.38	27889.43	33166.3
.80	15910.71	28293.69	33647.1
.75	16141.34	28703.81	34134.8
.70	16328.25	29036.19	34530.0
.65	16612.68	29541.98	35131.5
.60	16805.04	29884.06	35538.3
.55	17097.77	30404.62	36157.4
.50	17295.76	30756.69	36576.1

Table 28. Radar Range (m) as a Function of RCS ( $m^2$ ) for given  $P_D$

## **APPENDIX IV: IMPROVED MODEL STUDY**

### **A. INTRODUCTION**

This appendix provides the outputs of the improved model. Research in decision aides and automation as well as meetings with the stake holder resulted in numerous runs of the improved model. The key human interaction times identified in the analysis of the base model (Plan Approval, Mission Evaluation and Threat Evaluation) were improved in 5 percent increments up to the maximum of 30 percent. The outputs of all six runs of the improved model for each scenario are provided below. This data was utilized to make the final decision on the appropriate level of reduction to be applied for the improved model presented in Section V: Results and Analysis.

### **B. SCENARIO 1 OUTPUT**

Figures 62-65 illustrate the 95 percent confidence intervals for the average value of the number of leakers, number of targets, C<sup>3</sup> time and the Probability of Raid Annihilation observed in the base case and all six improved cases. These confidence intervals were generated using Arena's Output Analyzer.

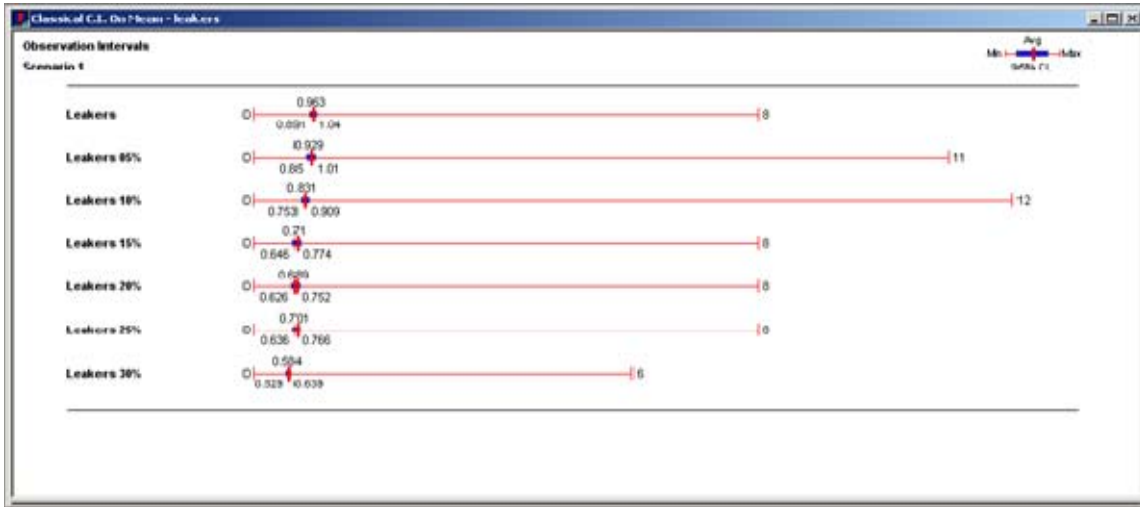


Figure 62. Average Number of Leakers per Improved Model

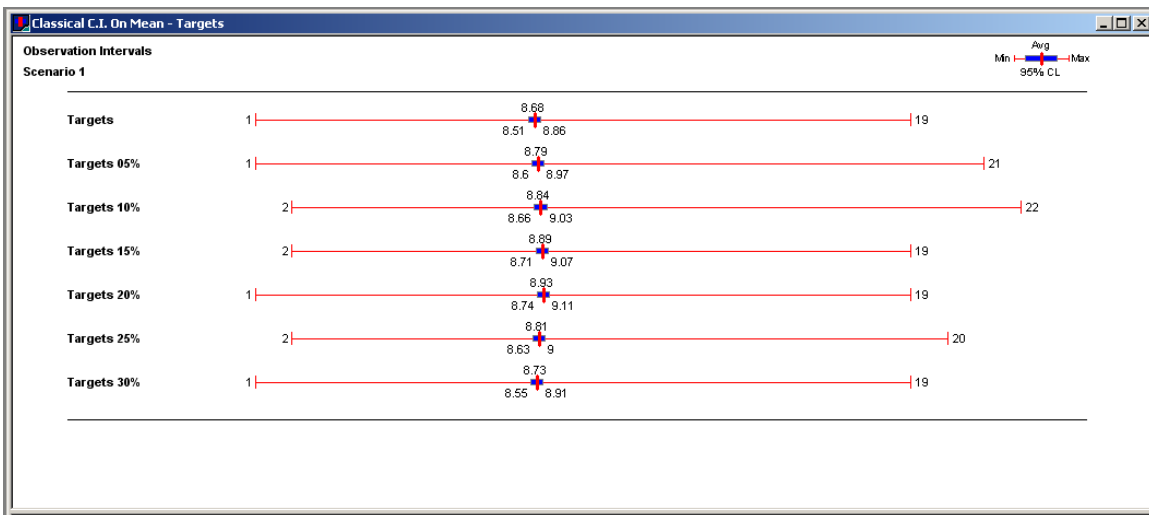


Figure 63. Average Number of Targets per Improved Model



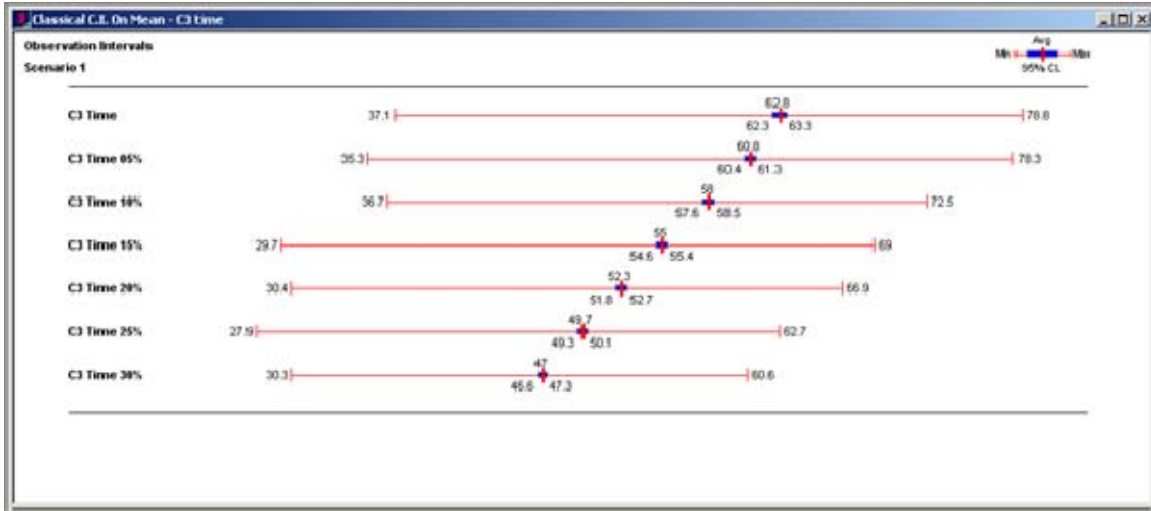


Figure 64. Average C<sup>3</sup> Time per Improved Model

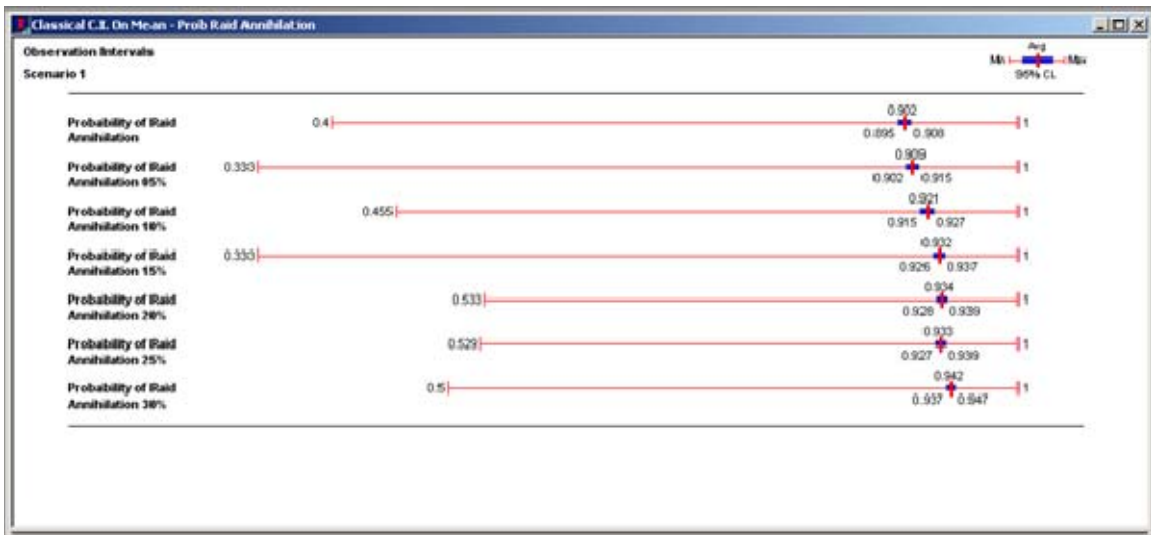


Figure 65. Average Probability of Raid Annihilation per Improved Model

Figure 66 illustrate the output from Arena's Process Analyzer (PAN). The PAN generates a quick overview of all the results in an easy to read table. The table displays the model cases that were run, the number of replications, the control variables that were adjusted and the average values for the key outputs. PAN also recommends the best case scenario based on whether the smallest or largest output of a response is desired.

Scenario Properties				Controls						Responses				
SI	Name	Program File	Reps	Validate Target Min	Validate Target Max	Mission Evaluation Min	Mission Evaluation	Plan Approval Min	Plan Approval Max	Targets	Leakers	C3 Time	Probability of Leakers	Probability of Raid
1	Base Case	6 - OA.TCT.P	1000	2.00	3.00	5.00	15.00	15.00	45.00	8.926	1.086	63.835	0.105	0.095
2	Improved Case-5%	6 - OA.TCT.P	1000	1.90	2.85	4.75	14.25	14.25	42.75	8.735	0.882	60.806	0.087	0.013
3	Improved Case 10%	6 - OA.TCT.P	1000	1.80	2.70	4.50	13.50	13.50	40.50	8.809	0.794	57.947	0.077	0.023
4	Improved Case 15%	6 - OA.TCT.P	1000	1.70	2.55	4.25	12.75	12.75	38.25	8.880	0.767	55.315	0.075	0.025
5	Improved Case 20%	6 - OA.TCT.P	1000	1.60	2.40	4.00	12.00	12.00	36.00	8.931	0.707	52.208	0.068	0.032
6	Improved Case 25%	6 - OA.TCT.P	1000	1.50	2.25	3.75	11.25	11.25	33.75	8.889	0.650	49.634	0.063	0.037
7	Improved Case 30%	6 - OA.TCT.P	1000	1.40	2.10	3.50	10.50	10.50	31.50	8.914	0.593	46.856	0.057	0.043

Figure 66. PAN Results for Scenario 1

There are slight variations in values provided from Arena's Output Analyzer and PAN. The variation can be attributed to the different strings being used by the random number generator within each analysis. The 30 percent case was recommended as the best option for the improved model based on the fact that it has the lowest average number of leakers (0.583), the lowest  $C^3$  time and the highest  $P_{RA}$ . PAN was unable to recommend a second option so the 95 percent confidence interval figures were used to make this determination. The next best option is the 20 percent model based on the fact that it has the second lowest average number of leakers (0.689) which equates to the second highest  $P_{RA}$  and it has the third lowest  $C^3$  time. The fact that the confidence intervals are smaller and fall within the intervals of the 25 percent case were also determining factors.

### C. SCENARIO 2 OUTPUT

Figures 67-70 illustrate the 95 percent confidence intervals for the average value of the number of leakers, number of targets,  $C^3$  time and the Probability of Raid Annihilation observed in the base case and all six improved cases. These confidence intervals were generated using Arena's Output Analyzer.

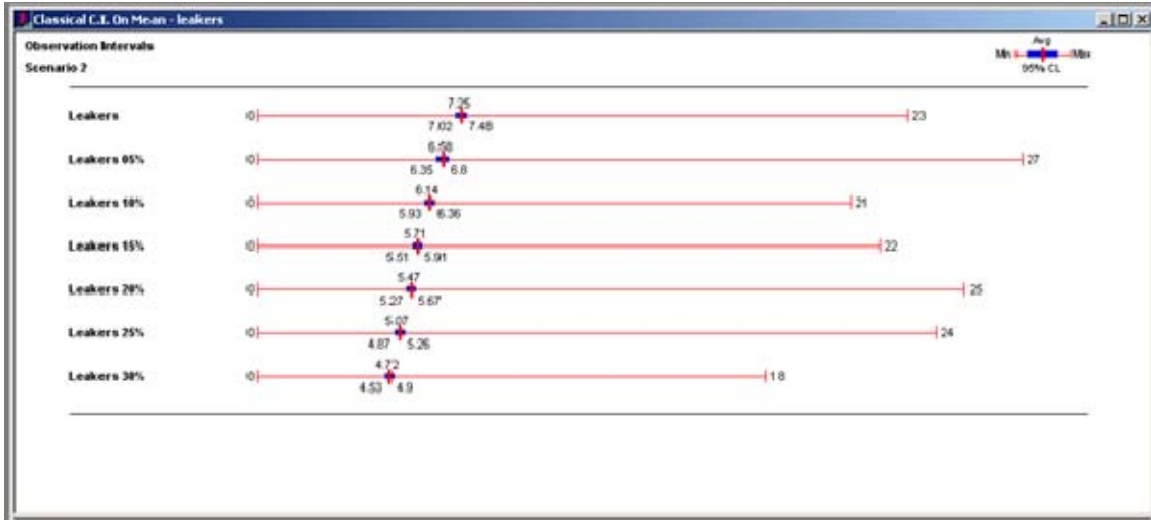


Figure 67. Average Number of Leakers per Improved Model

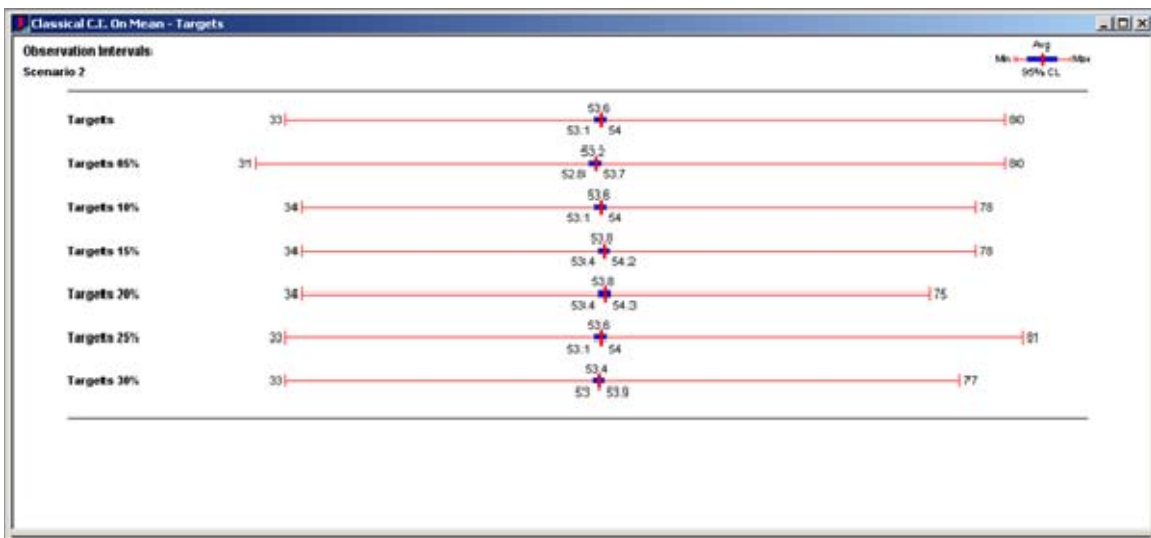


Figure 68. Average Number of Targets per Improved Model

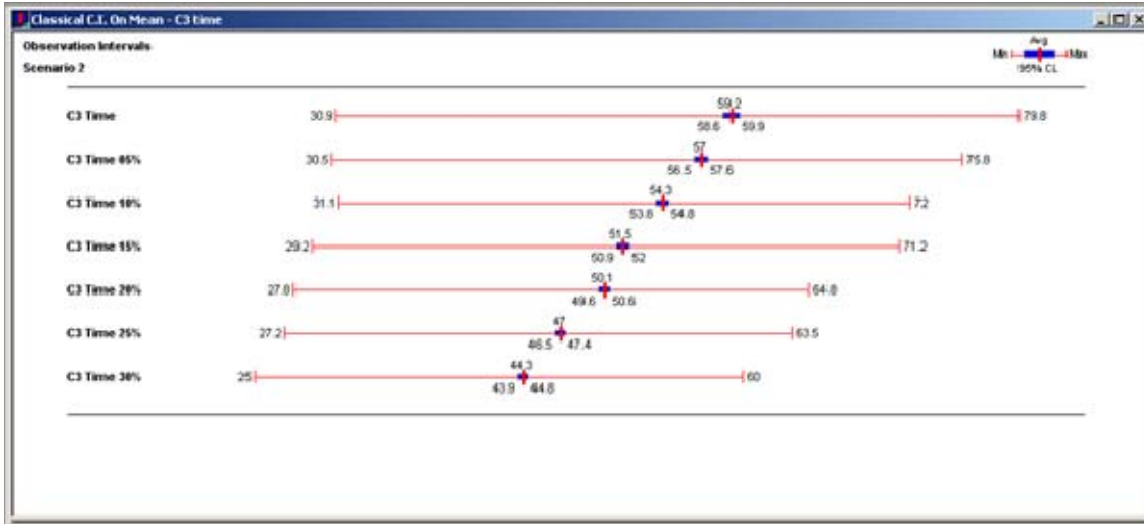


Figure 69. Average C<sup>3</sup> Time per Improved Model

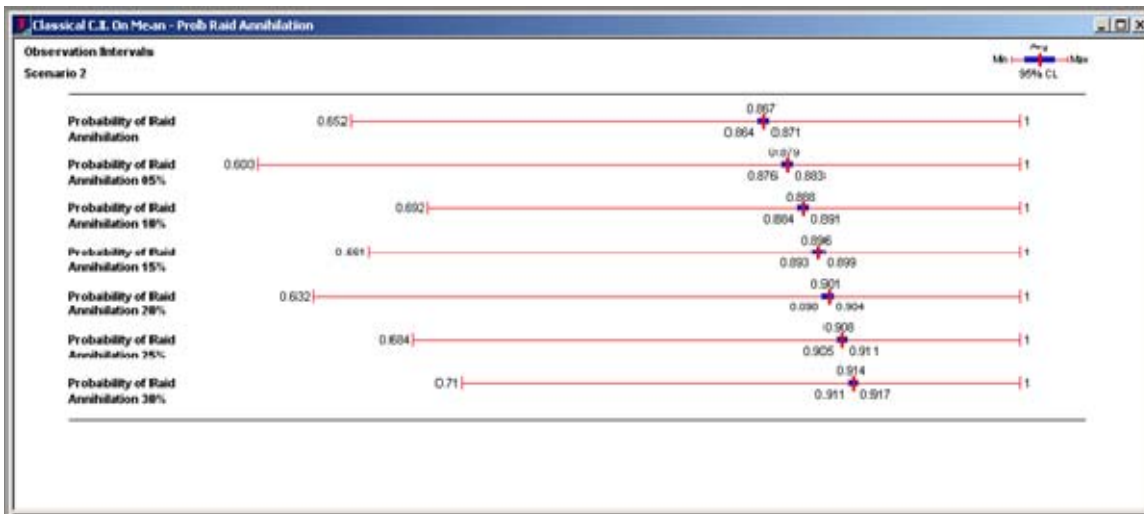


Figure 70. Average Probability of Raid Annihilation per Improved Model

Figure 71 illustrates the output from Arena's Process Analyzer (PAN). The PAN generates a quick overview of all the results in an easy to read table. The table displays the model cases that were run, the number of replications, the control variables that were adjusted and the average values for the key outputs. PAN also recommends the best case scenario based on whether the smallest or largest output of a response is desired.

SI	Scenario Properties			Controls						Responses				
	Name	Program File	Reps	Validate Target Min	Validate Target Max	Mission Evaluation Min	Mission Evaluation	Plan Approval Min	Plan Approval Max	Targets	Leakers	C3 Time	Probability of Leakers	Probability of Fail
1	Base Case	3-OA.TCT.P	1000	2.00	3.00	5.00	15.00	15.00	45.00	53.552	7.252	59.247	0.133	0.867
2	Improved Case 5%	3-OA.TCT.P	1000	1.90	2.85	4.75	14.25	14.25	42.75	53.218	6.576	57.030	0.121	0.879
3	Improved Case 10%	3-OA.TCT.P	1000	1.80	2.70	4.50	13.50	13.50	40.50	53.558	6.144	54.288	0.112	0.888
4	Improved Case 15%	3-OA.TCT.P	1000	1.70	2.55	4.25	12.75	12.75	38.25	53.789	5.712	51.468	0.104	0.896
5	Improved Case 20%	3-OA.TCT.P	1000	1.60	2.40	4.00	12.00	12.00	36.00	53.842	5.468	50.085	0.099	0.901
6	Improved Case 25%	3-OA.TCT.P	1000	1.50	2.25	3.75	11.25	11.25	33.75	53.952	5.068	48.954	0.092	0.908
7	Improved Case 30%	3-OA.TCT.P	1000	1.40	2.10	3.50	10.50	10.50	31.50	53.423	4.718	44.320	0.086	0.914

Figure 71. PAN Results for Scenario 2

There are slight variations in values provided from Arena's Output Analyzer and PAN. The variation can be attributed to the different strings being used by the random number generator within each analysis. The 30 percent case was recommended as the best option for the improved model based on the fact that it has the lowest average number of leakers (4.718), the lowest  $C^3$  time and the highest  $P_{RA}$ . PAN was unable to recommend a second option so the 95 percent confidence interval figures were used to make this determination. The next best option is the 25 percent model based on the fact that it has the second lowest average number of leakers (5.068) which equates to the second highest  $P_{RA}$  and it has the third lowest  $C^3$  time.

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS

AT3	Advanced Tactical Targeting Technology
AMSTE	Affordable Moving Surface Target Engagement
ATO	Air Tasking Order
AMW	Amphibious Warfare
MW	Mine Warfare
AAW	Anti-Air Warfare
ADW	Air Defense Warfare
ASW	Anti-Submarine Warfare
ASUW	Anti-Surface Warfare
BATGRU	Battle Group
BF	Battle Force
BG	Battle Group
BIT	Built-In Test
CIWS	Close-In Weapons System
C2	Command and Control
C2W	Command and Control Warfare
C <sup>3</sup>	Command, Control, and Communication
ACC	Commander, Air Combat Command
COA	Common Operating Area
CS	Common Services
CS	Common Services
DX/DR	Data Extraction/Data Reduction
CONOP	Concept of Operation
COTS	Consumer Off the Shelf
CUs	Cooperating Units
CEC	Cooperative Engagement Capability
DIS	Data / Information Services
dBm <sup>2</sup>	Decibel-meter squared
DAU	Defense Acquisition University's web site
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
DCE	Detect Control Engage
DCE	Detect, Control, and Engage
DoDD	DoD Directive
ES	Electronic Warfare Support
EO	Electro-optical

EQ	Equation
EPS	Expeditionary Pervasive Sensing
EXCOMM	External Communication
FAC	Fast Attack Craft
FAB-T	Family of Beyond Line-of-sight Terminals
FIAC	Fast Inshore Attack Craft
FPB	Fast Patrol Boat
FD/FI	Fault Detection / Fault Isolation
Ft	Feet
FP/C	Force Planning / Coordination
GIG-BE	GIG-Bandwidth Expansion
GIG	Global Information Grid
GPS	Global Positioning System
GAO	Government Accountability Office
GWS	Gun Weapons System
HE	High Explosives
HVU	High Value Unit
HM&E	Hull, Mechanical & Electrical
HUMINT	Human intelligence
IFF	Identification Friend-or-foe
IED	Improvised Explosive Devices
INS	Inertial Navigation Systems
IA	Information Assurance
IR	Infrared
IFC	Integrated Fire Control
INTEL	Intelligence
JDL	Joint Directors of Laboratories
JITC	Joint Interoperability Test Command
JROC	Joint Requirements Oversight Council
JTDLMP	Joint Tactical Data Link Management Plan
JTF	Joint Task Force
Km	Kilometers
LAN	Local Area Network
MCCDC	Marine Corps Combat Development Command
MTTR	Mean-Time-To-Repair
MOEs	Measures of Effectiveness
MOPs	Measures of Performance
m	Meters
ME	Mission Execution
MOSA	Modular Open System Approach



NDC	Naval Doctrine Command
NSA	National Security Agency
NM	Nautical Mile
NSW	Naval Special Warfare
NWDC	Naval Warfare Development Command
NAV	Navigation
NRT	Near Real Time
NCW	Network Centric Warfare
OODA	Observe, Orient, Decide and Act
ONR	Office of Naval Research
OA	Open Architecture
OAAM	Open Architecture Assessment Model
OACE	Open Architecture Computing Environment
OATCTEPM	Open Architecture Time Critical Target Engagement Process Model
OAWSDM	Open Architecture Warfare System Domain Model
OSJTF	Open Systems Joint Task Force
Ao	Operational Availability
OV	Operational View
OSS	Optical Sighting System
OASIS	Organization for the Advancement of Structured Information Standards
PAD	Planning, Assessment & Decision
PTTI	Precise Time and Time Interval
PAM	Precision Attack Missile
Pd	Probability of Detection
Pfa	Probability of False Alarm
PMG	Program Managers Guide
R	Range
RCS	Radar cross section
RT	Real time
REDS	Real Time Execution Decision Support
RV	Remotely Controlled Vehicle
RPG	Rocket Propelled Grenade
ROE	Rules of Engagement
S/D	Search / Detect
SOA	Service Oriented Architecture
SEDP	System Engineering Design Process
S/N	Signal to Noise
SIAP/SIGP	Single Integrated Air or Ground Picture
SIAP	Single Integrated Air Picture

SPO	Special Projects Office
m2	Square Meters
SOW	Statement of work
STW	Strike Warfare
TAO	Tactical Action Officer
TADILs	Tactical Digital Information Links
TACSIT	Tactical Situation
TTNT	Tactical Targeting Network Technology
TTP	Techniques, and Procedures
TCT	Time Critical Targeting
TDMA	Time Demand Multiple Access
TR	Training
TRADOC	Training and Doctrine Command
TSAT	Transformational Satellite
TEL	Transporter erector-launcher
UN	United Nations
USN	United States Navy
USAF	United States Air Force
VLS	Vertical Launch system
W/AS	Weapon / Asset Services
WMD	Weapons of Mass Destruction

## LIST OF REFERENCES

- Adams C. Network Centric, Rush to Connect [homepage on the Internet]. Aviation Daily; 2005. [cited 2007 Mar. 11]. Available from:  
<http://integrator.hanscom.af.mil/2005/June/06162005/06162005-06.htm>.
- A Future Naval Capability: Time Critical Strike [homepage on the Internet]. Arlington (VA): Office of Naval Research (ONR); 2001. [cited 2007 June 10]. Available from: [http://www.onr.navy.mil/media/extra/fncs\\_fact\\_sheets/time\\_critical.pdf](http://www.onr.navy.mil/media/extra/fncs_fact_sheets/time_critical.pdf).
- Barkenhausen J. Quick Fv Overview. FORCENET Information Sharing; 2004 Aug. 29; n.d., 24 p.
- Bell M. FORCenet: The OPNAV View [presentation]. US Chief of Naval Operations (N61F); 2004 Sept. 21. 22 p.
- Boghammar Photo. [Internet Resource]. Accessed on 2007 April 20. Available at:  
<http://www.warboats.org/SBU13.htm>
- Brickner WK. An Analysis of the Kill Chain for Time-Critical Strike [dissertation]. Monterey (CA): Naval Postgraduate School; 2005 June. 127 p. ADA435726.
- Briggs JN. Target Detection by Marine Radar. London (UK): The Institution of Electrical Engineers; 2004. 705 p.
- Buede DM. The Engineering Design of Systems: Models and Methods. Hoboken (NJ): John Wiley & Sons, Inc; 2000. 488 p.
- C-14 Photo. [Internet Resource]. Accessed on 2007 April 20. Available at:  
<http://www.globalsecurity.org/military/world/china/pcfg-cat-pics.htm>
- C-701 Discussion. [Internet Resource]. Accessed on 2007 April 20. Available at:  
<http://www.globalsecurity.org/military/world/china/c-701.htm>

- Cohen D, Lapid R, Gur A. Analytical Methods, Measures of Effectiveness and Simulations. In: Naveh B, Lorber A, editors. Theater Ballistic Missile Defense. 192 volumes. Reston (VA): American Institute of Aeronautics and Astronautics, Inc.; 2001. Vol 192: 30 p. p.301-330
- DAU Webmaster. Naval Open Architecture [homepage on the Internet]. Fort Belvoir (VA): Defense Acquisition University; n.d. [cited 2007 Apr. 7]. Available from: <https://acc.dau.mil/oa>.
- Deerin V, Grates P, Hedge T, Martinez M, Mcarthy P, Pugh K, Radojkovic S. Open Architecture as an Enabler for FORCENet: Architectural Concepts and Models to Implement FORCENet [dissertation]. Monterey (CA): Naval Postgraduate School; 2006 Sept. 145 pages total.
- Defense Acquisition Guidebook. Washington D.C.: Defense Acquisition Policy Working Group; 2004 Apr.
- Defense Industry Daily. CEC: Cooperative Engagement for Fleet Defense (updated) [homepage on the Internet]. Defense Industry Daily; 2007 Mar. 12. [cited 2007 Apr. 4]. Available from: <http://www.defenseindustrydaily.com/2007/03/cec-cooperative-engagement-for-fleet-defense-updated/index.php>.
- Department of the Air Force (United States) The Joint Targeting Process and Procedures for Targeting Time-Critical Targets. Washington (DC): Air Land Sea Application Center; 1996 May. 196 p.
- Department of Defense (United States) Directive. DoDD-5000.1 ed. Defense Acquisition. Washington D.C.: Under Secretary of Defense, Acquisition Technology and Logistics; 2003 May 12.
- DoD Architecture Framework Version 1.5 Volume I: Definitions and Guidelines [homepage on the Internet]. Defense Information Systems Agency; 2007 Apr. 23. [cited 2007 Sept. 8]. Available from: [http://jitic.fhu.disa.mil/jitic\\_dri/pdfs/dodaf\\_v1v1.pdf](http://jitic.fhu.disa.mil/jitic_dri/pdfs/dodaf_v1v1.pdf).

Edwards MJ. Requirement for Open Architecture (OA). Department of the Navy: Office of the Chief of Naval Operations [DoN: CNO]: Memorandum; 2005 Dec. 23; Washington, DC: DoN: CNO.

Friedman T. The Naval Institute Guide to World Naval Weapon Systems. Annapolis: Naval Institute Press, 2006.

Future Naval Fires [homepage on the Internet]. Newport (RI): Navy Warfare Development Command; n.d. [cited 2007 Feb. 10]. Available from:  
[http://www.nwdc.navy.mil/Conops/Sea\\_Strike/NavalFires.aspx](http://www.nwdc.navy.mil/Conops/Sea_Strike/NavalFires.aspx).

Galligan D, Galdorisi G, Marland P. 10th ICCRTS\_Paper\_053 The Future of C2 Net Centric Maritime Warfare -- Countering a 'Swarm' of Fast Inshore Attack Craft. Defence Technology Agency, NZ -- SPAWAR Systems Center, US -- Defence and Science Tech Laboratory, UK: 10th International Command and Control Research and technology Symposium; 2005 Apr.; McLean (VA): International Command and Control Research and technology Symposium; 2005, 21 p.

Gardner G. Imagine...and act [home page on the Internet]. Arlington (VA): National Defense Industrial Association; 2005. [cited 2007 Mar. 25]. [about 29 screens]. Available from:  
[http://www.dtic.mil/ndia/2005precision\\_strike\\_peo/gardner.ppt#446,1,Imagine...and act](http://www.dtic.mil/ndia/2005precision_strike_peo/gardner.ppt#446,1,Imagine...and act).

Green M. Statement Of Work (SOW) - Open Architecture as an Enabler for FORCEnet: Task 2 - Time Critical Targeting. Monterey (CA): Naval Postgraduate School: Department of Systems Engineering; 2006.

Global Security Organization.hormuz\_80.gif. In: GlobalSecurity.org [discussion list on the Internet]. 2005 Apr. 27; 18 18 pm [cited 2007 Apr. 23]. [about 1 screens]. Available from:

[http://www.globalsecurity.org/military/world/iran/images/hormuz\\_80.gif](http://www.globalsecurity.org/military/world/iran/images/hormuz_80.gif)

GlobalSecurity.org. [discussion list on the Internet]. Cited 2007 May 21. [about 1 screen]. Available from: <http://www.globalsecurity.org/military/world/china/c-701.htm>

- Hannan M. Defense US Air Force [photo on the Internet]. Riverside (CA): Defense Visual Information Center; 2002 Apr. 28. [cited 2007 June 2]. Available from: [http://www.dodmedia.osd.mil/DVIC\\_View/Still\\_Details.cfm?SDAN=DFSD0405184&JPGPath=/Assets/Still/2004/Air\\_Force/DF-SD-04-05184.JPG](http://www.dodmedia.osd.mil/DVIC_View/Still_Details.cfm?SDAN=DFSD0405184&JPGPath=/Assets/Still/2004/Air_Force/DF-SD-04-05184.JPG).
- Hatley D, Hruschka P, Pirbhai I. Process for System Architecture. New York: Dorset House Publishing Co. Inc., 2000.
- Hayes, Bradd C. Naval Rules of Engagement: Management Tools for Crisis [homepage on the internet]. Santa Monica, CA: RAND/UCLA Center for the Study of Soviet International Behavior; 1989 Jul. [cited 2007 Jul. 10]. Available from: <http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA228098>
- Hebert AJ. Air Force Magazine Online [homepage on the Internet]. Arlington (VA): The Air Force Association; 2003 Mar. [cited 2007 Apr. 4]. Available from: <http://www.afa.org/magazine/march2003/0303killchain.asp>.
- Information Assurance Directorate, NSA. Global Information Grid [homepage on the Internet]. Washington, DC: National Security Agency (NSA); n.d. [cited 2007 Feb.]. Available from: <http://www.nsa.gov/ia/industry/gig.cfm?MenuID=10.3.2.2>.
- Johns Hopkins University Applied Physics Laboratory (JHU APL). The Cooperative Engagement Capability, Johns Hopkins APL Technical Digest 1995; 16 (4): 377-396. Available from: <http://www.jhuapl.edu/techdigest/td1604/APLteam.pdf>. Accessed 2007 Apr.
- Lambeth BS. Air Power Against Terror: America's Conduct of Operation Enduring Freedom [dissertation]. Santa Monica (CA): RAND Corporation; 2005. 456 p. United States Central Command Air Forces, Shaw AFB, SC.
- Luessen LH. A Self-Consistent Context for Unit- and Force-Level Tactical Decision-Making, Naval Engineers Journal 2003; Winter: 67-77.

- MacKenzie CM, Laskey K, McCabe F, Brown PF, Metz R. OASIS [homepage on the Internet]. OASIS SOA Reference Model TC; 2006 Aug. 2. [cited 2007 July 25]. Available from: <http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf>.
- Marzolf GF. Time-Critical Targeting: Predictive versus Reactionary Methods: An Analysis of the Future [dissertation]. Maxwell AFB (AL): The School of Advanced Airpower Studies; 2004 Mar.. 72 p. Air University Press, Maxwell AFB, AL.
- Mayo RW, Nathman J. FORCEnet Implementation Strategy: Sea Power 21 Series, Part V: Forcenet: Turning Information into Power [homepage on the Internet]. Washington, DC: National Academy of Sciences; 2003. [cited 2007 Mar.]. Available from: <http://www.nap.edu/catalog/11456.html>.  
Paragraph 5.1.5
- Morehouse J. Time Critical Targeting. US Air Force: 1st Annual Interoperability Conference; 2002 Mar. 26; NDIA; n.d., 13 p.
- Morrison JG, Kelly RT, Moore RA and Hutchins SG. (1997). [Tactical Decision Making Under Stress \(TADMUS\) - Decision Support System](#). 1997 IRIS National Symposium on Sensor and Data Fusion, MIT LincolnLaboratory, Lexington, MA, 14-17 April 1997.
- National Commission on Terrorist Attacks (USA) The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upon the United States. Washington (DC): US Government Printing Office; 2004 July 22. 585 p. Available from: <http://www.gpoaccess.gov/911/index.html>
- Naval Open Architecture Contract Guidebook: Future Combat Systems Open Architecture. Version 1.0. Washington, DC: PEO IWS 7.0; 2006 July 7.
- Naval Power 21...A Naval Vision [homepage on the Internet]. Washington (DC): US Navy; 2002 Oct.. [cited 2007 June 10]. Available from: <http://www.nwdc.navy.mil/Conops/files/NP21.pdf>.

- National Research Council, Committee on the FORCENet Implementation Strategy,.  
ForceNet Implementation Strategy. Washington (DC): National Academies Press;  
2005. 260 p.
- Naveh BZ. Defense Policies and Strategies. In: Naveh BZ, Lorber A, Zarchan P, editors.  
Theater Ballistic Missile Defense. 192 volumes. Reston (VA): American Institued  
of Aeronautics and Astronautics, Inc.; 2001. Vol 192: 10 p.
- Open Architecture Assessment Model (OOAM). version 1.0 ed. Washington, DC: PEO-  
IWS; 2005 Mar 8.
- Open Architecture (OA) Computing Environment Design Guidance Version 1.0.  
Dahlgren (VA): NSWC/DD; 2004 Aug 23. Prepared for PEO IWS.
- Open Systems Joint Task Force. Program Manager's Guide Version 2.0 [Internet].  
Arlington (VA): 2004 Sept. [cited Feb. 2007.]. Available from:  
[http://www.acq.osd.mil/osjtf/pdf/PMG\\_04.pdf](http://www.acq.osd.mil/osjtf/pdf/PMG_04.pdf).
- Payne C. Principle of Naval Weapon Systems. Annapolis: Naval Institute Press, 2006.
- Perry WL, Button RW, Bracken J, Sullivan T, Mitchell J. Measures of Effectiveness for  
the Information-Age Navy: The Effects of Network-Centric Operations on  
Combat Outcomes. Santa Monica (CA). The RAND Corporation; 2002. 151 p.
- Pike J. Tactical Digital Information Links (TADIL). [homepage on the Internet].  
Unknown: Federation of American Scientists; 2000 Apr. 23. [cited 2007 Mar. 2].  
Available from: <http://www.fas.org/irp/program/disseminate/tadil.htm>.
- Rudderow T. 2002 Vision... Presence... Power [homepage on the Internet]. Washington,  
DC: OPNAV N80 Office; 2002. [cited 2007 Apr.]. Available from:  
<http://www.navy.mil/navydata/policy/vision/vis02/vpp02-ch2b.html>.
- Rushton RT. Open Architecture, The Critical Network Centric Warfare Enabler. United  
States Navy: ASNE Day 2004; 2004 June 28; Arlington (VA): n.d.,
- Simonoff AJ. A Conceptual Architecture for Naval Effects Based Operations. Dahlgren  
(VA): Naval Surface Warfare Center Dahlgren Division; 2006. 7 p.



Straight of Hormuz map. [Internet Resource]. Accessed on 2007 March 17. Available at:  
[http://www.globalsecurity.org/military/world/iran/images/hormuz\\_80.gif](http://www.globalsecurity.org/military/world/iran/images/hormuz_80.gif)

Strei TJ. "Network-Centric Applications," Open Architecture in Naval  
Combat System Computing of the 21st Century, 01 April 03

Toomay JC. Radar Principles for the Non-Specialist. 2<sup>nd</sup> Ed., Raleigh (NC): SciTech  
Publishing, Inc., 1998.

Ullman DG. "OO-OO-OO!" The Sound of a Broken OODA Loop. CrossTalk, April  
2007. <http://www.stsc.hill.af.mil/CrossTalk/2007/04/0704Ullman.html>

Document: Universal Naval Task List, OPNAVINST 3500.38B/MCO 3500.26/USCG  
COMDTINST M3500.01B, January 30, 2007

Various Authors. Cooperative Engagement Capability [home page on the Internet].  
Federation of American Scientists; 2000 Feb. 16. [Military Analysis Network;  
cited 2007 Mar.]. [about 1 screens]. Available from: <http://www.fas.org/man/dod-101/sys/ship/weaps/cec.htm>.

Wiggins JF. GAO-02-204R: Joint Warfighting: Attacking Time-Critical Targets.  
Washington (DC): General Accounting Office; 2001. 8 p.

Wikipedia Contributors. Yemen. In: Wikipedia, The Free Encyclopedia [discussion list on  
the Internet]. [Wikipedia]; n.d.; [cited 2007 Apr. 21]. [about 3 screens]. Available  
from: <http://en.wikipedia.org/w/index.php?title=Yemen&oldid=124535153>

Young BW. Future Integrated Fire Control. Northrop Grumman: 10th International  
Command and Control Research and Technology Symposium: The Future of C2;  
2005 June 15; Washington (DC): 2005, 22 p.

Young JJ. Memorandum: Naval Open Architecture Scope and Responsibilities [Internet].  
Washington D.C.: Assistant Secretary of the Navy RD&A; 2004 Aug. 5. [cited  
2007 Mar. 13]. Available from:  
<http://acquisition.navy.mil/content/view/full/4495>.

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