2005-06

Maritime domain protection in the Straits of Malacca

Buschmann, Jeff

Monterey, California. Naval Postgraduate School

NPS-97-05-001

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Maritime Domain Protection in the Straits of Malacca

by

LT Jeff Buschmann, LT Tracey Crider, LTC Guillermo Ferraris
LT Enrique Garcia, 1st LT Hasan Gungor, LT Shannon Hoffmann
LT Micah Kelley, ENS Cory MacCumbee, Mr. Robert Malloch
LCDR Chris McCarthy, ENS Jacob McIlvaine, Mr. David Rummler
CAPT Serdar Sari, Mr. Tiong Ngee Teo, LT David Walton, Jr.
LT William Westmoreland, LT Matt Wiens, ENS Alexis Wise
ENS Greg Woelfel, MAJ Russ Wyllie

Mr. Han Hiong Ang, Mr. Kok Meng Chang, Mr. Chay Chua
Mr. Dolev Cfir, Mr. Kim Hua Er, Mr. Yew Seng How
Mr. Yu Chih Hsu, Mr. Wee Tuan Khoo, Mr. Swee Jin Koh
LT Rick Kratzer, Mr. Lawrence Liang, Mr. Joel Lim
Mr. Tat Lee Lim, LT Jennifer Lorio, LT John Lukacs
Mr. Chee Mun Ng, Mr. Winston Ong, Mr. Chin Khoon Quek
Mr. Dinesh Raghavan, Mr. Mark Tan, Mr. Nai Kwan Tan
Mr. Amos Teo, Mr. Hong-Siang Teo, Mr. Matthew Tong
Mr. Keat Hoe Yeoh, Mr. Yoke Chuang Yong

June 2005

Prepared for: Deputy Chief of Naval Operations for Warfare Requirements and Programs (OPNAV N7), 2000 Navy Pentagon, Rm. 4E392, Washington, DC 20350-2000

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2005	**3. REPORT TYPE AND DATES COVERED** Thesis Technical Report	
4. TITLE AND SUBTITLE: Maritime Domain Protection in the PACOM AOR			**5. FUNDING NUMBERS**
6. AUTHOR(S) Jeff Buschmann, Tracey Crider, Guillermo Ferraris, Enrique Garcia, Hasan Gungor, Shannon Hoffmann, Micah Kelley, Cory MacCumbee, Robert Malloch, Chris McCarthy, Jacob McIlvaine, David Rummler, Serdar Sari, Tiong Ngee Teo, David Walton Jr., William Westmoreland, Matt Wiens, Alexis Wise, Greg Woelfel, Russ Wyllie			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Deputy Chief of Naval Operations for Warfare Requirements and Programs (OPNAV N7), 2000 Navy Pentagon, Rm. 4E392, Washington, DC 20350-2000			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Hostile acts of maritime piracy and terrorism have increased worldwide in recent years, and the global impacts of a successful attack on commercial shipping in the Straits of Malacca make it one of the most tempting target locations for maritime terrorism. In an attempt to develop a system of systems to defeat and prevent terrorism in the Straits of Malacca, this study developed three significant commercial shipping attack scenarios (Weapons of Mass Destruction (WMD) shipment, Ship As a Weapon (SAW), and Small Boat Attack (SBA)), and used a Systems Engineering Design Process (SEDP) to design alternative architectures that offered promising ways to defeat these attacks. Maritime Domain Protection (MDP) architecture alternatives combined five separate systems: a Land Inspection System, a Sensor System, a Command and Control, Communications, and Intelligence (C3I) System, a Response Force System, and a Sea Inspection System. Individual models for each system were developed and combined into overarching integrated architecture models to evaluate overall performance. The study results showed that solutions tended to be threat-specific, and current capabilities were mixed. While solutions were found to effectively reduce risk in all threat scenarios, these sometimes came at great expense. Alternatively, cost-effective solutions were also found for each scenario, but these sometimes gave limited performance.

14. SUBJECT TERMS Maritime Domain Protection, Systems Engineering, EXTEND, MANA, TAWS, AREPS, Smart Container			**15. NUMBER OF PAGES** 647
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA 93943-5001

RDML Patrick W. Dunne, USN
President

Richard Elster
Provost

This report was prepared for the Deputy Chief of Naval Operations for Warfare Requirements and Programs (OPNAV N7), 2000 Navy Pentagon, Rm. 4E92, Washington, DC 20350-2000.

This report was prepared by Systems Engineering and Analysis Cohort Seven (SEA-7):

LT Jeff Buschmann
LT Tracey Crider
LTC Guillermo Ferraris
LT Enrique Garcia
1st LT Hasan Gungor
LT Shannon Hoffmann
LT Micah Kelley
ENS Cory MacCumbee
Mr. Robert Malloch
LCDR Chris McCarthy
ENS Jacob McIlvaine
Mr. David Rummler
CAPT Serdar Sari
Mr. Tiong Ngee Teo
LT David Walton, Jr.
LT William Westmoreland
LT Matt Wiens
ENS Alexis Wise
ENS Greg Woelfel
MAJ Russ Wyllie

Reviewed by:

EUGENE P. PAULO
SEA-7 Project Advisor
Maritime Domain Protection in the Straits of Malacca

RAVI VAIDYANATHAN
SEA-7 Project Advisor
Maritime Domain Protection in the Straits of Malacca

Released by:

CARSON K. EOYANG
Associate Director for Education
Wayne E. Meyer Institute of Systems Engineering

LEONARD A. FERRARI, Ph.D.
Associate Provost and Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Hostile acts of maritime piracy and terrorism have increased worldwide in recent years, and the global impacts of a successful attack on commercial shipping in the Straits of Malacca make it one of the most tempting target locations for maritime terrorism. In an attempt to develop a system of systems to defeat and prevent terrorism in the Straits of Malacca, this study developed three significant commercial shipping attack scenarios (Weapons of Mass Destruction (WMD) shipment, Ship As a Weapon (SAW), and Small Boat Attack (SBA)), and used a Systems Engineering Design Process (SEDP) to design alternative architectures that offered promising ways to defeat these attacks. Maritime Domain Protection (MDP) architecture alternatives combined five separate systems: a Land Inspection System, a Sensor System, a Command and Control, Communications, and Intelligence (C3I) System, a Response Force System, and a Sea Inspection System. Individual models for each system were developed and combined into overarching integrated architecture models to evaluate overall performance. The study results showed that solutions tended to be threat-specific, and current capabilities were mixed. While solutions were found to effectively reduce risk in all threat scenarios, these sometimes came at great expense. Alternatively, cost-effective solutions were also found for each scenario, but these sometimes gave limited performance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS, ACRONYMS, AND SYMBOLS

ACTD	Advanced Concept Technology Demonstration
AIS	Automatic Identification Systems
AOI	Area of Interest
AOR	Area of Regard
APDS	Air Particulate Detection System
APM	Advanced Propagation Model
AREPS	Advanced Refractive Effects Propagation System
ASL	Above Sea Level
ATC	Air Traffic Control
ATS	Automated Targeting System
BADD	Biowarfare Agent Detection Device
BIT	Built In Test
BPS	Bits Per second
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C3IS	C2, Communications, Intelligence, and Sensors
C4I	Command, Control, Communications and Computers
CBRN	Chemical, Biological, Radiological, Nuclear Devices
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive Devices
CCR	Call Completion Rate
CEP	Circular Error Probable

CF	Canadian Forces
CIC	Combat Information Center
CIP	Common Intelligence Picture
COA	Course of Action
COI	Contacts of Interest
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operating Picture
COTS	Commercial Off the Shelf
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DID	Defense In Depth
DOD	Department of Defense
DTED	Digital Terrain Elevation Data
DWDM	Defense Wavelength Division Multiplexing
EEI	Essential Elements of Information
ELINT	Electronic Intelligence
EO	Electro-Optical
EPA	Environmental Protection Agency
ESM	Electronic Support Measure
FAA	Federal Aviation Administration
FER	Force Exchange Ratio
FLIR	Forward Looking Infrared Radar

FSO	Free Space Optics
FTZ	Free Trade Zone
FY05$	Fiscal Year 2005 Dollars
GDP	Gross Domestic Product
GEO	Geostationary Earth Orbit
GHz	Gigahertz
GPS	Global Positioning System
GRT	Gross Registered Tons
GT	Gross Tons
HAA	High Altitude Airship
HAEAR	High Altitude Endurance Aerostat Radar
HF	High Frequency
HFSWR	High Frequency Surface Wave Radar
HIV	High Interest Vessel
HSV	High Speed Vessel
HUMINT	Human Intelligence
HVU	High Value Unit
IA	Information Assurance
ID	Identification
IDS	Intruder Detection System
IFF	Identification Friend or Foe
IMB	International Maritime Bureau
IMO	International Maritime Organization

IPR	In-Progress Review
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
ITU-R	International Telecommunication Union-Radio
JC4I	Joint Command, Control, Communications, Computers, and Intelligence
kt(s)	Knot(s)
KT	Kiloton
LEO	Low Earth Orbit
LLNL	Lawrence Livermore National Laboratory
LNG	Liquefied Natural Gas
LOS	Line of Sight
LWIR	Low Wave Infrared Radar
MAC	Maritime Assault Capability
MAEAR	Medium Altitude and Endurance Aerostat Radar
MALSINDO	Tri-lateral Initiative by **Malaysia, Indonesia, and Singapore**
MANA	Map Aware Non-Uniform Automata
MDA	Maritime Domain Awareness
MDA	Missile Defense Agency
MDP	Maritime Domain Protection
MDT	Mean Down Time
MIFC	Maritime Intelligence Fusion Center
MIFCPAC	Maritime Intelligence Fusion Center Pacific
MILCON	Military Construction

MIO	Maritime Interdiction Operations
MMSI	Maritime Mobile Service Identity
MOE	Measure of Effectiveness
MOP	Measure of Performance
MPA	Maritime Patrol Aircraft (depending on usage)
MPA	Maritime and Port Authority (depending on usage)
MRT	Mean Resolvable Temperature
MT	Motor Transport
MTBA	Mean Time Between Arrivals
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
MV	Motor Vessel
MWIR	Mid Wave Infrared Radar
NBC	Nuclear, Biological, and Chemical
NCW	Network Centric Warfare
NIMA	National Imagery and Mapping Agency
NM	Nautical Mile
NORTHCOM	United States Northern Command
NPS	Naval Postgraduate School
NRT	Near Real Time
NSTF	National Security Task Force
NSWC	Naval Special Warfare Command
NVG	Night Vision Goggles

O&S	Operations and Support
OCC	Operation and Control Centre
OEM	Original Equipment Manufacturer
OHD	Office of Homeland Defense
OODA	Observe, Orient, Decide, Act
OR	Operations Research
OTH	Over The Horizon
PACOM	Pacific Command
P_{det}	Probability of Detection
PE	Parabolic Equation
PERMA	Planning, Embarkation, Rehearsal, Movement, and Assault
P_{fa}	Probability of False Alarm
PK SE	Probability of Kill Single Engagement
QFD	Quality Functional Deployment
RAM	Reliability, Availability, and Maintainability
R&D	Research and Development
RDT&E	Research, Development, Testing, and Evaluation
RF	Radio Frequency
RMP	Recognized Maritime Picture
ROE	Rules of Engagement
RSA	Regional Systems Architecture
RT	Real Time
SAW	Ship As a Weapon

SBA	Small Boat Attack
SBR	Space Based Radar
SDH	Synchronous Digital Hierarchy
SEA	Systems Engineering and Analysis
SEA-7	Systems Engineering and Analysis Group 7
SEDP	Systems Engineering Design Process
SLOC	Sea Lines of Communication
SONET	Synchronous Optical Network
SPF	Singapore Police Force
SSPT	Ship Size Per Team
STE	Special Test Equipment
STAR	Special Tactics and Rescue Unit
STRAITREP	Strait Reporting (Straits of Malacca and Singapore Reporting System)
TAWS	Target and Acquisition Weapons Software
TCP	Transmission Control Protocol
T_{CLASS}	Time to Classify
T_{DET}	Time to Delete
TDSI	Temasek Defense Systems Institute (Singapore)
TEU	Twenty Feet Equivalent Unit
TISS	Thermal Imaging Sensor System
TMIS	Total Maritime Inspection System
TNT	Trinitrotoluene
TRAC	Training and Doctrine Analysis Center (U.S. Army)

TRL	Technology Readiness Level
TTD	Time-to-Detection
TTG	Time-to-Go
TTID	Time-to-Classification/Identification
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
USCG	United States Coast Guard
USN	United States Navy
VBSS	Visit, Board, Search, and Seizure
VHF	Very High Frequency
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
VTS	Vessel Traffic Service
WMD	Weapons of Mass Destruction

ACKNOWLEDGMENTS

The students of System Engineering and Analysis Cohort Seven would like to thank the following faculty and staff of the Systems Engineering Curriculum and the Wayne E. Meyer Institute for their instruction and dedication to excellence in preparing us to complete this thesis project work.

Professor Gene Paulo
Professor Ravi Vaidyanathan
Professor Jeff Crowson
Professor Doyle Daughtry
Professor Mike Green
Professor Robert Harney
Professor Otto Heinz
Professor Thomas Hoivik
Dean Wayne Hughes
CAPT Starr King, USN
CAPT Jeff Kline, USN
Professor Bard Mansager
LCDR Russell Gottfried, USN
Professor and Department Chair David Olwell
Professor Patrick Parker
Professor Paul Sanchez
Professor Mark Stevens
CDR Brett Foster, USN

Additionally, we would like to thank our families for their patience and understanding over the past year and a half. Without their support, none of this would have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The 2005 Naval Postgraduate School (NPS) Cross-Campus Integrated Study, titled "Maritime Domain Protection in the PACOM AOR," was the result of the combined effort of 21 NPS Systems Engineering students, 26 Singaporean Temasek Defense Systems Institute (TDSI) students, 4 students from other NPS curricula, and 21 NPS faculty members from different NPS departments. Utilizing tasking provided by the office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs (OPNAV N7) to the NPS Wayne E. Meyer Institute of Systems Engineering, the study examined ways to defeat and prevent terrorism in the Maritime Domain. The OPNAV N7 tasking directed the Meyer Institute to conduct a study to design and assess conceptual integrated architecture alternatives for large ship security and inspection in the Straits of Malacca. The NPS Systems Engineering and Analysis Cohort 7 (SEA-7), in conjunction with the Singaporean TDSI students, used the Systems Engineering Design Process (SEDP) shown in Figure 1 as a systems engineering framework to conduct the multidisciplinary study (the "Implementation" phase of the SEDP was not performed due to the study's conceptual nature).

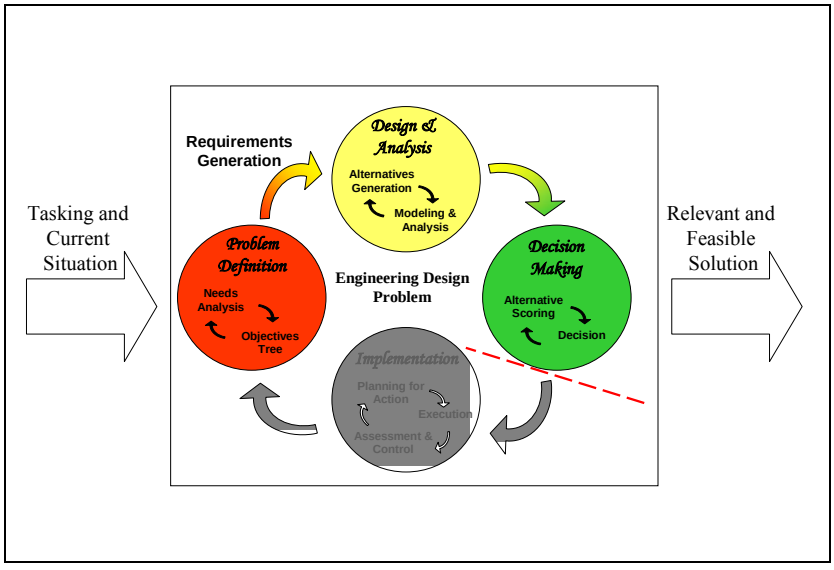

Figure 1. SEDP

The SEDP was an iterative process used to scope and bound the MDP problem, determine requirements, and to design architecture alternatives to meet stakeholder needs, wants, and desires.

The highest value of oil, container, and bulk cargo pass through the 500-mile-long Straits of Malacca. Unfortunately, this critical and susceptible shipping channel exists in a region of the world where piracy and terrorism thrive in a geographically vulnerable and limited-infrastructure environment. Hostile acts of maritime piracy and terrorism have increased worldwide in recent years, and although no large-scale maritime attacks have occurred to date in the Straits of Malacca, the global political and economic impacts of a successful attack on commercial shipping in this region make it one of the most tempting target locations for acts of maritime terrorism.

The SEA-7 Study developed three significant commercial shipping attack scenarios and designed several architecture alternatives that offered promising ways to better defend against these possible future attacks in the Maritime Domain. Scenario 1 was a Small Boat Attack (SBA) by an explosives-laden speedboat against an oil tanker in the shipping channel. Scenario 2 was a Ship As a Weapon (SAW) attack in which an oil tanker rammed into a pier in Singapore. Scenario 3 was a Weapons of Mass Destruction (WMD) attack involving the shipment of a 20-KT, Russian-made, nuclear device. In order to defend against these attacks, the cohort defined an MDP architecture alternative as a combination of five systems: a Land Inspection System, a Sensor System, a Command and Control, Communications, and Intelligence (C3I) System, a Response Force System, and a Sea Inspection System.

Using the SEDP as a guide, the SEA-7 Cohort defined the problem, created threat scenarios, generated requirements, identified alternative system solutions, developed and executed an integrated modeling and simulation plan, and conducted analyses to draw conclusions and make recommendations. The cohort initially estimated the economic impact of a successful attack for the three threat scenarios and identified the cost and capabilities of the current "As-Is" MDP architecture, centered on Singapore, to defend against these attacks. These results are shown in Table 1, along with the desired probability of defeat values presented to the Pacific Command (PACOM) stakeholder.

Scenario	Current Ten-Year Total MDP System Cost (FY05M$)	Unmitigated Attack Damage Cost (FY05B$)	Probability of Defeat	
			Current	Desired
1 – SBA	N/A	0.8 - 3.6	~0%	80%
2 – SAW	38 - 40	2.5 - 4.9	~80%	90%
3 – WMD	638 - 715	180.1 - 215.9	~2%	60%
N/A = Not Applicable.				

Table 1. Maritime Attack Defense Status and Damage Estimates

This table shows estimates of the current MDP system cost, the estimated attack damage cost, and the current and desired defeat probability for three threat scenarios. Varying gaps exist between the current and desired probabilities of defeat.

The SEA-7 Cohort developed generic system alternatives and evaluated them for their ability to improve on the current system within a five-year time horizon. By direction, the MDP Study did not consider political and legal ramifications, and assumed full cooperation of participating nations surrounding the Straits of Malacca. The study compared the "As-Is" MDP architecture to these potential alternative architectures based on performance, risk, and total system cost. Architecture performance was defined as the probability a given architecture would defeat each attack scenario. Risk was defined as the expected damage cost for a single attack in each scenario. The estimated total system cost for each architecture included the procurement cost of MDP System components, the procurement cost of required commercial system components, operating and support costs, and shipping delay costs. These costs were not a determining factor in the design of the various system alternatives, but the total system cost was used as a tool to make relative comparisons.

In order to quantify the performance of the different system alternatives and multifaceted architecture combinations, SEA-7 developed an integrated modeling plan using a modular approach. The modeling plan had the different system groups first develop individual models which were used to evaluate and optimize the system performance for each system alternative. Integrated architecture models were then used to link the different system model outputs together and evaluate the performance of the entire system of systems. This approach allowed numerous modeling tools to be used

throughout the modeling effort, including EXTEND™, Microsoft Excel™, Naval Simulation System (NSS), and Map Aware Non-Uniform Automata (MANA).

The key findings of this study were:

Overall MDP

- Commercial shipping involved various international participants in a largely unregulated, vulnerable industry that was critical to the worldwide economy. As a result of the multidiscipline, interrelated nature of the MDP problem, a Systems Engineering approach was critical—there was no other approach that would necessarily focus on the entire problem as an integrated whole.

- No single solution existed to the extremely difficult MDP problem. Solutions tended to be threat-specific, and current capabilities were mixed, depending on the threat. In all threat scenarios, solutions were found to effectively reduce risk, although sometimes at great expense. Cost-effective solutions were found to reduce risk in all threat scenarios, although the amount of reduction was sometimes less than desired.

WMD Scenario

- The largest gain in architecture performance in a WMD scenario came with the addition of a Cargo Inspection System installed in the highest volume ports-of-origin for cargo destined for the area of interest. The Land Inspection System alternative that was evaluated also relied on industry participation, using qualified "Trusted Agent" shipping companies to help find or deter WMDs from being loaded in their shipping containers. This allowed resources to be focused on nonparticipating shippers, since they were deemed more likely to transport illegal cargo. The cost to the shipping industry was significant for this Land Inspection System alternative.

- A less costly architecture alternative offered a significant improvement over the "As-Is" architecture in a WMD scenario, although the overall improvement was marginal. This lower-cost architecture alternative used an improved Sensor System and a Sea Inspection System that searched suspect ships en route. Due to the incidence of false alarms, this Sea Inspection System was only cost-effective when used with a C3I System that could accurately correlate positive detections with a source (i.e., radiation due to pottery, medical equipment, etc.) and determine whether an appropriate response was required.

SAW Scenario

- The "As-Is" Force System that loaded Sea Marshals on high-value contacts of interest (COIs) at five NM with the harbor pilot was effective, given the specifics of the scenario. Only slight improvements in performance were attained with longer engagement times; however, increasing Sea Marshal training and armament significantly improved close-in performance.

- The Rapid Response Force alternative was not effective when COI hostile intent was determined at five NM—there simply was not enough response time to brief and deploy the forces. However, if hostile intent was determined at or before ten NM, the Rapid Response Force was highly effective.

- Throughout this scenario, improvements in performance were possible by increasing the amount of time the response forces had to counter the attack. The largest increase in time-to-respond was achieved by improving the Sensors' capability to detect large ships out to 250 to 300 NM. Improvements in C3I capabilities resulted in more timely decisions, but the increase in response time was less than that obtained by the Sensors' improvement.

SBA Scenario

- Loading Sea Marshals on high-value COIs transiting an area of interest was a cost-effective solution alternative to counter the small boat suicide attack scenario. This method of point-defense was one active means of hardening the target against the attack. Methods of passive defense also showed promise, such as only permitting double-hull ships into a threat area or installing blast-resistant coating on ships' waterlines. Although both passive and active defenses would require some level of cost, they both served to minimize the damage resulting from a small boat suicide attack.

- Friendly force patrol craft were not effective when used to randomly patrol the Straits. This alternative was also considerably more costly than using Sea Marshals, although it would serve to indicate presence and potentially deter some attacks.

- Although defeating a suicide boat attack in progress was very difficult, an increase in Sensors' ability to track small boats in the area of interest could give additional benefits. Intent or anomaly detection software could potentially detect trends or aberrant behavior by small boats that could be the precursor to, or preparation for, an attack. Additionally, if SBAs were

> to become commonplace, being able to backtrack to find the port of origin for attacking boats could allow resources to be focused in a region that could find terrorist bases, thereby halting attacks before they occur.

The threat scenarios, assumptions, and results of this study were only a point-evaluation of the very complex MDP problem. All of the models used in the study were intentionally created with variable inputs that could be changed to suit other geographical, force, or threat situations. The approach and analysis used in this study, coupled with the adaptability of the models, gave decision makers a tool to use for future analysis.

The 2005 NPS Cross-Campus Integrated Study was an academic exercise and was not endorsed by any branch of the U.S. Armed Forces. Examining MDP in its entirety was extremely challenging due to the immense scope of the problem. The SBA, SAW, and WMD scenarios were used to facilitate analysis and do not represent official views or policies of the Navy or any government. Although all elements of MDP were not evaluated to the maximum extent possible, they were evaluated to the extent practical given the limited time available for this study. SEA-7 nonetheless concluded that the results are informative and provided insights to decision makers involved in addressing the complex issues associated with this topic.

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 INTRODUCTION

1.1 BACKGROUND

1.1.1 Worldwide Shipping and Commerce

The import and export of oil and goods on a scale large enough to sustain the modern global economy would not be possible without seaborne shipping. Over 90% of world trade is carried by the international maritime shipping industry, with the remaining 10% being delivered via expensive air cargo and fixed path land/rail routes.[1] In particular, the geography of Asia dictates that most international trade moves by sea, since interior land transport infrastructure has not been highly developed.

Commercial shipping is characterized by a blend of dense traffic through straits and along coasts accompanied by long-distance, open-ocean transit. The global pattern of commercial goods shipments consists of large tonnages of low-value resources shipped throughout Asia to industrialized economies, which add value via manufacturing processes. These industrial economies then ship out relatively smaller tonnages of high-value consumer goods, creating a two-way path through the Malacca Straits.[2] Global economic growth is contingent on this free flow of commerce along Asian-Pacific trade routes. Additionally, oil is the key energy source powering the modern economic sectors of the Asian-Pacific region and the world. The dependency on oil imports from the Middle East emphasizes the strategic importance of shipping lanes (see Figure 2).

[1] Industrial College of the Armed Services, "Spring 2001 Industry Study: Final Report Transportation," *Industrial Studies 2001*, http://www.ndu.edu/icaf/industry/IS2001/transportation.htm, (accessed 22 January 2005).

[2] *Review of Networked Economies*, Vol. 3, Issue 2, June 2004 (Source: Institute of Transport and Maritime Management Antwerp-University of Antwerp (ITMMA-UA) based on People's Republic of China (PRC) Statistics Ministry of Communication, American Association of Port Authorities (AAPA), and port authority data).

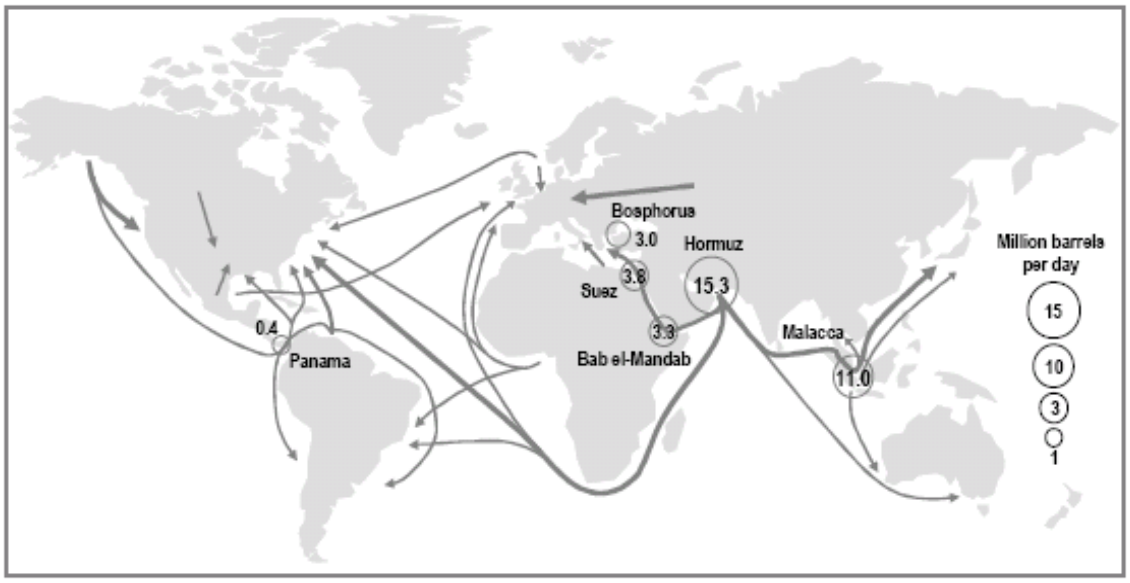

Figure 2. Oil Transit Routes (Millions of Barrels Per Day)

The constricted Straits of Malacca and the dependency on oil imports from the Middle East emphasize the strategic importance of strategic shipping lanes.[3]

The major sea lines of communications (SLOCs) are constricted at several key straits, the most important of which are located in Southeast Asia: the Malacca, Sunda, Lombok, and Makassar Straits. These transit routes cross the waters of several countries including Malaysia, Indonesia, and Singapore, with Singapore's port facilities serving as a major node for refueling and transshipment. The United States and many concerned nations in the international community are proactively addressing potential vulnerabilities with regard to protection of vital SLOCs. An indication of this trend is the demand for military naval and air capabilities in the Asian-Pacific region.

1.1.1.1 Shipping Volume

The overall shipping industry has seen a generally increasing trend in total trade volume. Over the last 40 years total seaborne trade estimates, in units of tonnes of cargo by miles traversed, have nearly quadrupled, from less than 6 thousand billion

[3] Jean-Paul Rodriue, "Straits, Passages, and Chokepoints: A Maritime Geo-Strategy of Petroleum Distribution," Hofstra University, (2004).

tonne-miles in 1965 to 25 thousand billion tonne-miles in 2003.[4] The international shipping industry transported 6.2 billion tonnes of cargo in 2003, with a fleet of 26,280 deep-sea cargo ships (see Table 2).[5] This trend is expected to continue, especially for oil shipments. China's oil consumption is expected to grow 93% in the next 20 years, while the rest of developing Asia will increase 53%, as compared to the U.S.'s expected growth of 22%.[6]

A1.4 *World Seaborne Trade* — *million tonnes*

Year	Iron Ore	Coal Coking	Coal Steam	Grain*	Baux./ Alum	Phos. Rock	Minor Bulk	Cont-ainer	Other Dry	Total Dry	Crude Oil	Oil Products	Total Oil	Gas Trade LPG	Gas Trade LNG	Grand Total
1986	311	141	134	187	42	45	555	173	555	2,143	1,030	400	1,430	22	35	3,630
1987	319	145	148	211	46	45	575	192	532	2,213	977	378	1,355	24	37	3,629
1988	346	155	158	216	49	47	603	211	550	2,335	1,086	415	1,501	23	41	3,900
1989	362	155	161	220	55	44	614	231	578	2,419	1,198	479	1,677	26	44	4,166
1990	347	155	182	215	55	37	607	246	626	2,469	1,155	446	1,601	28	55	4,151
1991	358	155	205	218	53	31	606	268	652	2,546	1,161	401	1,563	30	52	4,190
1992	337	154	214	224	48	30	618	292	673	2,589	1,245	406	1,650	32	53	4,325
1993	352	156	206	223	51	27	626	322	687	2,649	1,354	436	1,790	34	55	4,528
1994	380	157	217	207	49	29	659	357	689	2,744	1,375	430	1,805	33	58	4,641
1995	402	160	242	216	52	30	699	389	696	2,886	1,400	446	1,846	34	33	4,800
1996	392	165	260	219	54	31	698	430	753	3,002	1,469	475	1,944	36	66	5,048
1997	428	169	281	229	55	32	707	470	789	3,160	1,554	494	2,048	37	74	5,318
1998	428	167	284	226	55	31	686	503	810	3,190	1,545	476	2,021	35	75	5,321
1999	405	161	303	247	54	31	683	559	799	3,241	1,584	502	2,086	37	82	5,446
2000	449	169	337	264	54	28	697	622	807	3,427	1,651	496	2,147	39	92	5,705
2001	454	166	369	260	54	27	698	640	852	3,520	1,645	546	2,190	36	94	5,840
2002	474	167	380	268	54	26	705	709	814	3,597	1,605	556	2,161	36	100	5,894
2003 (f)	516	172	416	269	54	26	719	787	782	3,741	1,688	577	2,265	37	106	6,149
2004 (f)	558	176	430	266	54	26	738	860	756	3,865	1,725	561	2,286	38	112	6,301
Average Growth																
2003-02	9.0%	2.9%	9.5%	0.1%	0.0%	3.5%	2.0%	11.0%	-3.9%	4.0%	5.3%	3.4%	4.8%	2.3%	5.9%	4.3%
1986-04	3.1%	1.2%	6.3%	1.9%	1.3%	-2.8%	1.5%	8.8%	1.6%	3.2%	2.7%	1.8%	2.5%	2.8%	6.4%	2.9%

Bulk and oil trades as per "Dry Bulk Trade Outlook" and "Oil & Tanker Trade Outlook", respectively. LPG trade covers OECD only.
* Includes soyabean

Source: Clarkson Research Studies

Table 2. World Seaborne Trade (Million Tonnes) (Source: Clarkson Research Studies)

The total tonnes of cargo transported by the international shipping industry have increased by over 42% since 1986 (from 3.6 billion to 6.1 billion). The growth rate has been higher in the recent past (e.g., 4.3% growth from 2002 to 2003 as compared to 2.9% from 1986 to 2004).

1.1.1.2 Shipping Chokepoints

A common concept in transport geography is a "chokepoint" that refers to a location that limits the capacity of circulation and cannot be easily bypassed. This implies that any alternative to the chokepoint involves a level of detour or the use of an alternative that amounts to substantial financial cost and time delays. Chokepoints are

[4] http://www.marisec.org/shippingfacts/worldtradeindex.htm.

[5] http://www.marisec.org/shippingfacts/Clarkson%20Report_Final%20Draft.pdf.

[6] United States Pacific Command, *Asia-Pacific Economic Update*, Vol. 2, (2002).

defined by several characteristics that impact voyage time, cost, and risk. These characteristics include location, physical geography, usage level, and access/port-canal infrastructure. Chokepoints are particularly susceptible to pirate attacks and shipping accidents in their narrow channels.

There are nine major chokepoints throughout the world. Figure 3 identifies the Malacca Straits as one of these key chokepoints.[7]

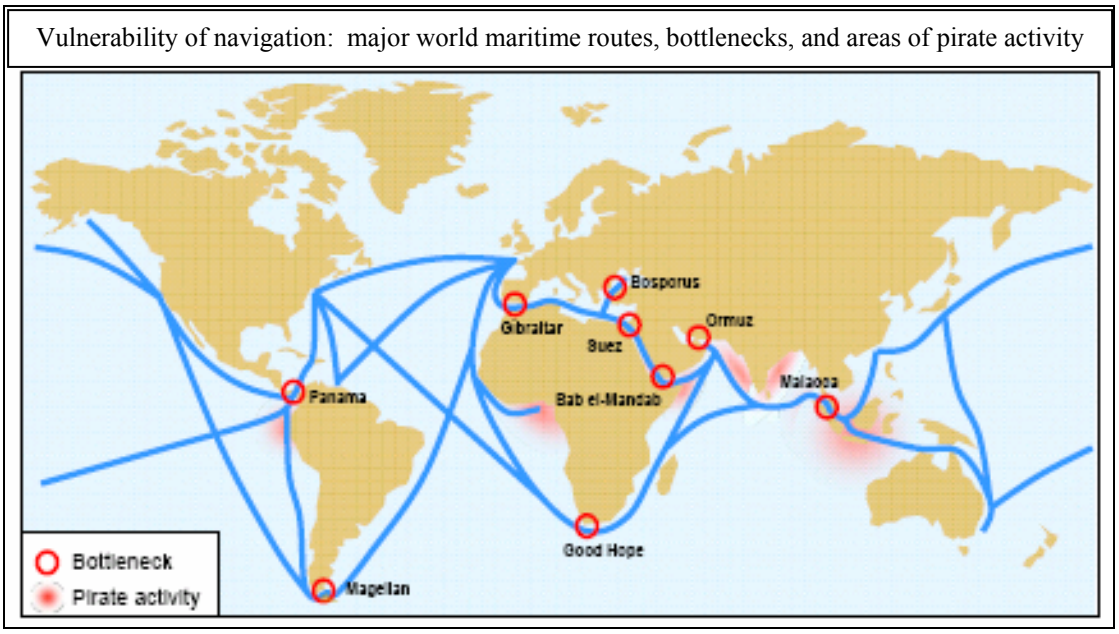

Figure 3. Geographical Chokepoints and Pirate Activity

The primary shipping routes throughout the world pass through nine major chokepoints, of which the Malacca Straits is one. This exemplifies the importance of the Maritime Domain Protection, especially in the Malacca Straits.

Table 3 identifies the aggregate global shipping value estimate by prioritized chokepoint or critical routes.[8, 9] Although the Strait of Hormuz is the largest transit for crude oil shipments, the Straits of Malacca have the highest shipping value for oil and

[7] John H. Noer and David Gregory, "Chokepoints – Maritime Economic Concerns in Southeast Asia," Center for Naval Analyses, (1996).

[8] Jean-Paul Rodriue, "Straits, Passages, and Chokepoints: A Maritime Geo-Strategy of Petroleum Distribution," Hofstra University, (2004).

[9] Erik Kreil, Country Analysis Briefs, "World Oil Transit Chokepoints," http://www.eia.doe.fov/emeu/cabs/choke.html, (accessed February 2005).

container/bulk cargo combined. Total crude volume through the Straits of Malacca is more than three times that of the Suez Canal traffic, and well over five times that of the Panama Canal.

Chokepoint/Critical Routes	Traffic (# of Ships/Yr)	Volume (Containers/Yr)	Container/Bulk Value ($B/Yr) (03$)	Oil (Mbbl/day)	Crude Oil Value ($B/Yr) (03$)	Maritime Shipping Value ($B/Yr) (03$)
Straits of Malacca	**50,000**	**30,500,000**	**$331.4**	11.0	$160.6	**$492.0**
Strait of Hormuz	25,455	9,545,455	$103.7	**15.0**	**$219.0**	$322.7
Bosphorous/Turkish Straits	**50,000**	14,625,000	$158.9	3.0	$43.8	$202.7
Suez Canal	16,000	9,900,000	$107.6	3.3	$48.2	$155.7
Panama Canal	13,000	9,495,455	$103.2	0.4	$5.8	$109.0
Bab el-Mandab	3,920	840,000	$9.1	3.3	$48.2	$57.3
Russian Oil and Gas Export Ports	2,545	1,145,455	$12.4	1.2	$17.5	$30.0

Table 3. Global Shipping Critical Chokepoints Comparison [8, 9]

More ships, carrying more net value cargo, transit the Straits of Malacca than any other chokepoint in the world.

1.2 THREATS TO COMMERCIAL SHIPPING

With three-quarters of the earth's surface covered by water, commercial shipping vessels must use shipping lanes that transit vast expanses of desolate ocean area. These shipping lanes pass through marine territory that is barely, if at all, monitored or policed by forces that could protect or assist any merchant vessels that become distressed. This vulnerability, coupled with the quantity and value of cargo that is shipped on the open seas, provides a tempting target for pirates. Additionally, the dependence of world trade on commercial shipping provides an attractive target for terrorists intent on disrupting the global economy. It is easy to connect the dots between the two, especially in geographic areas such as the Straits of Malacca where both piracy and terrorism not only survive, but thrive in a geographically vulnerable and limited-infrastructure environment.

1.2.1 Maritime Piracy

According to statistics published by the International Maritime Organization (IMO), the number of pirate attacks on commercial shipping has increased almost five-fold since the mid-1990s (see Figure 4).

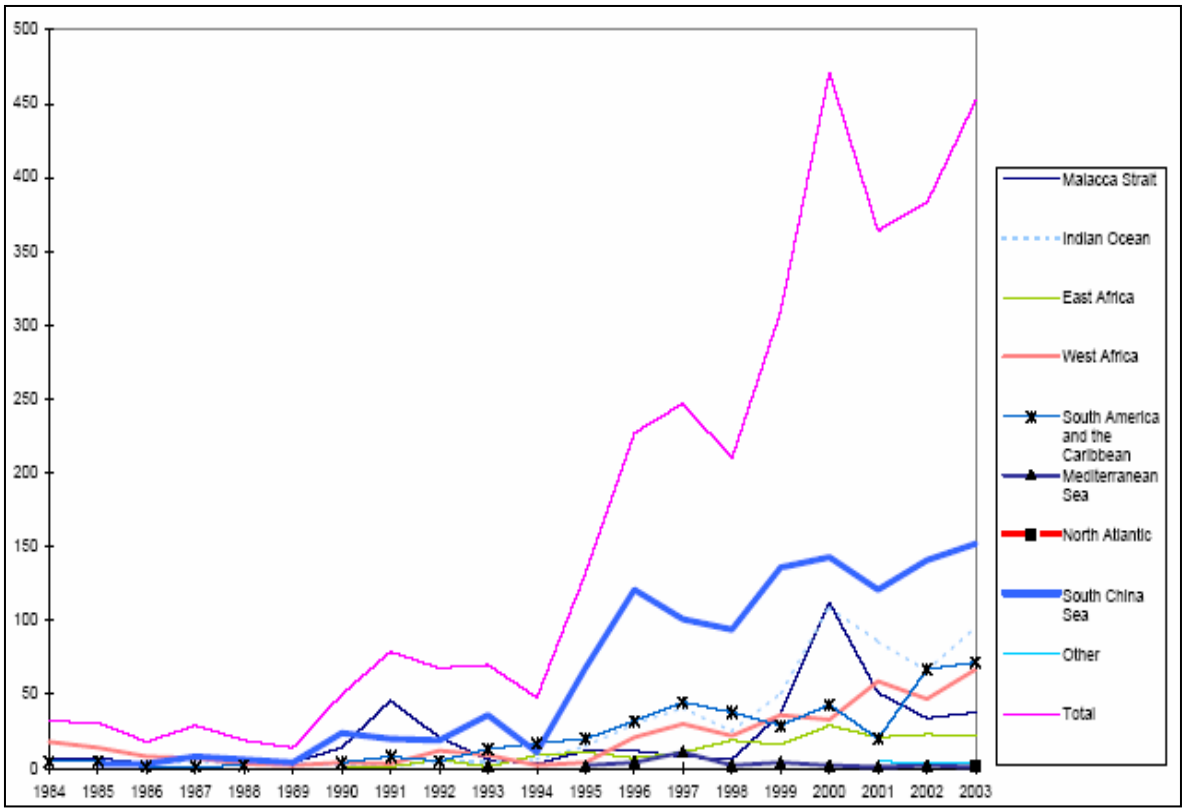

Figure 4. Pirate Attacks on Commercial Shipping 1984-2003 (Source: IMO)

The number of pirate attacks on commercial shipping has increased almost five-fold since the mid-1990s. Most attacks usually occur in the Malacca Straits region or the South China Sea.

These attacks predictably occur primarily in shipping lanes that are close to land, as unpopulated shorelines give cover and sanctuary, and security infrastructure is weak or non-existent. The Straits of Malacca are one such place in eastern Asia, where many pirates "belong to organized crime syndicates comprising corrupt officials, port workers, hired thugs, and businessmen who dispose of the booty."[10] An example of such piracy is summarized in the following incident, reported in the International Maritime Bureau's (IMB) Weekly Piracy Summary.

> In a typical incident, on 21 September (2000), 21-masked pirates raced two speedboats alongside and boarded the Malaysian-flagged tanker, MT Petchem (passing through the northern Malacca Straits towards Singapore).

[10] Gal Luft and Anne Korin, "Terrorism Goes to Sea," *Foreign Affairs*, Vol. 83, No. 6, (2004): p. 62.

> The ship was sailed to a location south of Johore where the pirate transferred the Petchem's cargo of 3,000 tons of diesel oil to an unknown tanker.[11]

These types of attacks, occurring on a regular basis and with increasing sophistication in the Malacca Straits, have caused Singapore's Deputy Prime Minister Tony Tan to warn, "Piracy is entering a new phase; recent attacks have been conducted with almost military precision. The perpetrators are well-trained, have well laid out plans." The financial impact that maritime piracy imposes on the global economy is estimated to be $16 billion per year.[12]

1.2.2 Maritime Terrorism

Osama bin Laden has warned, in no uncertain terms, "By God, the youths of God are preparing for you things that would fill your hearts with terror and target your economic lifeline until you stop your oppression and aggression." This direct threat of attacks against the global economy was reiterated by senior members of the al Qaeda-linked Indonesian terrorist group Jemaah Islamiyah, who "have admitted that the group has considered launching attacks on Malacca shipping."[13]

One terrorist attack that achieved mixed results occurred in October 2002, when the French tanker LIMBURG was rammed by a speedboat loaded with explosives in the Gulf of Aden off the coast of Yemen. Although the new double-hulled ship remained afloat (see Figure 5), the force of the impact "left an oval-shaped hole about 26 feet wide, with the edges indented inward, in the ship's hull which was charred on the starboard side."[14] If more attackers had been involved, or if the cargo had been more volatile, the outcome could have been far more severe.

---

[11] International Maritime Bureau (IMB), *Weekly Piracy Summary*, Kuala Lumpur, Malaysia Maritime Liaison Office, Newsletter, (January/February 2001).

[12] Gal Luft and Anne Korin, "Terrorism Goes to Sea," *Foreign Affairs*, Vol. 83, No. 6, (2004): p. 62.

[13] Gal Luft and Anne Korin, "Terrorism Goes to Sea," *Foreign Affairs*, Vol. 83, No. 6, (2004): pp. 63-64.

[14] Abeidoh, Rawhi, ABC News Website, http://www.vic-info.org/RegionsTop.nsf/0/b55fcf7a272859580a256c4c006ce233?OpenDocument, (accessed 19 July 2005).

Figure 5. Damage to the French Tanker LIMBURG, October 2002

The vulnerability of high-value cargo vessels has been illustrated by numerous attacks using small speedboats and explosives. Increased coordination and effectiveness is very likely in the future, therefore more severe outcomes can be expected.

Another foreboding attack occurred in March 2003:

> The Dewi Madrim, a chemical tanker off the coast of Sumatra, was boarded by ten pirates from a speedboat. They came at three o'clock on a moonless morning; armed with machine guns and machetes and carried VHF radios. They disabled the ship's radio, took the helm and steered the vessel, altering speed, for about an hour. Then they left, with some cash and the captain and first officer.[15]

Although the attackers used the pirate-tested means of driving speedboats alongside to board the tanker, their intention was clearly not to steal cargo from the ship. This situation was eerily reminiscent of the 9/11 hijackers, who only learned to fly large airplanes while airborne, but not to takeoff or to land.

[15] Simon Elegant and Kuala Sepetang, "Dire Straits. Ships That Pass Through Some of the Busiest Waterways in Asia are Often the Target of Pirates. Is a Terrorist Attack Next?" *Time Asia*, http://www.time.com/, (accessed 17 April 2005).

1.3 U.S. AND SINGAPOREAN MARITIME DOMAIN PROTECTION (MDP) INITIATIVES

1.3.1 U.S. Initiatives

The Global War on Terrorism caused the United States and other nations to assess and analyze their strengths and weaknesses as related to Homeland Security and Homeland Defense. The maritime domain has been recognized as one area that contains many opportunities for terrorist attack. MDP initiatives represent attempts by government agencies and organizations to reorient within their areas of responsibility and focus resources on the numerous vulnerabilities of the maritime domain. A list of MDP initiatives was compiled by the Maritime Domain Protection Group.[16] These initiatives represent the capabilities of current U.S. MDP efforts. They also represent simultaneous efforts at the national and local level, often independent and uncoordinated. This "stovepipe" architecture significantly degrades the rapid collection, analysis, and dissemination of actionable intelligence to decision makers.

Current MDP initiatives can be categorized into a MDP Observe, Orient, Decide, Act (OODA) loop.[17] "Observe" initiatives are concerned with acquiring as much data and information from as many sources as possible, as quickly as possible. They represent a shift in the "intelligence gathering" paradigm away from focusing collection efforts on specific threat countries, organizations, or geographic regions. Situational awareness in the maritime domain requires knowing everything all the time, i.e., maritime omniscience. "Orient" initiatives address gathering, fusing, disseminating, and sharing information. They cover issues including databases and shared information, dissemination and cooperation, and a common intelligence picture. "Decide" initiatives address identifying and assigning responsibilities as opposed to identifying decision makers. This category contains the fewest initiatives as identifying decision makers presents the biggest challenge in an information system. "Act" initiatives represent

[16] The initiatives are excerpted from "'As Is' National Maritime Domain Protection System," Naval Postgraduate School Maritime Domain Protection Task Force, December 2004.

[17] Ibid.

anticipation of possible missions derived to protect assets that are open to attacks from the maritime domain.

1.3.2 Singaporean Initiatives

Several Singaporean initiatives of note are their National Security Architecture, Armed Navy escorts for suspect ships, Malaysia, Singapore, and Indonesia (MALSINDO), and harbor Automatic Identification System (AIS).[18, 19] Singapore's National Security Strategy integrates and synergizes the work of different national security agencies in the operations, intelligence, and policy domains. It includes establishment of the National Security Task Force (NSTF), staffed by both police and military elements, to maintain a comprehensive watch over the island and to integrate operational responses on land, in the air, and at sea. The Armed Navy escorts involve the deployment of armed security teams by the Republic of Singapore Navy onboard some merchant ships. The uniformed security teams will escort vessels entering or leaving the port, but only within Singaporean waters. MALSINDO is a trilateral initiative by countries bordering the Malacca Straits, which involves year-round coordinated armed maritime patrols. Seventeen ships from Indonesia, Malaysia, and Singapore conduct around-the-clock naval patrols in the countries' respective territorial waters. A "hotline" has been setup linking the three naval command centers in Batam, Lumut, and Changi to improved coordination.[20] Another Singaporean effort includes accelerated implementation of the AIS to ensure that ships over 300 tons were fitted by the end of 2004. The AIS is an autonomous, self-synchronizing, Interrogator-Transponder System analogous to the Federal Aviation Administration (FAA)-required Identification Friend or Foe (IFF). The transmissions include identifiers, cargo codes, speed, heading, and other pertinent

---

[18] National Security Coordination Centre, *Fight Against Terror*, Singapore's National Security Strategy, (2004).

[19] The Straits Times Interactive, "Armed Navy Escorts for Suspect Ships," http://straitstimes.asia1.com.sg/, (accessed 28 February 2005).

[20] "Piracy and Maritime Terror in Southeast Asia," International Institute for Strategic Studies, Vol. 10, Issue 6, (July 2004): pp. 1-3.

information. In addition, mandatory fitting of ship alert systems will see all vessels operating in the port of Singapore fitted with the AIS by 2006.[21]

1.4 PURPOSE

The purpose of this study was to serve as the Systems Engineering and Analysis (SEA) Integrated Project for SEA Cohort 7 (SEA-7). This cross-campus capstone effort for the SEA students is sponsored biannually by the NPS Wayne E. Meyer Institute of Systems Engineering. The tasking memorandum, dated 9 November 2004 (Appendix A), entitled this study "Maritime Domain Protection in PACOM," and gave the following initial problem statement:

> Design a conceptual System of Systems to defeat and prevent terrorism in the Maritime Domain. Design and assess integrated alternative architectures for sensor, communications, command and control, and reactive force for a coalition of nations, focusing on large ship security, and threats to and from large ships, in the Straits of Malacca. Additionally, design and assess alternative architectures for cargo inspection to include a total ship inspection sub-system that could detect and identify explosive and other dangerous materials so to prevent the use of a large cargo ship as a terrorist vehicle.

The study was directed to remain outside of the political and diplomatic realms, assuming full international cooperation in the Southeast Asian region. The study focused on a generic solution, with capabilities transferable to other geographic areas with necessary modification. Additionally, the study focused on achieving a technical solution within a five-year timeframe. Thus, only technologies with a Technical Readiness Level 4 ("technology component and/or basic technology subsystem validation in laboratory environment")[22] or greater were considered. With Pacific Command (PACOM) as a key stakeholder, the study sought to answer two questions: 1) What is the most effective use of current resources in theater? and 2) Where should resources be focused for the most future cost-effectiveness?

---

[21] "Security Alert, Comprehensive Measures Set to Enter Force in 2004," *IMO News*, No. 1, 2003, www.imo.org, (accessed 12 March 2005).

[22] U.S. Department of Defense, Technology Readiness Assessment (TRA) Deskbook, September 2003.

1.5 REGIONAL CHARACTERISTICS

Although the geographic location was given in the problem tasking document, no specific threat scenarios were identified. SEA-7 performed a threat analysis and identified three plausible threat scenarios to use for the MDP Study.

1.5.1 Geography

The Malacca Straits are located between Sumatra and the Malaysian Peninsula and serve as a major international navigation route linking the Indian Ocean with the South China Sea. The Straits are 500 miles long and from 10 to 220 miles wide. The relatively narrow and shallow shipping channel varies in width, containing three stretches that are less than 24 miles wide. At these points, the 12-mile territorial waters claimed by each of the coastal states, Indonesia and Malaysia, overlap and together cover the whole width of the Straits. In addition, the shipping channel sometimes runs through the territorial water of one or the other of the coastal states, even when the overall width is more than 24 miles.

The Straits of Singapore are the eastern continuation of the Malacca Straits, linking them to the South China Sea. They run between the Indonesian Islands on one side and the southern coast of the state of Johor, Malaysia and the island of Singapore on the other. They are 75 miles long from east to west and are never more than 12 miles wide. The navigation passage frequently runs within the 6-mile limit of the waters of the littoral states. Phillips Channel, located in the Singapore Straits, is only 1½ nautical miles wide at its narrowest point, forming one of the world's most significant traffic bottlenecks. The Malacca Straits can be bypassed through the Sunda, Lombok, Makassar and Ombai-Wetar Straits, which are all within Indonesia's archipelagic waters.[23]

[23] Yaacov Vertzberger, "The Malacca-Singapore Straits: The Suez of the South-East Asia," The Institute for the Study of Conflict, (1982): pp. 57-63.

1.5.2 Meteorology

Due to its geographical location and maritime exposure, the climate in the Straits of Malacca region is characterized by uniform temperature and pressure, high humidity, and abundant rainfall. The average daily temperature ranges from a minimum of 73°-79°F (~23°C) to a maximum of 88°-93°F (~34°C). Temperature extremes can go as low as 67°F (~19°C) and as high as 101°F (~30°C). Typical pressure variations are 4hPa, with pressure extremes recorded at 1016.9 hPa and 1002.0 hPa. Relative humidity averages 84%, with daily fluctuations from above upper 90% in the early morning to around 60% in the midafternoon. Rainfall is heavy, with an average annual rainfall of 92.8" (South Florida, by contrast, receives 56"). Although there is no distinct wet or dry season, rainfall maxima occur in December and April, while the drier months are usually February and July. The high humidity conditions existing in the Malacca Straits makes radio frequency (RF) ducting an issue of concern. Surface-based ducting (occurring 15% to 20% of the time) and evaporation ducting (occurring all the time) are of concern for RF propagation above 3GHz.[24]

1.6 MARINE CHARACTERISTICS

The Straits of Malacca are narrow and shallow straits that are sheltered by land masses to the northeast and southwest. As a result, the marine characteristics are relatively mild and uniform. Generally, the Malacca Straits do not experience extreme sea states or typhoons, though the seas can be choppy, at times ranging up to Sea State 3. The sea state in the more expansive Andaman Sea to the northwest and South China Sea to the east can reach Sea State 5. The weather and wind direction is mostly dictated by the northwest (December to April) and southeast (June to October) monsoons. Average water temperature is around 88°F (~31°C) during the day and 79°F (~26°C) during the night. The water temperature is quite constant and isothermal, and it is very closely associated with the air temperature as expected, due to the shallow depths of the water. The currents in the Straits of Malacca are quite constant, averaging around 1/3 to 2 kts

[24] Data from the National Environmental Agency's Website, http://app.nea.gov.sg/, (accessed 17 February 2005.

through the year. The monsoons control the currents elsewhere, driving inflow waters from the Bay of Bengal through the western channels from June to August during the northwest monsoon. When these winds die, southeastward currents gradually form and are maintained and enhanced by the southeast monsoon from December through February.[24]

1.6.1 Shipping Traffic Density

The Straits of Malacca provide passage to nearly 700 ships per day, 135 large transport vessels per day, two-thirds of the world's liquefied natural gas (LNG) shipments, and approximately 80% of China's imported crude oil.[25] Annually, more than 1,100 fully laden super tankers pass eastbound through the straits, many with only a meter or two of clearance between keel and bottom.[26] More than 30% of all seaborne commercial traffic navigates the Malacca Straits, providing a vital source of income for millions of Asians.

Since the busiest commercial routes flow through the Straits of Malacca, its crowded, shallow, and narrow passages are a concern for maritime and environmental safety. The 1½-mile wide Phillips Channel in the southeast entrance to the Malacca Straits makes these straits a highly vulnerable chokepoint. If the Straits of Malacca were closed, transit time and distance for nearly half of the world's fleet would divert through the Sunda or Lombok Straits, adding four sailing days. Additionally, tanker demand would increase beyond its current near-capacity condition, and freight rates would rise for a period of time.[27] All excess capacity of the world fleet would be absorbed, with the strongest effects on oil and dry bulk shipments.

---

25 John H. Noer and David Gregory, "Chokepoints – Maritime Economic Concerns in Southeast Asia," Center for Naval Analyses, (1996).

26 United States Pacific Command, *Asia-Pacific Economic Update*, Vol. 2, (2002).

27 Erik Kreil, "World Oil Transit Chokepoints," Country Analysis Briefs, http://www.eia.doe.fov/emeu/cabs/choke.html, (accessed February 2005).

1.7 THREAT SCENARIOS

Three threat scenarios were developed to encompass current and potential future threats to the maritime domain in the Straits of Malacca. The threats were based on either proven threats, similar to the small boat attack against the French tanker LIMBURG, or known potential threats, such as the smuggling of a nuclear weapon into a congested port. Research and brainstorming uncovered the majority of the major terrorist threats to shipping (see

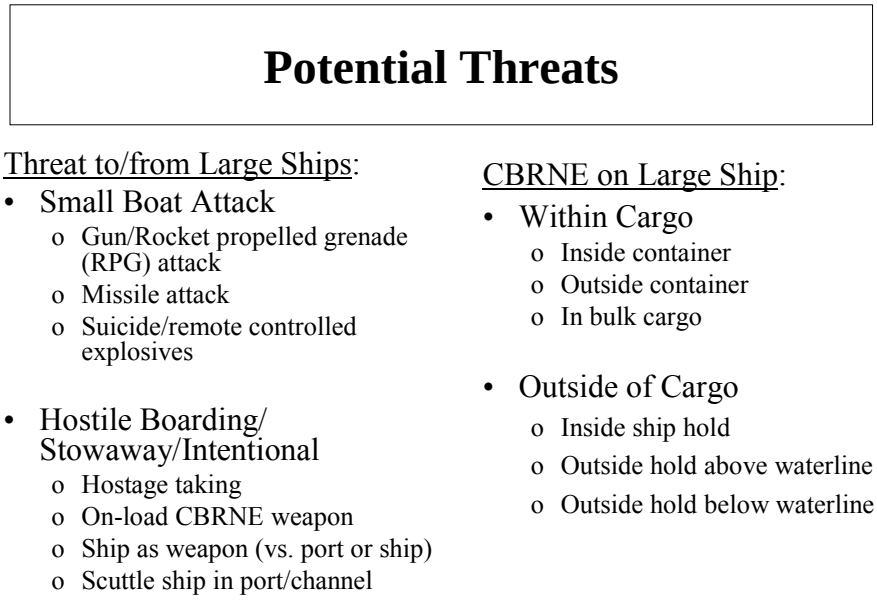

Figure 6), with an emphasis placed on the operating conditions in the Straits of Malacca.

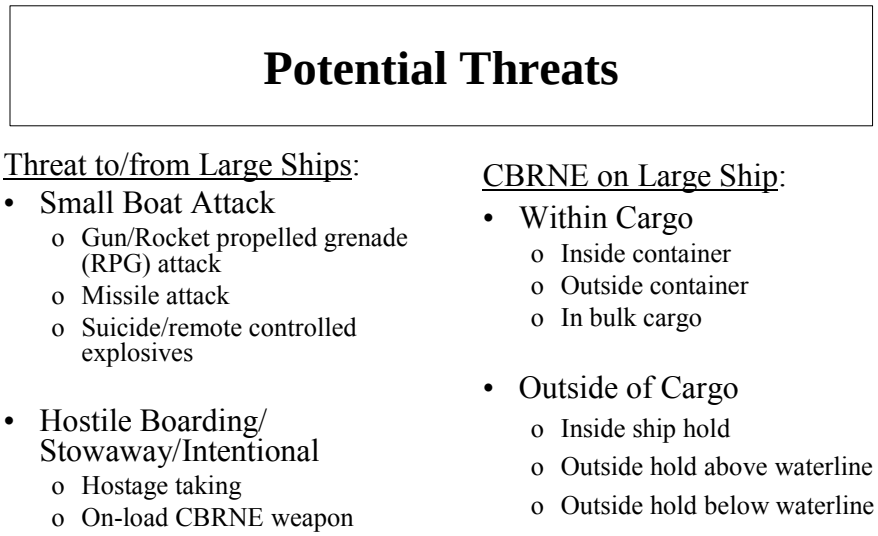

Figure 6. Potential Maritime Domain Threats to Shipping

The SEA-7 Cohort developed this list of potential major terrorist threats to maritime shipping in the Straits of Malacca.

With the focus on that region of the world, three major threat scenarios were selected: the SBA against a large merchant vessel, a SAW attack against a port facility (specifically liquid natural gas tankers), and the smuggling of a weapon of mass destruction (WMD) into the region. These scenarios were deemed to include the most credible shipping threats in the region, but they also included many of the factors that were found in other threats.

A threat risk graph was developed to show the relative likelihood of an attack verses the relative consequences of the attack (see Figure 7).

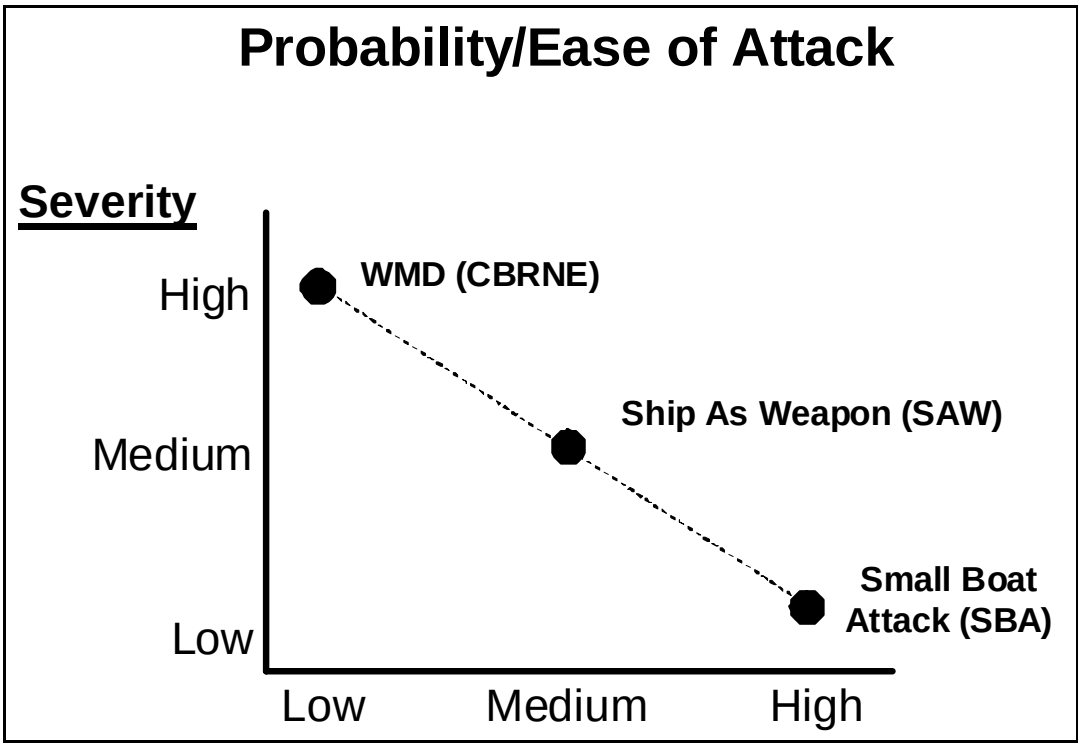

Figure 7. Threat Risk Comparison

The WMD scenario became more critical than a SBA or SAW. Even though there is a higher probability of a SBA or SWA, the severity of a successful attack using a WMD is higher.

It showed that the most likely type of attack was the SBA; however, this type of attack had the lowest level of consequences. This type of attack has been successfully conducted twice: first against USS COLE while in port in Aden, Yemen, and then against the French tanker LIMBURG off the coast of Yemen. In both cases there was substantial damage to the hull of the ship, and in the case of COLE there was loss of life. However, in each case there were limited consequences. With COLE, the U.S. Navy was forced to raise its security measures, and was denied the use of one of their warships for several months. The LIMBURG suffered significant damage to the hull, and lost several thousand gallons of oil from the cargo hold; however, it was back in service within weeks. Both of these attacks gained notoriety in the media because they were successful, yet they had very little lasting impact on either the Navy's operational policies or the shipping company's practices.

The second type of attack considered was the SAW. The potential for this type of attack has been demonstrated to be within the capabilities of current terrorist organizations, and an attack of this type would have a significant financial impact on the target country. In a documented incident in the Straits of Malacca, a group of terrorists took control of a large merchant vessel, had one of their operators maneuver the vessel for several hours, and then debarked the vessel, taking only the captain and first mate of the merchant ship. This proof of concept operation showed that the terrorists were capable of taking and operating a large merchant vessel for their attack. This type of attack could be devastating if the hostage vessel were rammed into either port or refueling facilities, which would render the port inoperable for a prolonged period of time. Scuttling a vessel within the approach to a major port was not considered because salvage crews could clear the obstruction in less than 24 hours.

The third major category of attack was the WMD attack. It is a stated goal of Al Qaeda to gain control over a nuclear device for the purpose of detonating it in a highly populated area. This threat could be further extrapolated to include the introduction of chemical or biological agents into a region with the intent to distribute them. A WMD attack would have the most significant financial and political impact on the target region.

1.7.1 Scenario 1 – Small Boat Attack (SBA)

The first scenario was a SBA scenario, designed to demonstrate the quick reaction capabilities of the maritime domain protection system. It was based on the French tanker LIMBURG attack off the coast of Yemen, where a speedboat carrying explosives rammed and blew a hole in the side of the tanker. The SBA scenario called for an explosives-laden small boat to attack a merchant vessel transiting the Straits of Malacca. The small boat was approximately seven meters long, capable of 30 kts, and loaded with 1,000 pounds of TNT armed with both an impact fuse and a remote detonator. The SBA scenario was set around midday with standard environmental conditions for the region. The scenario had the small boat exiting from the area around Pulau Assan, a fairly narrow portion of the Straits that is frequently congested. This allows the maritime domain protection system to be tested against a very time-critical target, in a congested traffic

area. The SBA scenario forced the system to react in a timely manner and to be selective enough to define not only the attack, but also to determine which ship is the target of the attack so that it can be defended.

1.7.2 Scenario 2 – Ship As a Weapon (SAW)

The SAW scenario focused predominantly on port security. This scenario was designed around a terrorist "ghost ship," or a ship that was reregistered and carries sufficient paperwork to be overlooked as a terrorist vessel. In the SAW scenario, JADEGAS was a "ghost ship" loaded with 5,200 m^3 of oil tanker tasked with ramming the Mobil Oil facilities on Palau Pesek in the Jurong Island Petrochemical Complex, a 12-square mile complex comprised of seven small islands in the port of Singapore. JADEGAS was a 113-meter vessel of 5,000 GT, and capable of speeds up to 14 kts. This scenario was set at night, with cooler temperatures and moderate environmental conditions. The SAW vessel was responsive to initial VHF hails, and compliant with all good seamanship practices. It was not until communications were severed with the onboard harbor pilot that there was any indication of danger from the vessel. When the vessel reaches the final breakwater, it accelerates at its maximum rate, and turns directly toward the piers. This scenario is designed to flex the maritime domain protection system's capabilities to work at night, in a limited time period to defend a high value unit. The threat of terrorists commandeering a vessel while at sea with the intent of using it as a SAW was not chosen as an alternative because of the current capabilities resident within U.S. and Singaporean forces to combat that situation. The U.S. Navy's capability to retake a vessel at sea has existed for several years, and the Singaporean defense forces have a special reaction force that has been trained for this purpose. The Special Tactics and Rescue (STAR) Unit is a tactical armed unit of the Singapore Police Force (SPF). Its "Maritime Assault Capability (MAC)" includes combating armed and dangerous criminals on vessels smuggling illegal immigrants or pirated goods.[28] Instead, a later detection of the attack was chosen, because it was a much harder problem to solve.

[28] Muhd Juffry Bin Joihani, "MAC for the Men in Black," *Police Life*, *The Singapore Police Force Magazine*, Vol. 31, No. 2, (February 2005): p. 37.

1.7.3 Scenario 3 – Weapons of Mass Destruction (WMD)

The third scenario was a WMD scenario, in accordance with the current threat of WMD throughout the world. In this scenario, a legitimate merchant vessel inadvertently transported a 40-foot container containing a 20-KT Russian-made nuclear weapon. The container housing the weapon was loaded in the port of Shanghai, China, with an ultimate destination of Singapore. The target container was one of 32 containers loaded at the Apple Ipod plant in Shanghais. All paperwork was valid and in order for the shipment. This scenario was chosen because of the existence of Russian-style nuclear devices (some of which are missing), the stated desire of terrorist organizations to negatively impact world trade, and the belief that if terrorist organizations were to get their hands on a WMD they would not hesitate to use it. This scenario tests cargo inspection on both the land and sea sides of the inspection process.

1.8 CONCEPT OF OPERATIONS (CONOPS)

A CONOPS was written in order to establish an operational framework for potential solutions to prevent and defeat the terrorist threat in the Straits of Malacca. The initial Maritime Domain Protection CONOPS was similar to the U.S. Federal Aviation Administration's (FAA) Air Traffic Control (ATC) system, with a force response capability. This system was divided into four subsystems:

1. Sensor capability.
2. Command, Control, Communications, and Intelligence (C3I) capability.
3. Force Response capability.
4. Cargo Inspection System.

The underlying structure to this system architecture resembled Network Centric Warfare, to include three overlapping "layers":

1. Sensor Network.
2. C3I Network.

3. Force Network.

Where possible, existing forces in theater were used to the maximum extent practical.

1.8.1 Sensor Network

A network of space, air, surface, or subsurface sensors (active and/or passive), either single or in combination, is used to locate and track surface contacts within the Area of Regard (AOR). The Sensor Network would effectively track all surface contacts above a minimum gross weight (initially 300 GT). This information is fed into the C3I Network, and its accuracy contributes to minimizing both Force and Inspection response time.

Two Cargo Inspection Systems were included. Both were capable of searching bulk and container cargo for WMDs. Nuclear, biological, chemical (NBC), and conventional explosives are viable threats. A "port" system inspected the cargo either in port or as it is loaded onboard a ship. A "ship" system inspected both the cargo loaded on a ship and the ship itself. Two levels of "ship" inspection systems exist: one quick, less thorough inspection for general or random ship inspections, and another slower, more detailed inspection for suspect/high risk ship inspections.

1.8.2 Command, Control, Communications, and Intelligence (C3I) Network

Regional C3I Command Center(s) assimilated information from the Sensor Net. An effective Command and Control (C2) capability enables the timely, accurate display of maritime domain information to the relevant commander. A redundant Communications Network ensures quick, reliable, two-way information flow throughout the AOR. Computers processed information for threat recognition and display, and a computer database tracks historical and expected shipping data. Intelligence was gathered from outside organizations, but will be fed into the C3I Net.

1.8.3 Force Network

An active and passive response capability was included to counter maritime terrorist attacks in the AOR. This response capability consisted of a layered defense, and possessed both destructive and nondestructive reaction options. Consideration was also given to cutting off the source of terrorist attacks by forcibly or nonforcibly taking out terrorist bases of operation and supply chains when intelligence or other means located them. The CONOPS also assumed that the response forces would provide transportation for active WMD Inspection Teams to a COI, when directed, in response to intelligence, an anomaly, or at random.

1.9 SCOPE

1.9.1 Participants

The Meyer Institute of Systems Engineering and Analysis 7th Cohort (SEA-7) consisted of 21 NPS students from a variety of backgrounds, including 13 U.S. Navy, 1 U.S. Army, 2 U.S. civilian (Northrop-Grumman), 2 Turkish Air Force, 1 Singapore Defense Science and Technology Agency, 1 Argentinean Army, and 1 Mexican Navy. The SEA-7 Cohort began work on the cross-campus Integrated Project in October 2004, with a requirement to be completed with the study, final presentation, and final paper by their 17 June 2005 graduation day. SEA-7 was joined by 26 students from Singapore's Temasek Defense Systems Institute (TDSI) in January 2005. These students arrived at NPS following a six-month course of study in Singapore, and would continue work on individual theses following their participation in the SEA-7 Integrated Study, in order to graduate in December 2005.

The SEA-7/TDSI students organized and coordinated the work and expertise of fellow students, professors, industry experts, and stakeholders from the NPS campus, U.S. Department of Defense, and U.S. National Laboratories in order to incorporate leading-edge technologies and capabilities to develop and meet the system requirements. In addition to the entities shown in Figure 8, representatives from the U.S. Coast Guard (USCG), U.S. Northern Command (NORTHCOM), Naval Special Warfare Command (NSWC), and Office of Homeland Defense (OHD) were consulted on topics that were appropriate to their area of expertise/interest.

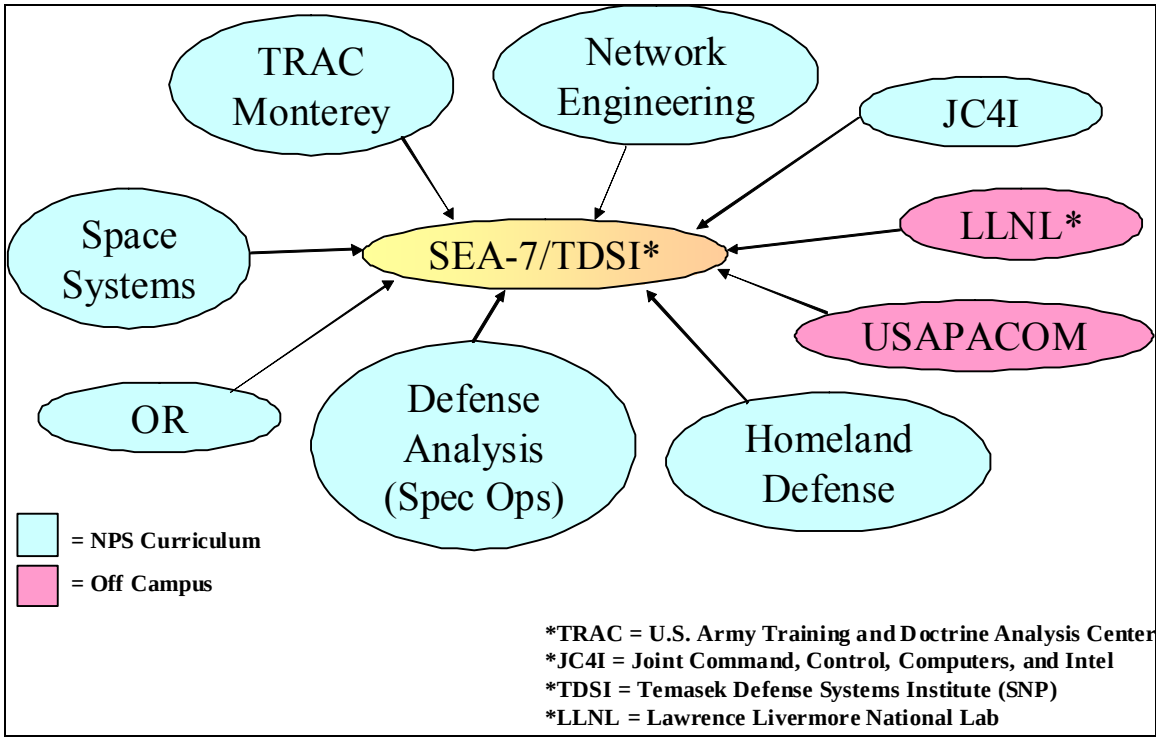

Figure 8. NPS MDP Study Participants and References

The SEA-7 project exemplifies the monumental effort involved with integrating the work of various groups and individuals, representing different areas of expertise and skill sets, from various locations. The project integrated students from Singapore's TDSI, incorporated the work of students from various curricula across the NPS campus, industry experts (Lawrence Livermore National Lab), and USPACOM.

1.9.2 Systems Engineering Design Process (SEDP)

The SEDP was used to guide and facilitate the many facets of work done in support of the MDP project. An iterative process, the SEDP allowed for constructive generation and organization of ideas based on continuous feedback. Progression through the SEDP was indicated by four phases: Problem Definition, Design and Analysis, Decision Making, and Implementation. The relationship among the phases is shown in the flow diagram of the SEDP (see Figure 9):

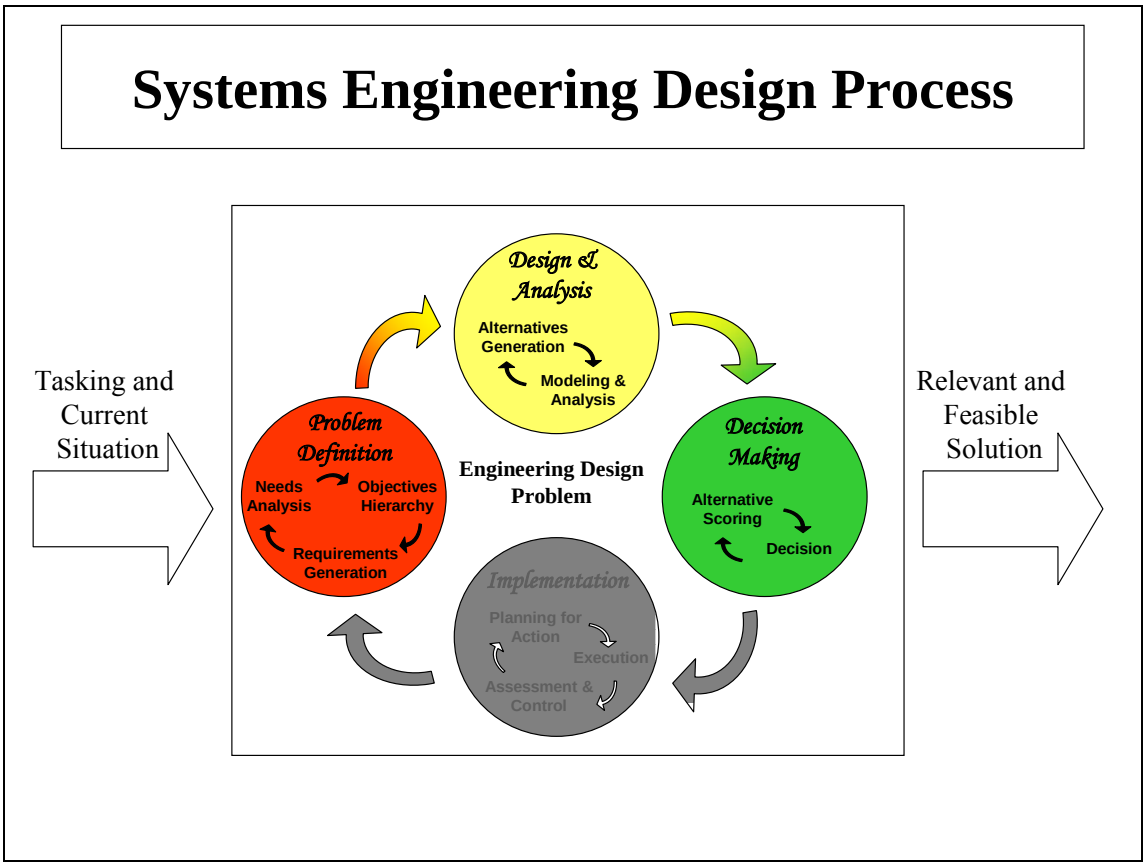

Figure 9. SEDP Flow Diagram

Supporting each phase was a unique subset of steps that focused on achieving the individual phase's goals. Similar to the iterative relationship between the phases, the subsets of tasks were also cyclic. The iterative steps contained within the iterative phases allowed for constant refinement and improvement during the process.

The goal of the Problem Definition phase was to unambiguously define the challenge at hand. Needs Analysis and Value System Design were the main steps in this phase. The Needs Analysis step attempted to identify system requirements by involving system decomposition, stakeholder analysis, affinity diagramming, Pareto analysis, functional analysis, and futures analysis. The Value System Design step attempted to arrange and rank the system requirements through the creation of a value hierarchy, followed by the determination and weighting of measures of evaluation.

The goal of the Design and Analysis phase was to generate and examine potential solutions to the problem. Alternative Generation and Modeling and Analysis were the

steps in this phase. The Alternative Generation step used morphological charts and structured brainstorming to develop multiple potential solutions to the problem. The Modeling and Analysis step sought to compare the alternatives by using technical performance models, agent-based models, and statistical analysis and modeling tools in an integrated overall modeling plan.

The goal of the Decision Making phase was to compare the modeling results for the alternatives and recommend the best course of action. The SEDP was only completed through the Alternative Scoring step for this conceptual study, since a decision recommendation was the desired final outcome. Therefore, the Decision step was not accomplished. Alternative Scoring ranked the alternatives based on five factors: cost, schedule, performance, risk, and commercial impact.

The goal of the Implementation phase would have been to execute the selected solution, monitor its progress, and solve the determined problem. This phase in the SEDP was beyond the scope of the project and, therefore, was not performed.

Throughout the application of the SEDP, changes and adjustments were made, and past work was revisited and revised as new information and insights became available. This constant modification resulted from the continual feedback inherent in the SEDP, and led to a more robust solution than would be available with a one-time-through approach. Thus, the SEDP served as an extremely useful framework to organize and structure the work that was done in the MDP Study.

1.9.3 Organization

Based on the MDP operational concepts, the SEA-7 Cohort was ultimately divided into four main groups: Sensors; Command, Control, Communications, and Intelligence (C3I); Force; and Sea/Land Cargo Inspection. Smaller groups of TDSI students were assigned to each of these main groups based on which of the six TDSI specialization areas they belonged to: Sensors, Communications, Information Assurance (IA), Operations Research (OR), Weapons Systems, and Land Systems. This organizational structure and the associated interfaces with external organizations are shown in the organizational chart in Figure 10.

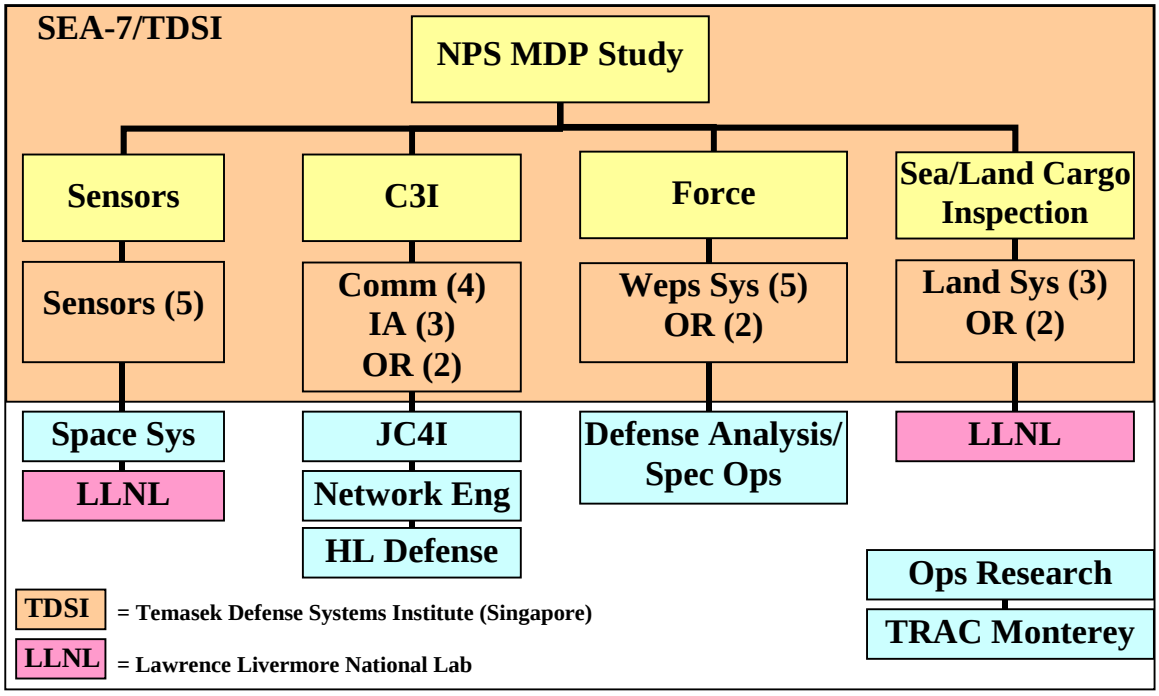

Figure 10. MDP Study Group Organizational Chart

The SEA-7 Cohort was organized according to the functions of the MDP System; Sensors, C3I (Command and Control, Communicate, and gather Intelligence), provide a Response Force, and Inspect. Students from Singapore's TDSI, represented Communications, Sensors, Weapons Systems, and Operations Research tracks that easily integrated into the functions-based organization.

The Sensors Group was responsible for designing a sensor network architecture to search, detect, and track surface vessels entering the AOR by providing real time data and information to the C3I Centers. The C3I Group was responsible for a communications network that could relay the information throughout the system, and for a C2/Intelligence Center to monitor activity in the AOR, and to process data and information to classify the intention of the vessels entering the AOR and facilitate decision-making to the operators. If a hostile, unfriendly, or unknown contact was identified, a force deployment strategy devised by the Force Group would be implemented to intercept the contact of interest (COI) for further inquiries or follow-up actions before any undesirable catastrophic or hazardous events occurred. On the other hand, if suspicious cargo was onboard on a vessel, a full-scale inspection would be

reinforced as dictated by the Sea/Land Cargo Inspection Group, and carried out by personnel from the Force Group.

1.10 METHOD

SEA-7 had two initial tasks: 1) to design a conceptual System of Systems to "defeat and prevent terrorism in the Maritime Domain," specifically focusing on the Straits of Malacca, and 2) to design and assess alternative architectures for cargo container inspection, including a total maritime inspection subsystem that could detect and identify explosives and other dangerous materials. The original group of 21 SEA-7 students was initially divided evenly into two groups that would handle the two tasks. The "MDP Group" would study the broader systems integration effort and focused primarily on Sensors, C2, and Force architecture. The "Cargo Inspection Group" focused mainly on a critical subsystem geared toward a total maritime inspection capability for WMD and explosive materials.

After dividing into the two research groups, an organizational structure was devised in which the MDP Group was responsible for the overall architecture, with the Cargo Inspection Group contributing as a functional component of the larger system. The MDP Group divided into three functional subgroups: Sensors, C3I, and Force (see Figure 10). The Cargo Inspection Group also separated into two subgroups: Sea Inspection and Land Inspection. Although the organizational structure was broken up into a system of subordinate groups, the original two groups (MDP and Cargo Inspection) stayed intact through the Needs Analysis phase. Following the Needs Analysis phase, each subordinate group then conducted individual work through the remainder of the SEDP.

The 26 TDSI students participated with the SEA-7 Groups in the final portion of the Problem Definition phase, through Requirements Generation and Alternatives Generation. With detailed requirements and alternatives to work on, the TDSI Groups broke off to perform individual work, while remaining in close contact with their SEA-7 lead group. At the completion of the Modeling and Analysis step of the Design and Analysis phase, the work of the TDSI Groups was combined with that of the

SEA-7 Groups into an integrated whole. This allowed the work of the Decision Making phase to be done with information from all groups, including student theses from across campus.

The entire process thus began with a large group and a common goal, divided into smaller and smaller groups to perform individual work, while maintaining close contact with one another, which then assembled their individual work into an integrated final product.

1.11 CHRONOLOGY

In July 2004, SEA-7 received preliminary information concerning the topic of the integrated project. In conjunction with a class project in the Systems Engineering and Architecture course, SEA-7 began a groundwork problem study of the broader topic of MDP. Following the phases of the SEDP, the preliminary study phase was concluded in October 2004 and progressed to a more focused Needs Analysis of "Maritime Domain Protection in PACOM." During this phase, a video teleconference was conducted with students from the TDSI program in Singapore to study methods and preliminary focus areas that would be covered when they arrived at NPS in January 2005.

The official tasking document was written in November 2004, and sent to stakeholders for comment. The Wayne E. Meyer Institute of Systems Engineering officially approved the tasking document for the Office of the Deputy Chief of Naval Operations for Warfare Requirements and Programs (OPNAV N7) in December 2004. Following tasking approval, SEA-7 conducted a campus-wide, open invitation briefing to generate interest for collaborative and follow-on thesis research.

Objective tree hierarchies for the overarching system and sublevel systems were designed and presented for the first in-progress review (IPR) in January 2005 and for the second IPR in February 2005. These IPRs generated important feedback from stakeholders, and were instrumental in beginning the Alternatives Generation phase of SEDP, which was concluded in March 2005. During the period of time between IPRs 1 and 2, SEA-7 students worked closely with their TDSI associates; organizing research efforts, planning meetings, and defining requirements that would prepare them

for IPR 2 and further reviews. Following IPR 2, in March 2005, notional inputs were generated for the Modeling and Analysis phase. On 16 March 2005, a design review meeting was held with all groups to determine the overall metrics and the focus of the modeling approach.

The third IPR, conducted on 29 April 2005, showcased initial modeling results from each team within SEA-7 and TDSI, and generated additional feedback on what analysis efforts should be advanced. The month of May 2005 saw continued refinement of models and analysis methods, while portions of the final paper were compiled for peer review. The final SEA-7 presentation of results and conclusions was conducted on 1 June 2005 at NPS in Ingersoll Auditorium before an audience of defense contractors, military professionals, professors, and fellow students.

2.0 PROBLEM DEFINITION

2.1 NEEDS ANALYSIS

Needs Analysis was the first step in the Problem Definition phase of the Systems Engineering Design Process (SEDP). The primary purpose of Needs Analysis is to develop a Revised Problem Statement, or Effective Need Statement, that reflects critical stakeholder concerns. It provided justification for proceeding further and expending time, effort, and other resources in the design process. The resulting Effective Need Statement was the cornerstone on which the entire subsequent design and decision process was built.

2.1.1 Needs Analysis – Maritime Domain Protection (MDP) Group

The Initial Primitive Need Statement presented to the MDP Group in the tasking memo (Appendix A) was to "Design a conceptual system of systems to defeat and prevent terrorism and piracy in the Maritime Domain." The intent was to design and assess integrated alternative architectures for a coalition of nations, potentially focusing on the Straits of Malacca. The group conducted Needs Analysis by utilizing a variety of tools including System Decomposition, Stakeholder Analysis, Input/Output Model, and Functional Analysis to determine an Effective Need Statement from the Initial Primitive Need Statement.

2.1.1.1 System Decomposition – MDP Group

System Decomposition enabled the group to identify a hierarchical structure and the major functions and components of a MDP system. The three levels of the hierarchical structure were super, lateral, and subsystems. The super systems relative to the MDP system were national defense, command, commerce, security, and the International Maritime Organization (IMO). Lateral systems included ground and air antiterrorism/security systems, nonorganic intelligence network, and maritime tracking networks. MDP subsystems included global positioning system (GPS) tracking systems, identification systems (e.g., the Automatic Identification System (AIS)), sensors,

response/inspection teams, Command and Control (C2) Systems, force, communication networks, and organic Intelligence, Surveillance, and Reconnaissance (ISR).

The system included structural, operating, and flow components. The structural components consisted of force (including patrol and inspection assets), ISR, C2 Centers (including analysis/response teams), Communications Systems, and decision support. Operating components included sensor networks, Inspection Teams, C2 Centers, Intelligence Centers, and communication networks. Flow components were MDP information, threats, and vessel status (i.e., hostile, unknown, friendly).

2.1.1.2 Stakeholder Analysis – MDP Group

Stakeholder Analysis began with the identification of critical assumptions and constraints on the problem. These assumptions and constraints set the boundary conditions for the problem and framed the range of problem solutions. These "boundaries" came from variety of sources and included assumptions ranging from strategic to tactical. In many cases, there was insufficient stakeholder access, based on the broad scope of this problem and the international implication of its results. Stakeholder Analysis was conducted primarily through research and interviews with "potential" stakeholders. The need for accurate and timely intelligence was a common need, want, or desire of each MDP stakeholder. An interview with a United States Coast Guard (USCG) operational intelligence officer provided insights into the operational issues of actual implementation.[29] He also identified limitations of current capabilities such as lack of operational intelligence, data fusion, sharing, and disseminating information. These current issues and limitations provided a basis for determining "what an MDP system should do (i.e., its functions)."

2.1.1.3 Input-Output Model – MDP Group

A basic system Input-Output Model was designed utilizing the information gained from the Stakeholder Analysis, in order to visualize the MDP

[29] Phonecon interview with CDR Barry Compagnoni, USCG Intelligence Officer, (East Coast), Key West, FL; current Masters thesis student in the Homeland Defense (HD) program at the Naval Postgraduate School, Monterey, CA, (13 March 2005).

architecture as a system with Inputs and Outputs. The Input-Output Model developed by the MDP Group (see

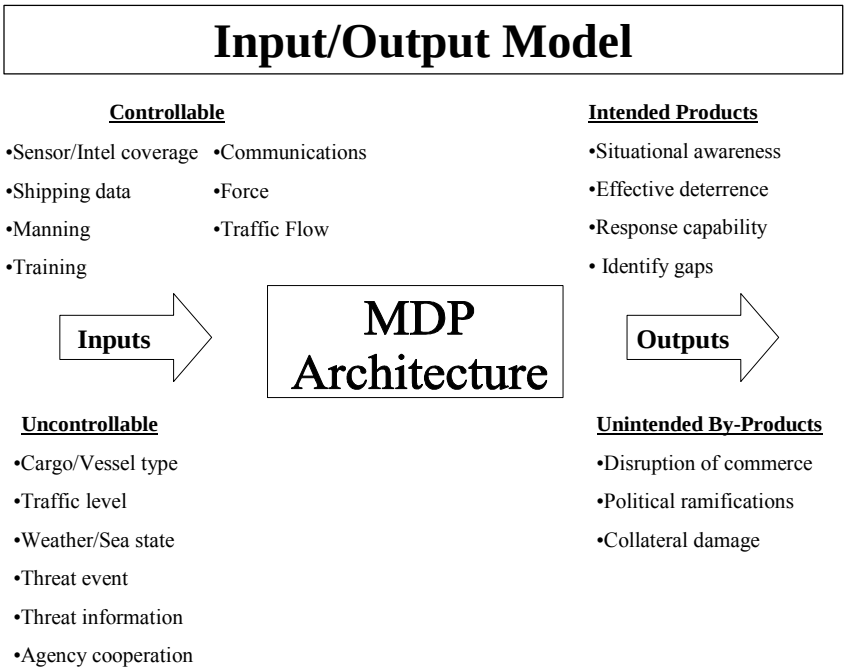

Figure 11) shows the Controllable and Uncontrollable Inputs and the resulting Intended Outputs and Unintended By-Products.

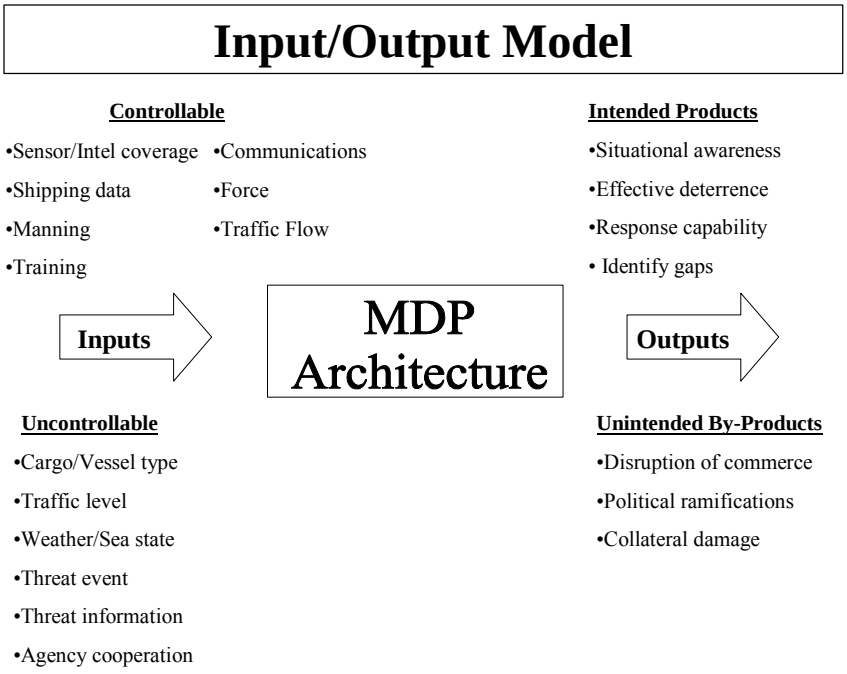

Figure 11. MDP System Input-Output Model

The Input-Output Model separated the MDP system from its surroundings, giving a different perspective of the system. This was useful for determining which parameters could be used to influence the system outcome, and which system outcomes were undesirable.

System design and performance would be affected by both Controllable and Uncontrollable Inputs. The Controllable Inputs (sensor coverage, communications, shipping data, traffic flow, manning, training, and force) led to the system's C3IS (C2, Communications, Intelligence, and Sensors) function. The Sensor and Intelligence Coverage Inputs indicated a requirement for an intelligence subsystem to provide the commander with relevant and timely information. Three types of Uncontrollable Inputs were identified: *unknown* such as threat event or cargo/vessel type; *estimable* such as threat information, agency cooperation, or traffic level; and *random* such as weather or sea state. The primary Intended Output of the system was to create a high level of situational awareness and response capability that would deter and prevent attacks. The nature of the threat was such that the intelligence "subsystem" would take Uncontrollable Inputs and develop a desirable Output through the analysis and fusion of data. Unintended By-Products included disruption of commerce, political

ramifications, and collateral damage. The costs associated with delays and/or rerouting led to the adoption of minimizing the impact on commercial entities as a system measure of effectiveness (MOE).

2.1.1.4 Functional Analysis – MDP Group

The Functional Analysis step of the Problem Definition phase determined what the system should do to meet the stakeholders' needs, wants, and desires. It provided a system overview of the process being designed. From this overview, objectives and metrics could be linked to functional areas in order to develop a value systems design for the system. The MDP Group identified what needed to be accomplished, established a hierarchy of these needs, and identified resources and components.

The components of the Observe, Orient, Decide, and Act (OODA) loop[30] best described the basic functions of the MDP system. The system had to Observe and Orient based on threats in the maritime domain, and then Decide on an appropriate action. The Observe function included collecting, searching, tracking maritime traffic, detecting hazardous material, and providing early warning. These functions could be generalized as surveillance and intelligence. Orient, Decide, and Act could be generalized as C2. Subsequently, OODA evolved into C3IS by combining the Orient and Decide functions into the Communications, Command and Control, and Intelligence (C3I) function, and associating Observe and Surveillance. The Decision component was further divided into C3I supporting functions. Each of these C3I Decision-supporting functions had associated subfunctions determined by asking the question, "What does the system component do?," while ignoring "how" the system would perform the function.

A Functional Flow Diagram (Figure 12) was developed as part of Functional Analysis in order to delineate the logical functional process of what the system would do.

[30] Robert Coram, Boyd: The Fighter Pilot Who Changed the Art of War, Back Bay Books, May 2004.

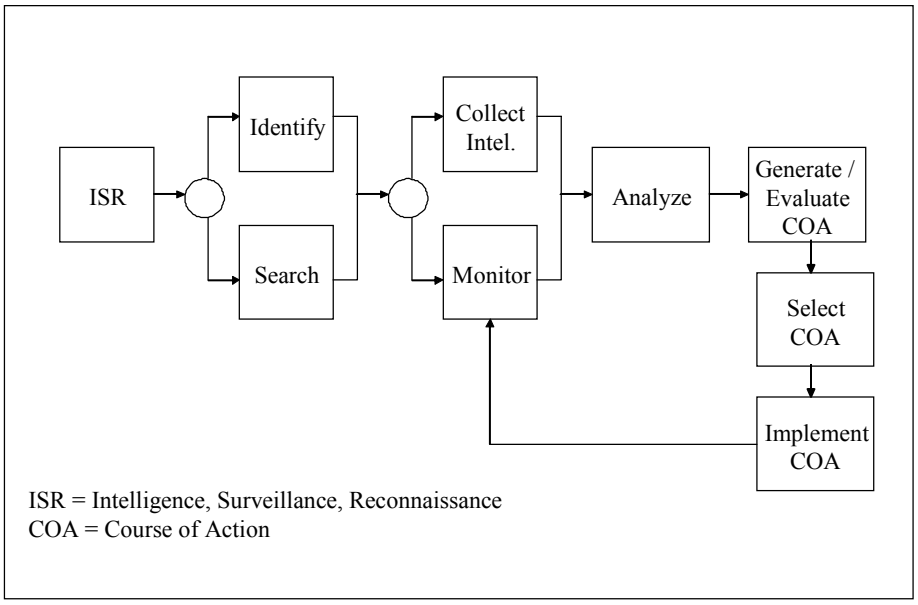

Figure 12. MDP System Functional Flow Diagram

The Functional Flow Diagram gave a chronological view of the way top-level functions related to each other. This perspective was useful for determining how the outputs from some functions served as inputs to other functions.

Stepping through the Functional Flow Diagram provided a picture of how the system would work. Once installed, the ISR system would actively "detect" by searching and identifying contacts. Intelligence would be collected while the contact was monitored. Analysis would provide information to enable the decision maker to choose the appropriate COA.

The Functional Flow Diagram was used as an aid in the creation of the Functional Hierarchy (Figure 13). The Functional Hierarchy delineated "what" the system did by the functions Sense, C3I, and Force.

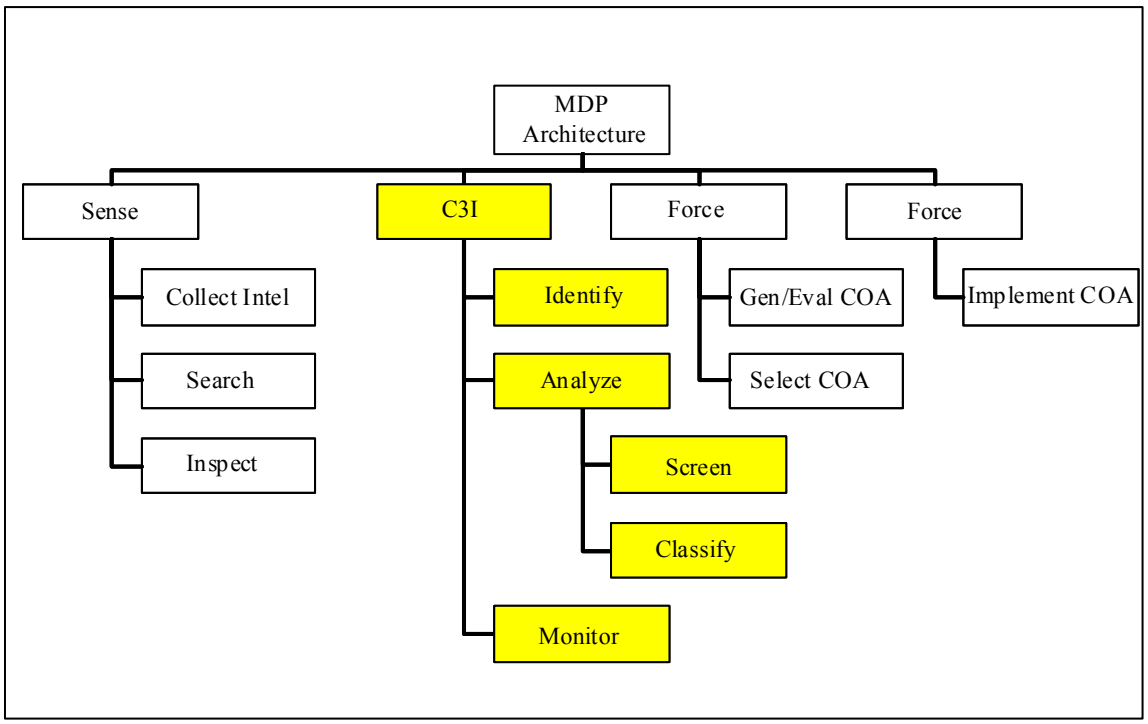

Figure 13. MDP Architecture Top-Level Functional Hierarchy

In order to effectively defeat an attack in the maritime domain, the MDP Architecture was required to perform these top-level functions with the associated subfunctions.

It also identified "how" the system accomplished each function. For example, C3I was accomplished by identification, analysis, and monitoring contacts of interest. The FHD also completed the evolution of the OODA loop to the C3I and Sensors subsystems.

Communications: Table 4 contains a list of the Communications subfunctions:

Communications
Transmit/Receive
Process -Voice -Data -Image
Sort -Filter -Fast Track
Interpret -Language -Data Type
Encrypt/Decrypt
Network

Table 4. Communications Subfunctions

This list of Communication Subfunctions was the basis for upper-level system requirements to enable the C3I System to operate in the overall MDP System.

The Communications architecture was required to be capable of transmitting and receiving multimodally, with the capability to process voice, data, and image exchanges. In addition to transmitting and receiving relevant data, the communications architecture needed to sort information—filtering communications to prevent data overload at one node or on one platform and ensuring actionable information did, in fact, receive appropriate action in a timely manner. Additionally, fast-tracking time critical, priority information to the correct decision and action components was required. Receiving timely and relevant information ensured a shared situational picture and common situational awareness between the C2 elements and the action elements.

Since the Communications architecture was designed for a coalition of nations, there would be a need for language translation during transmission and/or at reception. In addition, data type would need interpretation at various nodes to ensure proper display and relevance. Another concern was the "symbology" differences associated with developing a system for multinational use. The communications network would not be effective unless relayed information could be readily understood such that individual action elements, regardless of nationality, had a clear operational picture and

the same understanding of C2 decisions that determined actions. Another consideration arising from the design of architectures for use within a multinational force structure was the difference among the nations in technology development and existing commercially and militarily available and incorporated technologies. Because of these inherent differences, data sorting and processing would differ from nation to nation, possibly requiring data conditioning between communications nodes or platforms. Security was a consistent concern in multinational operations and it necessitated encryption and decryption capability at transmission and reception nodes.

The Communications architecture would network a variety of communications equipment, nodes, platforms, and other applicable technologies. Therefore, a function of the Communications architecture was to effectively network any existing technologies included in the design architecture as well as any newly developed or designed technologies specific to the overall MDP architecture. Function-specific characteristics were also identified (see Table 5).

Communications
Networked
Anti-jam capable
Interoperable -Between services -Between coalition countries -Display characteristics and symbology
Coverage -Ship to ship -Ship to shore -Space and Satellite -Nodes/platforms
Capable Bandwidth
Connectivity -Between systems
Redundant -Multiple nodes -Multiple paths
Robust -Recovery -Absence of critical nodes or paths -Maximum flow through paths and nodes
Secure
Compatible
Reliable -Pfail (nodes, total architecture) -Mean Time Between Failures (MTBF) -Weather

Table 5. Communications Characteristics

This initial list of characteristics would help define design and engineering requirements, help determine objectives, help determine and apply Measures of Effectiveness (MOEs), and further develop the overarching MDP System throughout the design process.

Information Assurance (IA): Successful integration of C3I was vital to the success of the mission. The extensive application of digital communication and inter-networking in modern operations required communication links to be protected to prevent exploitation by adversaries. This section aimed to describe IA and the application of IA mechanisms in MDP communication needs.

IA was defined as: "Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities."[31]

IA study focused on establishing an IA plan to protect and defend the information and information systems of the MDP forces, to ensure their confidentiality,

[31] Joint Pub 3-13, *Joint Doctrine for Information Operations*, (9 October 1998): pp. 1-9.

integrity, availability, authenticity, and nonrepudiation. The information systems encompassed the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. The IA challenge involves protecting these in an integrated and coherent manner.[32]

The key IA functions were reliability, authenticity, confidentiality, data integrity, and access control.

Elements of the system needed for operational readiness or fighting were required to be continuously available. Reliability was the ability of a system to maintain or restore an acceptable level of performance during operations by applying various restoration techniques. It was also the mitigation or prevention of service outages due to system failures by applying preventive techniques. It was a measure of the availability and performance of the system.

Authenticity validated the identity claims of the sender and the data. It was the ability to know that the data received was the same as the data sent and the claimed sender was in fact the actual sender. Authorization was the act of granting rights and/or privileges to users permitting them access to an object.

Confidentiality prevented disclosure of data (entire message/selected fields/traffic characteristics). The ability to communicate such that the intended recipients could know what was being sent, but unintended parties could not determine what was sent.

Data integrity ensured data was unchanged from its source and not accidentally or maliciously modified, altered, or destroyed during the transmission, storage, and retrieval. In doing so, data integrity safeguarded the condition of data to ensure accuracy, currency, consistency, and completeness.

Access control was a means of enforcing these authorizations based on some pre-defined security policies and by comparing the user's authorizations with the policy to determine whether access to a managed object should be allowed.

---

[32] Department of the Navy, IA Pub-5239-01, *Introduction to Information Assurance Publication*, (May 2000).

Command and Control (C2): The definition of C2, as documented by the Joint Chiefs of Staff, included four main functions: organize, plan, coordinate, and identify lead agency.[33] For the purposes of this MDP System, our group identified two additional functions necessary for the C2 System to perform: direct and control forces.

The primary function of the C2 System was to organize. Before any action could be taken, the Command system must first organize a hierarchy of decision makers with a clearly delineated chain of command. This effort established the lines of communication and responsibility that would be necessary to carry out further functions.

The second function of the C2 System was to plan. Any scenario or mission required a plan to give meaning to the organization. Organization was the primary function because the components of the system (the planners themselves) were required first to be in place before any plan could be constructed. Sufficient time devoted to the development of a plan was important, because a bad plan could be linked to failure. Planning was also the first instance when ideas and information were sorted and filtered by decision makers. The filtering of ideas and information was the essence of decision-making.

The third function of the C2 System was to coordinate. This function involved the coordination of a coalition between nations, action groups, and elements of technology tasked with carrying out the plan.

The fourth function was to identify the lead response agency, coalition, or elements. A characteristic of the lead response agency would be identifying jurisdiction, or the region in which operations might be carried out.

The fifth function, directing (addresses both interoperability and compatibility), involved managing all aspects of the system, including performance. Interoperability ensured integration between major systems, ranging from coalition forces to intelligence networks outside the system. Compatibility ensured there was no

[33] Interview with Senior Lecturer Thomas Hoivik, "C4I MOEs and MOPs," Naval Postgraduate School, Monterey, CA, (3 February 2005).

interference between components within the system, such as the fusion of sensor data within the Data Fusion and Intelligence Center.

The directing function was not synonymous with the sixth function of controlling forces. Controlling forces involved both leadership and tactical influence that was required to be tailored for each scenario. Because each scenario for the C2 System would likely be different, it would be important to devote time to maintain the resources and readiness of the systems employed by the MDP System.

Intelligence: The Functional Analysis of the Intelligence System yielded five main functional areas. These areas were planning and directing, collection, processing and exploiting, analyzing and integrating, and disseminating. These main functional areas outlined the Intelligence System process that transformed the inputs and created the outputs from the model. The first functional area of the Intelligence System was planning and directing. The planning could be described as strategic, operational, and tactical. The level of planning corresponded to the time constraint on the Output. The strategic level of intelligence planning dealt with the allocation of resources and assets such as sensors, satellites, and data collection platforms. The operational level of planning involved the daily operations of the Intelligence System. The normal daily operations for an Intelligence Center included the monitoring and tracking of threats and all intelligence gathering and fusion. The tactical level of planning involved the mission-specific intelligence and the near-real-time (NRT) directing of collection assets.

The next main functional area of the Intelligence System was the collection of data. Technical collection could be very expensive and the collection process was considered to have limited resources. One important consideration for the collection process was determining how much information should be collected. "Increased collection also increased the task of finding truly important intelligence."[34] Another important consideration for the collection function was the amount of data collection devoted per source type. There were different capabilities and limitations to

[34] Interview with LT Lowenthal, USCG Data Fusion Center Alameda, CA, 9 March 2005.

the various types of collection methods. A collection mix was important to cover all the different sources of data collection.

After collection, the data needed to be processed and exploited before any analysis could be completed. The intelligence collected by technical means did not arrive in a ready to use form. Lowenthal states, "Processing and Exploitation are key steps in converting technically collected information into intelligence."[35] There was a great disparity between the emphasis on collection and exploitation. The result is that much of the collected data and information was never used because there were not enough assets to process and exploit the information into useable forms for analysis. The ratio between collection and processing should have been one that ensured the information out there could be collected, but also maintained enough processing such that large amounts of information were not lost.

The next step in the intelligence process was the analysis and integration of the processes information. There were two major types of analysis that were completed at this step. The first was the short-term or current analysis and the second was the long-term or future analysis. Depending on the policy maker's needs and the situation, there could be more emphasis placed on either type of analysis at any given time.

The final function in the intelligence system was the dissemination of the intelligence. This process of delivering the information from the intelligence side of the house to the operators was highly standardized. The lines of communication to the commanders in the field were required to be open such that priority information could be passed. This would provide the commanding authority with the most up-to-date and relevant information on which to base decisions.

2.1.1.5 Effective Need Statement – MDP Group

The product of the Needs Analysis step is a revised problem statement, called the Effective Need Statement, reflecting the most significant needs and desires of

[35] Interview with LT Lowenthal, USCG Data Fusion Center Alameda, CA, 9 March 2005.

the stakeholder. After iterative analysis of all components and tasks in the Needs Analysis step, the MDP Group Effective Need Statement evolved to read:

> "An adaptable architecture that prevents maritime domain acts of piracy from supporting terrorism. Objectives include increasing security of maritime assets while minimizing impact on commerce."

This statement encompassed the project goals and was in accordance with the problem statement. The objective of minimizing impact on commercial maritime traffic ensured that needs identified in Stakeholder Analysis were covered.

2.1.2 Needs Analysis – Total Maritime Inspection System (TMIS) Group

The TMIS Group performed the Needs Analysis step in order to transform the Initial Problem Statement into an Effective Need Statement. The Initial Problem Statement presented to the TMIS Group from the Tasking Memo (see Appendix A) was:

> Design a conceptual System of Systems to defeat and prevent terrorism in the Maritime Domain… design and assess alternative architectures for cargo inspection to include a total ship inspection sub-system that could detect and identify explosive and other dangerous materials so to prevent the use of a large cargo ship as a terrorist vehicle.

The TMIS Group performed Needs Analysis using the following tools: System Decomposition, Stakeholder Analysis, Input-Output Model, and Functional Analysis.

2.1.2.1 System Decomposition – TMIS Group

The first Needs Analysis tool the TMIS Group used was System Decomposition, which broke the system down into the major functions that would be used in determining the solution to the problem. As a result of System Decomposition, the following main functions were established:

- Search designated containers or container ships.
- Detect appropriate materials.
- Locate the detected materials.
- Identify the materials.

- Communicate findings to appropriate decision makers.

In order to accomplish these functions, several component structures were defined. The *structural* portion of the TMIS consisted of the various land and sea inspection equipment. The *operational* portion consisted of the individual system operators and their respective prime movers. The *flow* portion of the component structure was primarily concerned with the flow of shipping traffic, cargo, and information.

For further definition of the TMIS structure, the system was described in relation to a system hierarchy of Superlative, Lateral, and Subordinate Systems. This perspective showed how the TMIS interacted within a system of systems architecture. The primary *Superlative* System of the TMIS was considered to be the SEA-7 MDP Group. Other Superlative Systems include groups such as customs agencies, immigration agencies, and other law enforcement or military groups. The *Lateral* Systems were established as land and sea inspection operations in other ports around the world. These Lateral Systems should work as a team with the TMIS to prevent the export of WMDs before leaving their areas of interest (AOIs). If necessary, these Lateral Systems should share intelligence with the TMIS to prevent weapons of mass destruction (WMDs) from entering the port of interest (Singapore). Identification and assessment of the *Subordinate* Systems in the overall structure revealed that the TMIS Group would be better divided into the two subordinate system groups: Land Inspection and Sea Inspection.

2.1.2.2 Stakeholder Analysis – TMIS Group

The Stakeholder Analysis performed by the TMIS Group was better illustrated in two parts: first, by defining the stakeholders and then addressing the specific questions asked of the stakeholders and their subsequent responses. The initial list of potential stakeholders began with members of the Maritime Domain Study Group at the NPS. Interviews with these initial stakeholders led to additional points of contact, all of which were potentially useful sources of information. An attempt was made to contact as many stakeholders as possible, especially those from outside of academia.

Unfortunately, time constraints and the complexity of the maritime shipping industry did not support interaction with the entire list of stakeholders. Comprehensive research was an essential instrument to understanding the needs and concerns of those involved. Other stakeholders, though not all inclusive, include shippers, carriers, port authorities, the World Shipping Council, port operators, customs, the USCG, port security, local police, transport vehicle operators, and local responders.

The information received from the stakeholders as part of the analysis was invaluable. Major differences among the stakeholders on many different levels of the problem were recognized. Each stakeholder had specific concerns that were often dissimilar depending on their background or specific area of expertise. Even agreements on limitations of the current system, or concerns regarding the study's focus, often resulted in more specific disagreements in the alternate systems.

After initial conferences with several stakeholders, the TMIS Group recognized a deficiency of knowledge concerning current technologies available for the study. The TMIS Group contacted Lawrence Livermore National Laboratories for an informational course in sensor technology. Following the session, Lawrence Livermore became a significant contributor to the rest of the study. They established the baseline of current and potential capabilities and limitations accessible to the potential TMIS.

2.1.2.3 Input-Output Model – TMIS Group

The TMIS Group used results from the system decomposition and information gained from the Stakeholder Analysis process to develop an Input-Output Model (Figure 14). This model provides a better understanding of what entered the system and what the system produced.

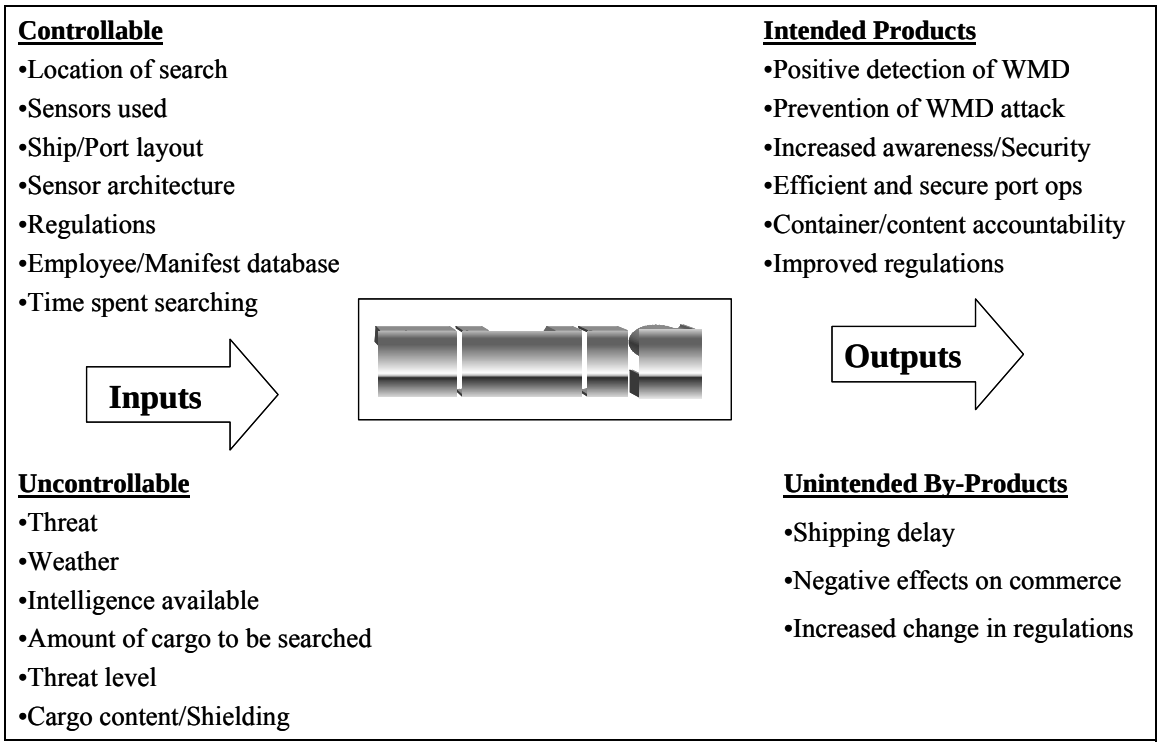

Figure 14. TMIS Group Input-Output Model

The Input-Output Model separated the TMIS from its surroundings, giving a different perspective of the system. This was useful for determining which parameters could be used to influence the system outcome, and which system outcomes were undesirable.

The Inputs were defined as either Controllable or Uncontrollable, while the Outputs were delineated as Intended Products or Unintended By-Products. The Controllable Inputs included the sensor architecture (position and type of sensors) as well as the time spent searching. Three types of Uncontrollable Inputs were identified: *unknown* such as cargo content/shielding, *estimable* such as amount of cargo to be searched, and *random* such as weather and available intelligence. The primary Intended Output of the system was to create a high level of security and an inspection process that would positively detect WMDs. Unintended By-Products included shipping delays and other negative effects on commerce, along with their associated costs.

2.1.2.4 Functional Analysis – TMIS Group

The Functional Analysis of the TMIS System was performed by iteratively decomposing the system functions into their component parts and arranging the system

functions into a Functional Hierarchy and a Functional Flow Diagram. The functional decomposition for the TMIS system resulted in four required functions: search, detect (this function incorporates the locate function), locate/identify, and report. Each function was broken into its constituent parts or subfunctions, as shown in Figure 15.

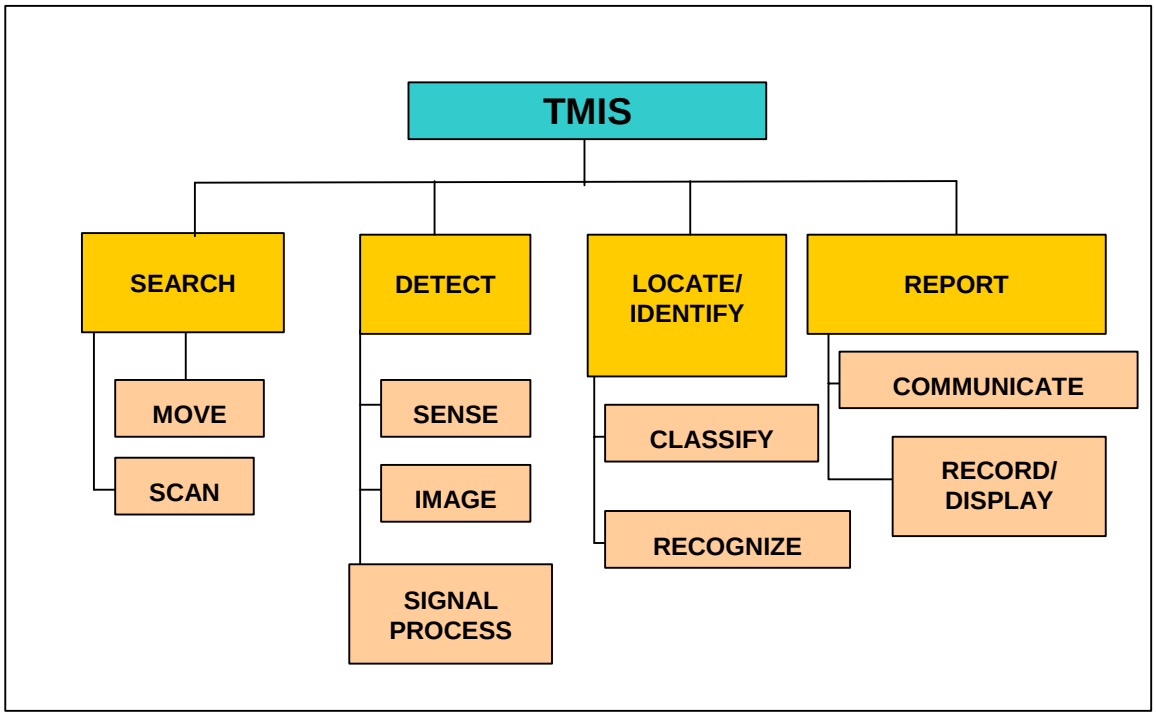

Figure 15. TMIS Functional Hierarchy

In order to effectively search cargo, the TMIS was required to perform these top-level functions with the associated subfunctions.

In order for the cargo inspection system to perform inspections on targeted vessels, the system was required to search the ship. The search function defined the system's ability to inspect the vessel and cargo. The move subfunction defined the system's ability to maneuver throughout the ship, while the scan subfunction included the ability to methodically examine desired locations on the ship. The scan subfunction included the sensor holding in position for a certain "soak" time to enable a thorough search.

The detect function defined the system's sensitivity to hazardous material. The sense subfunction more specifically defined the required sensitivity for the different

sensors. The image subfunction described the ability of the sensors to display the output in a graphical or picture-type format. The signal process subfunction defined the ability of the sensors to give an output to the operator, whether automatic or requiring human interpretation. The locate/identify function described the system's ability to determine the position and makeup of any hazardous material onboard. Subfunctions included being able to recognize the material by type and classifying the material as dangerous or not.

The system was also required to report the status and results of the inspection at any time. This function included the communicate subfunction for transmitting and receiving results among Inspection Team members and to higher authority. The record/display subfunction was also included for the system to display data and findings to the operators and generate reports to be communicated to the C2 element for the system.

The TMIS Group developed a Functional Flow Diagram (see Figure 16) from the Functional Hierarchy in order to show the intended system process.

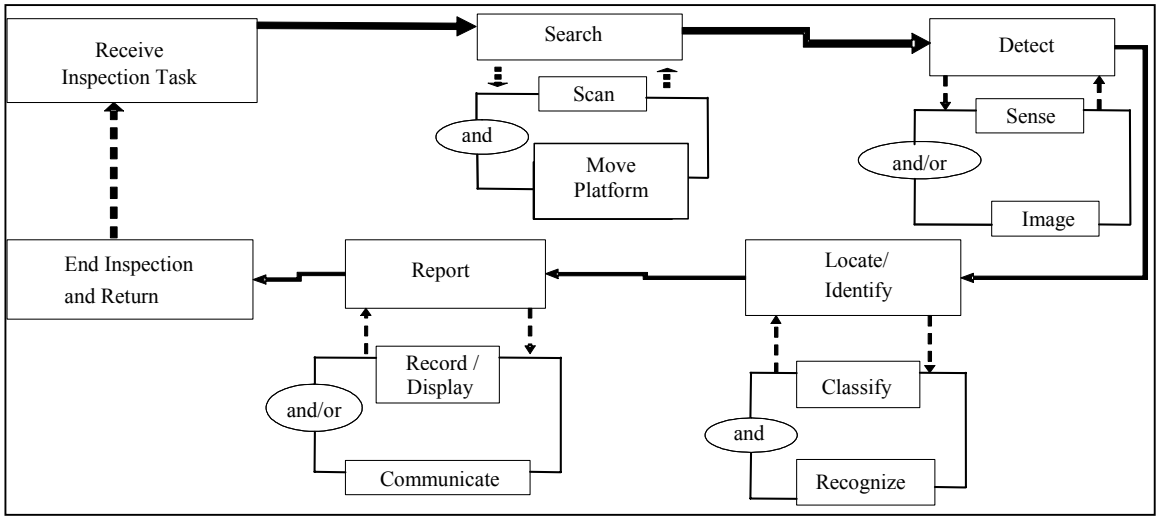

Figure 16. TMIS Functional Flow Diagram

Initially, the Inspection System received its tasking and transited to the COI. From there the search process began. During the search process the Inspection Team would maneuver to scan the container cargo and various parts of the

ship. A detection was made by the use of sensors or other imaging devices for the materials of interest. If a detection was made, the team continued to use their sensors to localize the source to a specific container or area of the ship. This was done by analyzing the data received from the sensors and human interpretation. During the location phase of the process, the team was also required to use their sensors to identify the material. Identification of the material included classifying the material as hazardous or not, and determining whether the material was supposed to be there. Finally, during the process, a report concerning inspection progress and completion was required to be made to C2 elements. The functional flow for the Sea Inspection System ended with the system returning to a state where it was awaiting tasking for the next inspection.

2.1.2.5 Effective Need Statement – TMIS Group

After analysis of all components and tasks in the Needs Analysis step, the TMIS Group's Effective Need Statement was developed as follows:

> "Design and assess alternative architectures for a total ship inspection system that will detect and identify explosives, chemical agents, biological agents and radiological sources before loading onboard ships or at sea to prevent the use of a large cargo ship as a terrorist vehicle for weapons of mass destruction while minimizing the economic impact on commercial shipping."

This statement encompassed the TMIS Group's goals and was in accordance with the problem statement.

2.2 OBJECTIVES HIERARCHY

2.2.1 Objectives Hierarchy – Overall

The Objectives Hierarchy provided detailed analysis of the functions the system must perform and the objectives the system must satisfy, and linked directly to basic quantitative measures. The Objectives Hierarchy delineated the different system functions, which it further broke down into subfunctions, objectives, and evaluation measures. The end product of the Objectives Hierarchy was an organized pictorial representation of the system breakdown, from top-level functions and objectives down to the evaluation measures that would determine system performance. The metrics

developed in the Objectives Hierarchy would be used to help generate system requirements.

2.2.2 Objectives Hierarchy – Sensors Group

The Objectives Hierarchy for the Sensor System was derived from the functional decomposition performed during the Needs Analysis step (see Figure 17). A number of sources were consulted and correlated to produce an adequately detailed functional breakdown for the system. The overarching requirements of collective exhaustiveness and mutual exclusiveness were of primary concern in this process.

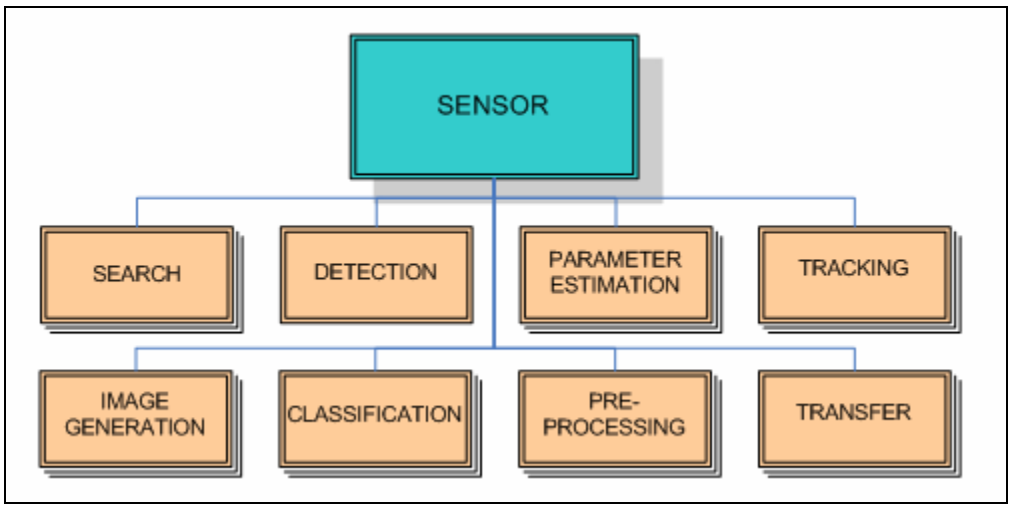

Figure 17. MDP Sensor System Top-Level Functional Decomposition

Only the first tier of the functional decomposition is shown. It is not necessary for all sensors to implement all the different functions (some sensors might implement just a subset); nevertheless, it is comprehensive across all possible Sensor Systems.

For each of these top-level functions, one or more objectives and subfunctions were developed as necessary. For example, tracking individual contacts using continuously scanning radar is a "Track-While-Scan" function that includes standard search radar functions, but also requires added mechanical orientation, signal processing, and software operations. Similarly, preprocessing functions include "interface requirements" associated with Communications Systems. Finally, specific metrics—MOEs and Measures of Performance (MOPs)—were designated for each objective.

Table 6 includes the functions, objectives, and MOEs/MOPs developed for the Sensor System.

FUNCTION	OBJECTIVES	MOE/MOP
SEARCH	• Provide overlapping coverage of Area of Regard (AOR) [area] (maximize) • Provide continuous and persistent coverage of AOR [time] (maximize)	• Range (max) • Search rate (max) • Scan pattern efficiency (max) • Dwell time (max) • Target revisit rate (max) • Time on station [for mobile sensor platforms] (max)
DETECTION	• Provide accurate and timely determination of presence of surface Contact of Interest (COI) within search volume of sensor (maximize)	• Probability of Detect P_{DET} (max) • Probability of False Alarm P_{FA} (min) • Detection range (max) • Time to detection (min)
PARAMETER ESTIMATION	• Establish the value of "observables" to the required level of accuracy (maximize)	• Number of observables (max) • Accuracy [parameter dependent] (max) • Update frequency (max)
TRACKING	• Maintain seamless "track vector" information of surface COIs as they move through the AOR (maximize)	• Accuracy (max) • Update frequency (max) • Handover integrity (max)
IMAGE GENERATION	• Provide accurate two- or three- dimensional imagery of surface COIs within AOR (maximize)	• Resolution (max)
CLASSIFICATION	• Perform accurate unitary, binary, etc. classification of surface COIs at the sensor node level (maximize)	• Discrimination resolution (max) • Time to classification (min) • Single-sensor probability of correct identification (max)
PREPROCESSING	• Perform as much sensor node level manipulation of locally generated data as possible [sensor dependent] (maximize)	• Data reduction ratio (max) • Synchronization accuracy (max) • Processing time (min)
TRANSFER	• Perform data/control interface operations at the local node to maximize communications efficiency (maximize)	• Data compression ratio (max) • Buffering capacity (max) • Latency (min)

Table 6. MDP Sensor System Functions, Objectives, and Metrics

This table captures in summary representation the arrangement of functions, objectives, and metrics (both MOPs and MOEs), defined for the sensor system.

For each of these metrics the desired direction of attainment is also expressed: maximize (max) or minimize (min). The complete graphical depiction of the Objectives Hierarchy for the Sensor System is shown in Appendix B. As part of the overall Sensor System suitability, a Reliability, Availability, and Maintainability analysis

will be executed, including a technology risk assessment for the applicable architecture alternatives.

2.2.3 Objectives Hierarchy – C3I Group

The Objectives Hierarchy for the C3I System was derived from the functional decomposition performed during the Needs Analysis step (see Figure 18).

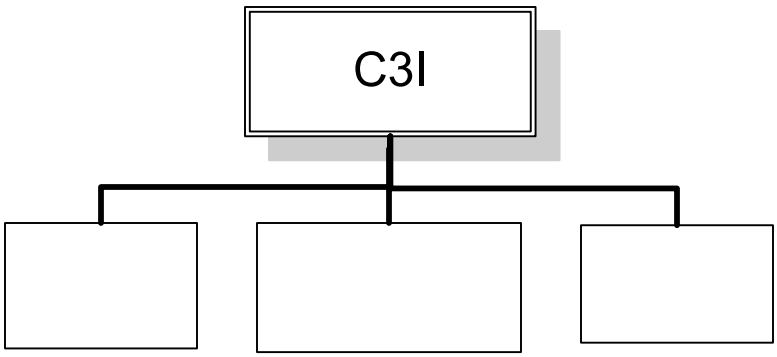

Figure 18. MDP C3I System Top-Level Functional Decomposition

In addition to identifying functions and subfunctions, the Objectives Hierarchy identified objectives, MOPs, and MOEs for the functions. The objectives, MOPs, and MOEs provided a means for comparative analysis of various architectures consisting of different system alternatives.

For each top-level function, specific objectives and subfunctions were developed to support the overall objectives of the C3I System. For example, subfunctions of C2 included plan, coordinate, and control forces. Complete graphical depictions of C3I's Objective Hierarchy are in Appendix C (APPENDIX C IS THE "FORCE SYSTEM GROUP OBJECTIVE HIERARCHY"---IS THAT THE SAME THING?).

C2: The baseline MOEs/MOPs for the C2 element of the Maritime Domain Protection System were derived from a capability requirements analysis of service doctrine provided by Senior Lecturer Thomas Hoivik. In addition to these broad measures, scenario specific MOEs/MOPs were developed to facilitate full definition of the operational environment. C2 MOEs and MOPs are shown in Table 7.

SUBFUNCTION	OBJECTIVES	MOE/MOP
PLAN	• Translate decisions into plans and orders • Contribute to the commander's perception of the enemy	• Tactical picture quality (max) • Percent action initiated by time ordered (max) • Dissemination time (mean) • Percent orders clarification requested (min) • Percent planning time forwarded (min) • Time from mission to order (min) • Time to decision ratio (min) • Percent of personnel informed (max) • Display processing time (min)
COORDINATE	• Filter, fuse, and prioritize information • Provide vertical, lateral, and diagonal redundancy • Satisfy the commander's critical information requirements, and make those elements of information available in a timely fashion, in the most useable form, supporting both supply-push and demand-pull • Reconfigurable, adaptable, scalable	• Accessibility (max) • Tactical picture quality (max) • Tactical picture consistency (mean) • Measure time from mission to order (min) • Time to decision ratio (min) • Percent of communications with alternate routes (max) • Dissemination time (mean) • Percent informed (max) • Number of orders issued (min)
CONTROL FORCES	• Supervise the execution of plans and orders • Possess the characteristics of survivability and sustainability • Provide rapid simultaneous access of multiple users throughout the chain of command and to external commands and agencies as appropriate • Display a scaleable, near real-time, shared picture of the maritime environment • Operational capability during transit and mobility • Facilitate rapid and frequent displacements • Organizational structure solidifying unity of command	• Time to execute control measures • Information refresh Rate • Time to react to displacement orders • Time to reorganize

Table 7. C2 System Subfunctions, Objectives, and Metrics

This table captures in summary representation the arrangement of C2 subfunctions, objectives, and metrics (both MOPs and MOEs), defined for the C3I System.

Communications/IA: The objectives, MOEs, and MOPs for Communications and IA, were developed as an integrated effort between the SEA-7 and TDSI Communications and IA tracks. The professional expertise the TDSI students brought into the process assisted greatly in the development of an effective Objectives Hierarchy that included functions applicable to the IA domain. Communications/IA MOEs and MOPs are in Table 8.

SUBFUNCTION	OBJECTIVES	MOE/MOP
TRANSMIT/RECEIVE (COMMUNICATIONS)	• Maximize successful and correct transmission and reception of data • Minimize data/transmission loss • Minimize the need for retransmission of data, images, or voice communications	• Average packet retransmission rate (x retransmitted packets per sec) • Error correction and recovery capability • Percentage of packet lost • Maximum/Average Latency (x sec) • Maximum/Average available bandwidth (x bits per sec) • Maximum/Average link utilization rate (% over time period) • Link redundancy per node
NETWORK (COMMUNICATIONS)	• Minimize network down time (inactivity or failure) • Efficient number of nodes required for data level and transmission level traffic • Maximize network robustness and redundant capability • Maximize network capability between sensors and communications nodes • Minimize data corruption due to overflow on links and/or collisions • Minimize nodal failures • Successfully reroute transmissions around failed nodes	• Average Throughput (bits per sec) • Percentage of Dropped Messages (for best-effort delivery) • Voice Call Completion Rate (CCR) • Average Time to Establish Communications between Major Nodes (x sec) • Mean Time Between Failure (MTBF) of Major Nodes (x sec) • Average set-up time per node (x sec) • Average downtime per node (x sec) • Average node recovery time (i.e., time for node to recover connectivity after outage) • Average Network Utilization Rate (% of nodes utilized) • Average Time to Reroute Communications Service (x sec) • Percentage of Successfully Rerouted Service • Scalability of Network (maximum number of nodes per area)
PROCESS (INFORMATION ASSURANCE)	• Maximize system redundancy in order to mitigate or prevent service outages from system failure	• Data display and upload rate • Refresh rate
SORT/FILTER	• Maximize time relevant transmission of time critical data • Prevent unauthorized disclosure and safeguard the condition of data to ensure accuracy, currency, consistency, and completeness • Grant rights and/or privileges to users permitting access • Enforce authenticity	• Average time for dissemination of time critical information • Data prioritization precision and accuracy • Percent of time critical data dropped • Proportion of data erroneously filter (and hence received at the incorrect node) • Data prioritization precision and accuracy • Minimize data transmission of nonapplicable information
SECURITY	• Maximize security of transmissions between coalition platforms/nodes/command and control/action elements • Maximize transmission and encryption of data • Maximize correct decryption	• Probability of failure of encryption • Probability of network exploitation due to encryption failure or dissemination

Table 8. Communications/Information Assurance System Subfunctions, Objectives, and Metrics

This table captures in summary representation the Communications and Information Assurance subfunctions, objectives, and metrics (both MOPs and MOEs), defined for the C3I System.

Intelligence: The objectives, MOEs and MOPs for Intelligence were developed based on operational user feedback and correcting deficiencies highlighted by recent

national Intelligence Systems failures. In addition to the measures of intelligence processing, scenario specific MOEs/MOPs were developed to facilitate full system evaluation of the effectiveness between our C3I System's architectures, based on measurable and quantifiable parameters in the subsequent modeling phase. Intelligence MOEs and MOPs are at Table 9.

SUBFUNCTION	OBJECTIVES	MOE/MOP
PLAN AND DIRECT	• Provide relevant information	• Planning time (min) • Prioritization time (min) • Ensure unity of intelligence effort (max)
COLLECT	• Utilize variety of sources, e.g., HUMINT, electronic intelligence • Coordinated informational processing • Maximize the systems availability • Systems shall be dynamically adaptable • Maximize all-source collection • Optimize use of collection assets	• Ensure 24/7 operation • Query time (avg.) • Proportion of collection tasking completed • Time (min) • Schedule error (avg.)
PROCESS AND EXPLOIT	• Provide situational refinement • Minimize time • Maximize accuracy/trustworthiness • Maximize thoroughness of information	• Minimize processing time (max) • Minimize assessment time (max) • Multiple correlation (max) • Systems automation (max) • Residual/unused collected data (min) • Collection and exploitation for combat (max) • Secondary indications (max)
ANALYZE AND INTEGRATE	• Maximize threat refinement • Maximize objectivity • Unbiased analysis	• Analysis time (min) • Situational awareness (max) • Accurate assessment of adversary/threat (including capabilities, vulnerabilities, and intentions/motivations) (max)
DISSEMINATE	• Maximize process refinement • Maximize usability for the commander • Maximize satisfying commander's information requirements	• Ensure capability of disseminating • 250 to 500 reports/min • Ensure information sharing "push/pull" capability • Support 10 to 25 C2 decisions per minute • Minimize percentage of unmet commanders Essential Elements of Information (EEI) (avg.) • Identity determination (max) • Timely accurate threat assessment (min) • Control, feedback, and resource management (max)

Table 9. Intelligence System Subfunctions, Objectives, and Metrics

This table captures in summary representation the Intelligence subfunctions, objectives and metrics (both MOPs and MOEs), defined for the C3I System.

2.2.4 Objectives Hierarchy – Force Group

The development of the Objectives Hierarchy involved the generation of the objectives, MOEs, and MOPs for the Force System. The initial layout of the Force System objectives was based on the Navy's Planning, Embarkation, Rehearsal, Movement, and Assault (PERMA) plan for amphibious operations, as shown in Figure 19.

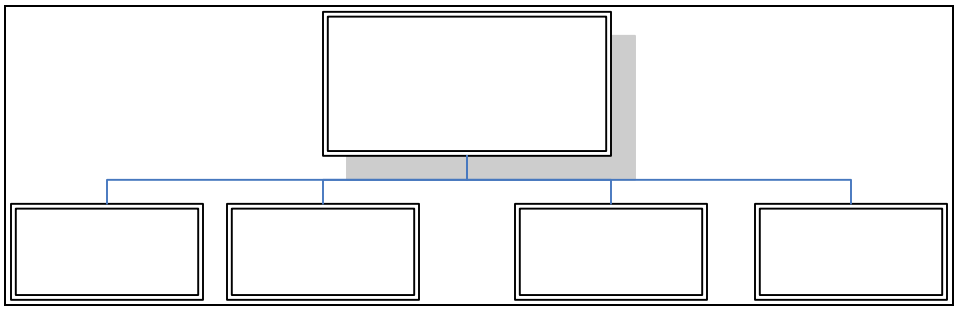

Figure 19. Force System Functions

This figure shows the overarching functions of the Force Group. These functions later dictated the metrics that would be used to evaluate the Force System architectures.

Staging, Deploying, Committing, and Recovering functions were determined to encompass all capabilities that the reaction force was required to perform. The Staging function was comprised of the Planning and Equipping subfunctions. Planning was defined as choosing the preplanned response that was best suited to the tasking received from the C2 Group. It was assumed that the C2 Center would assign the reaction force with a target and tasking to either engage or inspect. The Equipping subfunction was designed to include the selection and collection of the correct equipment for the mission. The Deploy function was comprised of both Embarkation and Transportation subfunctions. Embarkation was intended to include the safe and expeditious on-load of the transportation vessel. The Transportation subfunction was derived to include the speed of transport as well as minimizing susceptibility of the reaction force while in transit. This led to the necessity of self-defense capabilities embedded within all of the transportation vessels. The Commit function was formulated to include either the Inspection of a suspect vessel or the Engagement of an SBA or SAW vessel. Finally, the

Recover function was designed to include either the Recall of the forces or the Redirection of the forces onto their next target.

For each of these top-level functions and subfunctions, one or more function objectives were developed, and specific metrics—MOEs and MOPs—were designated for each objective. Table 10 includes the functions, objectives, and MOE/MOPs developed for the Force System. The complete graphical depiction of the Objectives Hierarchy for the Sensors System is shown in Appendix B.

FUNCTION	OBJECTIVES	MOE/MOP
STAGE	• Minimize time required to select correct preplanned response • Minimize time required to equip correct gear	• Time to select plan • Percent of gear needed for mission available • Percent of incorrect gear issued • Average time to equip force
DEPLOY	• Minimize time required to Embark force • Minimize transportation time to objective	• Average time to embark • Percent of gear and personnel damaged • Average time to transport force • Average amount of damage sustained by force during transit
COMMIT	• Neutralize threat • Find Weapons of Mass Destruction (WMD)	• Ratio of ships damaged vs. ships attacked • Amount of damage to high value unit • Percent of missions completed • Percent of targets neutralized vs. engaged • Percent of WMD located
RECOVER	• Minimize time required to return reaction force to staging area • Minimize time required to reallocate force to new target	• Average time to recall • Percent of equipment lost per mission • Average time to redirect • Percent of equipment and personnel out of service after mission

Table 10. Force System Functions, Objectives, and Metrics

This table shows functions and objectives were used to evaluate the Force architectures' performance.

2.2.5 Objectives Hierarchy – Land Inspection Group

The overall Land Inspection objective was to detect hazardous materials, while minimizing impact on the economy. The challenge for the Land Inspection Group simplified down to determining whether inbound cargo was legitimate, legal, and matched the manifest. A secondary consideration was whether or not dangerous

materials were added to the cargo in transit and/or shipment. To address these two concerns, the system was required to maintain accountability of containers, target suspect containers, detect hazardous materials within the cargo, and finally communicate the results both internally and externally. Figure 20 illustrates the top-level functional decomposition for the Land Inspection System.

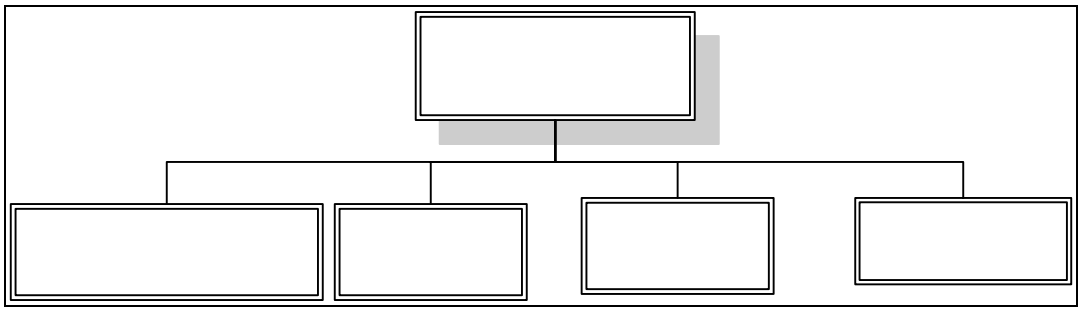

Figure 20. Land Inspection System Top-Level Functions

This figure depicts the top-level functions of the Land Inspection System. The Land Inspection System must be able to maintain container accountability, target suspect containers, detect hazardous material and contraband, and communicate the results to a Data Fusion and Analysis Center as well as a C2 unit.

For each top-level function, specific objectives and subfunctions were developed as necessary to support the overall objectives of the Land System. To maintain accountability of containers, the system was required to track changes of custody and location of containers throughout their shipment. Also, targeting suspect containers required the system to assess and validate the origin, manifest, destination, and integrity of each container, determining whether specific containers were suspect or not. The detection of hazardous materials was to be accomplished through searching the cargo and locating and identifying hazardous material. Finally, the results and information were required to be communicated through transmission, receipt, recording, and display to appropriate personnel. Table 11 shows the functions, objectives, and metrics of the Land Inspection System. The complete graphical depiction of the Objectives Hierarchy for the Land Inspection System is shown in Appendix D.

FUNCTION	OBJECTIVES	MOE/MOP
MAINTAIN ACCOUNTABILITY	• Provide custody and location information of containers	• Average time container location is uncertain • Number of discrepancies in custody chain • Number of containers not in database
TARGET	• Establish procedures and triggers for classifying suspect containers	• Number of containers targeted for inspection • Number of targeted containers with negative inspection results • Average classification time of containers as suspect/not suspect
DETECT	• Increase probability of detection of hazardous materials • Detect 80% of WMD	• Number of hazardous materials located and identified • Average number of false alarm rates of system and sensor subsystems • Average search times of sensor employed • Number of containers inspected • Percent of containers never inspected • Probability of detection of each threat type • Number of WMDs missed
COMMUNICATE	• Provide integrated information to both internal and external agencies for assessing cargo containers • Maximize accessibility of information by applicable agencies • Maximize accuracy of database entries • Minimize time delay in reporting detection of hazardous materials	• Delay time in notification of suspect containers • Average response time to detection of hazardous materials • Number of agencies able to access information

Table 11. Land Inspection System Functions, Objectives, and Metrics

This table shows each function of the Land Inspection System, along with the objectives and subfunctions associated with that function. Included are the metrics used to evaluate how well the system performs each function.

2.2.6 Objectives Hierarchy – Sea Inspection Group

The Sea Inspection Group developed the Objectives Hierarchy from the Effective Need Statement and the Functional Analysis (see Figure 21). The group started with the main functions categories of Search, Detect, Locate/Identify, and Communicate. These terms come directly from the functional analysis and describe the major functions of the system. The group then developed subfunctions from each of the main functions. For example, the Search function was broken into the subfunctions of searching the ship

and searching the cargo. A further breakdown revealed that the system needed to search internal spaces as well as the external structure of the ship.

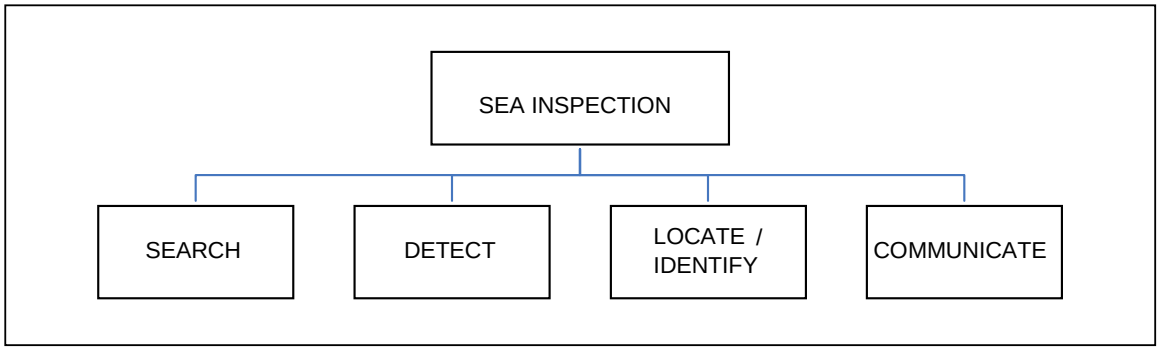

Figure 21. Sea Inspection System Top-Level Objective Hierarchy

This figure depicts the top-level functions of the Sea Inspection System. The Sea Inspection System must be able to search a ship, detect the hazardous materials, locate and identify those materials and then communicate those results to a C2 entity.

From the main functions and subfunctions the team developed the objectives for the system. These objectives were intentionally selected to be general but measurable, as the team needed to measure how well each proposed alternative met an objective. For example, the objective of the Search function was to maximize the search efficiency of the system. The Sea Inspection Group further defined this objective by the use of a subobjective. For the Search function, the subobjectives determined that the system should be able to search as much of the ship (inside and outside) and cargo as possible, as quickly as possible while maintaining a high level of thoroughness, a high level of mobility, and using the appropriate level of manpower to most efficiently complete the task.

In order to measure the effectiveness of each alternative, the group identified at least one metric for each objective. These metrics were used to evaluate how well the system accomplished the objective. These metrics would be used in the modeling and analysis phase to select the best alternative for the system and are included in Table 12. The complete graphical depiction of the Objectives Hierarchy for the Sea Inspection System is shown in Appendix E.

FUNCTION	OBJECTIVES	MOE/MOP
SEARCH	• Minimize manpower necessary to facilitate search • Provide man-portable, highly sensitive sensor devices • Provide for a thorough and complete search of containers and vessel (maximize volume searched)	• Maximum operators and team size • Average search rate of teams • Maximum search time allowed for inspection • Minimum shipping delay time
DETECT	• Maximize effective detection range (maximize) • Maximize effective detection time (minimize) • Maximize efficient sensor sensitivity	• P_{DET} (max) for specific weapon or explosive • P_{FA} (min) for specific weapon or explosive • Detection range (max) • Time to detection (min) • Shipping delay time • Number of detections
LOCATE/ IDENTIFY	• Provide identification capabilities in gear (max) • Locate material in timely manner (minimize) • Locate material accurately (maximize) • Maximize human factors objectives, including sea environment accommodation, indicator readings for day and night at-sea conditions, etc. • Minimize training time • Maximize training effectiveness • Maximize sensor flexibility (max) • Provide quick identification after detection and location	• Average location time from detection • Average location error • Positive location ratio • Process execution time (min) • Usability rating for gear (from teams) • Successful identification ratio • Identification time (min) • Shipping delay time (min)
COMMUNICATE	• Maximize high data rate for external communications • Provide long distance communications • Provide communications onboard ship • Provide secure communications • Provide report generation format • Data security (high)	• Average data rate (max) • Data range (max) • Timeliness of reports (max) • Average signal range • Ratio (jammed/total transmission) • Ratio (intercepted/total transmission)

Table 12. Sea Inspection System Metrics

This table shows each function of the Sea Inspection System, along with the objectives associated with that function. Included are the metrics used to evaluate how well the system performs each function.

2.3 REQUIREMENTS GENERATION

2.3.1 Requirements Generation – Overall

Since the SEA-7 Cohort did not receive specific requirements from any clients or stakeholders, the Requirements Generation step was especially important to establish

guidance and direction for follow-on work. The cohort began generating top-level system requirements by looking at the threat scenarios, and determining estimates for both the probability each attack would occur and the resulting probability of defeat a stakeholder would logically desire versus each attack (see Figure 22).

Small Boat Attack (SBA) • Probable – Demonstrated • Defeat 80%	**WMD – Chem/Bio** • Occasional – Likely to occur • Defeat 90%
Ship As Weapon (SAW) • Probable – Proven capability • Defeat 90%	**WMD - Nuclear** • Remote – Unlikely, but possible • Defeat 60%

Figure 22. Threat Scenario Likelihood and Defeat Requirement Estimates

Without specific client requirements, the SEA-7 Cohort proposed likely estimates and defeat probabilities for each threat scenario. These proposals were accepted and used for the remainder of the study.

In addition to threat-specific requirements, overall system requirements were derived, which applied regardless of attack type. These top-level overall requirements were as follows:

- Ninety percent operating capability no later than December 2010 (five years).
- 24/7 capability.
- All-weather capability.
- Interoperable with existing systems.
- Daily system operational availability ≥ 0.9.

These top-level requirement proposals were presented to the PACOM stakeholder for approval, and they were not changed. In all of these top-level requirements, "defeat"

was defined as countering a single attack such that damage was $100,000 or less. Also, these estimates all used a 95% confidence interval.

In addition to top-level system requirements, top-level system objectives were generated to give a reference starting point for follow-on work. As objectives, these criteria were flexible and could be changed, if required, in order to meet the top-level requirements. Similar to the top-level requirements, top-level objectives were defined for each scenario and for the overall system. The top-level system objectives for each threat scenario are shown in Figure 23.

Small Boat Attack (SBA)	Identify Hostile Intent with 90% accuracy
	Engage SBA by 250m from target
	Neutralize SBA by 65m from target
Ship As a Weapon (SAW)	Identify 99% of high-risk SAW threats (hazardous cargo)
	Identify SAW attack with 95% accuracy
	Engage SAW by 2,000m from pier
	Neutralize SAW by 500m from pier
WMD	Detect Chemical, Biological, Radiological, Nuclear (CBRN) material prior to Critical Area

Figure 23. Top-Level Scenario-Specific System Objectives

Derived from the top-level system requirements, the SEA-7 Cohort derived top-level system objectives for each threat scenario. These objectives, while flexible, were useful as a starting point for further study.

The overall top-level system objectives were defined as:

- Evaluate MDP system cost.
- Evaluate commercial system cost.
- Evaluate commercial delay cost.
- Evaluate expected damage cost for each threat scenario.

These top-level, overall system objectives eventually translated into the MOEs and metrics that were used to evaluate the performance of the different integrated system architectures.

2.3.2 Requirements Generation – Sensors Group

Requirements generation for the Sensors System utilized the Effective Need Statement, Needs Analysis, and the Sensors Group's Objectives Hierarchy. These combined artifacts provided the seed material for collaborative efforts in discussions and brainstorming sessions attended by SEA-7 and TDSI personnel. These sessions combined a system-level perspective from the SEA Sensors Group and a well-developed, discipline-specific perspective from the Sensors Track TDSI professionals to give a large collection of system attributes and "desirables." In addition, the CONOPS (Section 1.8.1) provided general guidance for the Sensors System:

> "A network of space, air, surface, or subsurface sensors (active and/or passive), either single or in combination, will be used to locate, track and classify surface contacts within the Area of Regard (AOR). Design parameters will be chosen so the sensor network will effectively track all surface contacts above a minimum gross weight (initially 300 tons). This information will feed into the C3I system, and its accuracy will contribute to minimizing both Force and Inspection response times."

From this guidance and analysis of the particular sensor system-level implications of the overall top-level objectives, a preliminary document was developed by the Sensor Group, working in conjunction with the other MDP Groups—particularly the C3I Group—and the newly assimilated TDSI students. This document included the following statement:

> Sensor system-level objective and overall concept: To provide a persistent, real-time, all-weather capability to locate, track and classify all defined contacts of interest (COI) within the AOR to support situational awareness and C2.

In order to satisfy these system-level objectives, the following attributes were determined to be required from the sensor system:

- 24/7, all-weather, real-time (RT)/near real-time (NRT) capability.
- Fully networked and dynamic tasking (Network Centric Warfare (NCW) basic tenets).
- Highly automated.
- Achieve multiple "sensory views" of each COI.
- High sensor data integration and association (fusion).
- Overlapping sensor coverage to provide seamless coverage over the entire AOR.
- High scalability/modularity.
- High connectivity (communications requirement).
- High information assurance (IA requirement).
- Very high operational availability (reliability, supportability, maintainability).

In order to attain these required attributes, the following basic system-level design requirements were identified:

- A **combination of sensors** (and platforms) networked to provide a common operational picture (COP). No single sensor type/platform could provide all of the necessary data.
- **Radar as primary provider** for COP. The specific "all-weather" requirement made this mandatory in a heavy-rainfall environment.
- **Augmented by other sensor capabilities** to meet classification and identification (ID) requirements, i.e., electro-optical/infrared (EO/IR), sonar, magnetic and also cooperative means (particularly vessel tracking systems like the Automatic Identification System (AIS)). Although radar was selected to be the primary sensor, the specific observables that can be

obtained by radar were of lower resolution than that required to provide classification and identification for most COIs.

From these system-level design requirements, the Sensors Group derived the following technical requirements for the Sensor System:

- **Sensitivity** (minimum detectability requirements).
  - Locate and track 99.9% of "large ships" (≥ 50m length – 300 gross registered tonnes (GRTs).
  - Locate and track 80% of "small boats" (≥ 7m length).
- **Area Coverage.**
  - Range: within the defined AOR.
  - Coverage: overlapping coverage within AOR.
- **Accuracy of Measurements** (position).
  - SAW (large ship): 50m Circular Error Probable (CEP).
  - SBA (small boat): 10m CEP.
- **Time Latency.**
  - Ability to meet C2 decision cycle timing constraints.

2.3.3 Requirements Generation – C3I Group

Requirements Generation for Communications and Information Assurance was primarily conducted by the TDSI Communications and Information Assurance tracks. Requirements were derived from the scenario (use case) descriptions, CONOPS, Effective Need Statement, and the Objectives Hierarchy.

Communications was the common thread that determined how all the other systems interfaced with the C3I System. Communications and Information Assurance requirements generation began with sensor interface requirements:

Interface Requirements (from Sensors)

- Bi-directional communications (from C2 to Sensors and from Sensors to C2 and Intelligence).
- Digital (analog-to-digital conversion for some existing legacy systems).
- Asymmetric bandwidth; less bandwidth will be needed to communicate directions and tasking from the C2 Center than to communicate constantly gathered information to the C2 Center from the sensor(s). This may also be priority-based.
- Time latency must be RT or NRT.
- Sensor or communications equipment self-test can be latent.
- Two operational modes (broadcast and query/interrogation and polling).
- Transmissions must be secure (Information Assurance concern).
- Topology (hierarchical, mesh, or other).
- Deployment to isolated sites.
- Mobile link capability.
- Deployed forces communications.
- Twenty-four hours a day/seven days a week.
- All-weather.
- Ability to meet C2 decision cycle times.
- Time to sense.
- Time to transmit.
- Time to apply applications and algorithms.
- Time to transmit any decision.
- Update rate.

Communications Requirements

- **Network topology.**
  - Hierarchical.
  - Mesh.
- **Capabilities.**
  - Accommodate mobile nodes.
  - Interoperable with existing systems.
  - Bi-directional channel.
  - Unicast and multicast.
  - Asymmetric bandwidth.
  - Digital.
  - Time latency.

IA Requirements

- **Topology.**
  - Layered.
  - Compartmentalized.
- **Capabilities.**
  - Control on accessibility.
  - Ensure integrity of information exchange.
  - Maintain confidentiality of classes of information.
  - Availability of information.
  - Interoperability across different protocols.

C2 Requirements

"Network centricity" and situational awareness drove C2 and intelligence requirement generation:

- **Achieve Interoperability:** Leads to self-synchronization and shared awareness.
  - Coalition Environment.
- **Achieve Sensibility:** The ability to make sense of a situation.
- **Orchestrate** a means to respond.
- **Support Agility:** Represent future threats and operational environments through foresight.
- **Robustness:** The ability to maintain effectiveness across a range of tasks, situations, and conditions (to measure must examine effectiveness of C2 Systems across full range of operating environments and relevant missions).
- **Resilience:** The ability to recover from or adjust to misfortune, damage, or a destabilizing perturbation in the environment (to measure how the system [commanders, force, and support systems] responds to stress, force, number of nodes (self-healing networks), collaborative decision making (more resilience = can withstand greater stress, disrupted for less time)).
- **Flexibility:** The ability to employ alternative ways to succeed and the capacity to move seamlessly between them (shift seamlessly to other alternatives). The ability to see changes in battle-space more rapidly (measure how fast decisions can be disseminated and implemented).

- **Responsiveness:** The ability to react to a change in the environment in a timely manner (the ability to control tempo rather than simply speed of response).
- **Innovation:** The ability to do new things and the ability to do old things in new ways (keeps enemy from adapting and learning how to thwart) denies the enemy an advantage due to learning (use experts to measure whether system is innovative).
- **Adaptation:** The ability to change work processes and the ability to change the organization methods:
    - Alter how information is distributed and how coalitions are organized.
    - Create new ways of dealing with coalitions.
    - Flatten organizational structures-modularity.
    - Develop more efficient work processes.
- Provide an **operational intent.**
- Be **scenario independent.**

Intelligence Requirements

The system requirements for an Intelligence System were typically very general and less technical. The two key requirements for the Intelligence System were timeliness and relevance. It was important for the decision makers to have pertinent information in the shortest amount of time. The other requirements of the system could be tied directly to the functional areas.

- **Plan Function.**
- **Relevant:** There must be a developed plan in order to ensure the correct information is given to the correct decision makers.

- **Collect Data.**
- **Available:** It is critical that the system be readily available through continuous operation and all source involvement.
- **Dynamically Adaptable:** This requirement ensures a level of completed tasking as well as the ability to handle tactical collection in an RT environment.
- **Process/Exploit.**
- **Timely:** Key factor in determining the effectiveness of the system. The intelligence can be relevant and accurate, but if it does not reach the decision maker with enough time to properly act on that intelligence, then the system has failed.
- **Accurate:** Correct processing of the raw data so analysts can make confident recommendations. Raw data is converted to information at this stage in the intelligence process.
- **Thorough:** The ability to process and exploit a large percentage of the collected data. If the system is unable to process enough of the collected data, collection assets are wasted and the system is inefficient.
- **Analyze/Integrate.**
- **Objective:** Unbiased look at the collected information and fuse the data together such that the most reliable intelligence is being disseminated to the decision maker. The analysis cannot be affected by any political or personal agenda because this would discredit the value of the intelligence to the operator.
- **Disseminate.**
- **Relevant:** There must be a developed plan in order to ensure the correct information is given to the correct decision makers when it is time to disseminate the intelligence.

- **Usable:** It is important for the system to be able to handle the high volumes of intelligence reports. Also, it is necessary for everyone involved in the situation to have access to those intelligence reports.

2.3.4 Requirements Generation – Force Group

The functions of the Force System determined how to meet the security needs of the maritime shipping industry at sea, specifically defending both existing infrastructure as well as transiting vessels from various attacks. The Force System was a necessary addition to forces in theater, because it represented a persistent threat to the terrorists in the AOR. To meet the objectives, the Force System had the following requirements:

- **All-Hours Capable:** The reaction force must be able to respond during both day and night crises.
- **All-Weather Capable:** The reaction force must be capable of responding to SBA attacks in weather up to Sea State 3 and SAW and WMD attacks in weather up to Sea State 5.
- **Self Sustaining:** All reaction forces must be capable of carrying all necessary equipment and inspection gear.
- **Long Range Response:** Inspection team must be capable of intercepting a suspect vessel at ranges exceeding 250 NM.

2.3.5 Requirements Generation – Land Inspection Group

The functions of the Land Inspection System determined how to meet the security needs of the maritime shipping industry on shore, specifically for the world's busiest ports. The Land Inspection System was necessary to increase the number of containers inspected in order to prevent hazardous materials from being shipped between countries or to be smuggled onto a large merchant ship. It was impractical to stop and thoroughly inspect every container without adverse economic effects. To meet the objectives, the Land Inspection System had the following requirements:

- System components available for implementation in five years.
- Detect hazardous materials to include chemical, biological, nuclear, radiological, and explosive (CBNRE) materials.
- Screen and inspect IMO standard 20-foot containers.
- Validate manifest for container processing and shipping.
- Be flexible for use in different port structures.
- Provide adequate present and past information about containers, shippers, and carriers.
- Communicate results.
- Use active and passive inspection technologies to increase the number of containers inspected and minimize delay.
- Provide targeting logic for determining which containers to inspect.
- Take ten minutes to initially scan containers.
- Have dedicated personnel for inspection analysis of sensor results.
- Improve intransit security of containers.

The following system attributes were also determined:

- **Secure:** The information used to target and inspect containers could not be susceptible to infiltrators or inadvertent receipt by unauthorized personnel.
- **Efficient:** The Inspection System was required to not unduly hinder the volume of container throughput. This would have a local affect as well as worldwide economic impact.

- **Cost Effective:** The benefit of having an inspection regime was required to provide a heightened level of security that outweighed adverse impacts on commercial shipping and port operations.
- **Minimize Risk:** The motivation of an Inspection System was to detect potentially illicit materials that could be used as WMD. The system was required to reduce the vulnerability of the commercial shipping industry to such an event.
- **Adaptability:** Shipping of containerized cargo was a detailed, complex industry that operated continuously. Since there were a wide range of variables that made each port unique, the system was required to be flexible in order to be implemented over a large range of various sized ports.

2.3.6 Requirements Generation – Sea Inspection Group

The Sea Inspection Group derived the system requirements from the Objectives Hierarchy and other inputs, especially the Stakeholder Analysis. The WMD scenario was used as a basis for the analysis. For each of the alternatives, the following detailed Sea Inspection System requirements were generated:

- Search a minimum of 80% of each ship in six hours; equal to 10½ containers/minute.
- For bulk carriers, to search 80% of each ship in six hours; equal to 373 cubic meters/minute.
- A source capable of supplying power for nine hours to sensors and communications equipment (150% of max search time).
- Sensor packages were required to be man-portable.
- Inspection teams were required to be available 24 hours a day.

- Sensor packages were required to operate effectively in the maritime environment.
- Communications were required to be established between Inspection Team members.
- Status and results of inspections were required to be transmitted to C2 elements.
- System components were required to be in existence or viable within the next five years.
- Other factors that were considered included: flexibility of technology (i.e., components that included several sensors in one unit), physical size of the technology, and redundancy of sensors.

3.0 DESIGN AND ANALYSIS PHASE

Design and Analysis was the second phase in the Systems Engineering Design Process. The objective of the Design and Analysis phase was to create and evaluate several potential solutions to the problem. Progress through the Design and Analysis phase was divided into the Alternatives Generation step and the Modeling and Analysis step. During Alternatives Generation, multiple system solutions to the problem were constructed and the current systems were analyzed. Under the Modeling and Analysis step, the feasible alternative solutions and the current systems were modeled and then analyzed with multiple trials based on predefined scenarios. All the data from the trials was recorded and evaluated. The Design and Analysis phase resulted in feasible alternative solutions and an analysis of the benefits and trade-offs of each potential solution as well as current systems.

3.1 ALTERNATIVES GENERATION STEP

The Alternative Generation step involved the "creative mental process of producing concepts and ideas in order to solve the problem."[36] Brainstorming of potential solutions was based on system requirements and objectives. These requirements and objectives bound the design space, and a feasibility screening process imposed realistic limitations on the physical and technological characteristics of the possible system solutions. In addition to creating new solutions to the problem, the current system (or recognition of the lack of a current system) was also included as a possible solution to the problem. Following the development and selection of possible solutions, the alternatives were modeled and analyzed.

3.1.1 Alternatives Generation – Sensors Group

Sensor System alternatives were developed based on system-level requirements. Initially, technological solutions were considered, and subsequently, through an iterative process, they were further qualified and refined.

---

[36] Eugene Paulo, "Alternative Generation," SI4001 Introduction to Systems Engineering, Supplemental Class Notes, (July 2004).

3.1.2 Design Space – Sensors Group

The overall Design Space for the Sensors System was captured using a morphological chart represented in Table 13. This chart was created in brainstorming sessions and through research in order to capture the spectrum of attributes any Sensor System was expected to have. Specific care was taken to be creative, innovative, and inclusive. System synthesis was performed through careful and collaborative grouping of attributes, i.e., sensor types with platform, connectivity, communication scheme, etc.

Platform	Sensor Type	Connect - ivity	AOR Coverage	Sensor Trigger Mode	Data Transmission Mode	Data Fusion Functions	Coverage (footprint)
Ground-	Conventional Radar (MW)	Stand-Alone	Integral	Autonomous	Synchronous (broadcast)	Distributed between sensors and fusion node	Broad area (surveillance)
Air- (manned) (unmanned)	Imaging Radar (MW)	Fully Networked	Sectors	Cued	Interrogate/ Respond (polling)	Centralized at fusion node	Limited area (surveillance)
Sea/Surface- (fixed-installation) (semi-fixed-installation)	Laser Radar	Clustered				Hybrid	Strip-Swath (Surveillance)
Sea/Subsurface- (fixed-installation) (semi-fixed-installation)	Conventional Sonar						Spot (Reconn)
Space- (new constellation) (existing constellation) -military -commercial	Imaging Sonar						
Land- (fixed-installation) (semi-fixed-installation)	EO-IR						
Mobile- (multiple platforms)	ESM						
	Transponder/ Beacon						

Table 13. Sensor System Morphological Chart

The morphological chart captures all technological alternatives considered. Of those, only the ones regarded as being not clearly infeasible were carried forward.

As seen in the chart, the result was a substantial number of different combinations of "systems." Nevertheless, considering the timeline for implementation and operation, some sensors clearly played a more probable and central role than others for particular missions. After an initial survey of the technology and considering the particular

requirements and scenarios defined for the project, two fundamental decisions regarding the design space were also made and carried forward from this point:

- Radar (different platforms) would be the primary asset for detection and tracking. This decision is basically driven by:
  - The "all-weather" requirement. No other Sensor System has the required capability to provide continuous coverage in adverse weather.
  - The need to detect and track both cooperative and noncooperative contacts. Cooperative contacts could be detected and tracked effectively by other means (any global positioning satellite (GPS)-based fleet monitoring system or AIS for instance), but that solution would not work for noncooperative COIs.
- AIS and EO/IR sensors would be augmentation assets for classification/identification (ID). In this case, AIS would be the main Sensor System for classification/ID for cooperative contacts and EO/IR Systems would be used for noncooperative COIs. EO/IR sensors, in particular, have severe environmental limitations, as will be seen later in this analysis.

These decisions did not intend to imply that radar was not capable—in some instances—of performing classification/ID or, conversely, that EO/IR or AIS could not perform detection and tracking, as was previously mentioned. They were just design decisions made with particular consideration of sensor-specific performance characteristics, advantages and disadvantages, and supported by historical data and operational experience.

3.1.3 Summary of Alternative Architectures – Sensors Group

Following the systematic approach, many probable, possible, and conceptual technological architectures were briefly explored and researched. The intent was to be as

inclusive and broad as possible, the only constraint being the time horizon established for the project (five years out), and to include the full spectrum of attributes in the analysis and selection of those alternatives deemed most fit for providing the required capabilities and not clearly infeasible, given the design and environmental constraints.

The following specific alternatives were initially selected from the original set for detailed evaluation. All the proposed alternatives had a baseline common configuration, which had the following characteristics:

- Sensor deployment was based on separate sectorized Area and Approach coverages. Areas I and II covered the critical narrow part of the Straits from Kelang to Singapore (roughly 200 NM). Areas III and IV covered the wider portions of the straits north of Kelang and Area V the wider portion south of Singapore. The approaches extended these areas to the 300 NM maximum ranges defined, into the Andaman and South China Seas.
- Radar (different platforms) was the primary means for detection and tracking. Each alternative had distinct characteristics based on the selection of the particular Radar System or systems that were selected in each case.
- All the alternatives included the following sensors as augmentation for the classification/identification function:
    - Fixed and relocatable EO/IR Systems to provide additional observation of critical point areas (critical infrastructure, choke points, intelligence-cued points, etc.).
    - Maritime patrol aircraft (manned fixed/rotary wing and unmanned aerial vehicles (UAVs)) in either preprogrammed or cued modes; in both surveillance and reconnaissance missions.
    - Maritime patrol vessels in either preprogrammed or cued modes; in both surveillance and reconnaissance missions.
    - AIS base stations (ground and space-based variants explored).

In addition to the baseline configuration, three distinct radar alternatives were designed and evaluated in a first iteration, for the primary detection and tracking function.

Ground Microwave and HFSWR Alternative:

- A network of ground-based, maritime surveillance microwave radar stations is the primary asset for Area coverage for Sectors I and II, and along the coast through Sectors III, IV, and V.
- Ground-based, High Frequency Surface Wave Radar (HFSWR) maritime surveillance radar stations are primary assets for Approach coverage and Area coverage for Sectors III, IV, and V.

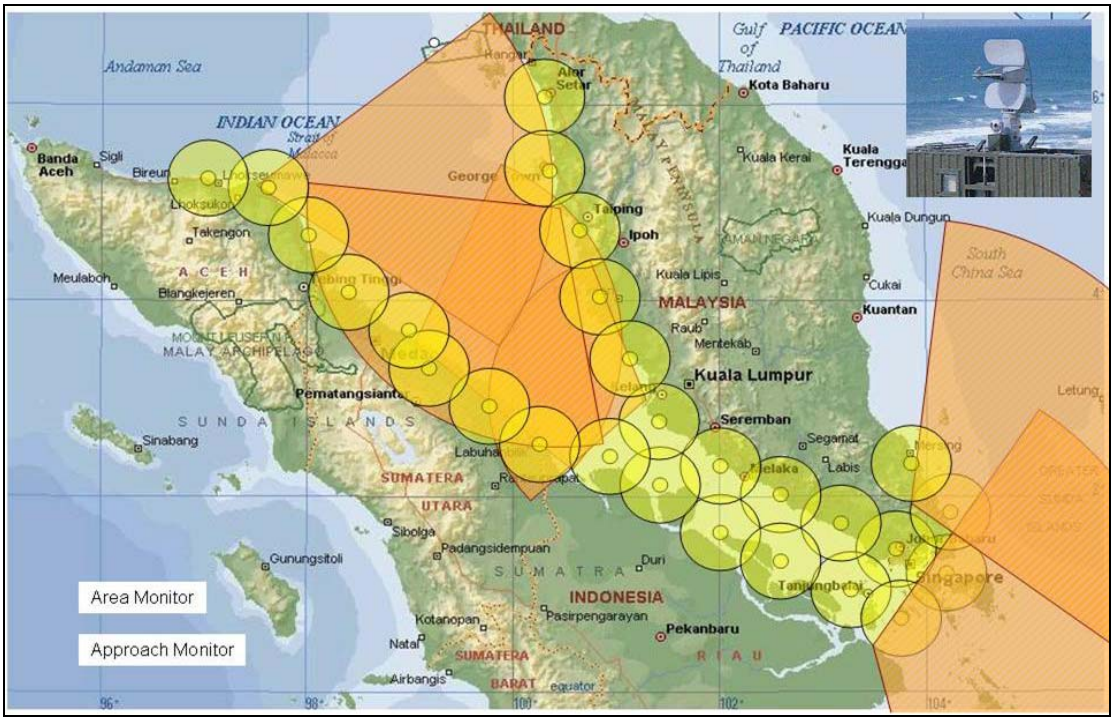

Figure 24. Ground Microwave Radar and HFSWR Alternative

This alternative considers HFSWR stations and microwave coastal radar stations. The former performs well in detection and tracking of all but the smallest crafts out to 200 NM; the later performs well against all vessels—including small, inflatable, fast boats—although only at a practical range of approximately 25 NM (antenna height dependent).

Ground Microwave and Space-Based Radar Vessel Tracking and Monitoring System Alternative:

- A network of ground-based, maritime surveillance microwave radar stations is the primary asset for Area coverage for Sectors I and II, and along the coast through Sectors III, IV, and V.
- A Low Earth Orbit (LEO) constellation of satellites is the primary asset to provide radar detection and tracking of maritime COIs in Area Sectors III, IV, and V and Approach coverages**.**

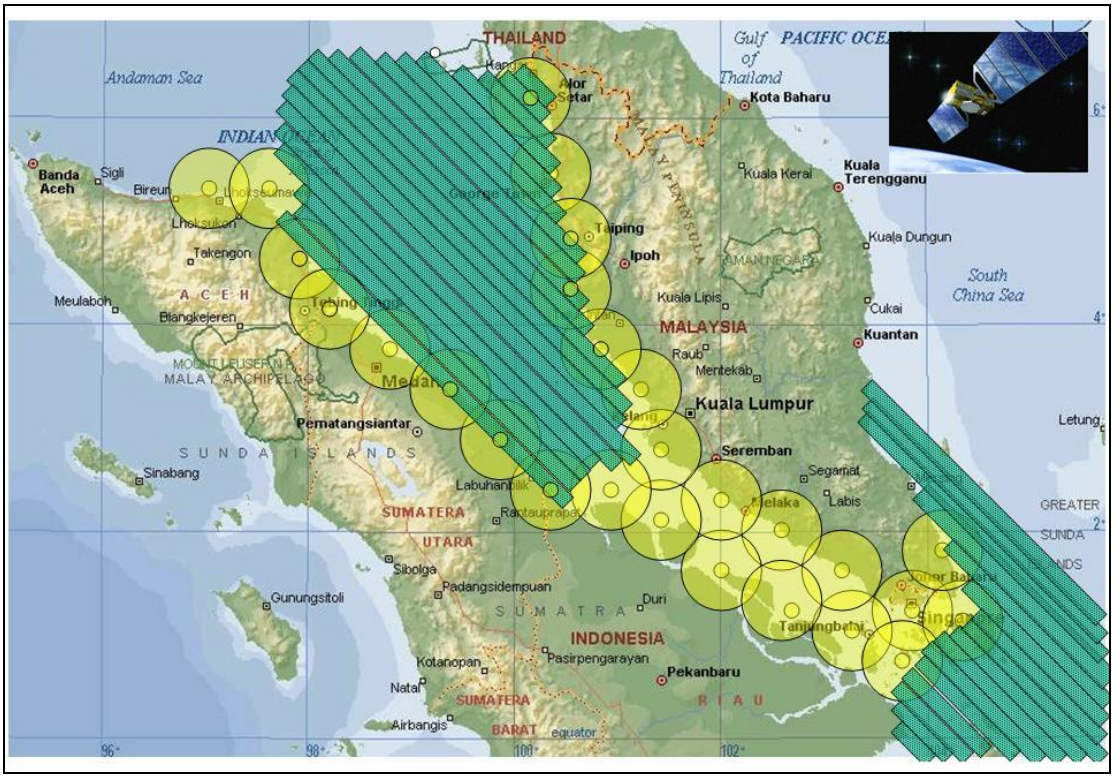

Figure 25. Ground Microwave Radar and Space-Based Radar Alternative

This alternative considers the use of Space Based Radar (SBR) to cover the areas where coastal radar systems cannot reach due to line of sight considerations. A constellation of no less than four satellites, in three orbital planes, is needed to get coverage and revisit times of approximately 30 minutes.

High Altitude Endurance Aerostat Radar - (HAEAR) Alternative:

- A network of high-altitude aerostats (70,000 feet) is the primary asset to provide radar (microwave) detection and tracking of maritime COIs in both Area and Approach coverages.
- A variation considered for this alternative includes an AIS transponder base station in the same aerostat platform.

Figure 26. HAEAR Alternative

This alternative considers the use of four HAEAR stations. These platforms are placed at approximately 70,000 feet—well above the jet stream region and outside controlled airspace—and allow coverages in excess of 350 NM from a single platform.

3.1.4 Feasibility Screening – Sensors Group

Sonar: The use of acoustic means (sonar) of detection and/or classification was part of an initial feasibility study, which recommended the elimination of this alternative due to severe environmental limitations. The specific information provided by that study is detailed in Appendix G, which provides detail for the Sensors Group.

HAEAR and Space Based Radar (SBR): A second iteration of the feasibility screening of the previously defined set of alternatives was performed, particularly focusing on the five-year technology horizon. As a result, the HAEAR and SBR alternatives were both eliminated from further consideration.

For the HAEAR, consultation with subject matter experts put the initial operating capability in the 15- to 20-year timeframe, mainly for power and weight considerations.[37] Although SBR seemed to be a more mature technology, maritime surveillance applications (meeting the requirements established for our system) were determined to be beyond the five-year time horizon as well. An overall assessment of technological risk for these two alternatives (HAEAR and SBR) showed that pouring additional dollars into the Research and Development (R&D) front end to accelerate the development of the technology to an acceptable level was not of great utility, given that other technology alternatives exist right now which are more advantageous (for performance, cost, and technology risk), as will be seen later in the detailed analysis of the selected alternatives.

Particularly for the aerostat solution, a tethered variant at a lower platform height (5,000 feet instead of 70,000 feet) was subsequently reviewed, and a new alternative was developed which used lower altitude and endurance tethered aerostats (referred to as Medium Altitude and Endurance Aerostat Radar or MAEAR). These platforms, based on proven technologies that are currently operational in many countries, could be used effectively to provide the needed capabilities out to the required maximum ranges. Although a significantly larger number of aerostats would be required due to the reduced coverage footprint, this option was considered far less technologically risky than the 70,000-foot HAEAR variant.[38]

As a result of this second and final iteration, two alternatives were defined as the baseline configuration for detection and tracking (radar-based). Both alternatives also included the common classification/ID augmentation sensors (EO/IR and AIS) as

---

[37] Dr. Kirk Evans, (Presentation at the USCG Maritime Domain Awareness Technology Forum) Department of Homeland Security, Santa Clara, CA, May 2005.

[38] Martin Steely, "Radar Aerostats Provide Cost-Effective Platform for Enhanced Observation," *Special Report: Jane's International Defense Review*, 1 April 2005.

previously defined. These alternatives, together with the "As-Is" System, are presented at the end of this section:

- Alternative 1: Ground Microwave Radar + HFSWR
- Alternative 2: MAEAR (Microwave Radar) + HFSWR

3.1.5 Quality Functional Deployment (QFD) – Sensors Group

As a measure to assure that the Sensors Group effectively met the expectations of the stakeholders and completely allocated system requirements, the Sensors Group developed Table 14, which depicts a basic QFD matrix. This provided an explicit cross-reference of functions (requirements) versus capabilities for the different sensors/platforms.

Technical Capabilities ⇨ / ⇩ Requirements	Ground-Based Microwave Radar	Ground-Based HFSWR	High Altitude Aerostat Radar	Ground-Based EO-IR	Airborne (MPA) Search Radar	Airborne (MPA) EO-IR	Shipborne Search Radar	Shipborne EO-IR	Space-Based Radar (VTS)	AIS/IMO Transponder System
24/7	x	x	x	x					x	x
All-Weather	x	x	x		x		x		x	x
Real-time/NRT (Latency)	x	x	x	x	x	x	x	x	NRT (2)	x
Overlapping Sensor Coverage	x	x	x	x	x	x	x	x		x
High Modularity/Scalability	x	x	x	x	x	x	x	x	x	x
High Connectivity	x	x	x	x					x	x
Locate & Track Large Ships (300+GRT; 50 m CEP)	x	x	x		x		x		x	x(1)
Locate & Track Small Boats (~7m; 10 m CEP)	x	x	x		x		x			x(1)
Classify & ID				x		x		x		x(1)

(1) Limited to cooperating vessels
(2) Revisit rate is a function of orbit and # satellites

Table 14. Sensors System QFD

The quality functional deployment matrix shows a clear cross-check reference of system-level requirements versus technical capabilities for each of the sensors considered.

3.1.6 2005 "As-Is" System – Sensors Group

A limited survey and analysis of existing Sensor Systems and capabilities in the region was performed and is detailed in Appendix G. This basic system included:

- Twelve radar remote-stations; seven in Malaysia (X/S band) and five in Singapore (X band).
- Three VTS authorities (Kelang, Johor, and Singapore).
- Seven AIS base stations, covering 180 miles from Kelang to Tanjung Piai in Malaysia.
- Two AIS base stations in the Singapore Straits.
- Several different MPA and patrol vessels.
- Ship's own sensors (mainly commercial-grade radar and AIS mobile stations).

As shown in Figure 27, there exists limited radar and AIS coverage in the Straits of Malacca, and the existing coverage is only available in the southern stretches of the Straits. The coverage extends from the vicinity of Port Kelang, Malaysia, southeast through the narrow portion of the Straits to Singapore. There is no coverage to the northwest of Port Kelang or to the east in the South China Sea.

Figure 27. "As-Is" Sensors System in the Straits of Malacca

The "As-Is" System was surveyed through existing open-literature and sources. There exists some very limited radar and AIS coverage south of Kelang, which extends along the Malaysian coastline through the Singapore Strait.

3.1.6.1 Alternative 1: Ground Microwave Radar + HFSWR

In addition to the baseline common configuration, the Sensors Alternative 1 utilized ground (coastal) microwave radar and HFSWR, including:

- A network of ground-based (coastal), maritime surveillance microwave radar stations that was the primary asset for coverage in Sectors I and II (Area).
- Ground-based, HFSWR maritime surveillance radar stations were the primary asset for coverage in Sectors III, IV, and V (Area), and approaches.
- Augmented by AIS base stations (ground-based variant selected), collocated with each radar station.

- Augmented by maritime patrol aircraft (manned, fixed-wing, selected) in both preprogrammed and cued modes. Reconnaissance missions with EO/IR payload (classification/ID) only.

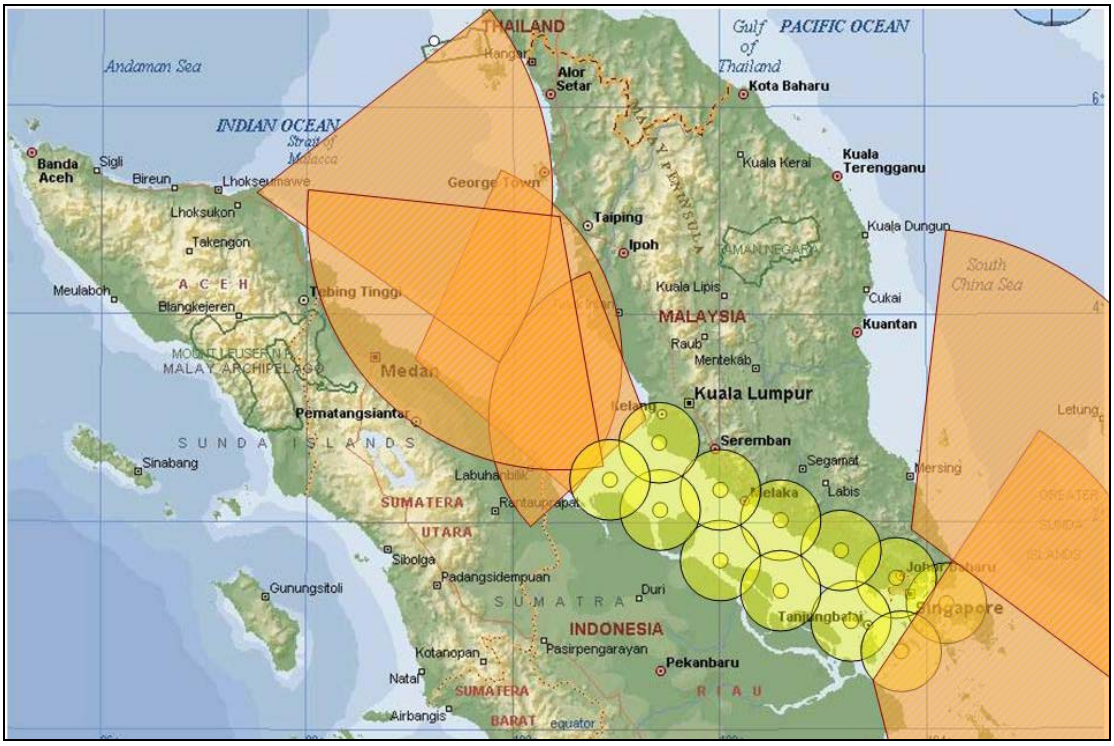

Figure 28. Sensors System Alternative 1 – Ground Microwave Radar and HFSWR

This alternative considers a slight variation of the previously defined coastal radar system. Instead of placing stations all the way north to the entrance of the strait, the coverage is limited to the critical area south of Kelang. HFSWR covers the approaches.

3.1.6.2 Alternative 2: MAEAR (Microwave) + HFSWR

This alternative was derived from the HAEAR variant, which was discarded during feasibility analysis due to technological risk, as previously discussed. In addition to the baseline common configuration, the Sensors Alternative 2 utilized MAEAR and HFSWR, including:

- A network of tethered maritime surveillance microwave MAEAR stations was the primary asset for coverage in Sectors I, II, and III (Area).

- Ground-based, HFSWR maritime surveillance radar stations were the primary asset for coverage in Sectors III, IV, and V (Area), and approaches.
- Augmented by AIS base stations (aerostat variant selected).
- Augmented by maritime patrol aircraft (manned, fixed-wing selected) in both preprogrammed and cued modes. Both surveillance and reconnaissance missions. Radar (detection and tracking), AIS, and EO/IR payload (classification/ID).
- Augmented by maritime local short-range surveillance microwave radar stations (existing) for major port approaches (George Town, Kelang, and Singapore).

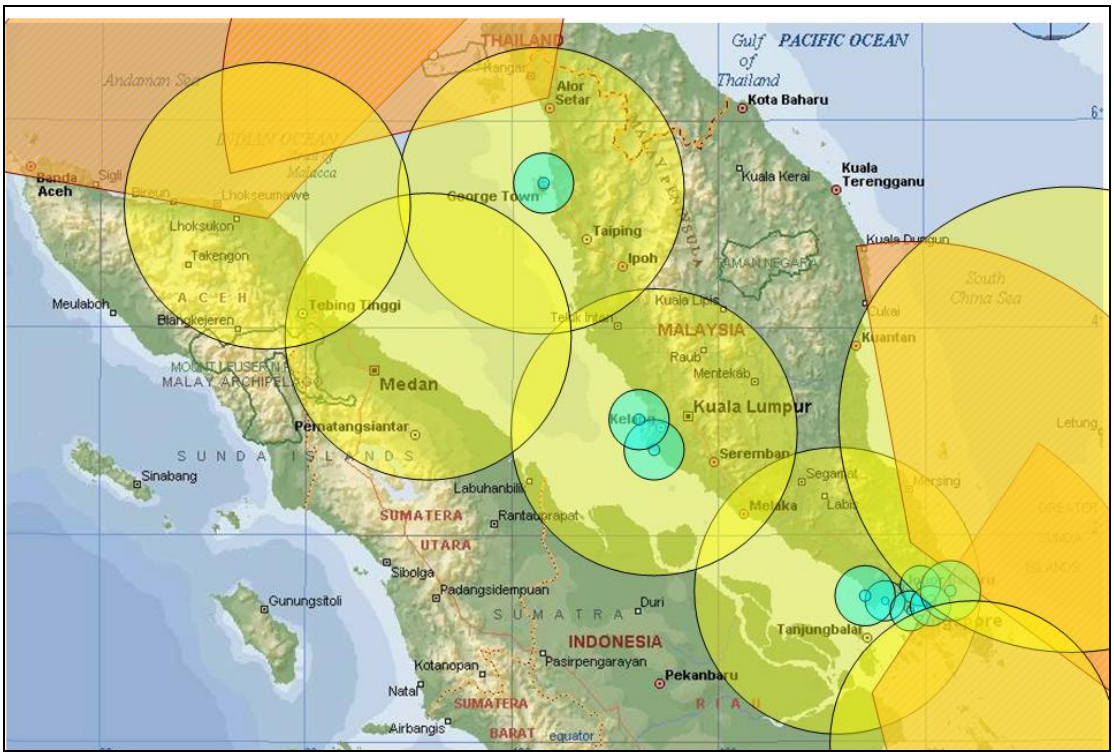

Figure 29. Sensors System Alternative 2 – MAEAR and HFSWR

This alternative was defined once the infeasibility of the HAEAR option was determined. Trading range (coverage) for altitude, a set of lower altitude (5,000 feet) tethered aerostats is used to get the required coverage along the area of the strait, while HFSWR covers the approaches out to an additional 200 NM.

3.2.1 Alternatives Generation – C3I Group

The C3I Group took an ideational approach to alternative generation. Ideation is the creative mental process of producing concepts and ideas in order to solve problems. The group relied on conceptual analogy, brainstorming, and research on existing technologies, designs, and capabilities to generate alternatives. The process was further divided into the Command and Control (C2)/Intelligence, Communications, and Information Assurance Subgroups.

3.2.2 Design Space – C3I Group

The C3I design space for technology and infrastructures ranged from existing systems to Technology Readiness Level 4 (TRL 4) Systems. TRL 4 was defined as technology that has been proven in the laboratory and ready to be field-tested and that could be 90% operational within five years.[39]

The Communications and Information Assurance technology included systems developed by Singapore and the United States. The C2 and Intelligence design space included technology and procedures used by the U.S. Coast Guard Maritime Intelligence Fusion Center (MIFC) West Coast in Alameda, California, and included in Singapore's National Security Strategy.

3.2.3 Alternatives Generation

The MIFC West Coast was the primary analogous system for the C2 and Intelligence architectures. It represented the first collocated C2 and Intelligence Center and served as the model for the configuration of subsequent centers. The group did not design separate C2 and Intelligence architectures, but developed alternatives that included C2/Intelligence Data Fusion Centers that provided the decision maker with operational intelligence. Operational intelligence is similar to "knowledge mobilization" as described by Edward R. Smith in "Effects Based Operations: Applying

[39] The Defense Acquisition Guidebook, Section 10.5.2: Technology Maturity and Technology Readiness Assessments, http://akss.dau.mil/dag/DoD5000.asp, (15 March 2005).

Network-Centric Warfare in Peace, Crisis, and War."[40] Knowledge mobilization was the ability to "tap" into knowledge (i.e., intelligence) wherever it was available to the decision maker.[41] Knowledge mobility, along with options, agility, and coordination, was how network-centric operations contributed to the conduct of successful effects-based operations.[42]

The Communications and Information Assurance teams were composed of TDSI students from those respective tracks. These teams were responsible for designing the communications and information assurance architectures. It was assumed that current computer technology was sufficient to handle all C2, intelligence, communications, and information assurance requirements. As a result, computers were only included in the system cost analysis.

The communications architecture alternatives were based on the requirements of the Intelligence and C2 Centers. The intent was to incorporate the redundant features of a "mesh" system with control of a hierarchical system.

Information Assurance alternative generation applied a Defense In Depth (DID) strategy that placed multiple barriers between an attacker and security-critical information resources. DID also provided added protection and increased security by increasing the cost of an attack. Figure 30 is a conceptual model of DID.

[40] Edward R. Smith, "Effects Based Operations: Applying Network-Centric Warfare in Peace, Crisis, and War," CCRP Publication Series, (November 2002).

[41] Ibid, p. 538.

[42] Ibid, p. 531.

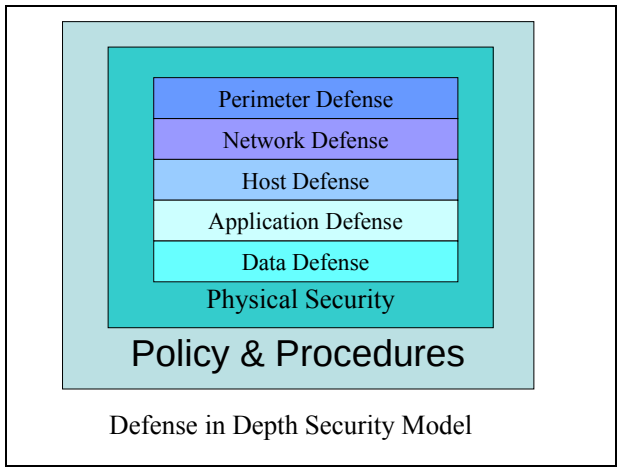

Figure 30. DID Security Model

The DID strategy places multiple security barriers between potential attackers and all layers of defense mechanism: perimeter defense, network defense, host defense, application defense, and data defense.

At the base of DID were formal security policies and procedures governing and protecting the entire system. These dictated the expected behavioral and protection requirement of the system. These policies were applicable to all layers of defense mechanism: perimeter defense, network defense, host defense, application defense, and data defense.

3.2.4 2005 "As-Is" System

There was no regional C3I System integrating Singapore, Malaysia, and Indonesia operating at the time of this report. Of the countries bordering the Malacca Straits, Singapore was best suited to react to and/or counter the threats represented in our scenarios. Singapore's National Security Architecture represented the only C2/Intelligence Center (see Figure 31).

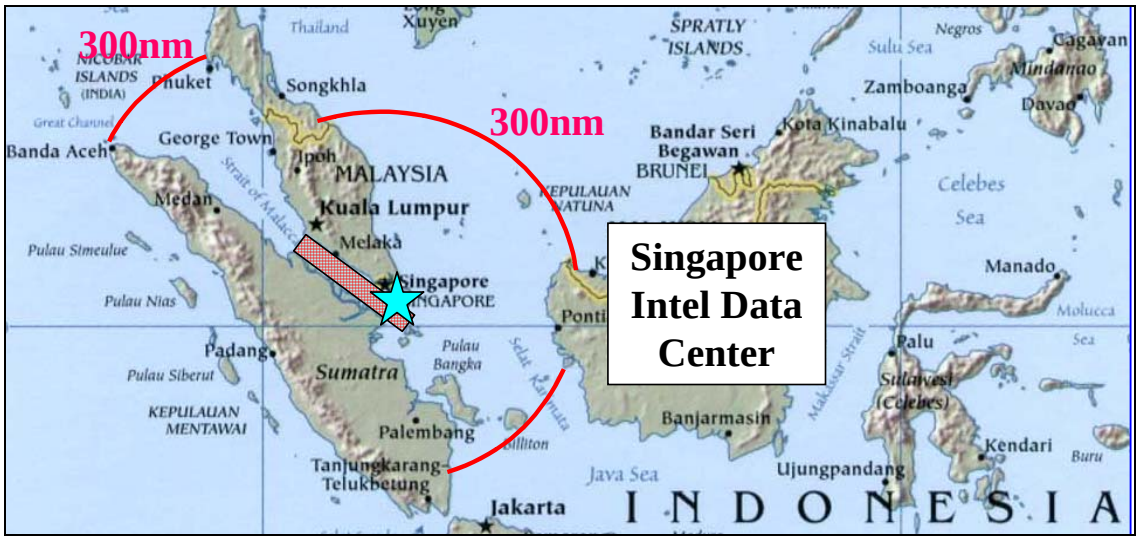

Figure 31. "As-Is" System: Singapore as the Only Maritime C2/Intelligence Presence

As shown on the map, Singapore's focus on Maritime Domain Protection is relevant to only a very small portion of the Malacca Straits region. Current Sensor range restricts their Maritime Domain Awareness to the highlighted area, stretching northwest to the port of Kelang. Malaysia and Indonesia only policed their respective territorial waters.

The aim of Singapore's national security architecture was to integrate and "synergize" the work of different national security agencies in the operations, intelligence and policy domains[43]. They established the National Security Task Force (NSTF), which was staffed by both police and military elements, to maintain a comprehensive watch over the island and to integrate operational responses on land, in the air, and at sea. The Ministry of Home Affairs set up the Homefront Security Center and the armed forces developed the Island Defense Operations Center as key components of the NSTF. Singapore also set up the Joint Counter-Terrorism Center for integrating intelligence at the national, regional, and international levels. In contrast to Singapore's externally focused security strategy, Malaysia and Indonesia were more focused on "territorial" or internal security.[44]

---

[43] Tony Yam, "Fight Against Terror, Singapore's National Security Strategy," National Security Coordination Centre, http://www.pmo.gov.sp/NSCS/FightAgainstTerror.pdf, (2004): pp.13-32.

[44] Dana R. Dillon, "Contemporary Security Challenges in Southeast Asia," *Parameters*, (Spring 1997): pp. 119-133.

The current "data fusing" architecture was determined to be highly centralized because Singapore represented the primary Maritime Domain Awareness System in the Malacca Straits. This system provided its relevance based on top-down, centralized planning in a hierarchal control flow. Vessel priority was determined to be "time-based" with respect to position relative to Singapore harbor. Data fusion and analysis was determined to be manual and sequential based on the ability to collect and process valuable information. There was a high potential for "backlog" in the sequential queue. The "As-Is Data Center" Systems utilized existing sensors in the area of responsibility (AOR) providing technical Electronic Intelligence (ELINT) collection (with only 5% provided from HUMINT. Authority was never delegated, which limited the system's adaptability to cope with new and diverse situations.

A cargo vessel entering the Straits of Malacca from the northwest would be tracked by George Town, Malaysia. Even though there is a submarine-laid fiber-optic cable (known as Sea-Me-We 3) that traverses the Malacca Straits, there was no system in place to ensure track information would be passed from George Town to Singapore. George Town could pass information to Singapore telephonically, but the lack of a formal intelligence sharing system impedes a common intelligence or operating picture. For the SAW and WMD scenarios, vessels would not be tracked by Singapore radar until they are in the vicinity of Kelang, approximately 400 km from Singapore. Its situation could not be assessed until after the harbor pilot boards in the vicinity of Klang. Singapore only tracks cargo vessels destined for Singapore.

3.2.4.1 Alternative 1

The first system alternative divided the Malacca Straits into two regions, each containing a similar C2/Intelligence Center, one located in the port of George Town at the northwest entrance to the Malacca Straits and the other in Singapore (see Figure 32).

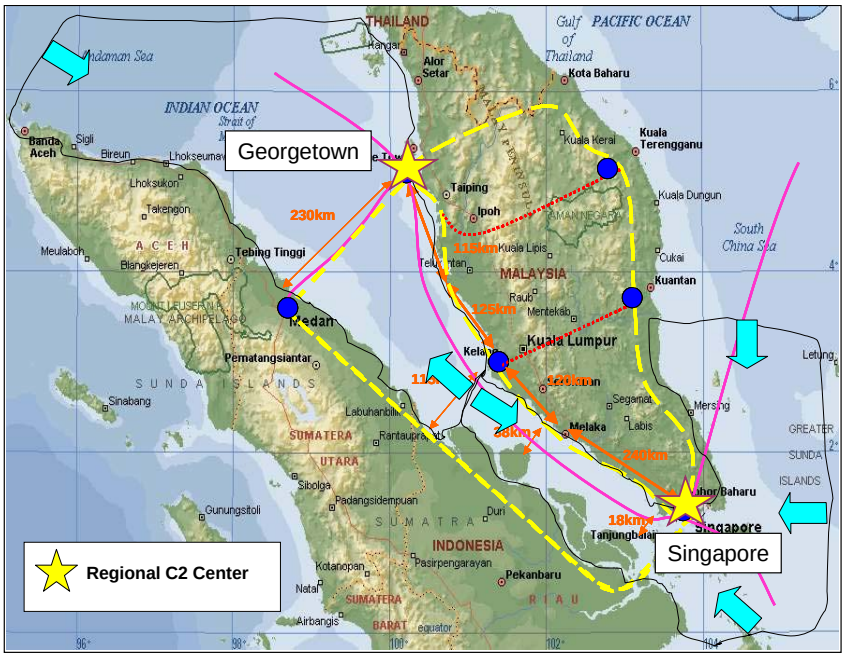

Figure 32. Alternative Architecture 1: Two C2/Intelligence Centers—George Town and Singapore

The regional architecture of Alternative 1 provides a common operating picture (COP) of the Malacca Straits Region. However, the C2/Intelligence Centers located at George Town in the northwest and Singapore in the southeast have a very large AOR for intelligence collection, data fusion, and C2.

George Town would be responsible for intelligence on traffic entering the straits from the northwest. Singapore would be responsible for traffic entering from the southeast, for example, from the South China Sea. Each center would be responsible for intelligence collection and data fusion and creation of a Common Intelligence Picture (CIP) of their area. The alternative also included a "network centric" communication architecture to facilitate sharing information to create a COP of the entire region. The COP was a result of each C2/Intelligence Center having access to each other's CIP. The communications network incorporated a fiber-optic backbone, wireless communications buoy stations, and Stratellites.

3.2.4.2 Alternative 2

Alternative 2 divided the AOR into four regions, each containing a Regional C2/Intelligence Center (see Figure 33).

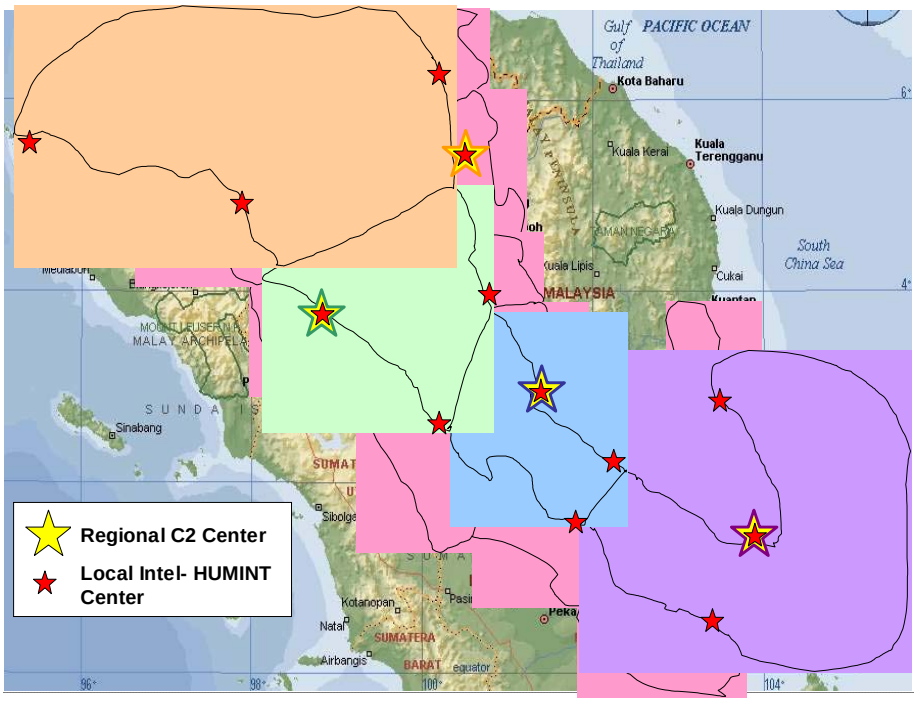

Figure 33. Alternative 2: Network Centric Architecture

The intent of Alternative 2 was to segregate the AOR into smaller sections of distributed operational responsibility and more manageable areas for analysis.

It included the same communications network as Alternative 1. The primary difference between Alternatives 1 and 2 was how the region was divided into "analysis segments." Three of the four regions were augmented by two data fusion cells. Singapore contained three data fusion cells to cover traffic coming directly south from the South China Sea. This provided nine data fusion cells spread throughout the Malacca Straits. The purpose of these cells was to aggregate intelligence into a "local" CIP, which was aggregated by the C2/Intelligence Center into a regional COP.

Another feature of Alternative 2 was a HUMINT intelligence network. Thirteen Intelligence Collection nodes, either separate or collocated with the data fusion centers, were spread throughout the region. These collection nodes provided a pipeline of information provided by someone seeing something out of the ordinary that, when combined with other information, could provide a warning to potential terrorist attacks.

The intent of the C2 System for Alternative 2 was to be "Self-Synchronizing".[45] It would adapt to a method of decision making (cyclic, interventionist, problem-solving, problem-bounding, selective control, control-free) based on the situation or scenario. This adaptability would be achieved through distributed authority to all regional C2/Intelligence Centers for actionable tasking and responsibility. A dynamic intelligence collection mix, as well as full counterintelligence based on information dissemination, contributed to the system's adaptability. Other self-synchronizing characteristics include clear command intent, competence among decision makers, and trust among decision makers at all levels. An historical example of self-synchronizing C2 was exhibited by the British fleet at the Battle of Trafalgar (1805).[46] Lord Nelson was entrusted with the main battle fleet to find and destroy the Spanish and French fleets. Traditional British tactics put Lord Nelson's vessels at a disadvantage when exchanging gunfire alongside the more heavily armed Spanish and French ships. He adapted to the situation and attacked perpendicular to the enemy's line, rather than parallel. Once the battle began, there was little opportunity for communication between British captains. The British victory was attributed to shared information about the battlespace, clear commander's intent, and competence and trust among decision makers at all levels.

Another feature of the Alternative 2 intelligence system was autonomous fusing that pushed the "track identification and classification" function down to the sensor domain. This was accomplished by collocating AIS transponders with sensors, similar to the current aviation Identification Friend or Foe (IFF) System. Intelligence analysis at the regional C2/Intelligence centers utilized consequence-probability and time-based parameters to determining threat priorities. Use of pattern recognition and intelligence agents, located at the local Intelligence Center, provided a more enhanced situational awareness over the "As-Is" and Alternative 1 Systems.

---

[45] David S. Albert and Richard E. Hayes, "Power to the Edge," CCRP Publication Series, (June 2003): pp. 98-102.

[46] Ibid, p. 28.

3.2.4.3 Communications Network

Both alternatives contained a network centric communications network linking all the intelligence sources to the data fusion cells and C2/Intelligence Centers. These intelligence sources included sensor platforms (as developed by the Sensors Group), land inspection, and external intelligence (sources outside the MDP System). The data fusion process, through aggregation and analysis, used the information from these sources to develop the CIP and COP. The network consisted of a communications and information assurance architecture.

Communications Architecture: The communications architectures consisted of a fixed network and a last mile network. The fixed network design consisted of combinations of the following: backbone (country to country), satellite (sensors nodes and sites to backbone), and access layers (aggregating or repeater nodes back to the backbone as well as role based access). The last mile network provided connectivity to the backbone. It consisted of one or more of the following: HF/VHF/UHF radio, microwave radar communications, free space optics, 802.11 a/b/g broadband Ethernet wireless, and 802.16 broadband Ethernet wireless. The 802.11 a/b/g can transmit directionally two miles and is line of sight limited. The 802.16 can transmit 30 miles and is directional (but can be made omni-directional through various placement schemes), but it had unknown space and power requirements.

Available technology options for long-range communications (defined as >20 miles) were fiber-optic networks, DWDM (dense wavelength division multiplexing), SONET/SDH (synchronous optical network/synchronous digital hierarchy), long-haul microwave links (line of sight) and satellite communications (VSAT). Technology options available for short range communications (defined as <20 miles) were short haul microwave links (with line of sight considerations), digital radios and traditional radios (HF/VHF/UHF), 802.11 a/b/g and 802.16 (as described above), ultra-wide band (UWB), and free space optics (FSO). Another technology used was the submarine-laid fiber-optic cable that ran along the Strait's sea floor from Singapore to Malaysia, part of a worldwide fiber-optic link system. A supplemental link, another submarine-laid fiber-optic cable known as Sea-Me-We 4, would connect George Town, Malaysia and Medan, Indonesia

by 2007. This fiber-optic link was laid around the world on the oceans' sea floor, providing connectivity both west and east of the Malacca Straits, as well as internally throughout the entire Malacca Straits. This 20,000-km system could scale to terabit capacities.

The backbone design consisted of a fiber-optics network. A fiber-optic backbone was chosen because of its reliability, security, immediate availability, information capacity, and speed of transfer. The overall network consisted of two loops: the Indonesia loop and the Malaysia loop, with the common crossover in Singapore and connectivity via the submarine laid fiber-optic cable between George Town and Medan. The fiber-optic backbone served as the main communications highway for all Command and Control nodes (high degree of supportability), and this highway provided link protection and routing capabilities. Each ring had its own fiber-optic network infrastructure that handled the connections to sensors, ground units (or sea going units), and command centers. Singapore and George Town served as the east-west gateways for fiber-optic transmissions along the submarine-laid cable. Public networks such as port authorities and disaster management centers plugged into the backbone network as the need arose. Fiber-optic services would be leased to participating countries. The large scale of the Malacca Strait area made using fiber-optic cable the most viable alternative. All of the technologies in the communications architecture were scalable to areas including the English Channel or the Strait of Gibraltar.

The challenge in designing the last mile network was remote sensor site connectivity. The last mile access network refers to the final leg (network segment) of delivering communications connectivity to a customer or end-user. The Sensor Group's alternatives included sensor sites along the Malaysian and Indonesian coastline where fiber-optic cable did not run. Line of sight wireless communications with repeater nodes connected the remote sites to the backbone network. The high cost of laying more fiber-optic cable (approximately US$60,000 per km inclusive of required infrastructure such as man-holes and pipelines) and the longer latency of satellites made wireless the most feasible option.

Despite the average yearly rainfall and temperature extremes in the weather patterns in the area of the Malacca Straits, the microwave capability was not significantly degraded, even in the worst weather conditions. Using the ITU-R530 model, availability of the microwave spectrum in the worst month for average rainfall had little degradation. The ITU-R530 model is the International Telecommunication Union Radio Communication Standard relating to propagation data and prediction methods required for the design of terrestrial line of sight (LOS) systems. The microwave spectrum was available greater than 99.993% of the time. This calculation assumed the following:

- Climate: maritime temperature, high humidity and coastal conditions.
- Rainfall: average 145mm/hour.
- Frequency of microwave used: 7.5GHz.
- Distance transmitted: 20 km.
- Path loss: atmospheric attenuation, branching, fading, multipath, and polarization are taken into account.

Links, both wired and wireless connectivity links, were classified by three types: A, B, and C; and each type had associated criteria: bandwidth, availability, reliability, bit error rate, recovery time, and latency. According to these criteria, Class A links (such as the fiber-optic backbone) had the highest performance, followed by Class B links (such as the wireless links from sensor to backbone) and, finally, Class C links (land lines and satellite links). Table 15 classifies the links according to the criteria.

Criteria	Class A Links	Class B Links	Class C Links
Bandwidth (Possibilities)	50 Mbps, 155Mbps, Gigabit Ethernet (1Gbps)	1.5/2 Mbps, 34/45 Mbps, 155 Mbps	2 Mbps, 384Kbps (ISDN line rates)
Availability	0.9999	0.999 (affected by weather and ducting)	0.9999 (varies)
Reliability	Very high	Good (weather dependent)	Very good
Bit error rate	Excellent (~10^{-9})	Good (~10^{-6})	Dependent on service level agreement (>10^{-6})
Recovery time	~50ms	100ms – 10sec	>1 min
Latency	Microseconds per km	Milliseconds per km	Tens of microseconds per km, or 500ms for satellite
Redundancy	Route and system	Partial route and system	Best effort service delivery

Table 15. Classification of Communication Links

Links were classified by types: A, B, and C. Each type had associated criteria: bandwidth, availability, reliability, bit error rate, recovery time, and latency. According to these criteria, Class A links (such as the fiber-optic backbone) had the highest performance, followed by Class B links (such as the wireless links from sensor to backbone) and, finally, Class C links (land lines and satellite links).

The communications architecture was scaleable to accommodate all of the C2 and intelligence alternative architectures. The existence of a backbone remained constant. In each communications alternative, the last mile portion changed with respect to the geographical placement of the C2 and Intelligence Centers and the feasibility of technology employment.

Information Assurance: Information Assurance's DID strategy applied layered defense to prevent direct exploitation of any vulnerability that existed in the system. It placed multiple layers of protection to prevent attackers from directly attacking the system to gain access to the security critical information resources. DID organized the security countermeasure mechanisms such that they were structurally implemented based on the purposes and degree of defense.

The following Information Assurance prevention and detection mechanisms were applied to secure the networked systems.

Prevention Mechanisms Firewalls filtered traffic to manage and reduce undesired types of traffic flowing into and out of the networks. The configuration included a "stateless" firewall to perform basic filtering, followed by a "stateful" firewall to perform more intelligent filtering. A "stateless" firewall is a firewall that treats each

network frame (or packet) in isolation. It has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet. A "stateful" firewall is a firewall that keeps track of the state of network connections (such as TCP streams) traveling across it. The firewall is programmed to know what legitimate packets are for different types of connections. Only packets which match a preset or known connection state will be allowed by the firewall; others will be rejected.

Virtual Private Network (VPN) provided confidentiality and integrity assurance by encrypting traffic for transmission over a shared network [Kaufman, 2002].[47]

Vulnerability scanners were used to detect known potential weaknesses of a host configuration. These weaknesses were patched and/or locked down accordingly to 'harden' the host's security. Examples of such tools include NESSUS [Nessus, 2003][48] and Retina Network Security Scanner [eEye, 2003].[49]

Software patches guarded against attacks made against vulnerabilities caused by security software problems detected after distribution and deployment.

Detection Mechanisms

An **Intrusion Detection System (IDS)** was used to identify potential attacks based on anomaly detection and/or misuse detection. IDSs are signature-based and only detect known patterns of attacks. IDSs were network-based (monitors network traffic) and host-based (monitors logs). Examples include SNORT [Snort, 2003] and ISS Real Secure [ISS, 1998].

Integrity Detection: Integrity assurance tools, such as Tripwire [Tripwire, 2003], were used to fingerprint the installed system and to determine changes that occurred following a suspected attack. It monitored key attributes of files that should

[47] Charlie Kaufman, Radia Perlman, and Mike Speciner, "Network Security: Private Communication in a Public World," 2002.

[48] Nessus.org., "Nessus," http://www.nessus.org., 2 July 2003.

[49] eEye, "Retina Network Security Scanner,".http://www.eeye.com/html/Products/Retina/index.html, 2003.

not have changed, including binary signature, size, expected change of size, etc. It was also a useful tool as part of the configuration management suite.

3.3.1 Alternatives Generation – Force Group

The Force Group alternatives were developed and redefined using an iterative process, and considered both existing systems and suggested uses for emerging technologies. Current Special Operations operators at both the Center for Anti-Terrorism and Naval Security Forces and the Naval Special Warfare Center Advanced Training Department validated the Force System alternatives. The support given by the personnel in these commands was instrumental in making the alternatives viable and effective.[50, 51, 52]

3.3.2 Design Space – Force Group

The Design Space for Force System alternatives included existing and potential technologies that could be implemented to 90% operating capability within five years. This limited the Force Group to utilizing TRL 4 or better, which ensured that the technology was proven in a laboratory setting and could be tested in the field in the near future[53]. The Force Group evaluated existing systems on their potential applicability as alternatives for the problem, initially focusing research to gain insights into generic capabilities that could be fielded. Due to the availability of data on U.S. forces, research was refined to look primarily at U.S. military force capabilities, with a limited evaluation of foreign service capabilities. Through this process, the Force Group was able to determine the baseline capabilities available in the Straits of Malacca region, and to design several viable alternatives to increase the capabilities of deterring and defeating terrorist acts in the Pacific Command (PACOM) AOR.

---

[50] Interview with CDR Tom Shiblor, stakeholders' questionnaire, Naval Special Warfare Group One, San Diego, CA, (10 March 2005).

[51] Interview with EN1(SWCC) Rob McKay, stakeholders' questionnaire, Naval Special Warfare Center Advanced Training Department, San Diego, CA, (10 March 2005).

[52] Interview with ENC(SWCC/PJ) Hager, stakeholders' questionnaire, Center for Anti-Terrorism and Naval Security Forces, Camp Lejeune, NC, interviewed by phone, (10 March 2005).

[53] The Defense Acquisition Guidebook, Section 10.5.2: Technology Maturity and Technology Readiness Assessments, http://akss.dau.mil/dag/DoD5000.asp, (15 March 2005).

3.3.3 Alternatives Generation – Force Group

A morphological chart showing the range of material solutions that were generated and evaluated is shown in Figure 34.

Force Alternative Morph Chart

STAGE		DEPLOY		COMMIT		RECOVER	
PLAN	**EQUIP**	**EMBARK**	**TRANSPORT**	**ENGAGE**	**INSPECT**	**RECALL**	**REDIRECT**
Land base	On Site	Helicopter	Helicopter	Fire Team Escort	Inspection Team (Onboard)	Helicopter	Helicopter
Surface High Speed Vehicle	HSV	MK-5	MK-5	Fire Team & Hull Coating		MK-5	MK-5
Inspection Platform	Land Base	TDSI Transport	TDSI Transport	Assault Team		TDSI Transport	TDSI Transport
		Armed Tug Boat	Armed Tug Boat	OTH Missile		Armed Tug Boat	Armed Tug Boat
				TDSI Transport			

Figure 34. Force Alternative Morph Chart

The morphological chart captures all technology alternatives considered to perform the Force functions. Of these, only those regarded as clearly feasible were carried forward.

This chart was later refined into the working alternatives after feasibility screening. All alternatives were developed with consideration of the requirements, focusing on defense against the specific threats named in the scenarios. The Force System in theater at the time of this report was very limited. The Singapore Navy had recently implemented a Sea Marshal program that was focused on maintaining the security of Singapore's ports. The Sea Marshals were selected from the Singapore Navy and were trained in retaking a ship that had been commandeered by terrorists. They were transported with the harbor pilot to escort all incoming high value vessels. The teams consisted of an engineer, a seaman, and a communications manager. This team was moderately capable of

establishing control of a ship as it entered Singapore waters to prevent it from becoming a SAW vessel. These Sea Marshals were the only active forces in theater that were capable of defeating any of the threats described in the SEA-7 scenarios. The SBA scenario was largely overlooked, with the exception of random, uncoordinated patrols of the Straits of Malacca by Singaporean Navy, Indonesian Navy, and Malaysian Navy patrol craft.

Using the refined MOEs and MOPs for each scenario, the Force Group worked in conjunction with TDSI Weapons Track personnel to develop a patrol craft that would be capable of intercepting and defeating SBA vessels, as well as acting as a harbor patrol boat to defend against a SAW attack and a transportation vessel for the WMD inspection teams.

3.3.3.1 SBA Scenario

The first unique set of capabilities that the reaction forces needed to have was the ability to combat the SBA threat. The two most difficult components of this problem were assessed to be the determination of hostile intent and the minimum time available to defeat the attack. The determination of hostile intent was assumed to be externally satisfied prior to engagement, through a combination of anomaly-recognition C3I software, ROE, communications, warning shots, etc. Thus, the Force Group only considered what would be required to physically defeat an attack in progress. The time available to defeat an attack in progress was assumed to be four minutes—the time required for a 30-kt speedboat to cover two NM. This narrow response time constraint led to alternatives which would be able to either completely cover the entire critical area, or to point-defend high value units (HVU) as they transited the critical area.

The first alternative to counter the SBA threat was the TDSI-selected patrol craft. The exact type of ship, deployment strategy, and weapon type was evaluated by the TDSI Weapons Track. Other alternatives considered were the use of armed helicopters and ground-based weapon systems.

An active point-defense alternative to counter the SBA threat was Sea Marshals escort teams that would be air- or surface-deployable to High Value Units (HVU), similar to the current procedure for all U.S. HVUs transiting through high risk

areas. These escorts would board the HVU as it entered the critical area, and offload as the HVU departed the critical area.

Although it was not specifically evaluated in this study, one promising way to passively point-defend HVUs in this scenario would be to outfit ship hulls with an explosive resistant coating. Coatings of this type were commercially available from LineX Corporation, and had been proven to significantly reduce the blast from conventional explosives. The Air Force Research Laboratory had applied the Polyurea to structures with an 80mm-thick coating, and it withstood blasts of 1,000 pounds of TNT with only minor displacement and minimal fragmentation.[54] The U.S. Navy had applied this substance in place of nonskid surface on the decks of ships and the hulls of submarines. It was determined that it could significantly improve the safety of the hull of a commercial ship if applied, and would reduce the fragmentation results of an external explosion. This option was only briefly considered to show the improvement in safety that the ship owners could gain if they coated their vessels with the explosive resistant covering.

3.3.3.2 SAW Scenario

The second unique set of capabilities that the reaction forces needed to have was the ability to combat the SAW threat. This threat could be countered in one of two locations. The first, and preferred, location was out at sea, as soon as C2 System realized that the vessel was intended for the SAW mission. This option allowed time for an assault team to be fully briefed and prepared for retaking the ship from the terrorists. The second location was inside the port security area, as assumed in the SAW threat scenario, which was very vulnerable due to the severely limited reaction time and reaction capabilities. With the discovery of a SAW attack inside the port security area, there was little time to plan a retake of the vessel. Instead, the SAW vessel had to be redirected or disabled prior to it reaching its target.

[54] Knox, Hammons, Lewis, and Porter, "Polymer Materials for Structural Retrofit," http://www.line-xicd.com/bomb/AF_TEST.pdf, 15 March 2005, p. 6.

The baseline alternative was the existing "As-Is" System. This incorporated the use of Sea Marshals loaded onboard all HVUs entering port. These Sea Marshals would be transported out to the vessel prior to its port entry, and they would be in communication with the port control facilities at all times. This would allow some increase in the limited response time associated with the SAW threat being recognized within port boundaries.

Another alternative utilized the TDSI-selected vessel, which would patrol the harbor and would be called in to respond to the SAW attack either within the port, or in close vicinity to the port. The patrol craft would try to stop the SAW vessel either through disabling the steering mechanism of the vessel, or through disabling the vessel's propulsion equipment.

An additional alternative for the port security force was a land-based patrol that consisted of an assault team that could be lifted out to retake the merchant vessel via helicopter. This team would have capabilities similar to those of U.S. Navy SEALs, in that they could conduct a hostile environment boarding while the ship was at sea.

3.3.3.3 WMD Scenario

The third unique capability set that was developed was the ability to transport an inspection crew out to a vessel, at sea and underway, and conduct an inspection of the ship and its cargo. The Sea Inspection Group developed the inspection equipment, and the Force Group was responsible for the transportation and operation of the equipment, as well as the safety of the operators while they conducted the inspection. This was a similar capability to the U.S. Navy's Maritime Interdiction Operations (MIO) teams. The MIO teams were sailors pulled from the general ship's crew and who received additional training to be able to safely board ships at sea, in order to conduct inspections of the ship and its cargo. These were traditionally 12-man teams, with ten inspectors and two personnel managers, and included adequate self-defense capabilities.

The first transportation alternative for the WMD scenario used a helicopter to carry the baseline 12-man team from a base in Singapore to the COI. Following their inspection, the boarding team would either ride the ship into port or depart the COI by air or by sea. The number of inspection teams that would be required for the active area was determined through analysis by the Sea Inspection Group.

The second transportation alternative for the WMD scenario used the TDSI-selected patrol craft to transport the inspection teams. The patrol craft was launched from a forward base located closer to the shipping lanes, such as one of the many islands to the northeast of Singapore or George Town on the northern approach to the Straits. This offshore option had the additional security of an armed escort for the inspection team while they were conducting the onboard inspection, although the forward bases would incur additional costs.

3.3.4 Feasibility Screening – Force Group

After the alternative concepts were generated, the Force Group focused on Feasibility Screening, and the QFD. Much of the Feasibility Screening was completed during the alternatives generation phase, but the alternatives were further refined to reflect feasibility drivers. The feasibility factors that were evaluated were the physical, economic, environmental, technological, and social constraints of operating in the Straits of Malacca AOR. One of the major factors was the physical restrictions of operation in the Straits of Malacca AOR such as the shallow water and narrow channels, the numerous coves and hiding areas in the Straits, and the abundance of traffic that was required to be filtered to find a SBA vessel. A preliminary economic evaluation revealed that helicopters would be too expensive as an alternative in the SBA scenario, since they would need to be airborne 24/7 to meet the short time-to-respond constraint. Additionally, ground-based weapons systems were assessed to be too expensive, since the number of independent systems required to completely cover the critical area was very large, and each system would need to be maintained and guarded.

One of the major environmental conditions was the restriction of the operating environment with the high humidity and high heat that restricted the amount of time that

the inspectors were able to function at their positions onboard the WMD COIs. Another major feasibility filter for the Force Group was the technology restriction. The requirement that was adopted for the project was that any technology used would be demonstrable at the time of the project, and could therefore be implemented within a five-year stand-up period. The only technology that fell outside of these criteria was the TDSI-selected patrol craft, the Sparviero hydrofoil, which was developed to integrate the TDSI Weapons track personnel into the project. The technology that was used in the development of the Sparviero was all subject to the same five-year implementation criteria; however, the entire system was not in existence at the time of this study, and therefore fell outside of the imposed feasibility criteria. A major social filter was the amount of innocent shipping that was delayed or destroyed as a result of false alarms in the SBA, SAW, and the WMD threat scenarios. There was a high level of importance placed on correctly identifying an attack, and limiting the damage to the surrounding vessels caused by the defense of a HVU.

3.3.5 Quality Functional Deployment – Force Group

Since the initial requirements that were developed through the Needs Analysis phase were the basis for the alternative concept generation, all of the nonspecific alternatives that had passed the feasibility screening satisfied at least some of the requirements. The QFD process ensured that all alternatives were defined in enough detail to ensure that requirements were met. The alternatives were refined and scrutinized for applicability to the scenarios, and detailed features were added. The QFD for the Force System alternatives were broken down by scenario, and are shown in Figures 35, 36, and 37.

HOUSE OF QUALITY
SBA SCENARIO

	TDSI Sparviero Ship	HSV-X1 Joint Venture Ship	11m Rigid Hull Inflatable Boat	SH-60B Helicopter	Mk-5 Boat	17 5-man Teams
Keep Small Boat Attack (SBA) >35m from HVU	X	X				X
Defeat 90% of SBAs	X	X				X
Maintain response capability up to Sea State 4	X		X		X	X
Implemented within 5 years						

Figure 35. Force QFD for SBA Scenario

This QFD shows the various material solutions considered for countering the SBA threat.

HOUSE OF QUALITY
SAW SCENARIO

SYSTEM REQUIREMENTS ⇨ **CUSTOMER REQUIREMENTS** ⇩	MDP-TDSI Sparviero Ship	11 m RHIB	Militarized Tug Boats	SH-60B Helicopter	03 (12 Men) Teams	16 (03 Men) Teams
keep SAW > 1,000 m from pier	x		x			x
engage & defeat 90% of SAW threats	x					
engage SAW by 2,000 m from pier	x		x	x	x	x
maintain responsive cap. 24/7	x	x	x	x	x	x
Implemented within five years	x	x	x	x	x	x

Figure 36. Force QFD for SAW Scenario

This chart shows the various material solutions considered for countering the SAW threat.

HOUSE OF QUALITY
WMD SCENARIO

SYSTEM REQUIREMENTS ⇨ / CUSTOMER REQUIREMENTS ⇩	MDP-TDSI Sparviero Ship	09 (12 Men) Teams	HSV-X1 Joint Venture Ship	11 m RHIB	SH-60B Helicopter	03 (12 Men) Teams
keep WMD > 20 nm from AOR	x	x	x	x	x	x
neutralize 99.9 % of threat	x	x			x	x
transport & utilize inspection gear	x	x	x	x	x	x
engage WMD carrying ship up to 200 nm	x	x			x	x
maintain responsive cap. 24/7	x	x				
Implemented within five years	x	x	x	x	x	x

Figure 37. Force QFD for WMD Scenario

This chart shows the various material solutions considered for countering the SAW threat.

3.3.6 SBA Scenario

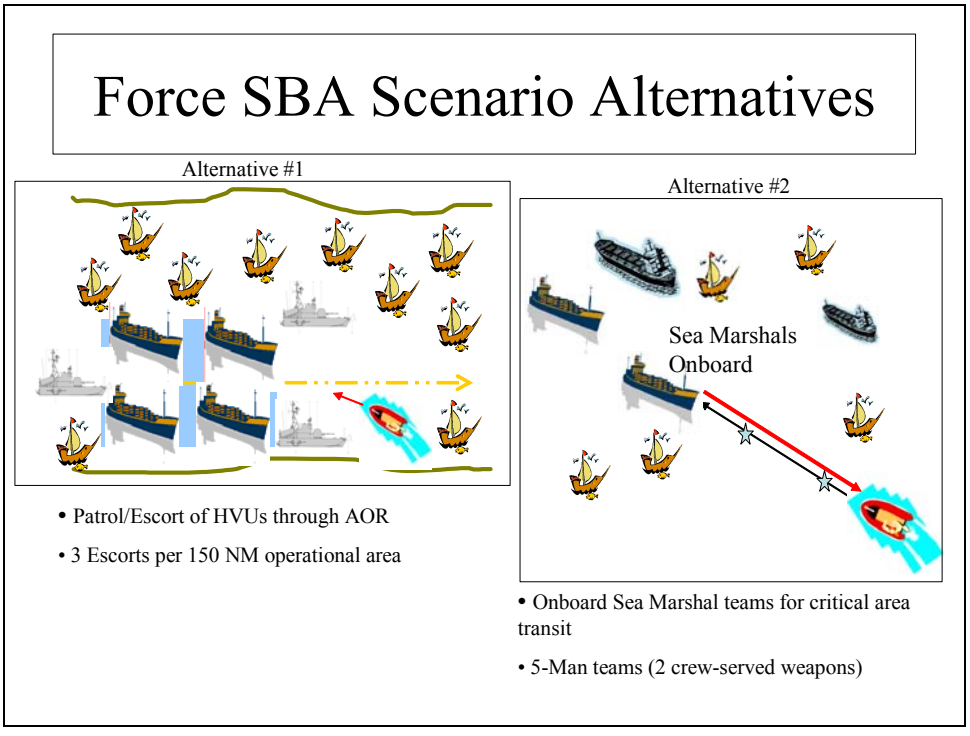

Figure 38. Force Group Alternatives for SBA Scenario

The Force Group developed two alternative solutions to counter the SBA threat. There was no "As-Is" System to defend against a SBA.

3.3.6.1 SBA 2005 "As-Is" System – Force Group

The baseline capabilities that were in place in the spring of 2005 were severely limited. The existing systems did not include any plan for persistent presence in the Straits of Malacca to counter terrorism; instead, it relied on intermittent patrolling of uncoordinated local military forces. Thus, it was assumed that there was no "As-Is" System to defeat the SBA threat.

3.3.6.2 SBA Alternative 1 – Force Group

Alternative 1 for the SBA scenario incorporated the TDSI-selected vessel on patrol in the critical area. The majority of the benefit in the SBA scenario would come in the form of active deterrence. The belief was that not only could the TDSI transport intercept SBA threats, if in range, but would show a friendly force presence within the critical area to deter possible threats, although no attempt was made to model or characterize this deterrence.

The patrol craft option was determined through interviews with both the Officer-in-Charge (OIC) for the U.S. Navy SEAL Detachment from Naval Special Warfare Group One, and the Center for Anti-Terrorism and Naval Security Forces, Learning Site Camp Lejeune staff personnel.[55] After evaluating and analyzing several patrol craft options, the TDSI Weapons Track team selected the Italian Sparviero hydrofoil as the desired patrol vessel.

In order to enable the Sparviero to be used as an alternative, the Force Group included a High Speed Vessel (HSV) as a floating logistics and support staging base to counter SBAs in the Straits of Malacca. The HSV would operate with the Sparviero patrol craft in a combination of patrolling and HVU convoy escort missions. The TDSI Weapons Track team determined that the best arrangement would be to split the AOR into two unique operating areas and have each area independently patrolled by the small boats in an effort to deter small boat attacks, and to react in the event of an attack. Personnel from the Naval Special Warfare Center Advanced Training

[55] Interview with CDR Tom Shiblor, stakeholders' questionnaire, Naval Special Warfare Group One, San Diego, CA, (10 March 2005).

Department[56] and the Center for Anti-Terrorism and Naval Security Forces[57] were instrumental in formulating the escort and patrolling patterns that would best cover the AOR. The counter-clockwise rotational patrol optimized the reaction times by ensuring uniform coverage within the AOR, while still showing force throughout the Straits. This option employed technology that was available, and could be produced and implemented within five years. This alternative also represented an increased capability with extended ranges and extended engagement thresholds that could be developed and implemented in the future. Although currently unrealistic, analysis was done to evaluate the use of over-the-horizon (OTH) missile systems to reduce the number of ships required to patrol the AOR.

3.3.6.3 SBA Alternative 2 – Force Group

Alternative 2 for the SBA scenario incorporated five-man Sea Marshal teams that would be transported out to each HVU transiting the Straits of Malacca. The SBA Sea Marshal team would be armed with two .50-caliber machine guns, one on the bow and one on the stern, and a control/communication station on the bridge. This allowed for maximum weapons coverage around the HVU. The Sea Marshal team would have Rules of Engagement (ROEs) to dictate their actions, and would be capable of operating independent of the onshore C2 Centers, relying heavily on visual observations and shipboard radar systems to identify threats. Analysis of required engagement ranges, operator training, and weapon accuracy revealed that the SBA would need to be engaged by 150m if the single-shot probability of kill was 50%. These escorts would board the HVU as it entered the critical area, and offload as the HVU departed the critical area. If the HVU's destination was within the critical area, the Sea Marshal escorts would remain onboard until the ship was pierside.

---

[56] Interview with EN1 (SWCC) Rob McKay, stakeholders' questionnaire, Naval Special Warfare Center Advanced Training Department, San Diego, CA, (10 March 2005).

[57] Interview with ENC (SWCC/PJ) Michael Hager, stakeholders' questionnaire, Center for Anti-Terrorism and Naval Security Forces, Camp Lejeune, NC, interviewed by phone, (10 March 2005).

3.3.7 SAW Scenario

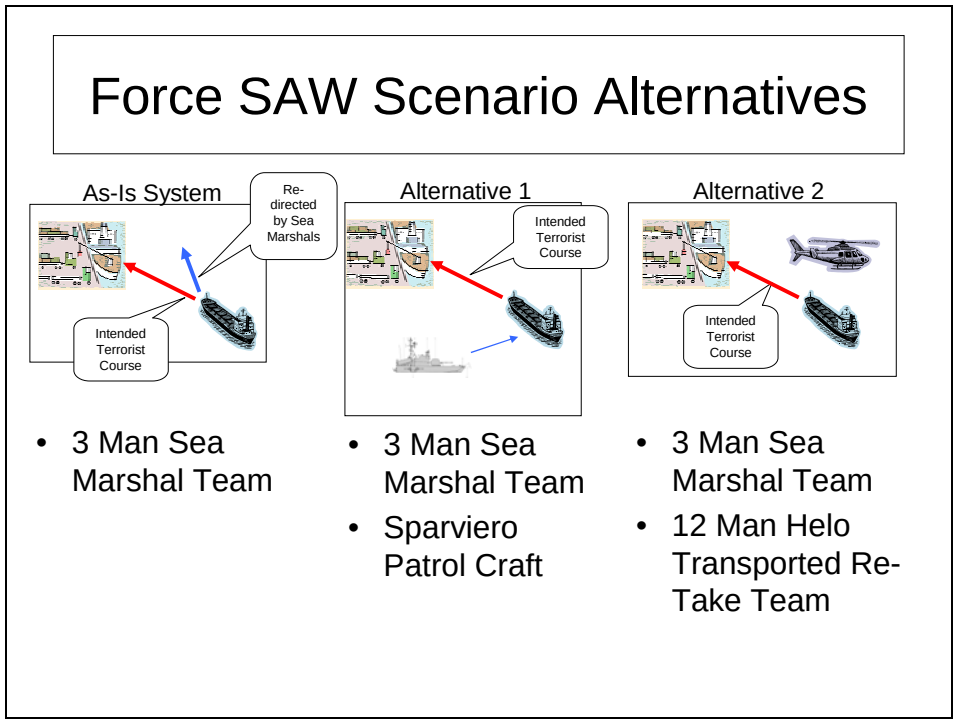

Figure 39. Force Group Alternatives for SAW Scenario

The Force Group developed two alternative solutions to counter the SAW threat. Both of these alternatives built on the "As-Is" System, which loaded Sea Marshals on high value ships five NM from the destination port.

3.3.7.1 SAW 2005 "As-Is" System – Force Group

The "As-Is" Force System alternative to counter the SAW attack incorporated the use of three Sea Marshals loaded onboard all HVUs entering Singapore. The Sea Marshal team was comprised of an engineer, a seaman, and a communicator, all Singapore Navy sailors bearing small arms and trained to retake a ship that was under the control of terrorists. A total of 16 Sea Marshal teams were required, assuming each team could make an average of three trips to the approximately 50 HVUs that entered Singapore each day. These Sea Marshals would be transported out to the vessel five NM prior to its port entry, along with the harbor pilot, and they would be in communication with the port control facilities at all times while onboard the merchant vessel. This procedure increased the time available to respond (minimum 15 minutes at 20 kts) as opposed to the SAW threat being recognized within port boundaries. The Sea Marshals

would be a valuable intelligence asset onboard the vessel as it entered the port, and they would be able to act as a first responder, defeating or at least mitigating any problems while any additional actions were taken to defeat the SAW. Although the capabilities of this team were procedurally limited due to the number of team members and the range at which they were embarked, they were assessed to be effective.

3.3.7.2 SAW Alternative 1 – Force Group

Alternative 1 for the SAW scenario used the Sparviero hydrofoil as a harbor patrol vessel, in addition to the current Sea Marshals. The Sea Marshals defensive capabilities would be improved through the use of disabling fire from the TDSI vessel, which would require a high degree of C2 coordination, with the Sea Marshals playing a key role in the designation of the vessel as a SAW ship. For this alternative, each of four Sparviero patrol craft were crewed by the normal 11-man crew and armed with the 76mm deck gun as well as .50-caliber machine guns. At all times, two hydrofoils would patrol the harbor and would be called in to respond to the SAW attack either within the port boundaries, or in close vicinity to the port. The crew would attempt to stop the SAW vessel either through disabling the steering mechanism of the vessel, or through disabling the steering or propulsion equipment with the 76mm and .50-caliber machine gun. Although this alternative was not effective when used alone, it was effective in conjunction with the onboard Sea Marshals.

3.3.7.3 SAW Alternative 2 – Force Group

Alternative 2 for the SAW scenario consisted of a land-based rapid response force team that could be airlifted out to retake the merchant vessel via helicopter, in addition to, and in support of, the existing three-man Sea Marshal team escorting each HVU into Singapore. This team would have capabilities similar to U.S. Navy SEALs, in that they could conduct a hostile environment boarding while the ship was at sea. A minimum of three teams and three SH-60B helicopters were required to meet the 24/7 requirement. Because of the time required to cold-start a helicopter and brief the special operations team, it was infeasible to expect that the reaction force would be effective if the SAW attack was not detected until the ship entered the port area.

Analysis revealed that this option essentially could only defeat a SAW attack that was detected at sea, unless the Sea Marshals onboard that could retake or redirect the SAW vessel. The in-port SAW attack detection used in the SAW scenario left the operators with very little time to adequately plan and respond to the SAW attack.

3.3.8 Weapons of Mass Destruction (WMD) Scenario

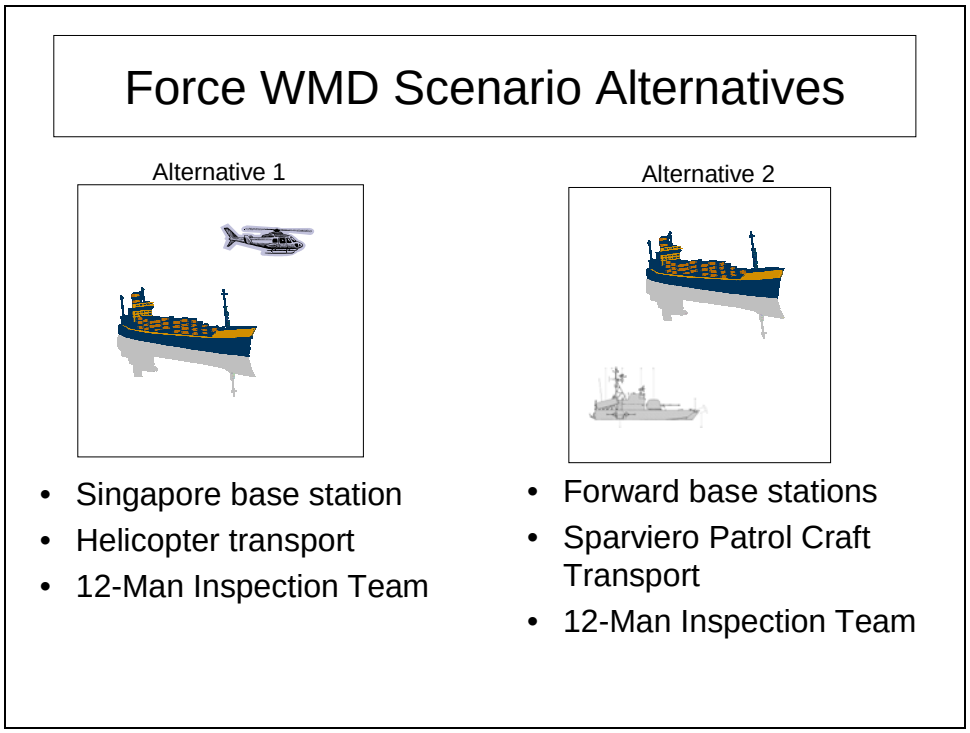

Figure 40. Force Group Alternatives for WMD Scenario

The Force Group developed two alternative solutions to transport the Sea Inspection team to COIs for the WMD threat. There was no "As-Is" Transportation System since there was no "As-Is" Sea Inspection System.

3.3.8.1 WMD 2005 "As-Is" System – Force Group

The "As-Is" Force Group transportation capability for the Sea Inspection System in the WMD scenario was nonexistent, due to the fact that an At-Sea Enroute Inspection System was not in use.

3.3.8.2 WMD Alternative 1 – Force Group

Alternative 1 for the WMD scenario transported the Sea Inspection team via SH-60B helicopter from a base in Singapore to the COI. Four Singaporean SH-60Bs were assumed to be able to carry the 12-man inspection team and their inspection equipment to a boarding point at least 250 NM from the Straits of Malacca. The choice of using a helicopter to transport the inspection team out to the vessel was made because of their current existence and the ease of implementation. Most COIs that entered the Straits of Malacca would be large merchant vessels that could easily and safely be boarded by helicopter teams. The other positive aspect of this alternative was that the inspection teams could be based at a single force concentration site, such as Singapore, and could be quickly transported out to the threat vessel at 250 NM in 1½ hours using a 167-kt cruise speed. Following their inspection, the boarding team would either ride the ship into port or depart the COI by air or by sea. The number of inspection teams that would be required for the active area was determined through analysis by the Sea Inspection Group.

3.3.8.3 WMD Alternative 2 – Force Group

Alternative 2 for the WMD scenario transported the 12-man Sea Inspection team via the Sparviero vessel to the COI. In order to achieve a 1½-hour transit time to the COI, this alternative required that the inspection teams be located at forward staging areas close to the major shipping lanes where the planned intercept would take place. This would be done by constructing bases on several of the surrounding islands in the Pualu Natuna area to the northeast of Singapore, and the George Town, Malaysia area to the northwest of the Straits of Malacca. Outlying bases would allow adequate time for the inspection team to equip and intercept the suspect vessel using one of six TDSI transport vessels as primary transportation, and to reduce delay costs by inspecting the vessel while it was in transit. This offshore option was able to be quickly implemented, and would have the additional security of an armed escort for the inspection team while they were conducting the onboard inspection, although the forward bases would incur additional costs.

3.4.1 Alternatives Generation – Land Inspection Group

The Land System Group alternatives were developed through a number of iterations integrating current shipping procedures, port operations, security measures, and technologies, both current and evolving. The final alternatives were refined through a combination of proven procedures with the means to inspect more containers without impeding the flow of commerce. Research and insight from the Port of Oakland, Lawrence Livermore National Laboratory, and U.S. Customs and Border Protection were key in finalizing our alternatives. With the large amount of variables that affect sensor performance, those sensors chosen for the alternatives may not give the best performance against specific threats in every scenario. However, they were used for consistency throughout the study for analysis and comparison of the alternatives.

3.4.2 Design Space – Land Inspection Group

The driving factor for inspecting cargo was the volume of containers that ports had to process. There were a considerable number of factors that contributed to a port's ability to process cargo, including overall facilities, local regulations and trade laws, amount of cargo, and security plans.

To best determine alternatives, the problem was bounded to evaluate current operations and handling infrastructure. This restricted the Design Space to comparing the best ways to implement inspection capabilities and techniques without introducing new techniques for processing cargo, such as conveyors or railroads. Most ports would not be able to support complete reconstruction since it would hamper operations, especially if it were to be done in a timely manner to support near future implementation.

3.4.3 Alternatives Generation

With the amount of cargo that was processed daily, attempting to thoroughly inspect everything processed would lead to a substantial increase in delay time, manning, required training, and total cost. Advancements in detection technologies, coupled with efficient procedures, could minimize these effects, while increasing the detection probabilities of hazardous materials and unauthorized personnel. A number of

technologies existed to detect hazardous WMD materials. The specific threat, amount, atmosphere conditions, and dispersion methods all affected the severity and impact of a successful attack. In generation of alternatives, an assessment of current or developing technologies was necessary to determine what was available to address the threats.

The morphological charts in Figure 41 summarize the variety of material and nonmaterial solutions considered and assessed.

ACCOUNTABILITY		DETECT			
CONTAINER HISTORY	VERIFICATION METHOD	NUCLEAR/ RADIATION	CHEM/BIO	EXPLOSIVES	FOREIGN OBJECTS
Origin	Human Intelligence	Gamma Ray Imager	Optical	Flash Chromotography	X-Ray Machine
Route	Surveillance System	High Purity Germanium	Arrays	Vapor Detector	Density Imager/sensor
Destination	Smart Container	Scintillaiton Counter	Flame Emission Photometry	Molecule Locator	Shape recognition
Contents	Canine	Neutron Generator	Photo Ionization	X-Ray	Anomoly recognition
Manifest	Manifest Comparison	Laser Infrared Flourescence	Infrared Spectrometry	Neutron Activation	Visual
Shipping Company	Robotic / Mobile Inspection	Semiconductor Detectors	Chemical Sensitive Electronics	Canine	Acoustic
	Human Inspection	Thermo Luminescence	Surface Acoustic Wave		
	Tamper Seals	LIDAR	Ion Mobility Spectrometry		
	Attached Sensors		Flow Cytometry		
	Unmanned Vehicles				
	Check points with sensors				
	Density Screening Unit				
	Wideband Radar				
	Divers				

LOCATE		COMMUNICATE	
AUTOMATED	INTERPRETATION	RECEIVE/ TRANSMIT	RECORD/ DISPLAY
Sensor Mapping	Human Search	Infrared	Computer Database
Data Analysis	Imaging Display	Radio (UHF, Walkie Talkie)	Voice / Video Recorder
Smart Containers	Animal Indication	Encoded Laser	Monitors
	Sickness Locality	Cable / Fiber	Audio / Visual Alarms
	Intelligence	Satellite Communications	
	Self-Report	Cell Phones	
		Internet	
		Verbal / Visual	

Figure 41. Land Inspection System Morphological Chart

This chart depicts the variety of material and nonmaterial solutions considered and assessed.

3.4.4 Feasibility Screening – Land Inspection Group

With a number of competing developing and proven technologies, the integration of procedures, accountability techniques, and use of sensors gave a wide selection of choices at first glance. To assist with the development of alternatives, there were characteristics that select components of the system had to possess.

The sensor packages had to contain some mobile sensors and some stationary sensors. There needed to be a means to recharge or power them without interrupting operations. With the standardization of containers, and without the option to open and inspect every one, the system needed to detect threats through the side of the container. The objective to prevent attacks dictated that sensors needed the capability to detect the presence of chemical, biological, and explosive threats without the agent being released into the air, if possible.

Tamper proofing, tracking, and securing of containers needed to cover the entire supply chain. The vulnerability of the containers is greatly due to the potential number of people and commercial industries that are responsible for the shipment from point of packing to final destination. The worldwide nature of the industry also meant the devices used to address the security of containers during transit needed to be affordable, maintainable, and usable by the majority of players.

Finally, the communications had to cover both port operations and support external decision makers. This called for secure, reliable, and real time information sharing as well as the ability to store large amounts of information for future use.

3.4.5 QFD – Land Inspection Group

	SYSTEM DESIGN COMPONENETS										
LAND SYSTEM QUALITY FUNCTIONAL DEPLOYMENT (QFD) REQUIREMENTS	Gamma Sensor	Neutron Sensor	Chem / Bio Sensor	Radiation Pagers	High-Purity Germanium Sensor	Container Security Devices	Training Program	In-Port Communications Network	Data Fusion and Analysis Center	Alert / Inspection Team	Trade Security Certification
Search Containers	X	X	X				X			X	
Detect Radiation				X	X		X		X	X	
Detect Bio/Chem			X				X		X	X	
Detect Explosives						X	X		X	X	
Detect Foreign Objects	X	X					X		X	X	
Provide Location Information	X	X	X	X	X		X		X	X	
Provide Human Interface	X	X	X	X	X	X	X		X		
Identify Material	X	X	X	X	X		X		X	X	
Communications	X	X	X	X	X	X	X	X	X	X	X
Container Accountability						X	X		X		X
Sensor Output Analysis							X	X	X	X	
Suspect Container Interrogation	X	X	X	X	X	X	X	X	X	X	X

Table 16. Land Inspection System QFD

QFD shows whether stakeholder requirements are met by system design components or not.

3.4.6 2005 "As-Is" System – Land Inspection Group

The existing inspection system in Singapore to prevent smuggling of WMDs and hazardous materials improved with the implementation of new security measures and initiatives. Singapore's participation in the current initiatives are detailed in Annex D. For physical security, Singapore had a process for their imports that were unloaded and headed into their country, and a different regime for transshipment cargo that was expected to be loaded on another ship. There were six Free Trade Zones in Singapore that allowed for goods to be exchanged among countries without customs being involved. It was unknown what, if any, inspection process existed for that cargo. For cargo that eventually ended up in Singapore, customs officials removed and inspected the cargo as

they deemed necessary (approximately 1.4%) and would repack the containers. Permits were required for processing though they might not accompany the cargo.

For transshipments or exports headed for the United States, U.S. Customs targeted roughly 4%-6% of the cargo. They used canines and x-ray, gamma ray, and radiation detectors to inspect the cargo. Though there were over 20 countries participating in the Container Security Initiative (CSI), the Land Inspection Group could not find which countries, if any, other than the U.S. had inspectors in foreign ports.

For the purpose of this study, it was assumed that shipments to Singapore that originated in the U.S. or in any other CSI country would be inspected in accordance with the existing U.S. inspection protocol. This allowed for analysis of the existing land inspection infrastructure that the U.S. used, both in the continental U.S. (CONUS) and abroad, and which could relatively easily be applied to cargo bound for another partner country

3.4.6.1 Alternative 1 – Land Inspection Group

The burden of cargo inspection carried a large cost; not only to inspecting countries, but also to the shipping industry. The time required to actively and manually inspect cargo made it impossible to inspect every container, especially in a major hub like Singapore. The first alternative took advantage of passive detection capabilities coupled with the normal process of shipping containers as seen in Figure 42.

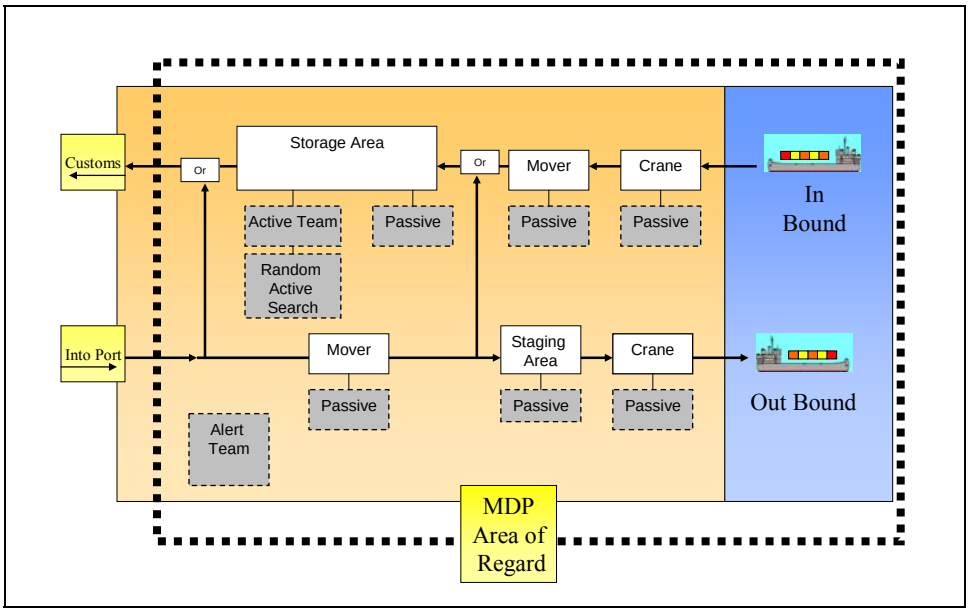

Figure 42. Land Inspection System Alternative 1 – Port-Centric Inspection System

Port centric alternative focuses heavily on a sensors network inside a port. It depends mostly on passive sensors. There are active alert teams for further investigation in case of positive alarms.

The Port-Centric alternative used the same active sensors for imaging and radiation detectors for randomly inspecting 5% of the cargo. There were also passive sensors on the pier cranes and transport vessels that moved containers throughout the port. Since containers were all loaded and unloaded using the same equipment, this allowed passive sensors to be in close proximity to containers in case something detectable was present.

The attachment of the sensors to the equipment would also allow for flexibility if threats changed or new technologies proved to better address specific threats. The ideal architecture would have sensors to address every type of threat. Due to the limited capabilities to detect chemical, biological, and explosives before they were released to the atmosphere, few effective sensor options existed.

The active teams inspected the cargo that was sitting in storage waiting for shipments to other destinations. This took advantage of dead time for staged containers. If a passive sensor alerted port operators, an active response team would report and investigate further with more accurate means. The land inspection allowed for containers

to be removed from the shipping process for further analysis without delaying an entire ship of containers. It was vital to detect materials before containers were loaded for sea. Having the ability to search containers one at a time would always have less commercial impact than searching at sea.

There was no targeting means employed in this alternative other than a passive system alarm. One hundred percent of containers were searched passively and 5% were randomly searched with an active inspection team. Any type of intelligence would assist in the active inspection selection process, but without the intelligence all containers were considered potentially hazardous.

3.4.6.2 Alternative 2 – Land Inspection Group

Alternative 2 expanded on Alternative 1, shifting more of the accountability of container security to the manufacturers, importers, carriers, brokers, and other employees throughout the supply chain. The "trusted agent" classification would be obtained in the same manner as the current Customs-Trade Partnership Against Terrorism (C-TPAT). The "trusted agent" certified shipper of goods must adhere to guidelines concerning procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance procedures.[58] Cargo containers arrived at the port and were accessed based on whether or not they were from a certified shipper. There were then three inspection triggers warranting an active inspection.

As containers were stuffed at the warehouse, mechanical tamper seals were fastened, and the containers verified and sealed, which is the first trigger. Upon arrival to the terminal, if the lock was damaged, missing, or suspect, an inspection team would thoroughly inspect the container until cleared for shipment.

[58] U.S. Customs and Border Protection, "C-TPAT Fact Sheet and Frequently Asked Questions," http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/fact_sheet.xml, (accessed 20 May 2005).

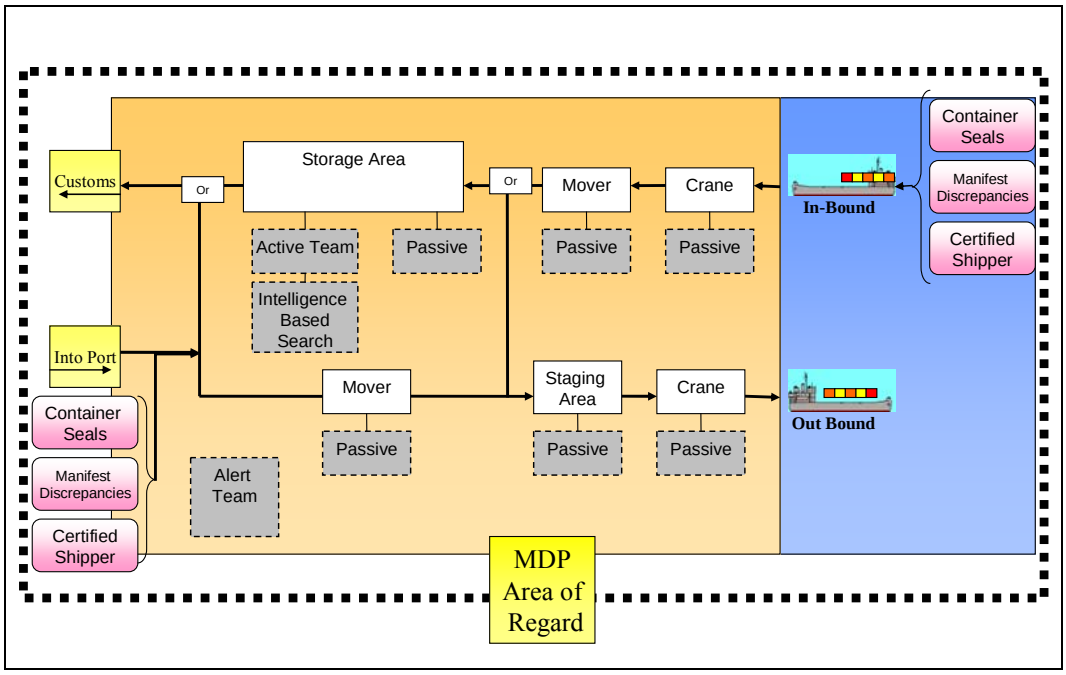

Figure 43. Land Inspection System Alternative 2 - Trusted Agent Inspection System

The Trusted Agent architecture reduces the number of possible suspect containers before they enter the port by depending on the C-TPAT security certification. This allows the system to identify suspect containers using a targeting process.

A second trigger to determine which containers to inspect would be the Automated Targeting System (ATS). ATS was a proven technology of information sharing that looked at a number of administrative, procedural, and anomaly recognition factors that might lead to containers being marked as suspect. There was always a heavy reliance on the quality of information that this system provided, but strict adherence to procedures and attention to trends could help focus inspection efforts.

A third inspection trigger was related to manifests. Though manifests were not always accurate, procedures and techniques have been developed, but are not yet in place, to screen information provided by them to better select and prioritize inspection-worthy containers[59]. Examples of additional data the maritime industry requires to make manifest data more relevant are:

[59] Coalition for Secure Ports. "Improving Port Security," http://www.secureports.org/improving_security/factsheet_screening.html, (accessed 15 May 2005).

- More specific and precise cargo descriptions.
- Name of party that is selling the goods to the importer.
- Name of party that is purchasing the goods.
- Point of origin of the goods.
- Country from which goods are exported.
- Ultimate consignee (final recipient).
- Exporter representative.
- Name of broker.
- Origin of container shipment.
- Name and address of business where container was stuffed.

In addition to the three triggers that warranted an inspection, a small percentage would also be inspected randomly. This would attempt to address the threats that had been loaded into containers that did not trigger an inspection by the three security measures in place.

The passive network of sensors would exist as in the Port-Centric alternative. The inspection teams would have the burden of responding to triggered inspections, random inspections, and investigating alerts by passive sensors. The more sensors in the process, the more false alarms were expected, which could slow inspection procedures and later impact commerce. It was impossible to predict specific detection capabilities of sensors without knowing what the threat of interest was, the environment the sensor would be working in, how much material was present, the type of storage container, and if there was shielding used. The nature of container shipping and procedures practiced by all major ports, as well as the operational concept, allowed assumptions to be made to address many of these variables.

3.5.1 Alternatives Generation – Sea Inspection Group

The Sea Inspection Group alternatives were developed by brainstorming and researching available technologies to generate ideas. The brainstorming sessions were used to generate very basic methods for the sea inspection problem as well as generating outside of the box ideas. The goal was to develop system alternatives using both existing technology and technologies that would be available within five years to ensure that the objectives generated during the needs analysis phase would be met. The Sea Inspection Group also made several trips up to Lawrence Livermore Labs in Pleasanton, California, to view actual systems that might be used in the alternatives generated.

3.5.2 Design Space – Sea Inspection Group

The design space given to the Sea Inspection Group was open to incorporating all existing and potential technology that could be implemented within the next five years. This criterion made some of the options infeasible. For example, the initial idea for searching containers was with the use of robot-mounted sensors. Although robotic technology has made significant progress, limits in battery capacity, mobility, and payload capacity (sensor weight) made these types of system alternatives prohibitive. As part of the Sea Inspection Group's visit to Lawrence Livermore Laboratories, the group was shown several sensor technologies that could be used in the alternatives. Other alternatives, such as neutron interrogation for radioactive sources, were found infeasible due to concerns regarding how they would work in a maritime environment. Through this process, two alternatives remained that were capable of being implemented in the next five years.

3.5.3 Alternatives Generation – Sea Inspection Group

The Sea Inspection Group used two processes to develop alternatives: Brainstorming and the Morphological Box. The brainstorming sessions took place over the span of two class weeks. The group started with a discussion of the group's objectives, restrictions, and limitations. Also discussed, was the aspect of ensuring that the inspection devices could be used for searching the ship internally, externally,

cargo-holds and the inside of containers. Most importantly, the group discussed the idea that all alternatives had to be feasible within the next five years.

After agreeing to these initial guidelines, the group separated to independently brainstorm and research viable technologies. Sources for these technologies can be found in the Modeling and Analysis and Cost Modeling sections of this paper. During the sessions that followed, each member discussed their self-generated list and the technologies behind each alternative. The alternatives were then combined into a master list from which the group pulled alternatives for each objective of the system. Some discussions concerning each alternative included feasibility and limitations of the ideas and served to remove some of the alternatives from the final list.

The group evolved the master list into a morphological chart that mapped each idea into its appropriate functional column. The functional columns come directly from the objective hierarchy. The goal of the morphological chart is to ensure that each function has options from which to choose for idea selection during alternative generation. Some of the ideas fit into several columns and some of the ideas from the master list did not fit into any of the columns because they did not meet the group's objectives or the system's functions.

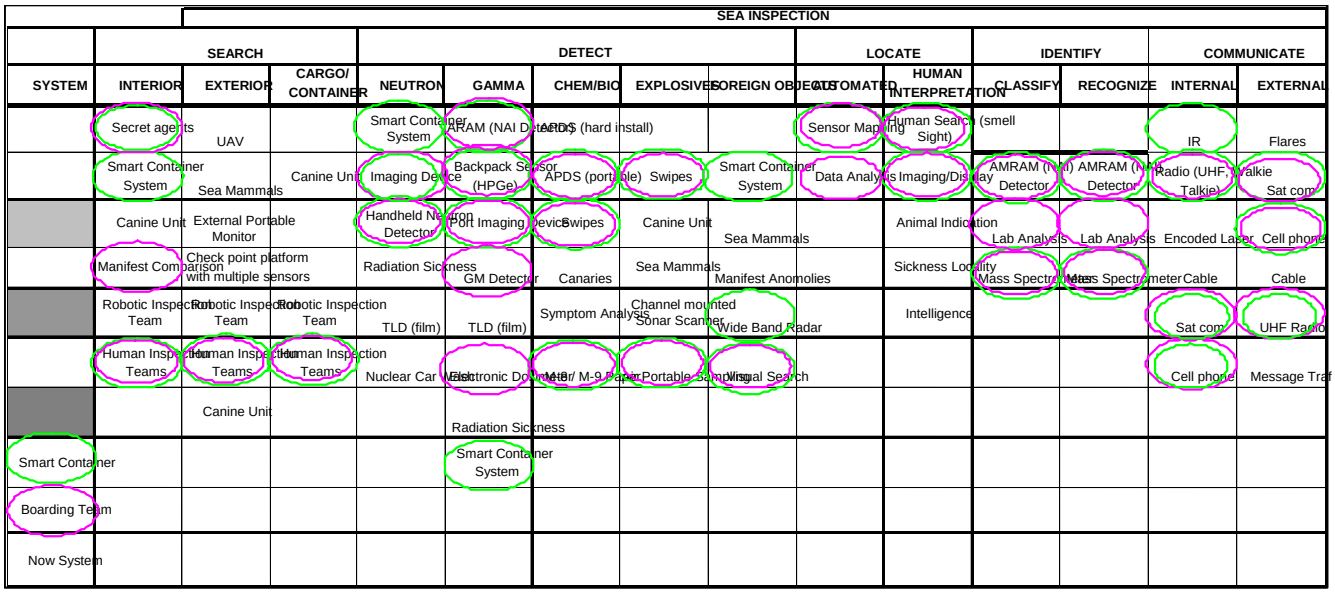

Figure 44. Sea Inspection Morphological Chart for Alternatives.

This morphological chart was generated for use in idea generation. The five functions are listed at the top of the chart and then the sub-functions are listed below. During alternatives generation, the group brainstormed and filled in the chart with options for different systems. Initial options came from individual research, briefings from national laboratories, web searches or individual imaginations. From there, two alternatives were generated and the options that correspond to that alternative are shown by the different colored circles. Green circles indicate the Boarding Team Alternative and pink circles represent the Honor System Alternative.

At this point, the group divided the alternatives into two different systems: The Boarding Team Inspection System and the Honor Inspection System.

Alternative 1: The Boarding Team Inspection System was defined as the use of human inspection teams to board and search suspect vessels for contraband material. This was to include cargo-holds and containers as well as the inspection of shipping documents.

Alternative 2: The Honor Inspection System was defined as the use of Smart-container devices installed on each container and in cargo-holds of ships. The sensor mapping capabilities inherent to some of these devices allows location of the suspect containers or cargo. Also, program requirements or standards would be established for the shipping companies to meet in order to bypass a boarding team inspection. A human boarding team is also used to search vessels that do not meet the

Honor Inspection System requirements or have Smart container devices alarming for reasons that cannot be mitigated.

The two systems contain similar aspects (e.g., the boarding team), but the Smart container devices were an added layer of protection and localization to be used by the human boarding team. The separation of the two systems was used to allow the high cost of the Smart container devices to be discarded if modeling and analysis showed they were not cost effective.

3.5.4 Feasibility Screening – Sea Inspection Group

Using the system requirements, the Sea Inspection Group produced a feasibility matrix (Figure 45) to assess the ability of the alternatives to produce the desired results. These requirements are discussed in the needs analysis section of this paper. The "current" system produced none of the desired results, as there was no current system. The Boarding Team Inspection System and the Honor Inspection System gave the group the ability to detect hazardous materials with current technologies (or in the next five years) in a maritime environment. The group assumed a 25-kg, weapons-grade, Uranium-235 source with one-quarter inch of Pb shielding as criteria for the detection of radioactive materials. This source assumption was used because it is large enough to be used in the production of the 20-KT nuclear device as given in the WMD scenario.[60] The one-quarter inch of Pb shielding was used because it was assumed that some amount of shielding would be used by terrorist agents to try to hide the nuclear device without large cost factors or issues due to the weight of the device.

[60] Federation of American Scientists, *Weapons of Mass Destruction*, "Nuclear Weapons Design," http://www.fas.org/nuke/intro/nuke/design.htm, (accessed 24 February 2005).

SYSTEM ALTERNATIVES						
Alternative	Technology 5 yrs	Keep Ship > 5 NMI	Operational in Maritime Environment	Power Reqmt	Detect Hazardous Materials	OVERALL
CURRENT	G	NG	NG	NG	NG	NG
BOARDING TEAM	G	G	G	G	G	G
HONOR	G	G	G	G	G	G

Figure 45. Feasibility Screening Matrix

Listed the three system alternatives are listed in the first column: the current system, Boarding Team alternative, and the Honor System alternative. The top row of the chart lists the objectives the group wanted to achieve and then went through each alternative to see if it would meet those criteria.

3.5.5 QFD – Sea Inspection Group

The Quality Functional Deployment matrix was a cross-check of customer requirements versus the design requirements that the Sea Inspection Group developed (Figure 46). Essentially, the design requirements the group generated for the alternatives generation were required to meet all the customer requirements that the group generated in the stakeholder analysis.

		Design Requirements								
		Gamma Sensor	Neutron Sensor	Chem/Bio Sensor	Explosive Detection	Human Inspection Team	UHF Radios	Satellite Communications	Smart Container Devices	Training Program
Customer Requirements	Search Vessel	X	X	X	X	X				X
	Search Containers	X	X	X	X	X			X	X
	Detect Radiation	X	X						X	X
	Detect Bio/Chem			X						X
	Detect Explosives				X					X
	Detect Foreign Objects					X			X	
	Provide Automatic Location	X	X	X	X				X	
	Provide Human Interface	X	X	X	X	X			X	
	Identify Material	X	X	X	X	X				X
	Internal Communications					X	X		X	X
	Exterior Communications					X		X	X	X

Figure 46. Sea Inspection System QFD

This figure shows both the design and customer requirements. The Xs indicate where the design requirements meet the customer's requirements.

3.5.6 2005 "As-Is" System – Sea Inspection Group

There was no current Sea Inspection System in place at the Port of Singapore (Figure 47). Shipping container security was dependent on the shipping companies' efforts to ensure that no contraband was packed inside the container before being sealed and placed onboard a ship. The locks on current container systems were easily broken or defeated, and no emphasis was placed on security after the ships left the loading docks.

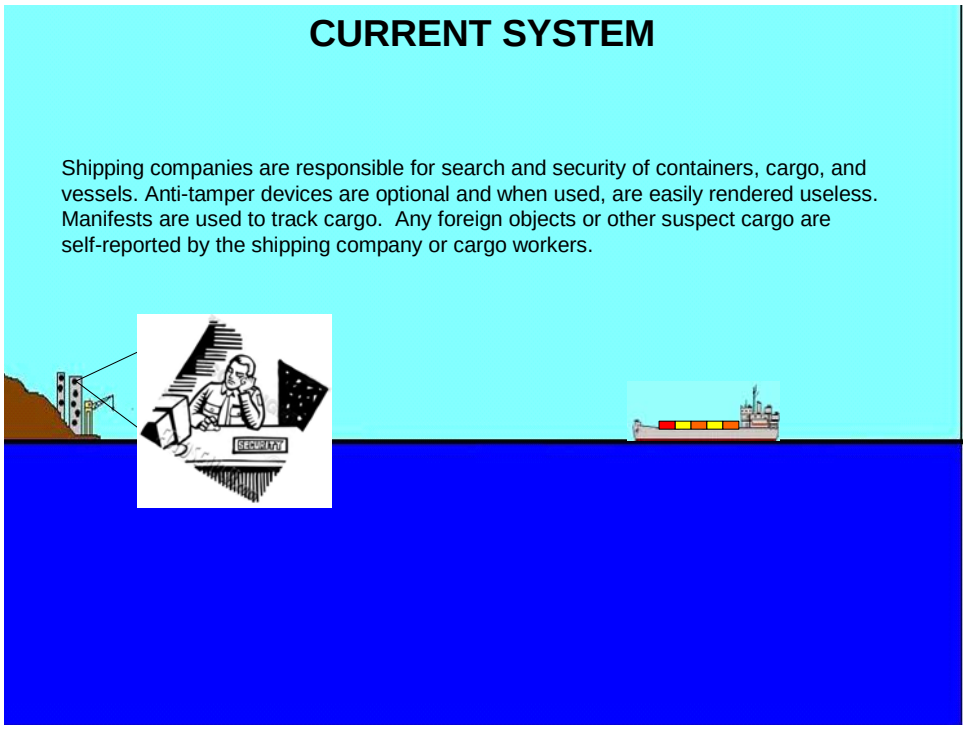

Figure 47. Current System

The Current System had no at-sea inspection. The ports had to rely on the shipping companies to report any discrepancies.

3.5.6.1 Alternative 1 – Sea Inspection Group

Boarding Team System: In the Boarding Team System (Figure 48 and Figure 49), shipping companies were responsible for the security of containers, cargo, and vessels. Hazardous materials (if any) were listed in manifest documentation that was used to track cargo. Any foreign objects, hazardous materials, or suspect cargo were self-reported by the shipping company or their cargo workers. Intelligence agencies used an algorithm that uses the vessel/cargo company history, manifest data, course data, and other intelligence and anomalies to identify suspect vessels and nominate them for a human inspection team. Human inspection was performed by teams of 12 men. They inspected the ship and shipping documents using portable dosimeter devices for radiation sensing and swabs or swipes for explosive sensing. Chemical/Biological inspections were performed with M-8/M-9 and M256 kits for chemical agents and portable

Air Particulate Detection Systems (APDS) for biological agents. An APDS located at Lawrence Livermore Laboratories was capable of conducting on-site chemical analysis.[61]

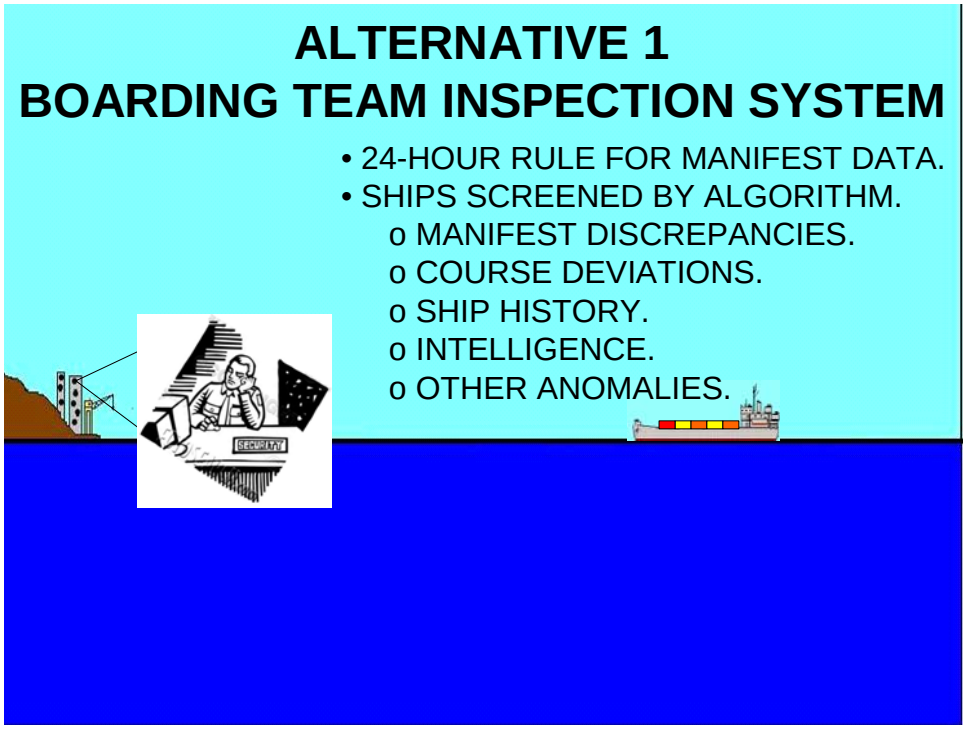

Figure 48. Boarding Team Inspection System

Shipping companies were responsible for reporting any discrepancies. If there were any discrepancies, ships were then boarded and inspected by boarding teams. Ships could also be randomly selected for an inspection by the boarding teams.

[61] Interview with Thomas McGrann, site visit to Lawrence Livermore National Laboratories, (14 January 2005).

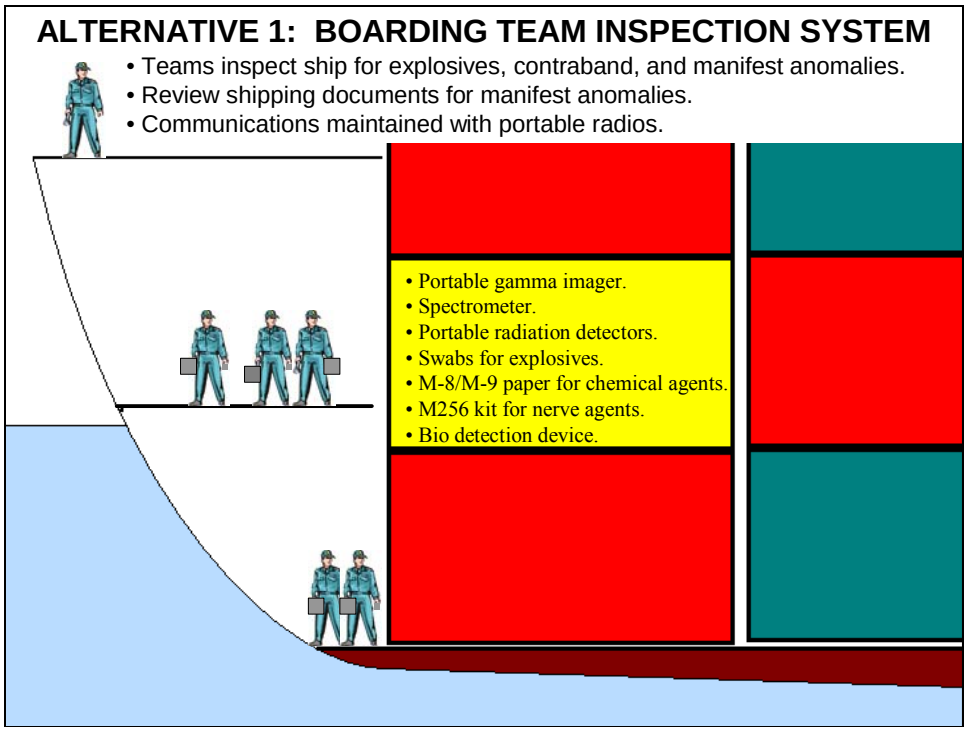

Figure 49. Boarding Team Inspection System

Each boarding team consisted of 12 men (selected in the Modeling and Analysis section), 10 of which actively inspected the ship with various sensors to detect chemical, biological, nuclear, or explosive materials that might be onboard. Backpack sensor packages and other handheld devices are designed to fit in small spaces between containers so that interior containers can be inspected for radiological and other threats.

3.5.6.2 Alternative 2 – Sea Inspection Group

The Honor System: This system included the continued use of manifest screening, intelligence, and ship history for screening vessels and shipping companies. It also included the installation and use of Smart container devices on all containers and cargo holds that incorporated antitampering, intrusion, tracking, radiation detection, communications, and reporting elements that gave stakeholders the location and status of cargo in real time. The Smart container devices used would employ a sensor mapping function and a central data station to localize any anomaly such as the presence of radiation. The key component of this system was that it was required to be mandatory for all shipping companies and vessels, thereby setting a minimum standard for security. After establishing a standard of security, and requiring the shipping companies to live up to this self-imposed standard, the vessels were allowed immediate access to their

destination port. If the shipping companies did not meet the minimum requirements they were automatically selected for a boarding team inspection. As a part of this system, random inspections of vessels would be conducted to ensure Smart container devices, installed air sampling devices and other requirements were installed and in good working order. The use of Smart container devices was sent to C2 elements by the Automatic Identification System (AIS) discussed in the C3I section of this paper. If a vessel or shipping company failed an inspection, their containers/vessels were not allowed immediate access to their destination port. Human inspection teams conducted active inspections of non-Honor System-compliant vessels and those that failed to meet the minimum standards. It was assumed that in order to reduce the delay costs incurred by having a boarding team inspecting their ship, 95% of shipping companies would begin using Smart container devices as soon as possible. The results of the 95% assumption can be seen in the Modeling and Analysis section of this paper. The inspection teams carried backpack sensors, handheld devices, and portable imaging devices for radiation detection. These devices allowed the search of interior containers onboard the vessel. The teams also carried explosive detection kits and portable sampling devices for chemical and biological hazards. The active portion of this system started at approximately the 250 NM distance from Singapore and was concluded in approximately six hours.

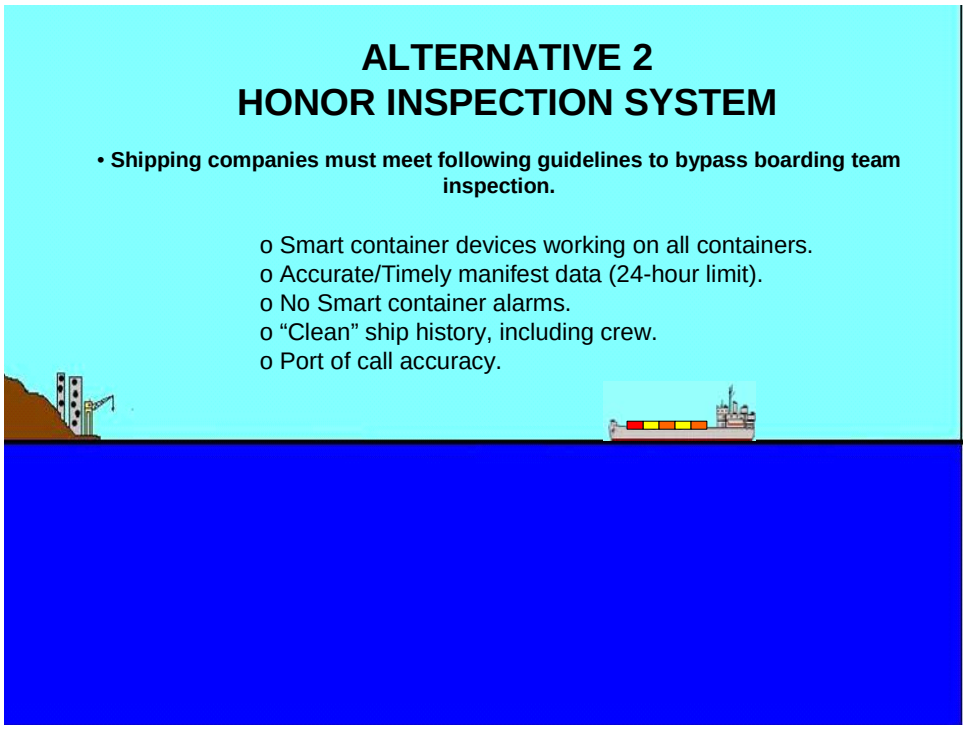

Figure 50. Honor Inspection System

Shipping companies still had to report manifests, but all shipping companies were responsible for installing Smart container devices on all containers. If the companies were compliant they bypassed active inspections.

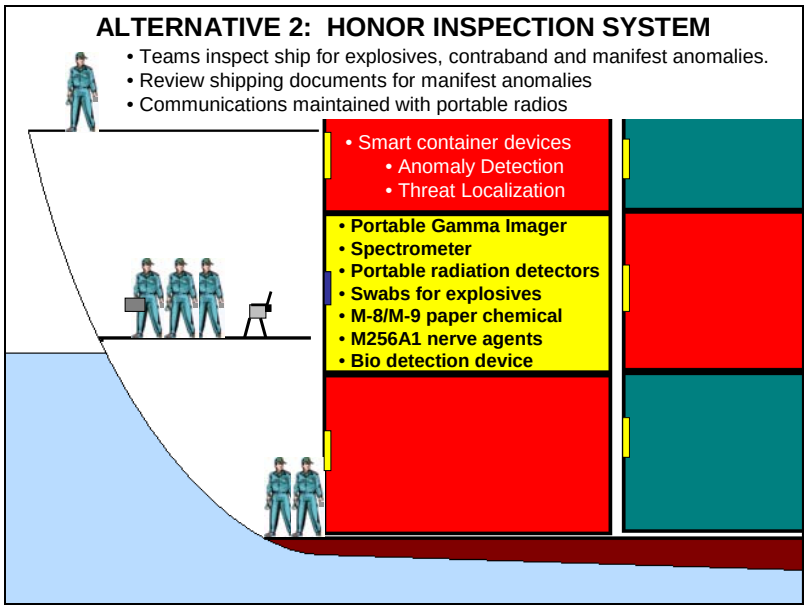

Figure 51. Honor Inspection System Shipboard Search

If a ship was not compliant with shipping standards or was randomly selected, it would be searched by a boarding team. The sensor packages included handheld sensors for detecting chemical, biological, radiological, and explosives. Backpack sensor packages and other handheld devices are designed to fit in small spaces between containers so that interior containers can be inspected for radiological and other threats.

4.0 MODELING AND ANALYSIS STEP

The Modeling and Analysis step simulated and examined the current and proposed alternative solutions developed during the Alternatives Generation step. Individual system models were developed to represent different aspects of each system, including cost and performance, in order to evaluate the system and the subsystem functions. Overarching system architecture models were also developed to link the different system models together for an overall output. Additional models were created to examine system architecture impacts, such as damage costs and delay costs. Data collected from the systems' Measures of Effectiveness (MOEs) and measures of performance were examined using statistical programs to determine the performance of each potential solution. The Modeling and Analysis process resulted in an understanding of the advantages and disadvantages of the various system alternative solutions to the problem.

4.1 OVERALL MODELING PLAN

Approach: A comprehensive modeling plan managed the compound, multifaceted transformation of system parameter inputs from each system group into values for the overall architecture MOEs and Metrics. Since each architecture consisted of up to five system components, the number of architecture variables was substantial: each of the five system components had either two or three alternatives that would be assessed in one or more of three different scenarios. This resulted in 123 different architecture/scenario combinations that were evaluated.

The SEA-7 Cohort chose a modular approach that combined the results from smaller-scale group system models (produced separately by the five different system groups) into relatively simple integrated architecture models that produced overarching performance results for architectures comprised of different system alternatives. This approach was chosen to avoid a situation in which the architecture performance results were dependent on a single model for four reasons:

1. The problem was complex enough that a single model would have been an enormous undertaking by an unfortunate few model developers.
2. The grand model would have been a single-point vulnerability.
3. A single model could have hidden local optimization for the different architecture system components.
4. This approach allowed different modeling tools to be used in order to best model the system.

Alternatively, the modular approach precluded any single-point vulnerability, and it allowed for more rapid progress, both as a result of parallel model development and because the end product was of a relatively smaller scale and less complex. Additionally, more in-depth analysis and a better understanding of system performance was possible since the best modeling tool was used for each system, and each system model was tweaked and analyzed to see which inputs and assumptions had the biggest effect on its local outcome.

Performance Measures: Inputs into the integrated architecture models were the outputs from the individual system performance and cost models. These inputs were then transformed into the following overarching performance measures:

- **MOE 1 – Performance.** The probability that an architecture would defeat a single attack, for each scenario.
- **MOE 2 – Risk.** The estimated damage resulting from a single attack, for each scenario.
- **Metric 1 – Commercial Impact.** The combined total of commercial system procurement cost, ten-year operating and support cost, and commercial delay cost.

- **Metric 2 – Maritime Domain Protection (MDP) System Cost.** The combined total of MDP System procurement cost and ten-year operating and support cost.

Assumptions

Inputs: Inputs into the overall modeling effort consisted of the attack scenario and an architecture comprised of a single system alternative for each applicable group (e.g., a Land Inspection System alternative is not required for Small Boat Attack scenario). Outputs from the individual group system models were combined to represent an overall architecture that was assessed for each scenario.

Description: A graphical depiction of the MDP Overarching Modeling Plan is shown in Figure 52. The five system groups individually designed performance models to represent their respective systems. Inputs to these smaller performance models and system variables within these models were evaluated and adjusted in order to determine the best alternatives for each local system. Similarly, cost models were individually designed to represent the MDP System and commercial acquisition, as well as ten-year operating and support costs for each group system alternative.

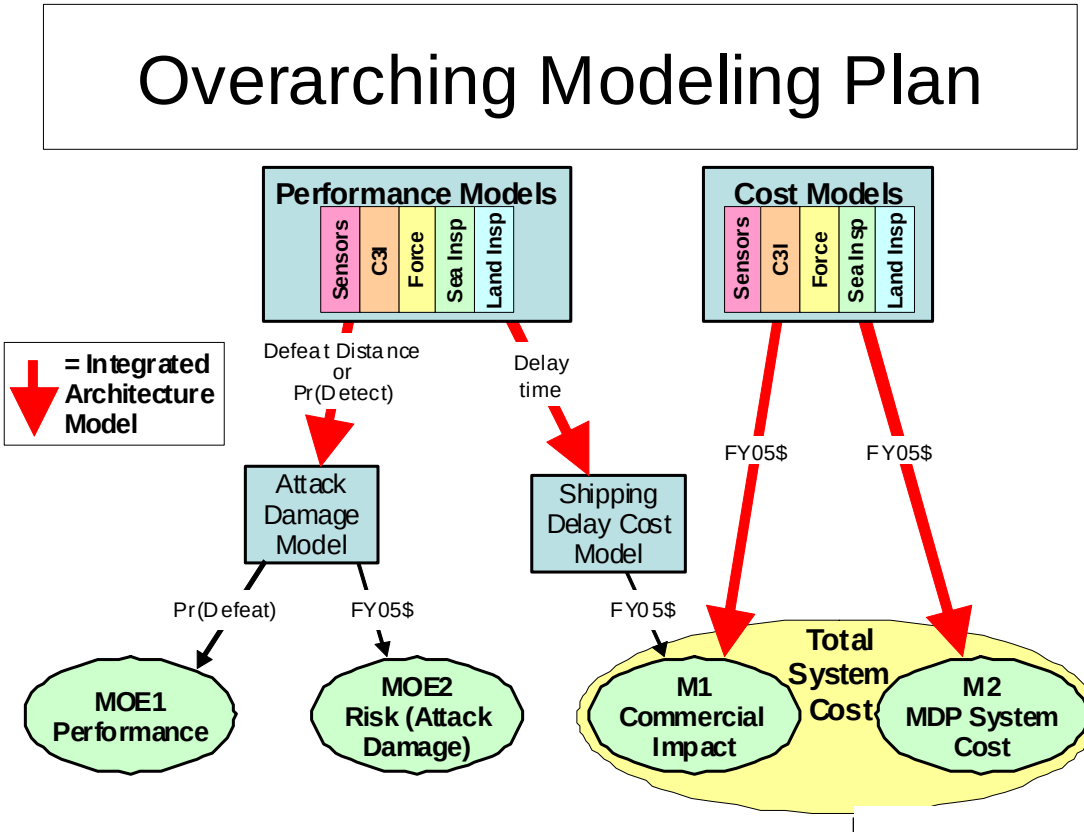

Figure 52. MDP Overarching Modeling Plan

The MDP Overarching Modeling Plan pictorially showed the process of utilizing integrated architecture models to transform inputs from individual system performance and cost models into the desired performance measure outputs.

Integrated architecture models were developed which converted outputs from the individual group performance and cost models into values for the overarching MOEs 1 and 2 (Performance and Risk) and Metrics 1 and 2 (Commercial Impact and MDP System Cost). In order to determine the Performance (MOE 1) and Risk (MOE 2), Attack Damage Models were designed which allowed the conversion of the distance at which a given attack was defeated into a damage cost (MOE 2) in dollars. If the defeat distance was far enough away, the attack was considered unsuccessful, and it counted positively toward the architecture's performance (MOE 1) or probability of defeat.

Similarly, a Shipping Delay Cost Model was designed which allowed the conversion of the total shipping delay time into a cost that contributed to

Commercial Impact (Metric 1). The system cost models divided the ten-year acquisition, operating, and support costs into systems required by industry, which contributed to Commercial Impact (Metric 1), and the MDP System itself, which contributed to MDP System Cost (Metric 2). Since costs were viewed as somewhat fungible between Commercial Impact (Metric 1) and MDP System Cost (Metric 2), a Total System Cost was determined by simply summing these two costs.

4.1.1 Performance Models

Each system group designed performance models that transformed external inputs that were unique to their system into outputs that would be used by a subsequent system group or to determine the integrated architecture performance. The inputs for the system performance models were dependent on the threat scenario, and the models were used to evaluate the impact of and subsequently select singular values for system variables, or factors. Using this method, each system group was able to optimize their local system model and determine the inputs and system variables that had the biggest effects on their local performance.

4.1.2 Cost Models

Cost Modeling was performed through two separate approaches. Commercial Delay Costs were determined from delay times produced from Performance Models. These delay times were then input into a Commercial Shipping Delay Cost Model, which determined the associated cost. Alternatively, System Costs were modeled directly, with costs broken down into Commercial System Costs associated with the shipping industry, and MDP System Costs associated with the MDP System. Each system group modeled both methods, as applicable, and the aggregate of the groups' individual work produced the Commercial Impact (Metric 1) and the MDP System Cost (Metric 2). All costs were adjusted as appropriate to reflect FY05$US.

4.1.3 System Cost (MDP System and Commercial System)

Each system group designed a cost model that took into account inherent costs directly associated with the separate MDP and industry-required propositions for a

lifecycle of ten years. Each group divided costs into the following categories, in conformance with DOD 5000:

- Research, Development, Testing, and Evaluation (RDT&E).
- Military Construction (MILCON).
- Procurement.
- Operations and Support (O&S).

4.1.4 Commercial Shipping Delay Cost Model

In addition, the groups developed independent performance and delay cost models, as appropriate, to estimate the relevant commercial impact costs incurred according to scenario and alternative system architecture. The results of the performance models provided the approximate delay time associated with each alternative and threat-based scenario. These impact costs were then translated into resultant costs incurred due to delay. Integration of these costs provided the quantitative metrics utilized for the analysis of all alternatives including the current system architecture.

A large-scale, high-impact change in port operations to increase security could be resisted, resented, and highly detrimental to world trade and consumer prices if cargo flow was significantly disrupted in the name of security. There have not been many known attempts, if any, to ship Weapons of Mass Destruction (WMDs) in cargo containers. It would be very difficult to convince shippers and consumers that a high cost system is worth the investment and the resulting cost due to delay. It was vital that any system implemented was not selected based on performance alone, but also with importance placed on minimal impact on the timely flow of containerized goods. The shipping delay cost model was completed to compare alternatives' impact on the shipment of containers based on the time it took to get through the system and the associated cost. The Sea Inspection Group looked at a larger-scale ship delay cost, while the Land Inspection Group focused on individual containers.

4.1.4.1 Individual Container Delay Cost Model

Approach: A container that was pulled out of the cargo movement system because of an alarm would clearly not get to its intended destination at the same time that it would have if the inspection system was not in place. For containers that contain hidden weapons, this is a desirable outcome. But for containers that have false alarms, a delay of any kind will negatively impact commerce and therefore must be considered in the selection of alternatives.

MOEs: The more times a false alarm resulted and a container was delayed, the more it cost both port security and the shipper, and, in turn, the consumer. Therefore, the fewer false alarms resulting (which was tied to sensor performance) and the shorter the wait time a false alarm took to be cleared (a function of the number of available alert teams to respond to a false alarm), the cheaper the system cost with respect to commercial delay.

Assumptions: The individual container delay cost model was based on a daily turn-around system. If a container was flagged falsely and pulled out of the system for further inspection, it had 24 hours to return to the system before it was assumed to have "missed its boat." Because of the extreme complexity of transshipments at a large-scale international hub like Singapore, this 24-hour-turnaround assumption was used to baseline the assumed delay cost impact of any given Land Inspection System. This was important to quantify the cost of a container being delayed for any amount of time, from 5 minutes to 24 hours. The individual container delay cost is based on the following equation:

Container Delay Cost = (FA Flat Cost) + (Delay Cost per Hour)*(# Hours Delayed), ***Equation 1***
For hours < 24

Container Delay Cost = (FA Flat Cost) + (Delay Cost per Hour)*(# Hours Delayed), ***Equation 2***
+ (Container Value)
For hours > 24

FA=False Alarm

There was a flat cost charged to the system every time a false alarm happened. This was based on the negative impact cost the false alarm will have on the smooth flow of containers through the existing port infrastructure. Then, with every minute that passes, an additional cost was levied to quantify the negative effects of a long wait in an alarm verification queue. Finally, if at the end of a 24-hour period a container is still awaiting alarm verification, an additional "miss the boat" cost is levied. This "missed intended shipment" cost was a large driver to overall commercial impact/delay cost because of the high jump in cost from a container that was just shortly delayed in the system to a container that was delayed for more than 24 hours, as shown in Figure 53.

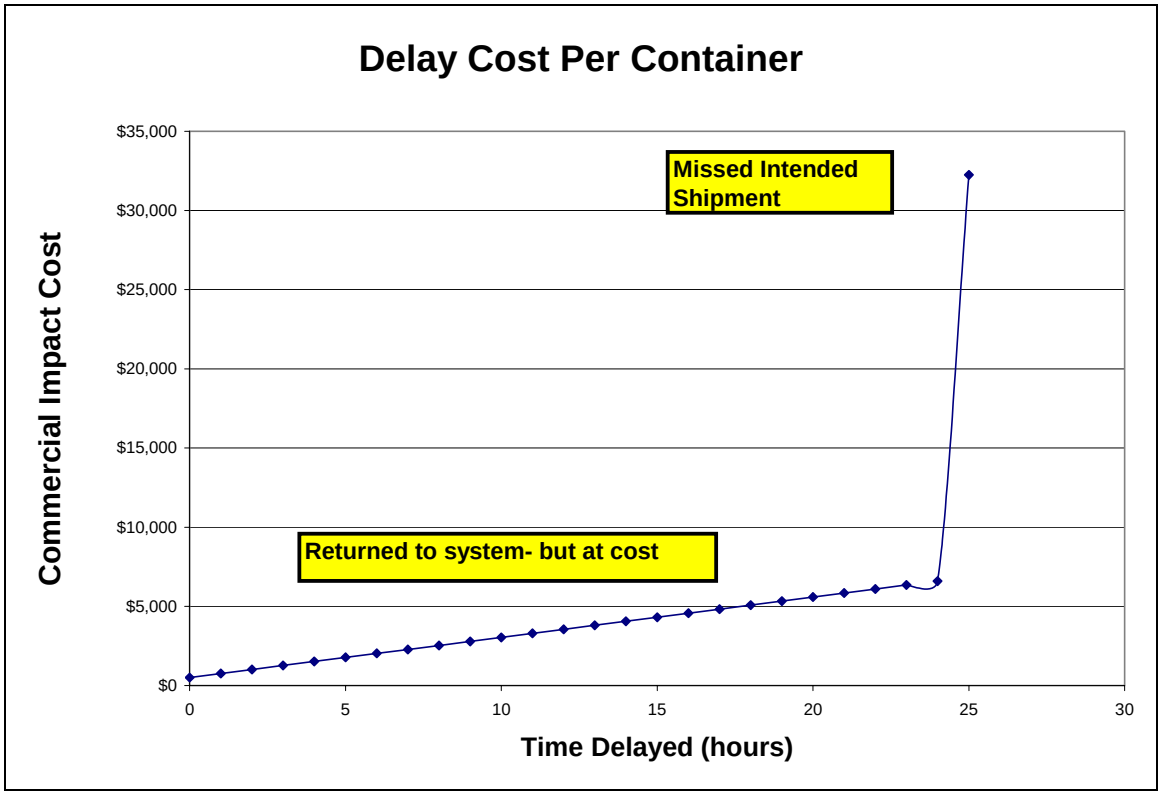

Figure 53. Commercial Impact Cost vs. Time Delay per Container

As the system causes a delay because a container is suspect, targeted, and inspected by active teams, commercial cost increases as delay time increases. If the process causes the container to miss the boat, impact on commercial cost will be much greater.

Inputs: The delay cost model was based on the average value ($25,397.50) of a U.S. Twenty Feet Equivalent Unit (TEU) container in 1998.[62] The flat cost of a false alarm was a composite estimate as a function of time, based on the extra equipment, manpower, and tracking costs incurred for that pulling a container from the system for alarm verification.

Description: The individual container delay cost model shown in Figure 53 was integrated into the dynamic process architecture model for Alternatives 1 and 2 through a Microsoft Excel worksheet used as a model output analyzer.

Results: The results of the based on the individual container delay cost model are aggregated into the results of the overall performance model discussed in the "Land Inspection- Performance Model" section (4.4.1) of this report.

4.1.4.2 Merchant Ship Delay Cost Model

Approach: The model the Sea Inspection Group used for the performance was also used to calculate the delay time caused by the inspection system(s). The parameters of the model needed to be changed to provide the model with the required assumptions.

MOEs: The MOEs for this model were the average delay for the ships and the delay cost incurred from that delay. In order to obtain a delay cost, the average delay for each ship was calculated by timing each ship in the system, adding up those times and dividing the total delay by the total number of ships arriving at the Port of Singapore at the end of the year, as such,

$$\bar{t} = \frac{\sum_1^n t}{n}, \qquad \textit{Equation 3}$$

$\bar{t}$ is the average delay for each ship
t is the delay for each ship.

[62] http://www.pmanet.org/pubs/pmaupdates/v11_iss11_update_11_1999.pdf, (accessed 30 May 2005).

If no delay could occur, all containers would enter Singapore, creating a total monetary value of

$$a = c \cdot N$$
$$a = 25K\,\$/container \cdot 21{,}329{,}100\,container/year \qquad \textbf{Equation 4}$$
$$a = 541{,}705M\,\$/\text{year},$$

Where:

c is the average container value imported/exported to/from U.S.[63]
N is the total number of containers per year into Singapore[64]

Any delay was considered to cause some fraction of the whole container throughput to not enter Singapore in that year. So, the delay cost is

$$DC = \frac{Containers_d}{Containers_{all}} a = \frac{bc\dfrac{1}{8{,}760}}{N} a$$

$$DC = \frac{\dfrac{1{,}230 \cdot 17{,}333}{8{,}760}}{21{,}329{,}100} 541{,}705M \qquad \textbf{Equation 5}$$

$$DC = \$61.5M,$$

Where

b is average number of containers per ship
c is total number of container ships entering port of Singapore.[65]

63 PMA Research, "Import Containers Surge on West, East, Gulf Coasts," PMA Update, Vol. 11, No. 11, (November 1999): pp. 1-4, http://www.pmanet.org/pubs/pmaupdates/v11_iss11_update_11_1999.pdf, (accessed February 2005).

64 Singapore Maritime Port Authority, "Information Center," Container Throughput PDF files, http://www.mpa.gov.sg/infocentre/pdfs/container-throughput.pdf, (accessed April 2005).

65 Singapore Maritime Port Authority, "Information Center," Vessel Arrival PDF files, http://www.mpa.gov.sg/infocentre/pdfs/vessel-arrivals.pdf, (accessed April 2005).

DC represents a total annual delay cost for an average of one-hour delay caused by the system. In order to get the actual delay cost, the model output was simply multiplied by *DC*.

Assumptions: Some basic assumptions for delay cost were made prior to modeling. The output of the model was the average delay in "hours per ship." This number needed to be converted into "dollars per year." In order to do this conversion, the monetary value of each container imported and exported from the U.S. was used since the Port of Singapore did not keep these statistics. The total number of ships per year arriving at the Port of Singapore and the average number of containers in a ship were used to calculate the monetary value of an average of one hour of delay.

Inputs: The inputs (Table 17) that went into this model were the same as the inputs for the performance model, again with slight differences for Alternative 2. Both models had a Mean Time Between Arrival (MTBA) and a Ship Size Per Team (SSPT) input. Each also included whether or not hazardous materials were onboard (Boolean), the inspection time and the number of teams. The only differences were with the probabilities of detection. Alternative 2, incorporated the probability of detection by the boarding team, but added in the probability of detection and false alarm by the Smart containers. All of these factors combined led directly to an overall delay cost.

			Values Chosen	
Treatment		**Values Evaluated**	**Alt 1 (BT)**	**Alt 2 (HONOR)**
Number of Teams		1,3,5,7,9	3	9
Inspection Time		3,5,6,7,8	7	8
Soak Time		1,2,4	1	1
P(Random Inspection)		1%, 2,5%, 5% , 7.5%, 10%	5.00%	1.00%
P(FA) Smart Containers		0.155, 0.198, 0.241, 0.284	N/A	15.50%
P(FA) Boarding Team		0.073, 0.088, 0.103, 0.107	11.70%	7.30%
Pd - Smart Containers	Neutron	0.5, 0.8	N/A	80.00%
	Gamma	0.6, 0.7	N/A	70.00%
	Chem/Bio	0.3, 0.4	N/A	40.00%
	Explosive	0.1, 0.2	N/A	20.00%
Pd - Boarding Team	Neutron	0.1, 0.25	25.00%	25.00%
	Gamma	0.1, 0.25	25.00%	25.00%
	Chem/Bio	0.2, 0.3	30.00%	30.00%
	Explosive	0.4, 0.5	50.00%	50.00%

		Alt 1 (BT)		Alt 2 (HONOR)	
Overarching MOEs		**Mean**	**Std Dev**	**Mean**	**Std Dev**
P(detect)	Boarding Team	0.248949237	0.006595327	0.241811536	0.004121632
	Smart Container	N/A	N/A	0.664141855	0.004725326
Commercial Delay Time (queue + false alarm)		0.2143 hr/ship	0.0255 hr/ship	0.5315hr/ship	0.0483 hr/ship
Commercial Cost		0	0	12,680 B$	5,551 B$
System Cost		16.93 B$	0.2857 B$	100,76 B$	1.995 B$

Table 17. Treatments and Evaluated Results for Model Runs

This table provides a summary of the treatments and values tested for the alternatives and the values chosen to be optimum. The bottom portion summarizes the output of the alternatives using the treatment values chosen above.

Analysis: The end result of the delay cost model is contained in Figure 54. More detailed analysis of each alternative's overall cost and delay cost incurred as a result of that system's performance is contained in the "Sea Inspection-Performance Model" section (4.5.1) of this report.

Delay Time vs. Delay Cost

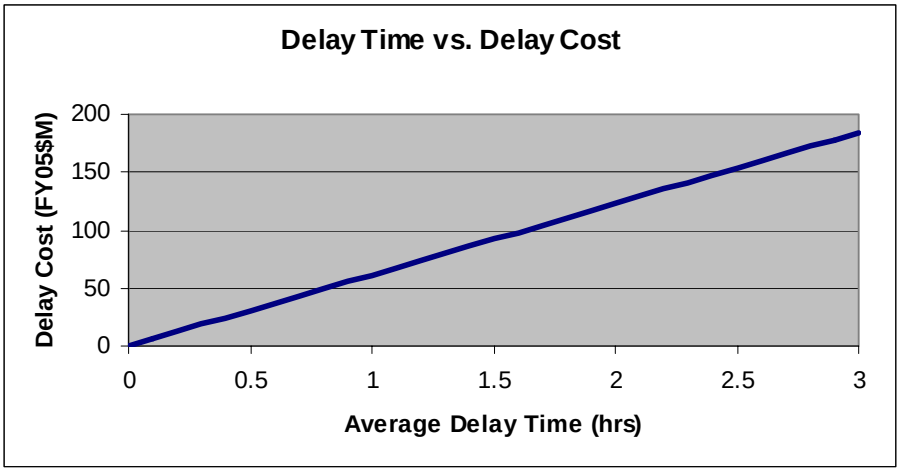

Figure 54. Delay Cost vs. Average Delay Time

This graph shows the relationship between the time each ship is delayed and the delay cost incurred by delaying the ship from entering port.

4.1.5 Modeling and Analysis – Sensors Group

4.1.5.1 Performance Model – Sensors Group

Modeling Approach: The performance of any Sensor System was dependent on two main factors: (1) Sensor Physics and (2) Sensor Integration and Deployment. Sensor physics could be captured by three groups of parameters, which, in most cases, were not completely independent from each other:

- Sensor-target interactions (sensor capabilities versus target signatures or observables, sensor-target geometry, etc.).
- Sensor-environment interactions (particularly weather effects on the propagation path of either emitted or reflected energy from the target).
- Sensor-specific parameters (wavelength, radiated power, sensitivity, field of view, etc.).

While sensor physics pertained to the specific system considered and the resulting "observables" or signatures for targets, sensor integration looked at the aggregate level, which is totally scenario-dependent.

The Sensors Group specifically looked at:

- Sensor-sensor interactions (cumulative probability of detection, coverage overlap, etc.).
- Sensor-location interaction (emplacement considerations as they relate to sensor line of sight, for example).

These main factors were taken into consideration and were specifically dealt with by separate—though interrelated—modeling "levels" as shown in Figure 55.

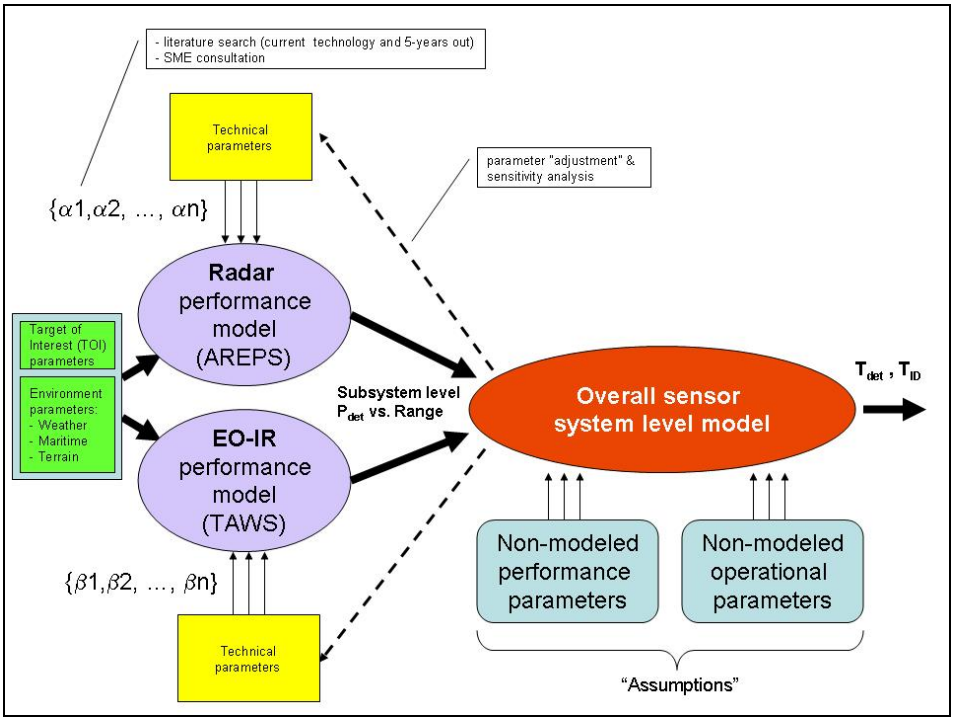

Figure 55. Sensor Modeling Approach

The diagram shows a conceptual representation of the two-tier approach to modeling implemented. The first low-level tier was concerned with the physics-based, individual radar and EO/IR sensor specific parameters, while the high-level tier focused on aggregate performance.

The first level of modeling, represented in the diagram by the radar and EO/IR ovals, was conducted by two separate TDSI Groups, which were specifically concerned with the physics-based modeling task. This modeling effort was conducted using two existing modeling tools: Advanced Refractive Effects Propagation System (AREPS) and Target and Acquisition Weapons Software (TAWS). AREPS was used for radar and TAWS for EO/IR. Application inputs included:

- Sensor-specific parameters (wavelength, scan rate, field of view, pulse length, antenna height, minimum resolvable temperature, etc.)
- Target-specific parameters (type, dimensions, radar cross-section, temperature, etc.).
- Environment-specific parameters (sea surface temperature, humidity, visibility, aerosols, clutter, wind speed, etc.).

The output results varied for each application, but both AREPS and TAWS provided the required information—in some cases through some manipulation of the output data—that basically consisted of a spatial distribution of probabilities of detection (P_{det}) as a function of range from the sensor.

These individual sensor probabilities of detection and ranges were subsequently used as inputs into the second tier, or aggregate level, of modeling. This second stage was conducted using mostly graphical tools and also some Microsoft® Excel spreadsheet models designed to automate repetitive calculations like sensor line of sight, coverage overlap, and sweep rate. Both paper and electronic maps were used extensively to plot and analyze coverage areas, number and type of sensors, emplacement and platforms selection, and trade-offs among these factors.

An analysis of reliability, availability, and maintainability for the different sensors used in the Sensor Group alternatives is shown in Appendix J.

MOPs and MOEs: At the aggregate level, a single MOP captured the overall performance of the sensor deployment alternatives selected for modeling: sensor coverage. This is functionally equivalent to range, and given our basic "cookie cutter" detection model assumption, it was defined to be the maximum range for which P_{det} is

unity. Range was considered to be dependent on three main factors: (1) target critical dimensions for the observable signature; (2) environment (weather/sea state); and, (3) for line of sight sensors, platform height.

Two other specific MOEs were selected for modeling purposes: (1) Time-to-Detection (TDet) and Time-to-Classification/ID (TClass/ID) as seen on Figure 56. These two MOEs basically captured aggregate effectiveness for the Sensor System. Given the "cookie-cutter" assumption made for the detection function, TDet was very straightforward to calculate because the delay was basically 0 from the moment that a contact was within the field of view of the detection/tracking sensor. Conversely, the TClass/ID had to take into account that if the target was not within the field of view of the sensor at time 0, consideration had to be given to the time required for a classification/ID-capable platform/sensor to be moved to the target area. Figure 56 shows that dependence.

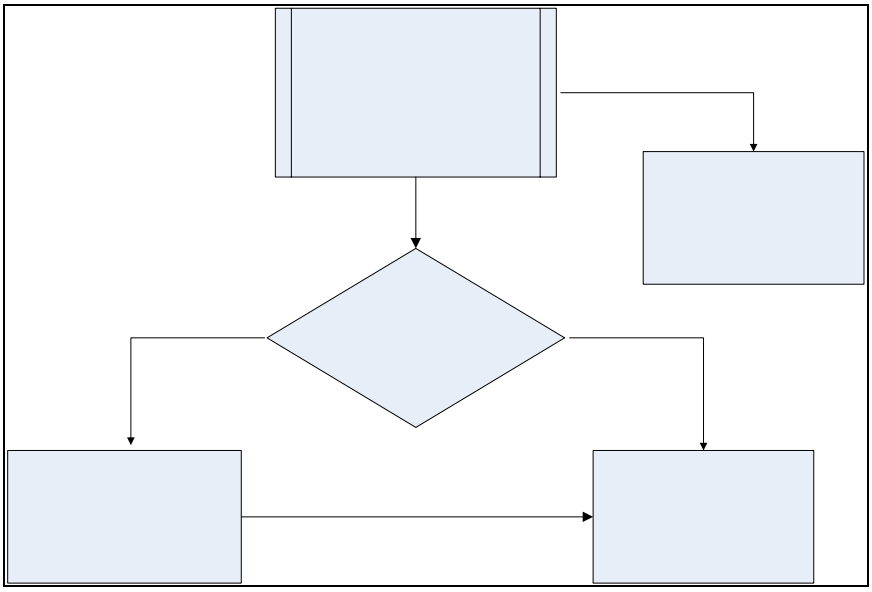

Figure 56. Time-to-Detection and Time-to-Classification/ID

Time-to-Classification/ID became the critical metric for the performance at the aggregate level. It included computation of the time required to position a classifying/ID-capable asset within "line-of-sight" distance to the contact of interest.

Finally, Time-to-Go One (TTG1) was an overall system-level MOE which was designed to capture the end result contribution of the sensor subsystem to the larger

MDP Integrated System. It was measured as the time remaining from the moment when a contact was detected and identified until it was—at least theoretically—in a position where it could execute its intended damage-producing effect (e.g., for the SAW scenario this would be ramming the pier of the Port of Singapore). The relationship between this metric and the MOEs TDet and TClass/ID is direct—distance divided by vessel speed—once the distance to the contact is determined, which was scenario driven (assuming a fixed given vessel speed).

TTG1 was computed for the different alternatives (and "As-Is" System) through worst-case assumptions regarding location. For instance, for Alternative 1 this was done basing the computations on distances and ranges from the most easterly radar station (coastal, tower-based, 300-foot tower) located in Tanjung Piang, Bintan, Indonesia and a potential "ship-as-a-weapon" vessel coming from the South China Sea. For Alternative 2, the same computations were performed using ranges and distances based on the use of the most easterly radar aerostat station (tethered at 15,000 feet above sea level (ASL)) located in Pulau Jemaja, Indonesia and also a potential "ship-as-a-weapon" vessel coming from the South China Sea. The classification/ID task was assumed to be executed by either AIS alone for Alternative 1, or AIS plus maritime patrol aircraft (MPA) for Alternative 2. In both cases, AIS base stations were considered to be collocated with the radar station (coastal aerostat mounted). The results from this modeling approach are shown in the "Results (Treatment and MOE Values)" section.

Assumptions: Some simplifying assumptions were made in order to make the problem more manageable within the scope and time limitations of the project. These are basically related to the detection probabilities, overlapping coverages, and classification and identification capabilities.

- **Detection Probability:** The cookie-cutter detection approach was adopted. A "cookie-cutter" sensor sees everything that is within its range R; that is, if the target is within the distance R to the sensor, then the probability of the sensor detecting it is unity (and conversely, the probability of false alarm P_{fa} is 0). This range R, therefore, became a

technology-driven design parameter, used to derive coverages for the different sensors considered.

Although initially this may have appeared to be an extremely relaxed assumption, the contrary could also be argued. The output from the modeling tool used for radar (AREPS) gave single scan P_{det} versus range. Assuming a typical scan rate of 30 rpm, this would place the target in the field of view of the sensor every two seconds, and given the relative slow speed of the target, the cumulative probability of detection should rapidly converge to unity for all large ships.

- **Coverage and Space-Based Aggregate Probability of Detection:** Wherever there was overlap in coverages, the assumption was made that there was no gain in P_{det} due to more than one sensor looking at it simultaneously. This assumption was also worst-case and hence conservative (the resulting system would not be designed with shorter than minimum ranges for worst case conditions). The basic consideration was that two neighboring stations would likely be looking at the same basic weather-related propagation effects and sensor-target geometries, and then if one sensor did not see the target, the neighboring sensor station would not see it either.

- **Classification/ID:** All large ships—above 300 GRT—were assumed to have operational AIS transponders installed, hence they would be within the field of view (when within range) of this Classification/ID Sensor System at all times. If, for whatever reason, AIS was not operational for these vessels, then that constituted an anomaly indication.

Description: For consistency, only the aggregate-level modeling results will be presented in this chapter. The detailed results from the low-level (physics) modeling effort are attached as separate appendices at the end of this report.

The results from the low-level "tier" were taken as inputs for the subsequent modeling stages; accordingly, the planning and design ranges for P_{det}=1 for

each type of sensor were selected based on sensor, target, and environmental considerations that resulted from this first "tier" of modeling. Additionally, all through the modeling phase some of the intermediate results being produced were iteratively used to enhance the alternative development and refinement process.

The "As-Is" System data was used in the first run of the model with basically two main purposes: (1) to evaluate the adequacy of the modeling approach and tools used; and (2) to assess and document the capabilities of the existing system. Successive iterations of the model at the aggregate level were later generated for the complete set of alternatives.

Results (Treatment and MOE Values): The basic treatments applied were totally dependent on the modeling tier considered. For the low-level models, these consisted of: (1) sensor-specific parameters, (2) sensor location and height, (3) target dimensions, and (4) weather. For the upper-tier (aggregate) modeling level, those treatments were basically combined and presented as sensor footprints or coverages.

While the low-level modeling and simulation tools used were mostly analytical (computer-based), the basic tool used to generate the aggregate level model was—as previously stated—graphical. Physics-based (from low-level modeling) coverages were derived and analyzed for each alternative. As previously stated, the low-level modeling results are attached in the corresponding appendices and only the aggregate modeling results will be shown here.

Aggregate-Level Performance Results: Digital Terrain Elevation Data (DTED) maps provided by the National Imagery and Mapping Agency (NIMA) were used to depict and evaluate the radar coverage for both the "As-Is" Systems and selected alternatives. DTED level 0 was available in an unclassified format and deemed suitable.

As previously stated, the aggregate model itself consisted of the representation of the physics-derived (from the low-level modeling tier) radar coverages over the DTED maps. These maps were used to determine the minimum number of systems required and the general location for the radar installations (a final selection of sites should be made after conducting more detailed field studies). "Calibrated" range

circles (drawn to scale) were developed for overlay onto the DTED maps, using the range data from the low-level models (particularly, AREPS for radar coverages).

In all cases, the calibrated radar range circles were computed for a probability of detection of 0.9 (P_{det}=0.9), a probability of false alarm of 10^{-8} (P_{fa}=10^{-8}), and an estimated target cross-section (RCS) of 800 m^2, approximately the size of an ocean-going freighter of 300 GRT or more, as required for the SAW scenario.

- **("As-Is" System)**
  - **Detection and Tracking (Radar):** See "As-Is Radar System" coverage in Figure 57.
  - **Classification/ID (AIS and EO/IR):** Based on a survey of the existing system, AIS coverage was assumed to be equivalent to the radar coverage. EO/IR performance was not modeled due to lack of information.

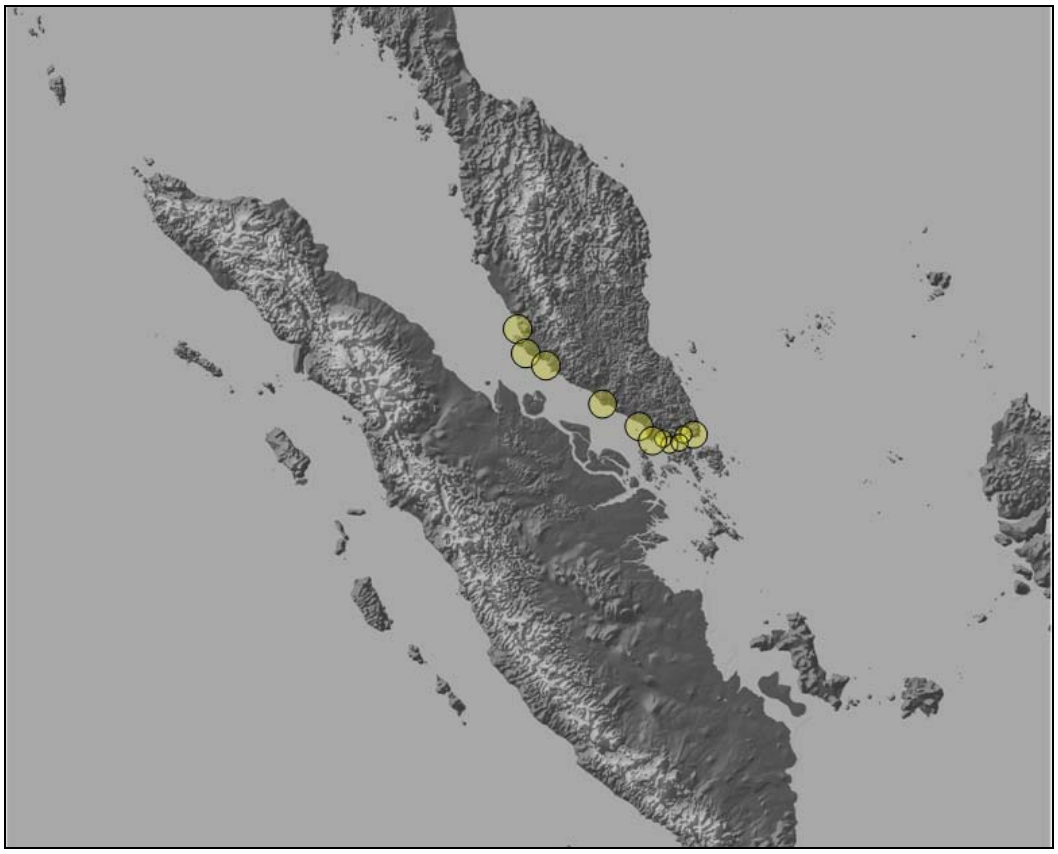

Figure 57. "As-Is" Radar System Coverage

It can be seen that the "As-Is" Radar System covers only a very limited portion of the "critical area." The radar stations are assumed to be mounted on 90-foot towers, resulting in calibrated range circles of 12 NM. The smaller range circles inside the Singapore Straits are 6 NM due to reduced antenna height.

- **Alternative 1**
  - **Detection and Tracking (Radar):** See "Coastal Radar Surveillance-Microwave" coverage in Figure 58 and "HFSWR" coverage in Figure 59.
  - **Classification/ID (AIS and EO/IR):** AIS base stations were assumed to be collocated with coastal radar stations; therefore, due to the increased antenna heights, extended ranges were obtained. EO/IR assets were assumed to be mounted on MPA and fixed sites at selected critical points (performance was not modeled at the

aggregate level). See "Coastal Radar Surveillance-Microwave" and "HFSWR" coverage.

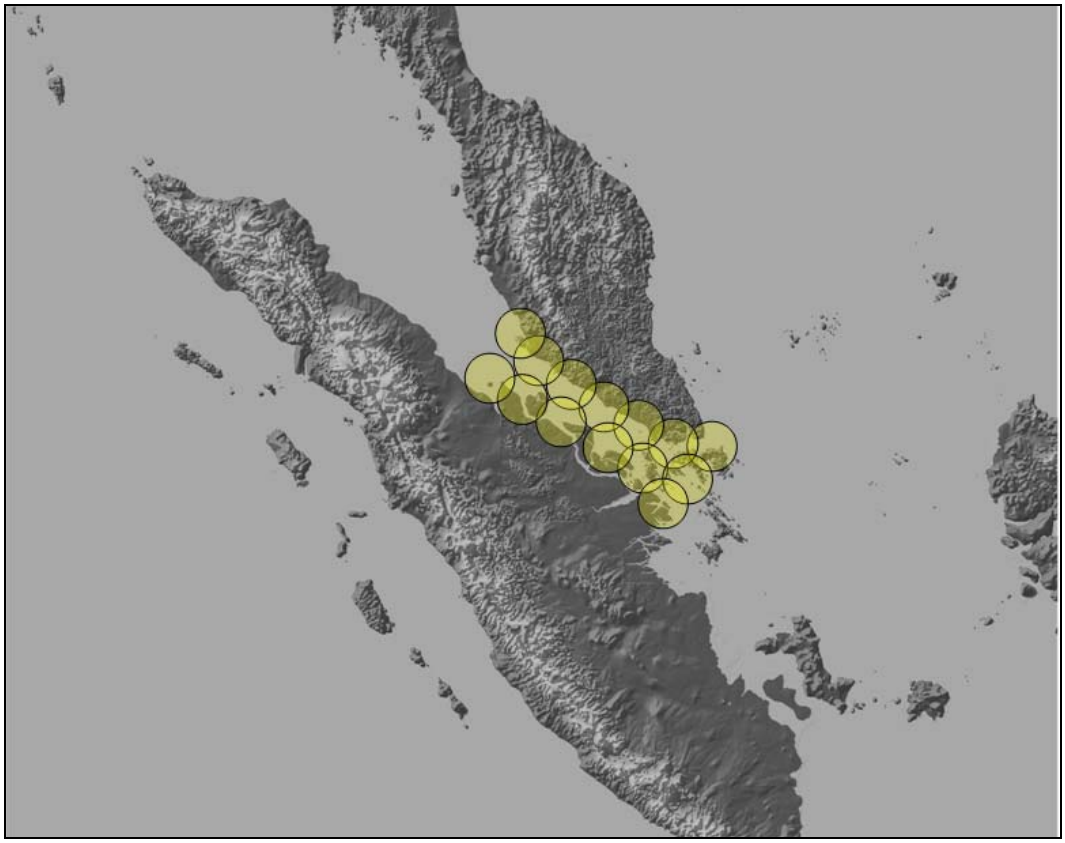

Figure 58. Coastal Microwave Radar Coverage

Alternative 1 includes a network of coastal microwave radar stations. Each radar antenna is mounted on 300-foot towers for a calibrated range circle of 25 NM, as required.

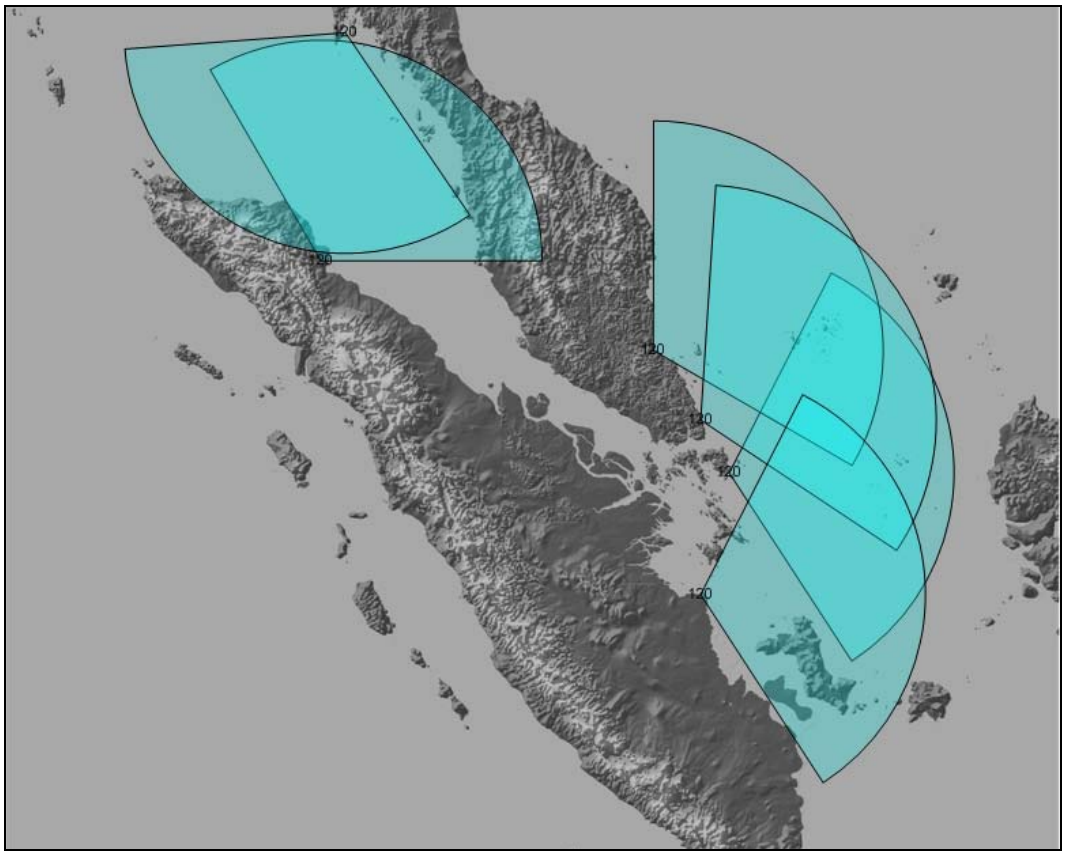

Figure 59. High Frequency Surface Wave Radar (HFSWR) Coverage

Alternatives 1 and 2 also include a network of coastal High Frequency Surface Wave Radar (HFSWR) stations. With current antenna array technology, each station covers a circular sector of 200 NM in a 120° arc. Sector overlap is desirable to increase Pdet.

- **Alternative 2**
  - **Detection and Tracking (Radar):** See "MAEAR" coverage, "HFSWR", and "MPA."
  - **Classification/ID (AIS and EO/IR):** AIS base stations were assumed to be collocated with deployed aerostats, therefore due to the increased antenna heights extended ranges were obtained. EO/IR assets mounted on MPA and fixed sites at selected critical points (performance not modeled at the aggregate level).

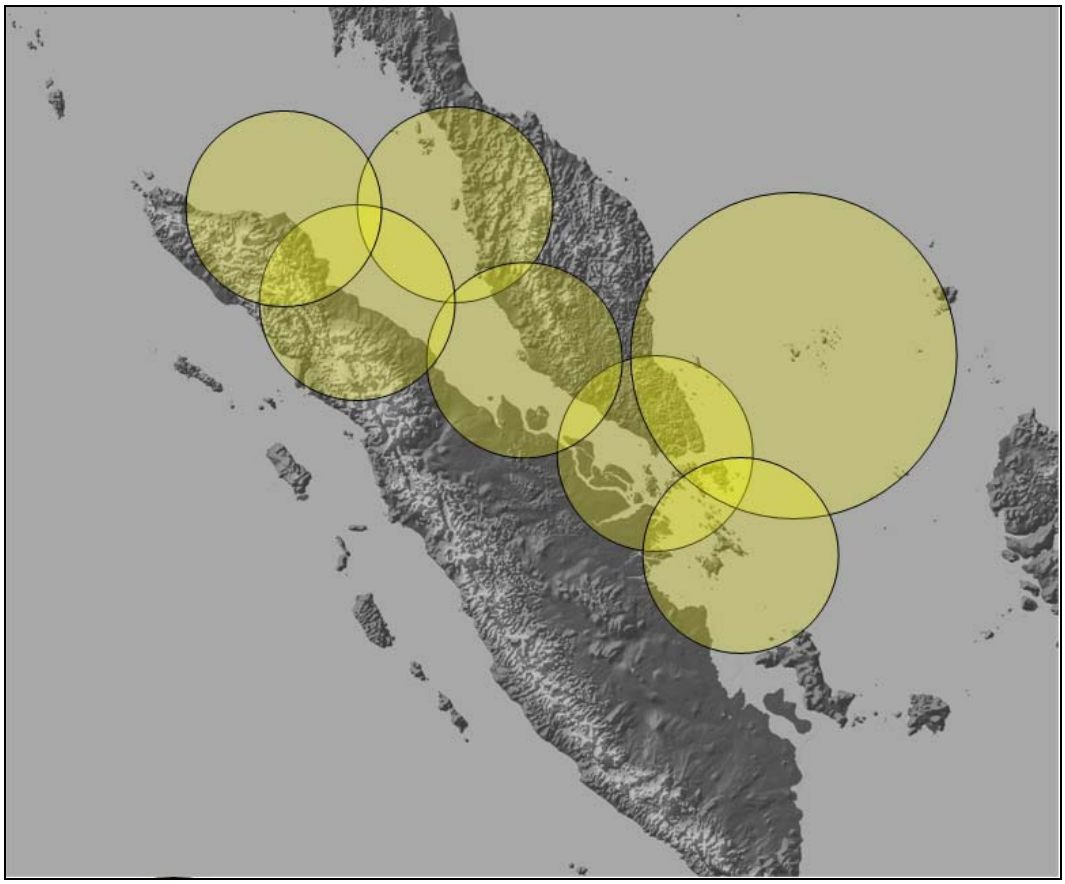

Figure 60. Medium Altitude and Endurance Aerostat Radar (MAEAR) Coverage

Alternative 2 includes a network of six 5,000-foot tethered aerostats along the straits and one 15,000-foot station in the South China Sea. The corresponding calibrated range circles are 90 NM and 150 NM, respectively. Detailed wind profiles were also used to calculate estimated uptime versus downtime ratios.

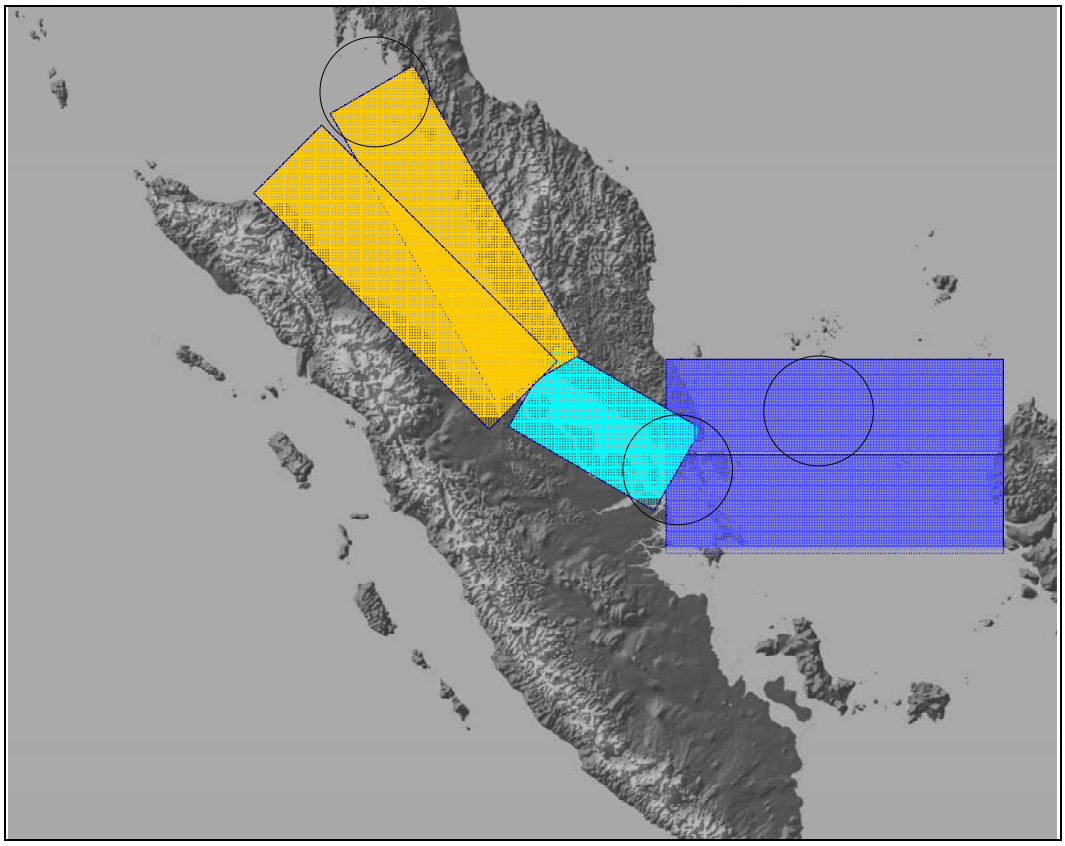

Figure 61. Maritime Patrol Aircraft (MPA) Radar Coverage

Alternative 2 also includes the use of MPA to cover the aerostat downtime periods. Three "search boxes" were defined, two are 300 NM by 100 NM in two "legs," and one (in the critical narrow area of the Strait) is 150 NM by 100 NM.

Using the results provided by the different models with regards to sensor deployment, performance, and coverages, the following estimations for the values of TTG1 were obtained for the different alternatives (see Table 18):

	95% C.I.	Architecture		
		"As-Is"	Alt 1	Alt 2
TTG1 (hrs)	High	1.80	4.00	16.50
	Expected	1.80	4.00	16.10
	Low	1.80	4.00	15.70

Table 18. Sensor Performance Modeling Output

The sensor performance model output is a "Time to Go" parameter indicating the time available to make decisions and complete response prior to attack success.

As it was previously explained, these values correspond to worst-case scenario computations based on the assumption of constant vessel speed (20 kts) and the SAW scenario, where a hostile vessel would be targeting the Port of Singapore. The resulting times reflect the different coverages (ranges) for detection and classification/ID. For Alternative 2 (aerostat-based) there is some variation, which is because MPA will have to be operational for the aerostat downtime (assumed to be 25%) and, in that case, the resulting "search boxes" (given typical P-3 "Orion" parameters) will produce optimistic and pessimistic values for TDet and TClass/ID.

Although these values of TTG1 allow a relative performance comparison among the alternatives, it is very important to note that they have little value if considered in isolation from the rest of the model. As will be seen further into the report, they were subsequently used as input parameters into the overall system-level MDP model, where they were basically analyzed in relation to the response force reaction times to derive valid conclusions.

The following graph (Figure 62) shows a performance (TTG1) versus cost representation for the "As-Is" and Alternatives 1 and 2. Costs are calculated for a ten-year time period and include procurement and operations and maintenance.

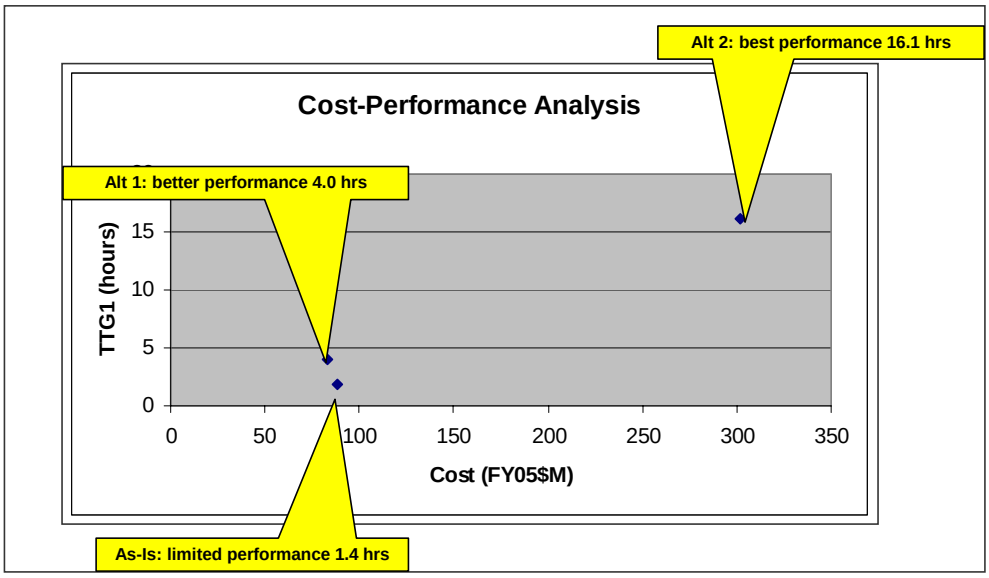

Figure 62. Sensors Systems Performance (TTG1) vs. Cost

The measures TTG1 for the "As-Is" and the two Alternative Sensor Systems selected indicate a moderate increase in performance with reduced cost and a significant increase over current capability at exceptional costs.

4.1.5.2 System Cost Model – Sensors Group

Sensor System Cost Estimation: In recent years, the communities surrounding the area of regard, as well as USPACOM, had improved the overall situational awareness capability within the Straits of Malacca and Singapore. The primary investment was the Straits of Malacca and Singapore Reporting System (STRAITREP). The STRAITREP System was a joint mandatory ship reporting system in the Straits using shore-based radar installations, Vessel Tracking Service (VTS)/AIS base stations, and Very High Frequency (VHF) communications to provide sensor coverage and facilitate communication. Singapore, Malaysia, and Indonesia had all committed resources and assets to the project, with the most substantial progress made by Singapore and Malaysia. Singapore improved the existing situational awareness capability with new and improved assets, while Malaysia undertook significant new construction and infrastructure installation.

Data Sources and Verification: An extensive investigation for existing sensor systems, including cost, was conducted, but limited to open and unclassified

sources. The primary source for existing and proposed national and civil defense assets was Jane's Information Group in both published and online (http://online.janes.com/) subscription service form. Collaborating material was sought generally when an ambiguity, lack of information, or potential conflict was revealed. Secondary sources included, but were not limited to, the public Singapore Government Website (http://www.gov.sg/), the Federation of American Scientists (http://www.fas.org/), and GlobalSecurity.org (http://www.globalsecurity.org/). Where applicable and available, support costs were derived from http://www.navyvamosc.com/.

Some cost data was available from the abovementioned sources, but the analogous systems and their operating cost were gained primarily from U.S. Department of Defense (DOD) sources including:

- DOD procurement documentation: Department of Defense Justification of Estimates, February 1998.
- P-3 System PBL Normalized Cost Opportunity Index, Department of the Navy, 1999.

Extensive efforts went into establishing collaborative relations or, at the very least, communication channels with operators, potential designers, and manufacturers of applicable equipments.

The TDSI component of the MPD Group added invaluable depth and technical expertise to the sensors costing effort. Collaboration meetings defined and detailed the operational norms including assets, utilization, port approach control, and interagency/interservice cooperation.

Current System Investigation: Based on the noted research, fixed radar stations have been installed at 12 designated locations in Malaysian and Singaporean waters and seven new VTS base stations have been constructed on the Malaysian side of

the Malacca Straits. Moreover, only VHF equipment is used to establish communication between the VTS authorities and the vessels using designated frequency channels.[66]

System Cost Assumptions: The Sensors Group approached the cost estimation using the following assumptions:

- STRAITREP assets were the only assets with 100% dedication and cost burden to the MDP mission.
- STRAITREP System costs included operation and sustaining costs only, including operator/technicians.
- National and civil defense assets specifically designated "maritime" (e.g., Navy Coastal Patrol Craft, Air Force Maritime Patrol Aircraft, etc.) were utilized at 20% for the MDP mission.
- Existing platforms (patrol vessels/aircraft, lighthouses, towers, etc.) and associated operating costs were not used in the overall models.
- New Point-to-Point (Sensor-to-C2) Communication System costs were not included.
- New sensor equipment (even for old platforms) and new construction costs, including Operations and Support (O&S), were used in overall models.
- Annual operation, maintenance, and support costs were estimated using 5%, 7%, or 10% of actual equipment costs.
- Personnel costs were estimated at $75K per person per year, with one person per new system unless otherwise noted.
- All costs were adjusted to FY05$US unless otherwise noted.
- The proposed systems were loosely analogous to the four primary systems described below for which accurate cost data was available, unless otherwise noted:
    - Fixed (coastal-based) Surface Search Radar: Scanter 2001 System.

[66] International Maritime Organization, Mandatory Ship Reporting Systems, *Resolution MSC.73(69)*, *Annex 10*, adopted May 1998.

- Fixed Wing/Rotary Wing Aircraft Radar: AN/APS-134.
- Tethered Airborne/Aerostat Radar: AN/APS-143.
- EO/IR System: Thermal and Imaging Sensor System (TISS); Boeing).

Sensor System "As-Is" Cost Estimate: The Current "As-Is" Sensor System included:

- Twelve medium to short range microwave radar stations located at Malaysian and Singaporean Ports and waterways.
- Three VTS authorities (Kelang, Johor, and Singapore).
- Seven AIS base stations in Malaysia, covering 180 miles from Kelang to Tanjung Piai.
- Two AIS base stations in the Singapore Straits.
- Various surface patrol and maritime patrol aircraft.

Singapore was operating 17 to 23 surface craft, and 10 rotary wing and 5 fixed wing aircraft capable of sensor platform hosting. Malaysia was estimated to be operating 7 to 18 surface craft, 12 rotary-wing and 10 fixed-wing aircraft. Indonesia was estimated at 0 MDP dedicated assets. Altogether, there are approximately 34 individual systems identified and in use in the Straits of Malacca and Singapore. System costs were approximated using comparable systems within the U.S. inventories.

For a conservative estimate, the Sensors Group used the reported inventories as being fully operational, but implemented at the assumed 20% for the MDP mission.

Life Cycle Categories	As-Is Costs (FY05$M)		
	Min	Mean	Max
Program Acquisition Cost	$ -	$ -	$ -
Procurement Cost	$ -	$ -	$ -
Prime Mission Equipment	$ -	$ -	$ -
MILCON	$ -	$ -	$ -
Operation and Support	$ 5,939,757	$ 8,863,785	$ 13,567,970
Ops and Maint	$ 4,109,757	$ 7,033,785	$ 11,737,970
Personnel	$ 1,830,000	$ 1,830,000	$ 1,830,000
One Year O&S Totals	$ 5,939,757	$ 8,863,785	$ 13,567,970
Ten Year O&S Total (FY05$M)	**$ 59.40**	**$ 88.60**	**$ 135.70**

Figure 63. "As-Is" System Cost Estimate

The "As-Is" System cost estimates are based on current inventory, operation, and support requirements, and utilization rates established by AOR operators.

Sensor System Alternative 1 Cost Estimate: Alternative 1 included:

- Eight HFSWRs for long-range detection and tracking.
- Fourteen new tower-mounted microwave surface search radars for medium and short range and small craft detection and tracking.
- Fourteen AIS base stations (collocated with tower-mounted radars).
- Nine Maritime Patrol Aircraft (MPA) fitted with new EO/IR equipment for identification and classification only. Note: Existing platform operating costs were not used in the overall models (i.e., "0 cost delta"), but new equipment (even for old platforms) and new construction costs, including O&S, were used.

Life Cycle Categories	Alt 1 Costs (FY05$M)		
	Min	Mean	Max
Program Acquisition Cost	$ 35,416,400	$ 35,416,400	$ 35,416,400
Procurement Cost	$ 21,016,400	$ 21,016,400	$ 21,016,400
Prime Mission Equipment	$ 21,016,400	$ 21,016,400	$ 21,016,400
MILCON	$ 14,400,000	$ 14,400,000	$ 14,400,000
Operation and Support	$ 4,095,820	$ 4,804,148	$ 5,866,640
Ops and Maint	$ 1,770,820	$ 2,479,148	$ 3,541,640
Personnel	$ 2,325,000	$ 2,325,000	$ 2,325,000
First Year Totals	$ 39,512,220	$ 40,220,548	$ 41,283,040
Nine Year O&S Totals	$ 36,862,380	$ 43,237,332	$ 52,799,760
Ten Year Acquisition and O&S Total (FY05$M)	**$ 76.40**	**$ 83.50**	**$ 94.10**

Figure 64. Alternative 1 Cost Estimate

The Alternative 1 System cost estimates are based on estimated inventory acquisition, O&S requirements, and utilization rates established by AOR operators.

Sensor System Alternative 2 Cost Estimate: Alternative 2 included:

- Six HFSWRs for long-range detection and tracking.
- Six MAEARs (at 5,000 feet) for medium- and short-range and small craft detection and tracking.
- One MAEAR (at 15,000 feet).
- Seven aerostat-mounted AIS/VTS transponder/interrogators base stations (collocated with radar systems).
- Nine MPAs fitted with new EO/IR, airborne surface long-range microwave radar, and AIS transponder/interrogator equipment for foul weather search, detection, track, identification and classification. Note: Existing platform operating costs were not used in the overall models (i.e., "0 cost delta"), but new equipment (even for old platforms) and new construction costs including O&S were used.

Life Cycle Categories	Alt 2 Costs (FY05$M)		
	Min	Mean	Max
Program Acquisition Cost	$ 165,462,733	$ 165,462,733	$ 165,462,733
Procurement Cost	$ 16,062,733	$ 16,062,733	$ 16,062,733
Prime Mission Equipment	$ 16,062,733	$ 16,062,733	$ 16,062,733
MILCON	$ 149,400,000	$ 149,400,000	$ 149,400,000
Operation and Support	$ 10,172,933	$ 13,582,106	$ 18,695,865
Ops and Maint	$ 8,522,933	$ 11,932,106	$ 17,045,865
Personnel	$ 1,650,000	$ 1,650,000	$ 1,650,000
First Year Totals	$ 175,635,666	$ 179,044,839	$ 184,158,598
Nine Year O&S Total	$ 91,556,394	$ 122,238,951	$ 168,262,787
Ten Year Acquisition and O&S Total (FY05$M)	**$ 267.20**	**$ 301.30**	**$ 352.40**

Figure 65. Alternative 2 Cost Estimate

The Alternative 2 System cost estimates are based on estimated inventory acquisition, O&S requirements, and utilization rates established by AOR operators.

4.1.6 Modeling and Analysis – C3I Group

The development of the C3I model was based on a desire to incorporate both the theory and practice of C2 into a single model. The intent of the model was to provide insight into what C2 architectures and strategies produce the best performance.

The main question the C3I Group wanted to answer was "can the MDP System make a good and timely decision?" The best way to model a timely and informed decision was by building two separate models (see Figure 66).

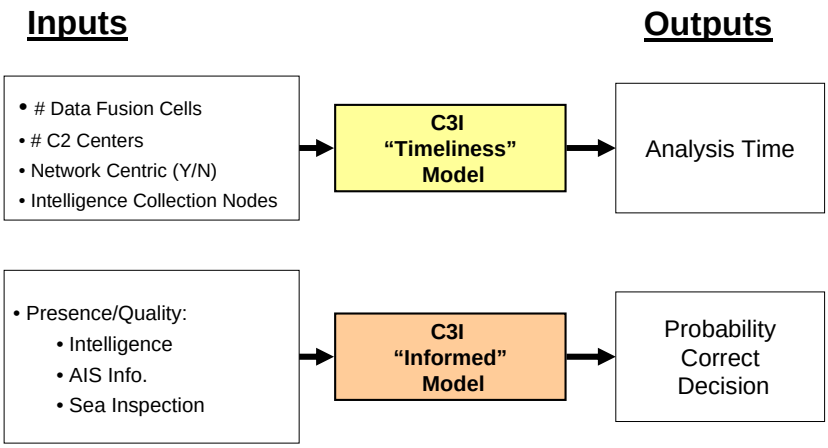

Figure 66. C3I Performance Model Overview

The intent was to model the presence of intelligence on which the decision maker could base an informed and timely decision, so two distinct models were used.

The group defined an "informed" decision as one based on the aggregation of verified information received from electronic intelligence (e.g., sensors such as radar), Sea Inspection, Land Inspection, or HUMINT. "Timeliness" meant analysis performed and a decision made with time to react through inspection or target engagement. The inputs to the "Timeliness Model" were varied and the outputs were used to compare Alternatives 1 and 2 to the "As-Is" System. The "Informed Model" inputs were held constant, as they were the outputs from Sensors, Sea Inspection, and Land Inspection Groups' models. This "aggregation" of information from multiple sources exemplified the data fusion process in a C3I System.

4.1.6.1 C3I Performance Models

Informed Model

Approach: The intent of the informed model was to determine the percentage of correct and incorrect decisions based on the presence or quality of information received from lateral systems of the overall MDP System, such as external intelligence, AIS information from sensors, or results of sea inspections. An information-scoring scheme was developed to analyze model outputs.

The flowchart in Figure 67 depicts the process of the informed model.

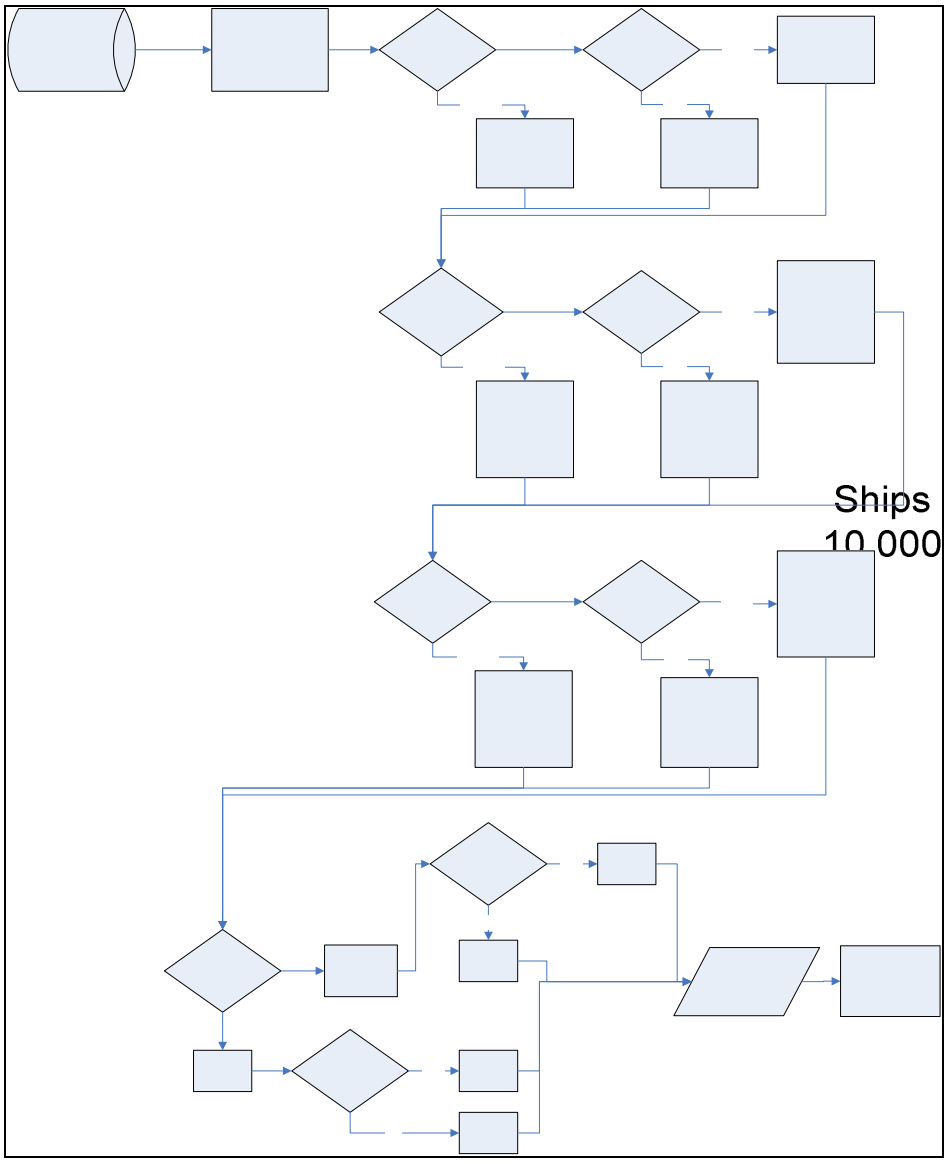

Figure 67. Informed Model Flowchart

This flowchart shows how an information packet travels through the model, collecting AIS, Sea Inspection, and External Intelligence to derive an information score.

Information from the lateral subsystems in the MDP System received a three-digit integer score, as summarized in Table 19. The first digit (the hundred's place) designated the quality of AIS information, the ten's place digit qualified Sea Inspection Information, and the last digit (the one's place) qualified External Intelligence (fed by the Land Inspection System alternative results).

	No Information	Good Information	Bad Information
AIS	100	200	300
Sea Inspection	10	20	30
External Intelligence	1	2	3

Table 19. Informed Model Information Scoring Scheme

This matrix represents the scoring method given the three different sources of information tags: No Information, Good Information, and Bad Information, each associated with a specific score. Having No Information on a ship rendered a score of $1*10^n$, where n = [0,1,2]. Having Good Information on a ship rendered a score of $2*10^n$, where n = [0,1,2]. Having Bad Information on a ship rendered a score of $3*10^n$, where n = [0,1,2]. The total score provided a means of analyzing the model outputs, i.e., decisions whether to inspect/engage or let the vessel pass.

The total score determined the selected decision relative to the scenario; SAW was to engage or not, WMD was to sea inspect or let pass. The final three-digit score was compared to a decision table to determine if the decision was to inspect/engage or pass.

Decision Score	Decision	Decision Score	Decision	Decision Score	Decision
111	Inspect	222	Pass	333	Inspect
121	Inspect	212	Pass	312	Inspect
112	Inspect	221	Pass	321	Inspect
131	Inspect	211	Pass	322	Inspect
113	Inspect	233	Inspect	331	Inspect
133	Inspect	232	Inspect	313	Inspect
122	Pass	223	Inspect	323	Inspect
123	Inspect	213	Inspect	332	Inspect
132	Inspect	231	Inspect	311	Inspect

Table 20. Informed Model Decision Table

Table 19 determined the decision based on the three-digit score. For example, a ship is generated and passes through the system, receiving a score of 100 for AIS, 20 for Land Inspection, and 2 for External Intelligence. The final score of 122 means there is no AIS information, but the cargo was inspected and passed by a Land Inspection port, and the External Intelligence is good (e.g., there are no reports of illegal cargo). This would result in a decision to allow the ship to pass with no Sea Inspection.

Out of 27 possible combinations, only 5 scores represented a decision to not engage or not inspect. The determination of the decision was based on knowledge of the operations at the Coast Guard's Pacific Maritime Intelligence Fusion Center (MIFC PAC) in Alameda, California. The model also represented decisions that were risk-averse, i.e., "it's better to be safe than sorry."

Each combination of inputs (see Table 21 for input combinations) was run 30 times. The assumption for the WMD scenario was that a WMD was present on each of 10,000 ships generated in the model. The SAW scenarios assumed a certain percentage of the 10,000 ships had some anomalous behavior. Running only anomalous ships through the model was done to evaluate the performance of the C3I System, given that an attack was occurring.

Assumptions: The following assumptions underlined the informed model:

- Physical delays associated with gathering information were not modeled.
- AIS transponders were located on all ships transiting in the AOR.
- All ships with anomalies had parties onboard that intended to use the vessel as a weapon.
- Only one decision was made per ship (10,000 decisions).

Inputs: The C3I Informed Model inputs were the outputs from the Sensors, Sea Inspection, and Land Inspection Groups' models (see Table 21), with the exception of the anomaly input. The model throughputs were individual ships processed through the MDP System (10,000 per run) and the model was determined to be scenario-dependent—input values changed based on the specific scenario being considered.

	"As-Is"		Alternative 1		Alternative 2	
Inputs	**WMD**	**SAW**	**WMD**	**SAW**	**WMD**	**SAW**
AIS (Y/N)	0.75	0.75	0.99999	0.99999	0.99999	0.99999
AIS G/B)	0.9	0.9	0.9	0.9	0.9	0.9
Sea Inspect (Y/N)	0.001	0.001	0.2489492	0.24895	0.6641419	0.66414
Sea Inspect G/B)	0	0	0.107	0.107	0.073	0.073
External Intel (Y/N)	0.02	0.02	0.47	0.47	0.94	0.94
External Intel (G/B)	0.99	0.99	0.88	0.88	0.94	0.94
Anomaly	0	0.01	0	0.01	0	0.01
(1-Inspection Error)	0.9999	0.999	0.9999	0.9999	0.9999	0.9999
(1-Pass Error)	0.995	0.995	0.995	0.995	0.995	0.995

Table 21. Input Values for C3I Informed Model

These inputs values for the C3I Informed Model are outputs from the models for the subsystems lateral to the C3I System: Sensors (AIS information), Sea Inspection and External Intelligence (fed by Land Inspection). This exemplifies the purpose of C3I: to enhance situational awareness by providing a common operating picture by aggregating information from multiple intelligence sources. See the respective group sections for a detailed explanation of the numbers above.

AIS, provided by the Sensors Group, represented vessel information that included Maritime Mobile Service Identity (MMSI), vessel call sign and name, vessel type, vector information, and manifest. External Intelligence was fed by the Land Inspection System alternative results. The anomaly input was only used for the SAW scenario. The C3I Group determined only 1% of the ships would display anomalous behavior. The inspection error and pass error inputs (last two rows in Table 21) represented the probabilities of making a Type I and Type II error. For this model, a Type I error occurred when the decision to let a ship pass was made, but it should have been inspected. A Type II error occurred when the decision to inspect a ship was made, but it should have been allowed to pass. Based on the numbers in Table 21, a Type I error occurred in 0.01% of ships inspected and a Type II error occurred in 0.5% of ships allowed to pass. These numbers represented a conservative view of the capabilities of the system. A Type II error had less risk associated with it, but such an error could increase costs and have a negative impact on commerce. A Type I error had more risk associated with it, and should be avoided.[67]

67 These percentages were determined by the C3I Group based on conversations with analysts from the U.S. Coast Guard Pacific Area, MIFC.

Outputs: The initial model outputs were the tallied count of decisions scored to:

- inspect/engage given the information warranted inspection or engagement;
- inspection and engagement decisions made in error;
- pass vessel without inspection or engagement; and
- pass vessel decisions made in error.

The probability calculations were based on 30 runs of 10,000 "vessels" each. Each vessel represented one decision, but multiple decisions could not be made on one vessel. For the WMD scenario, the probability of making the decision to send an inspection team was calculated by:

$$\frac{[Inspected \ + \ Inspected \ in \ Error]}{Total \ number \ of \ ships}.$$

For the SAW scenario, probability of sending an engagement force to intercept the ship displaying anomalous activity was given by:

$$\frac{[Engaged \ + \ Engaged \ in \ Error]}{Total \ number \ of \ ships \ with \ anomalies}.$$

MOEs: The MOE provided by the informed model was the probability of deciding to send inspection team in response to the WMD scenario, or engagement forces to a suspect vessel with respect to the SAW scenario. The C3I's intelligence source for the SAW scenario was an anomaly. The group defined an anomaly as information from a highly reliable source that a vessel had deviated from a "norm," i.e., suddenly changed course, refused to obey International Maritime Organization (IMO) regulations, did not follow its float plan, did not follow the traffic separation scheme, did not board the harbor pilot at the appropriate rendezvous point, or refused to obey posted speed restrictions.

Description: The Informed Model was a queuing model using Extend™ v.6. The inputs were read into Extend from a Microsoft Excel™ file. The Extend™

outputs were read back into an Excel™ file where they were sorted and tallied. Figure 68 is a screen capture of the Informed Model in Extend™.

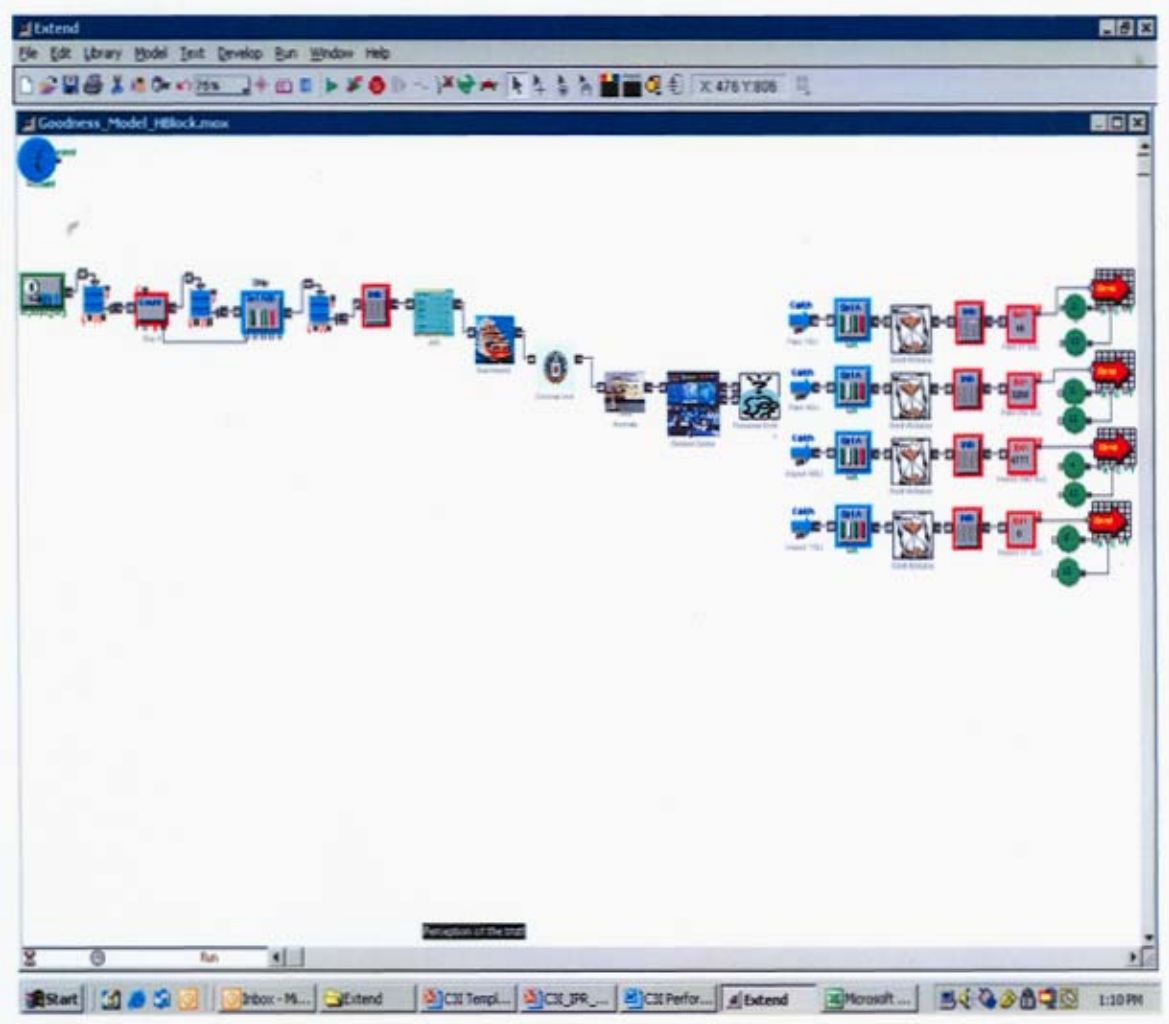

Figure 68. EXTEND™ Screen Shot of "Informed Model"

The above screen shot of the "Informed Model" shows the fow of ships as AIS, Sea Inspection, and External Intelligence (Land Inspection) information on the ship is "gathered" and assigned a decision score in each corresponding information block.

Timeliness Model

Approach: Another measure of performance was data fusion process time. This was the time it took to aggregate and analyze information from the lateral systems. After discussing the various relationships between each subgroup within MDP,

it was decided that "Time To Go" (TTG) would be the overall metric for C3I analysis time. TTG was defined as the time it took each group to do their job represented as a "chunk of time" out of the total time given to respond to a particular scenario. Thus, the timeliness output was a "most likely" time to accomplish data fusion.

The flowchart in Figure 69 depicts the process of the timeliness model.

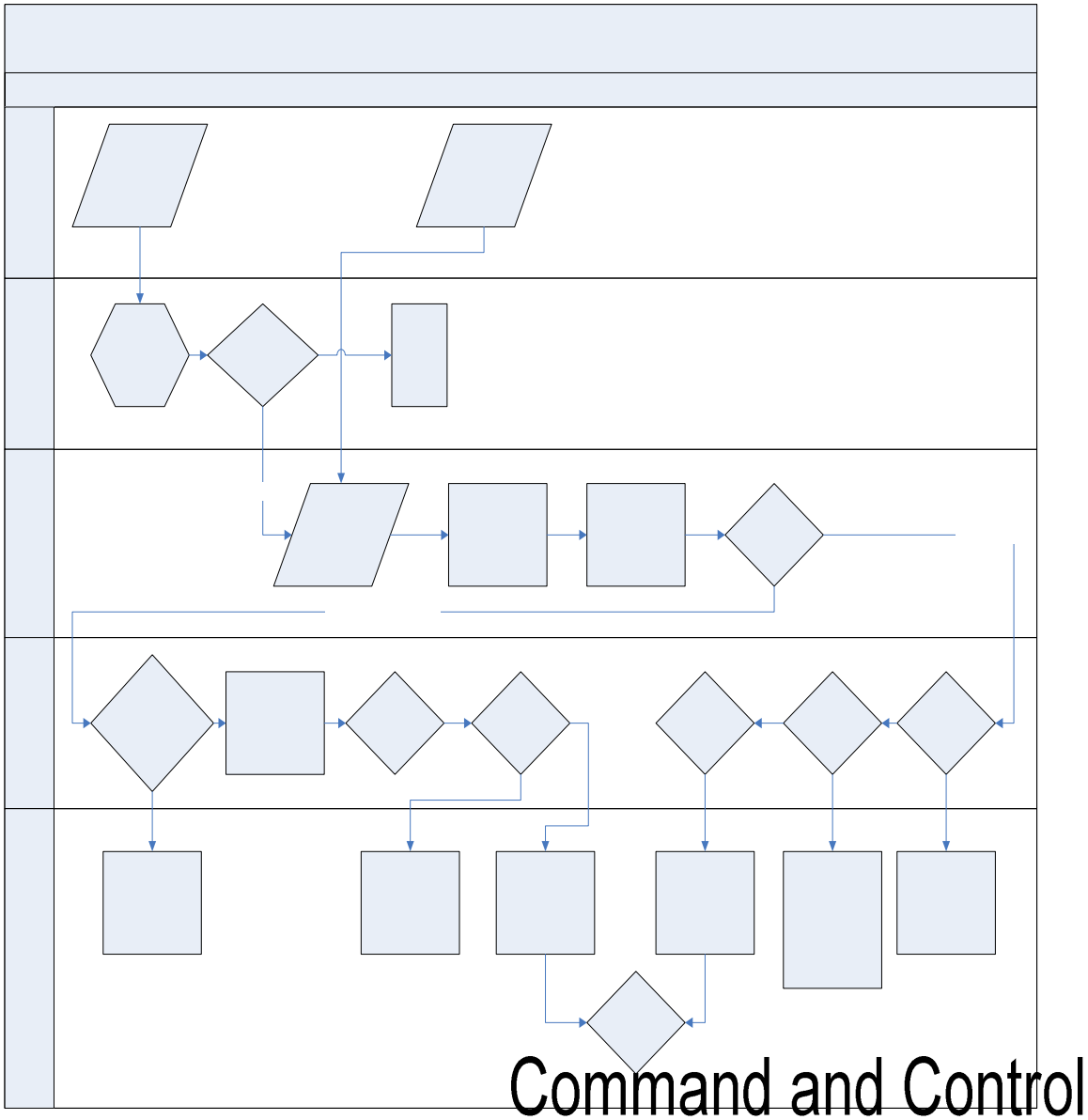

Figure 69. Swim-Lane Flowchart of "As-Is" System in the "Timeliness" Model

This swim-lane flowchart outlines the main processes that occur in the "As-Is" Model. Note that the swim-lane highlights the particular area of the model in which the process occurs.

ate
tion

Sensor

Description

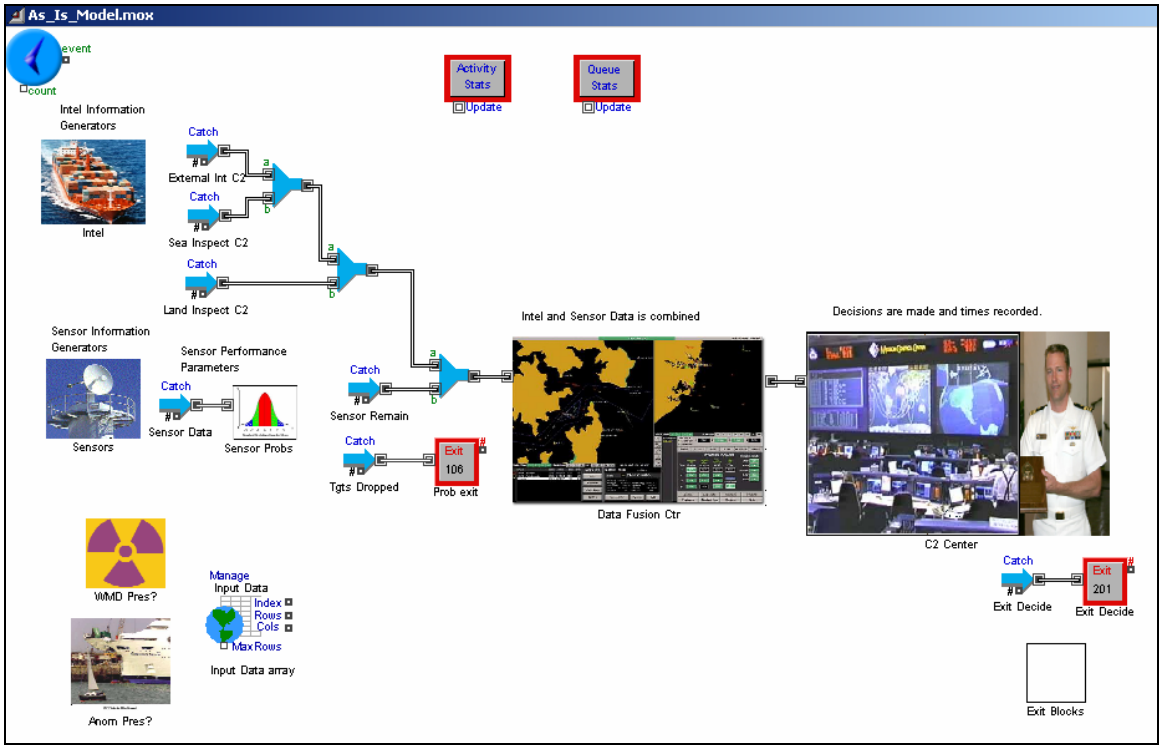

Figure 70. Screen Capture of the "As-Is" System in the Timeliness Model

The model represents the flow of maritime information from sensors and information sources to the Data Fusion Center and C2 Center. This model was built to replicate the process performed at the USCG MIFCPAC in Alameda, California.

- General Description:
  - The model's intent was to represent the decision making process of a maritime C2 Center and to quantify that process by determining the time to make a decision on a certain piece or group of information (MOE).
- Description of the information passing through the system:
  - The items passing through the model represented pieces of information originating from two sources: Sensors and Intelligence Collection. Each piece of information was randomly assigned a track number (which was dependent on the traffic density, the entire area of regard, and the individual sensor areas of regard). The pieces of sensor information were also randomly

assigned a CEP that was based on a distribution provided by the Sensors Group. Once all sources were combined, each piece of information was randomly assigned a priority between 1 (lowest) and 5 (highest). Comparisons were made based on continuous addition of pieces of information to the track row and type of information column.

Considering the overall MOE of time, the Modeling Group applied the need to model information flow from the viewpoint of the commander in charge of the C2 Center. As though presented on a large map display screen, information about contacts and ships came into the model Data Fusion Center from various sources. The sources, or object generators, were designed to encompass all of the possible inputs of information that might be collected by a Data Fusion Center. At Alameda, for example, contact information could be updated by checking computer databases, receiving reports from analysts in the field, or by reviewing electronic intelligence databases.

The overarching assumption for this model was that as data came into the Data Fusion Center, an analyst or watch stander accumulated the various pieces until a sufficient amount of data was available to warrant making a decision or completing an analysis of the ship. A functional flow diagram of this process is represented in Figure 71.

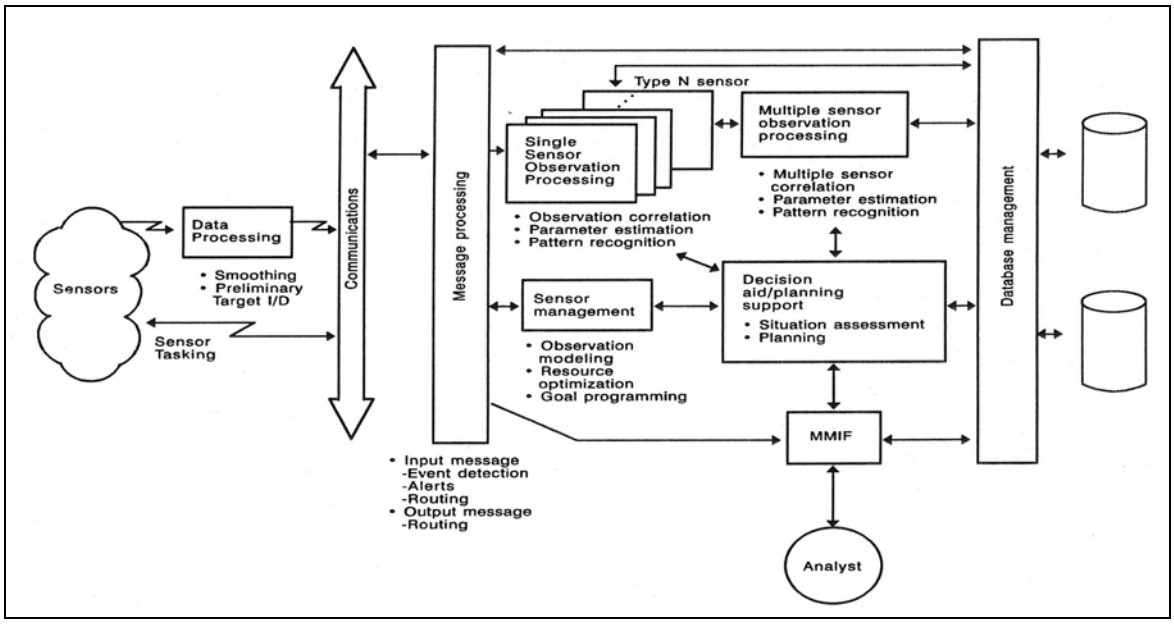

Figure 71. Functional Flow Diagram of a Data Fusion Center

This closely approximates the process used at USCG MIFCPAC Alameda. Note that both communications and analysts play a key role in this process.

Given the variety of sources in this category, the C3I Group created a generic generation block called "external intelligence." The other sources of data were from "sensors" (i.e., radar and AIS), and MDP "Land Inspection" Systems. The interarrival times of each source of information were chosen to be as accurate a reflection of reality as possible. Therefore, sensor data should arrive with 10 to 100 times the frequency of a report from an agent in the field.[68]

With this concept of data generation in mind, it was important to note that each object generated in the model represented a piece of data concerning a ship. Therefore, each data "ball" was given a randomly assigned number between one and the total number of ships expected to be tracked on a given day based on a ship density input.

This decision, or analysis, could be a call for action, or merely the belief that this ship was of no concern. Either way, sufficient knowledge of the ship was available to render some conclusion about what should be done regarding a particular contact. Thus, as data accumulated in the model, the number of pieces of information

68 Interview with LT James Holt, stakeholders' questionnaire, Alameda, California, (12 March 2005).

about a ship increased until a sufficient level was reached. Because the number of the ships was randomly assigned to the data balls, the time that it took for a sufficient amount of information to build up accurately reflected the systematic arrival of information in the real world. Thus, once "three" pieces of information were received about a ship, the time was "stamped," or recorded, providing the overall metric of time to analyze.

The other real world process that was replicated in the C2 model (see Figure 72) dealt with the prioritization of information for "high interest vessels" (HIVs). During the visit to MIFCPAC Alameda, the watch officers noted that if there was a situation that required immediate action, the appropriate information was walked directly from the Data Fusion Center to the admiral in charge of the C2 Center. The prioritization of information was replicated in the model through use of a priority score randomly assigned to a certain percentage of data balls. Once a ball was given the highest priority, it was "fast-tracked" directly to a decision wherein the time was recorded.

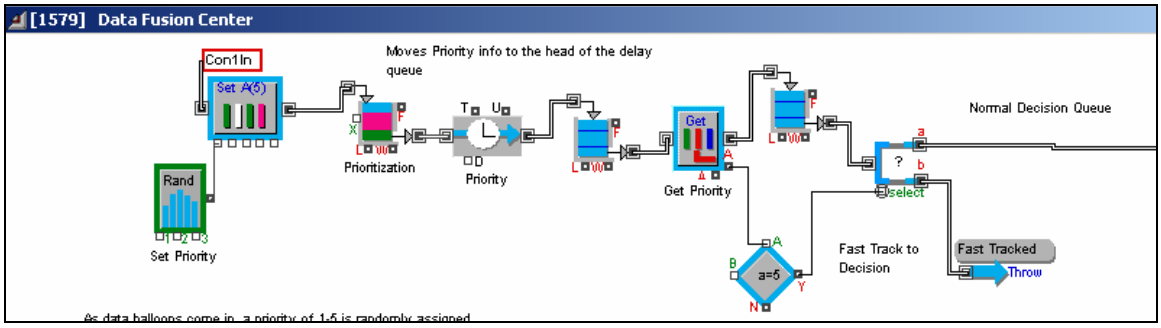

Figure 72. Screen Capture of the Data Fusion Center Block in the "Timeliness" Model

Note that as information arrives, it is given a priority by an analyst, which is represented by the delay. The priority data is then separated from normal data and sent to the fast track queue.

Microsoft Excel™ was used to compile the output data from the model (see Figure 73).

	Sensor Data	Ext Intel	Anomaly	Land Inspect	Sum	Data Arrival Time	Decision Time
1	5	2			7	8.58	11.98
2	3				3	5.78	5.56
3	3				3		3.39
4	3				3	2.28	3.67
5	3				3		3.07

Figure 73. Screen Capture of Output Excel Spreadsheet Used to Record Decision Time

The row number indicates ship number. The first column is where all sensor data is placed. The next three columns contain external intelligence, anomaly, and land inspection data. The next column is the sum of all data columns for a particular row. "Data Arrival Time" is the time when the decision was made. The last column is the time when the last piece of information arrived before the decision was made.

For example, in row one, five pieces of data regarding ship number 1 was accumulated from sensors and two pieces of information from an external intelligence source. Within each spreadsheet was an imbedded formula that prevented more than three data balls arriving per ship. Since the ability to record the decision time and keep track of the number of pieces of information on each ship was independent of the modeling program, but still linked to the model, future models that were built to explore various C2 architectures, or alternatives, could still reference the same spreadsheet as though accessing a database. In the real world, the process of connecting "sensors and decision makers to achieve shared awareness" is called network-centric warfare.[69] By corollary, the C3I Modeling Group was able to generate network-centric alternatives because they possessed these characteristics. For example, the architecture for Alternative 2 called for four C2 Centers and nine Data Fusion Centers linked in a network-centric manner. This was accomplished by simply replicating the architecture for the "As Is" model four times and having each C2 Center reference the same decision spreadsheet. Thus, four times the amount of data could be analyzed at the same time, theoretically generating faster decision times.

69 Ralph S. Klingbeil and Keith M. Sullivan, "A Proposed Framework for Network-Centric Maritime Warfare Analysis," Report #A928614, Naval Undersea Warfare Center Division, (15 July 2003).

MOEs:

- Time to make a decision (based on gathering any three pieces of information)

Assumptions:

- Track duplication had been resolved.
- Given "position" was accurate.
- Information assurance problem systems are in place as information was assumed correct and reliable.
- Track duplication was resolved.
- A decision on all tracks was made.
- The area of regard was divided evenly amongst the specified number of sensors.
- Full sensor coverage, which may have included AIS, VTS, VMS, but not necessarily land-based sensor assets.
- Items in the model were "data packets" with information in specific ships.
- Data fusion process included track assignment, priority assignment, and prioritization of data packets.
- Data fusion and command and control centers were collocated.
- Priority Assignments:
    - 1-4: Low to High some action required within… (hours, days…).
    - 5: Severe—action required immediately ("fast track").

Inputs:

- From Sensors Group:
    - Track Quality: $P_{track.}$
    - Track Quality: $P_{fa.}$
    - Position Error: CEP mean.

- Position Error: CEP variance.
- Traffic Density.

- Anomaly Probability (determined by the C3I Group).
- External Intelligence (may be HUMINT, Electronic Intelligence, or other types).
- Internal Intelligence: Land Inspection information.
- Internal Intelligence: Sea Inspection information.

4.2 SYSTEM COST MODEL – C3I GROUP

Approach: In order to evaluate "system value" using quantitative performance and cost measurements, a systems cost analysis was performed on each of the three individual C3I design alternatives. In order to predict the future cost of the C3I Systems, actual data was used when possible, but the predominant technique used analogies of similar technology components and operational personnel staffs. A triangular distribution was developed through the estimation of low, mean, and high aggregate estimation for each component of the C3I System (e.g., facilities, personnel, equipment).

Translating the C3I Group functional requirements into budget requirements allowed for traceability and ensured direct comparison of each functional requirement, which allowed trade studies to occur.

MOEs:

- Total Ownership Cost for the ten-year system R&D, Procurement, O&S, and Disposal costs

Inputs: The Research, Development, Testing, and Evaluation (RDT&E) costs were estimated as a function of total system procurement cost, with RDT&E for stratellites and UAVs provided from analogies from programs of record. The military construction (MILCON) cost of the C2 Center and Intelligence collection nodes were scaled from military and commercial building cost per square foot. The USCG MIFIC Alameda was used as a basis for required space for a C2 Center, multiplied by a factor of 1.25 for security, video-teleconferencing capability, and survivable construction. The

number of personnel used to staff a C2 Center was directly representative of existing operational staffs currently used at the USCG MIFIC Alameda. A 5:1 personnel-to-position staffing ratio was used, similar to the operating capability at Alameda. The personnel salary was an input variable that was burdened for lights, space, training, and benefits. This input variable could be modified for implementing U.S. Navy personnel or local (Singaporean/Malaysian/Indonesian) personnel to staff the C3I Systems.

In the development of the personnel cost estimation, given the wide spectra of designators for military personnel, it was assumed that the staff would be multidisciplined and highly skilled analysts. The following are the position titles envisioned for this system:

- Commander (Officer)
- Command And Control Watch Standers
- ELINT–Sensor Tracking Engineer
- Intelligence (Officer)
- Intelligence Watch Standers
- Communications Specialist
- Communications Operator
- Information Assurance Supervisor
- Information Assurance Specialist
- Support/Logistics/Maintenance
- Intelligence (Data Fusion Specialist)
- Intelligence (Support Analysts)
- Intelligence (HUMINT Specialist)
- Intelligence (Support Analyst)

Description: In order to get the better cost estimation, given the different subsystems, the components' costs were statistically summed to derive the total system cost, instead of adding the best "guesses" for each component. Each of the components were quantified in terms of their statistical properties (mean, standard deviation, range,

most likely, highest, lowest, etc.), and a Monte Carlo simulation was performed, varying each element in accordance with its statistical properties. A probability distribution was built for the cost of each of the components.

The **Regional Systems Architecture (RSA) Alternative (Alternative 1)** consisted of two mirrored systems connected by a communication network grid. Each C2/Data Fusion Center had a fixed staffing level supporting 24/7 "around the clock" operations with a mission critical ratio of 5:1. This alternative relied heavily on ELINT collection via sensor data and maintained a large area of regard (AOR), using sequential processing and queuing. This was chosen as a rapidly implementable alternative, which was feasible within the political constraints of the region. This alternative supported each of the three SBA, SAW, and WMD scenarios.

The **Network Centric Warfare Systems Architecture (NCW) Alternative (Alternative 2)** exploited the preprocessing and data fusion concept. This design contributed to a common operating picture (COP), and all were organized in a self-synchronizing structure with distributed authority. The HUMINT network focused on social networks and all-source collection. The Communications System was a layered, gracefully-degrading system using a fiber-optic backbone, networked maritime wireless communication buoy stations, stratellites and fixed-wing UAVs. This alternative invested heavily in technology and had a greater number of connected nodes, which provided for enhanced capability, with the sum of the parts being greater than their individual contribution.

4.2.1 System Cost – C3I Group

The existing Singapore Primary Maritime Domain C2/Intelligence Center relied on independent operations and defined territorial responsibility. The Singapore sensor network gave limited correlation sensor data and relied heavily on ELINT collection. The Communications Systems were fully reliant on the fixed infrastructure and were nonredundant.

As expected, C3I Alternative 1 showed a marked improvement in both the SAW and WMD scenarios, but was noneffective for the SBA scenario, where there was too little reaction time. Figure 74 shows the total system cost for each alternative.

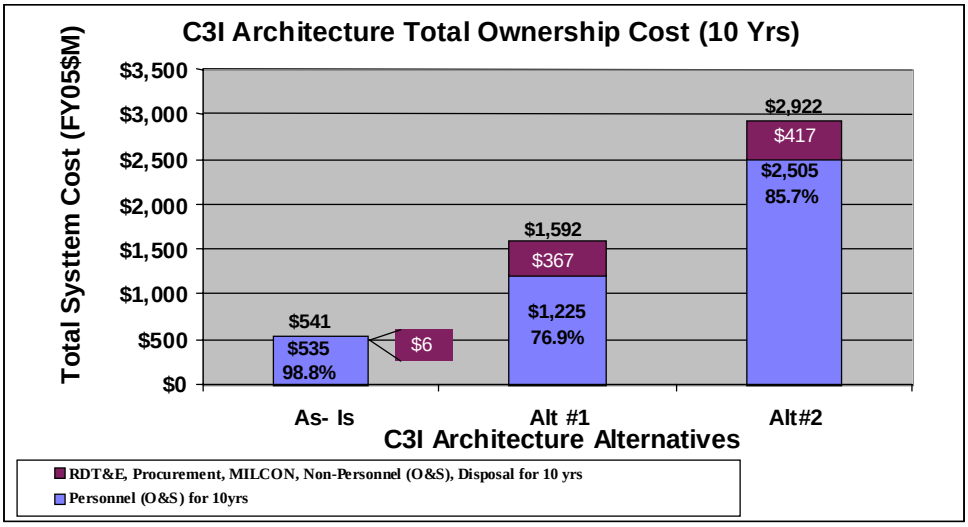

Figure 74. C3I Alternative Systems Total Ownership Cost Comparison

For each of the three C3I design architectures, operating personnel account for the largest contribution to system cost. Although these mission-critical personnel are 77% to 99% of system cost, if was determined that the greatest performance benefit could only be realized through the use of cognitive humans ("Eyeballs and Intellect").

Overall: Figure 75 compares the percentage of "correct" decisions of each alternative from the "Informed Model" with their relative costs.

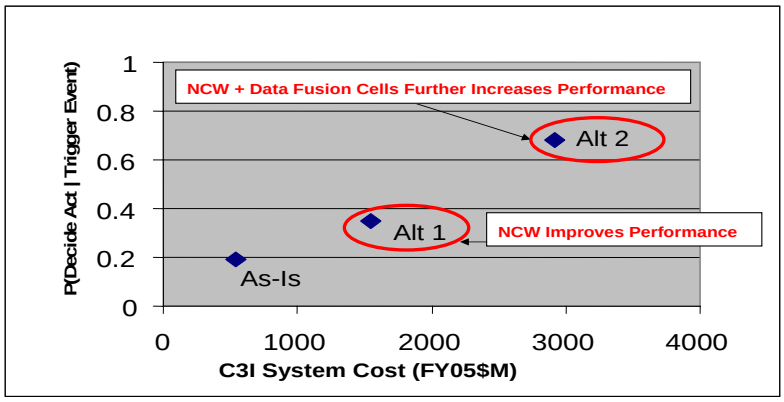

Figure 75. P(Decide Act | Trigger Event) vs. Cost

Only 20% of the "As-Is" System decisions were correct. The presence of a COP in Alternative 1 increased the percentage of correct decisions to 35%. The largest gain came from adding data fusion cells in Alternative 2, but at a cost of $2.9B.

A correct decision was defined as a decision to inspect given there was a WMD onboard, or the decision to engage if the ship displayed anomalous activity of a SAW. The probability of false alarm, i.e., an incorrect decision, for the C3I System was defined as the decision to act in the absence of a trigger event. Figure 76 compares the percentage of incorrect decisions for each alternative and their relative costs.

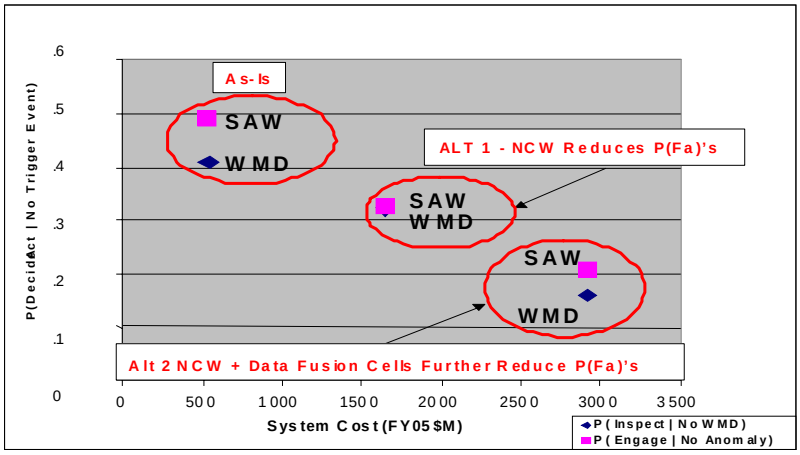

Figure 76. P(Decide Act | No Trigger Event) vs. Cost

The probability of deciding to act given there was no trigger event represents a C3I "false alarm." Relative to an annual traffic density of approximately 59,000 cargo vessels, the "As-Is" System incorrectly identifies 290 SAWs and over 230 vessels carrying WMDs. Alternative 2 reduces this to only 118 SAWs and 95 WMDs, but at a substantial cost.

Figure 77 shows the outputs of the Timeliness Model compared to the C3I "As-Is" and Alternative System costs showed that reduced analysis time increased response time.

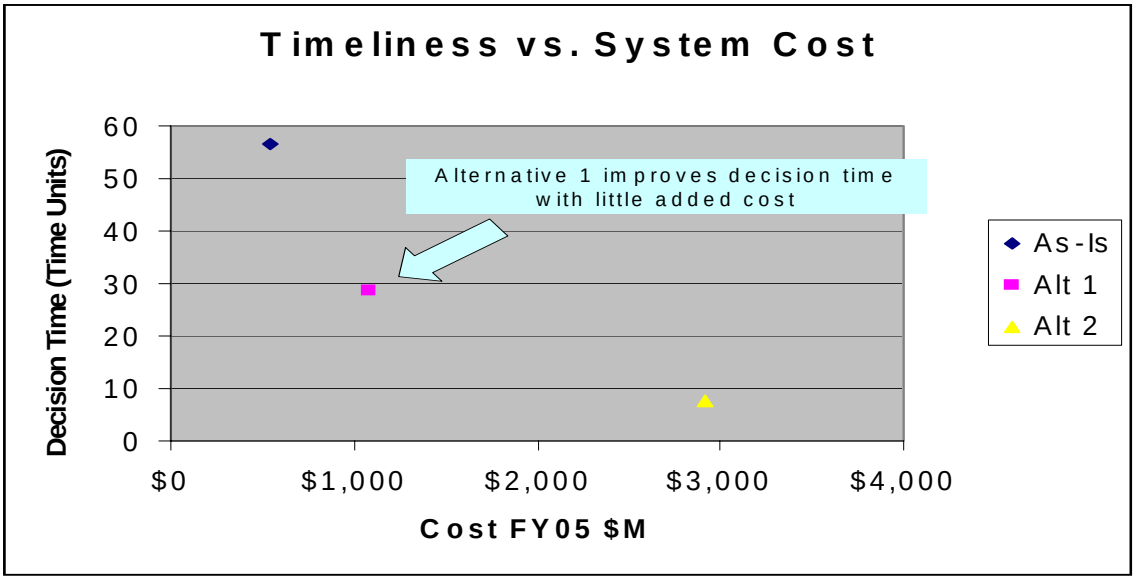

Figure 77. C3I Timeliness Model Performance vs. Cost

This graph shows that the cost of C3I alternatives increases as the performance of the alternatives in the timeliness model improves.

4.2.2 Analysis – C3I Group

The box plots in Figure 78 and Figure 79 display the data from model runs using Minitab 14™, a statistical software application. It indicates Alternative 2 provided the highest probability of making the decision to inspect a vessel if WMDs were onboard.

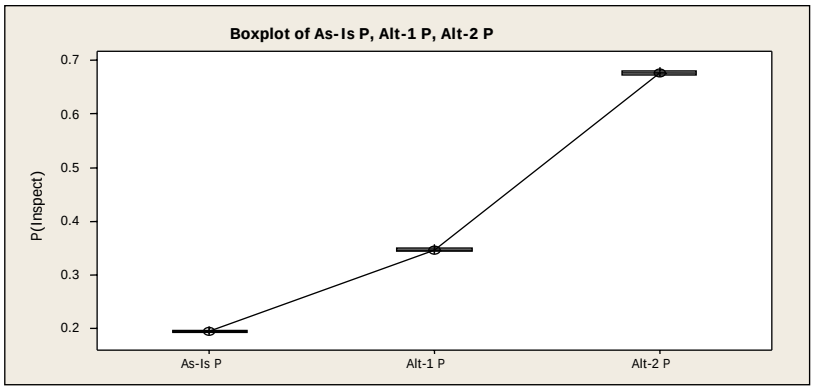

Figure 78. Box plot of Informed Model Outputs for WMD Scenario

As can be seen from the box plot and interval plot for the probability of deciding to inspect, the aggregation of the lateral feed system using Alternative 2 results in the highest probability for deciding to inspect a vessel given WMD is onboard. Furthermore, there is a statistically significant difference between the performance of the "As-Is" System and Alternative 2.

Small standard deviation values result in no overlap between the "As-Is" System and the two alternatives. The three systems are statistically significant given a 95% Confidence Interval (there is a significant difference between the performance values of each system).

SAW Scenario: The box plot in Figure 79 is an analysis of data from Informed Model runs using Minitab 14™. It indicates Alternative 2 provided the highest probability of making the decision to send a reaction force, given that a ship was going to be used as a weapon.

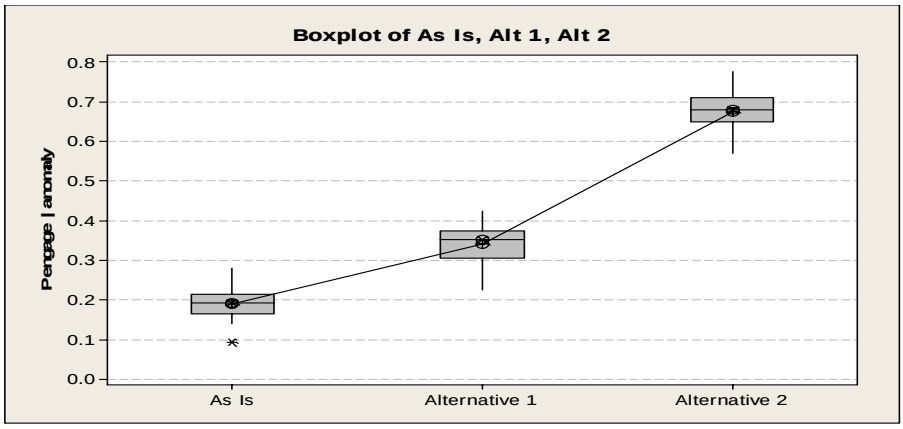

Figure 79. Box plot of Informed Model Outputs for SAW Scenario

As can be seen from the box plot and interval plot for the probability of deciding to send an engagement force, the aggregation of the Lateral feed System using Alternative 2 results in the highest probability for deciding to engage a SAW. Furthermore, there is a statistically significant difference between the performance of the "As-Is" System and Alternative 2.

Timeliness Model: The effect a COP has on analysis time is shown in Figure 80.

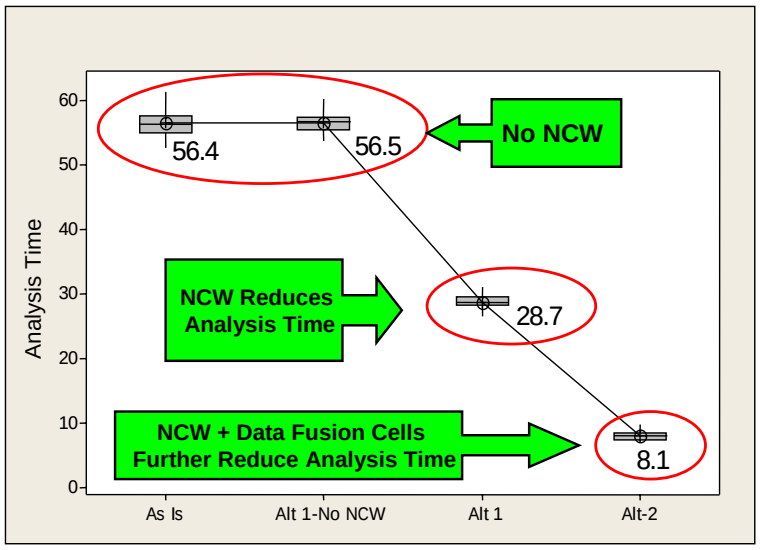

Figure 80. Box Plot of COP Effect on Analysis Time

This plot shows the C3I modeling results, by comparing the analysis times for the different architectures. The COP resulted from the NCW characteristics of the communications network linking the multiple intelligence sources to the C2/Intelligence Centers.

The analysis time of 56.5 in Figure 80 represents Alternative 1 minus a network centric communications architecture and the resultant COP. Simply dividing the AOR into two regions and providing a COP did not reduce analysis time. Alternative Architecture 1, which called for a Communications System that provides a COP, cut analysis time in half to 28.7. The addition of data fusion cells in Alternative 2, which represented dividing the area into more manageable areas for analysis, significantly reduced analysis time.

When the output spreadsheet was examined more closely (see Figure 81), about 1% of all decisions exhibited a phenomenon that was termed "confusion." Confusion occurred when both C2 Centers in the model attempted to access the spreadsheet at the same time for the same contact. For example, C2 Center #1 read a value of "2" and added "1," and C2 Center #2 also read the value of "2," and added "3." In this case, since the operations occurred at the same time, the sum immediately exceeds the logic checks built into the model and the condition for a decision to be reached (the sum of 3-5) never occurs. While an anomaly, this process could indeed occur in the real world in a scenario in which the update rate for the Network Centric System caused two or more C2 Centers to be slightly out of sync.

89	3				3	2.285421	1.282853	
90	3				3	5.651667	7.38458	
91	10	3			13	20.0575	10.48285	91
92	3				3	8.557124	4.28458	
93	4				4	6.29502	6.681799	93

Figure 81. Excel™ Spreadsheet Screen Shot of C3I "Timeliness" Model Output Data

An example of the spreadsheet output for information "confusion." Cell 91 shows a sum of 13, indicating that data for cell 91 was referenced by two C2 Centers simultaneously.

4.3 MODELING AND ANALYSIS – FORCE GROUP

4.3.1 Performance Model – Force Group

Approach: The Force Group's modeling effort was conducted using a split approach. Each of the scenarios was modeled independently, using the modeling software that best fit the scenario. The modeling was undertaken using two primary

groups. The first group consisted of two TDSI Operations Research (OR) students who focused on using Map Aware Non-Automata (MANA) software to model the SBA scenario. The main Force Group modeled the SAW scenario with EXTEND™ software and the WMD scenario using Microsoft EXCEL™.

One of the major drivers for the model construction plan was the fact that the results from the other groups (C2 and Sensors) would not be available until the end of the modeling period. Because of this, the Force Group designed models to run with a wide variety of inputs that would be determined from the outputs of these other group modeling efforts. The Force Group conducted numerous model runs using representative ranges of these inputs, and, when available following individual group modeling, the Force Group selected the modeling runs that corresponded to the outputs from the other MDP Group models.

The OR students evaluated the Force System alternatives against the SBA scenario, using a graduated engagement range scale. Because all of the MDP Group models would need to be integrated, the initial runs were conducted using a graduated scale of engagement ranges, to determine their associated engagement success probability distributions. This translated into a probability of success for an engagement given a set range (or amount of time) for the engagement.

The main Force Group and professionals at TRAC Monterey helped the MANA Group, introducing the MANA software and coordinating the use of the software with the New Zealand Defense Technology Agency proprietors. MANA was designed, in conjunction with Project Albert, to be a Complex Adaptive System model that was an improvement over the existing ISAAC/EINSTein model. It was designed with additional capabilities that allowed better distinctions in force-on-force interactions.[70]

The Force Group modeled the SAW scenario with EXTEND software, to determine the probability of each alternative in successfully neutralizing the SAW threat before it could reach its intended target. This model output was in the probability of

[70] MANA 3 Beta Version, New Zealand Defense Technology Agency, http://nzdf.mil.nz/_mana, 15 May 2005.

defeat of a SAW attack versus engagement time, which was converted into range. This model was run to show both the value of the response force, as well as the importance of the time allowed by C2 for the engagement.

The Force Group modeled the WMD scenario with Micosoft Excel, to determine the time-speed-distance required to deliver an inspection team to a contact of interest (COI) at least 250 NM from the critical area. The model output was simply the time to transport the inspection team from a given base location to a COI.

MOEs: The MOEs that were used by the Force Group were derived from the Force System Objective Hierarchy (see Appendix C). The primary MOEs that were to be estimated by the Force models for the SBA and SAW scenarios were the probability of defeat (Pdef) and range of defeat for each Force System alternative. For the WMD scenario, the MOE was transport time, the time to transport the sea inspection team from a base station to a COI.

Assumptions: One of the first assumptions made by the modeling groups was that of perfect intelligence. It was assumed that the C3I Group would not vector the reaction force onto an inadvertent target, and therefore all tasking was against valid targets. This allowed the Force Group to focus on evaluating the capabilities of alternatives, rather than the probability of false targets being destroyed. Another major assumption was made concerning the sensors associated with the reaction force. It was assumed that if the target was within the range of the onboard sensors, the target would be seen and recognized. This assumption was justified by the fact that the targets in question were often within visual range, and the sensors were mature, reliable technology.

There were several assumptions that were unique to the SBA scenario MANA model. MANA entity characteristics were assigned and maintained as constants throughout all SBA scenario model runs. This allowed the model to display operational performance rather than decision making patterns of the system. Another assumption was that for SBA Alternative 1 (Sparviero Patrol/Escort) the use of Over-The-Horizon Missile Systems would be permitted. While it was recognized that this would not be

tactically sound with current weapon technology, this assumption was made to show the value of extending the engagement envelope beyond traditional line of sight. A third assumption that was made was that the Sea Marshals in the SBA Alternative 2 (Sea Marshal Escort) would be in place prior to the HVU being attacked. This was a realistic assumption because CONOPS have them being loaded onboard the HVU prior to its entry into the critical area. All of the assumptions that were made for the MANA model were maintained throughout all of the modeling runs, and were constant for all of the individual alternatives.

Several of the assumptions for the SAW scenario EXTEND model were the same as those made for the SBA MANA model. The probability of false alarm (Pfa) was precluded, allowing the Force Group to focus on the force interactions rather than the decision-making process. The targets assigned were assumed to be within sensor range. This was a valid assumption because of the close engagement ranges that were being modeled for this scenario. Another assumption was made that the operational availability of the forces would remain constant at 0.9 throughout all model runs. This was done to show the standard performance of the equipment, not a time-scaled degradation of the alternative's performance that required good service practices to maintain the equipment in normal operating mode. Another assumption was made that the engagement boundaries would be set by the geography of the port. This assumption was determined from the specifics of the scenario, and artificially limited the engagement time remaining after detection of hostile intent. Because the SAW attack was not detected until it was already in the Singapore port area, the engagement would not be conducted outside five NM.

Assumptions for the WMD scenario EXTEND model included a constant transportation speed, a calm sea state and good weather, and a compliant boarding.

Inputs: The modeling inputs were also broken out by the model scenario. The three models each had independent inputs, which were derived either from documented sources, like Jane's Fighting Ships,[71] or through interviews with operators. A range of

[71] Jane's Fighting Ships, Jane's Publishing Inc., 4th floor, 115 5th Avenue, New York, NY.

input factors were evaluated in each Force model, which led to the selection of the most advantageous factor values to represent the scenario-specific performance of each Force System alternative. A summary of the input factors and the values selected for each alternative in each scenario is shown in Figure 82.

Force Modeling Factors

Scenario	Factor	Values Evaluated	Values Chosen		
			As-Is	Alt 1	Alt 2
SBA	Probability of Kill Single Engagement (PKSE)	0.3 - 1.0	0	0.8	0.5
	Engagement Range	100m - 50nm	0	9nm/ 50nm	150m
SAW	Sea Marshal Force Exchange Ratio	1.5, 2.0, 2.2, 2.5	2.2	2.2	2.2
	Engagement Range	.5nm - 5nm	5	5	5
	Probability of Kill Single Engagement (PKSE)	.05-.5	0	.25-.5	.5-.95
WMD	WMD Inspection Team Transport Speed	150kts , 46kts	0	150kts	46kts

Figure 82. Force System Modeling Input Factor Variables

This figure shows the variable inputs to the Force System models, along with the values that were selected for each Alternative.

The SBA scenario MANA model was capable of assigning attributes to the individual entities in the model. The blue force and red force entities were the only ones that were modified from the default neutral settings. Constant inputs included the blue force operational availability, red force characteristics, blue force combat capabilities, and blue force location. The blue force entities were given the capabilities associated with the alternative, and then were run against highly hostile red forces that were determined to engage the HVUs. The two major variable factors that were addressed in the SAW model were the probability of kill single engagement (PKSE) and the range of

engagement. The Force modeling factors and the range of values evaluated are shown in Figure 82.

The SAW EXTEND model was constructed to simulate the determination of hostile intent at any distance, and was run at discovery distances from 5 to ½ NM from the port facilities. The primary inputs that were controlled for this model were the combat capabilities of the Sea Marshals ("As-Is" System), of the TDSI transport vessel (Alternative 1), and the Rapid Response Force (Alternative 2). The remainder of the inputs to the model, such as target ship speed, number of terrorists onboard, and location of response vessel, were determined through random number generators based on normal distributions. The treatments that were considered for the SAW model were the force exchange ratio (FER) of the Sea Marshals (number of enemy killed per Sea Marshal), the engagement range, and the single engagement probability of kill (PKSE) for the TDSI transport vessel engagements and the Rapid Response Force engagements, as shown in Figure 83.

The WMD EXCEL model simply used the maximum cruise speed for each alternative mode of transportation. The SH-60B helicopter used in WMD Alternative 1 was assumed to travel at 150 kts, while the Sparviero hydrofoil used in WMD Alternative 2 was assumed to travel at 46 kts.

Flowchart: The SBA and SAW Force models used a similar operational flow path. Because both the SBA and SAW scenarios were essentially force engagements, they could be considered similar problems. The flowcharts assumed that the decision to engage had already been made before the target entered the Force Modeling System. The target was then evaluated, primarily to see if the response forces were available and in range, and then acted on. The results of the action could be a missed target, a deterred target or a defeated target.

Figure 83 shows a nominal data flowchart for the Force models.

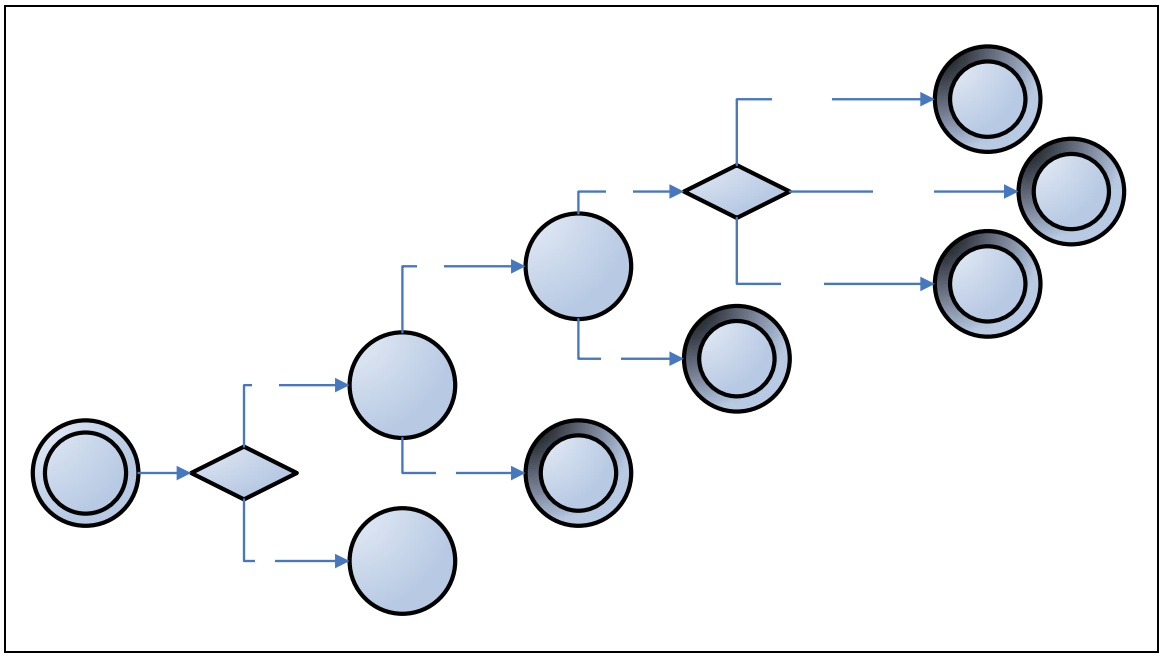

Figure 83. Operational Probability Flowchart for Force Models

This flowchart shows the operational flow through either the SBA or SAW models used by the Force Group. It shows both successful and unsuccessful interceptions, and the necessary steps that must be completed to get to the next stage.

Description: The models used by the Force Group were validated through an in-depth review of the model structure as well as a review of the model results by both the faculty and staff of the NPS and off-campus Special Operations personnel. While the models did not depict the environment and all interactions perfectly, they were a valuable tool for gaining insights into the maritime domain protection problem.

The SBA scenario MANA modeling suite was used to try to capture the behaviors of surface combatants in an engagement; specifically, the actions in a small boat attack As a Complex Adaptive System, MANA was designed to simulate human interactions on the battlefield. The MANA model was designed to look for emerging patterns in engagements and any trends in performance that were differentiated by alternatives. MANA was run 25,000 times for each alternative to determine if there were any underlying patterns that would emerge through statistical analysis.

Yes

The MANA model was used to evaluate both the Sea Marshal alternative (Alternative 2) and the Sparviero patrolling alternative (Alternative 1) for the SBA

Vessel in AOR

Hazard?

scenario. Model runs were performed while varying the single engagement probability of kill (PKSE) and the engagement range to determine the most favorable combination of the two. The MANA model was manipulated to reflect a one, two, and three patrol craft escort pattern. The recorded output for each run included: 1) whether or not the target was neutralized or deterred; 2) the range of neutralization; and 3) the time it took to neutralize the target. This was then used to calculate the average neutralization range for each alternative.

The SAW scenario EXTEND model was used to help identify key performance parameters and applications of the SAW scenario alternatives. The model was constructed to be capable of depicting the two alternatives and the "As-Is" System with only minor modifications. Initially, Sea Marshal performance was run against variable numbers of terrorists and variable amounts of time to retake the ship. The next set of runs was for Alternative 2, which incorporated the use of a helicopter delivered Rapid Response Force team to retake the vessel. The final set of runs evaluated the Sparviero patrol craft operating as a harbor patrol boat (Alternative 1). In all SAW model runs, the ship speed was determined by a uniform random number between 7 kts and 20 kts. This resulted in an average of 13½ kts, giving a mean time of 22 minutes between the detection of hostile intent and pier impact.

These runs allowed the Force Group to explore not only the force exchange ratio (FER) of the Sea Marshals, but also the PKSE of the patrol craft and the Rapid Response Force team. This data was then compiled and used to determine the Force alternative capabilities.

The WMD scenario EXCEL model was a very simple time-speed-distance calculation. The distance was determined to a COI located 250 NM from the critical area. Speed was a result of the transport vehicle, either helicopter or Sparviero hydrofoil.

4.3.1.1 Results

Small Boat Attack (SBA) Scenario: Figure 84 graphically depicts the performance (measured as probability of defeat) of the different Force alternatives against the SBA scenario.

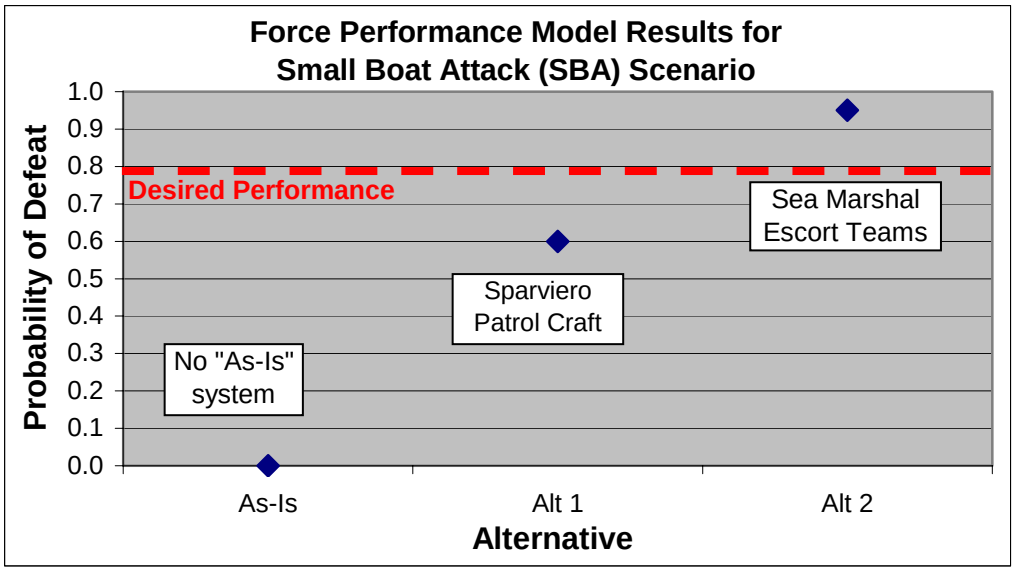

Figure 84. Force Performance Model Results Comparison of Alternatives for SBA Scenario

The Force Group model results for the SBA scenario show that the Sea Marshal Escort team was the most effective alternative, followed closely by the Sparviero patrol craft used as a convoy escort.

2005 "As-Is" Capability - None. There was no "As-Is" Force System for the SBA scenario, thus it was assessed that attacks of these types would not be defeated by the MDP System.

Alternative 1 – Sparviero Patrol Craft. The MANA model results showed that six Sparvieros in a patrolling role, which included the ROE to engage at 50 NM, generated only a 60% success rate against the SBA. The six Sparvieros were divided into two three-ship patrols, each responsible for one-half of the critical area of the Straits.

Alternative 2 – Sea Marshal Team. The MANA model showed excellent performance of the Sea Marshal Escort team at ranges outside of 100m (see Figure 85). If the ROE was in place for the Sea Marshals to engage the SBA at 150m, there was a 92.5% defeat rate outside of the 65-meter minimal damage range, and a 95% defeat rate outside of the 35-meter hull breach range. This capability was based on the knowledge of the SBA intent, and the permission to engage the SBA at 150m.

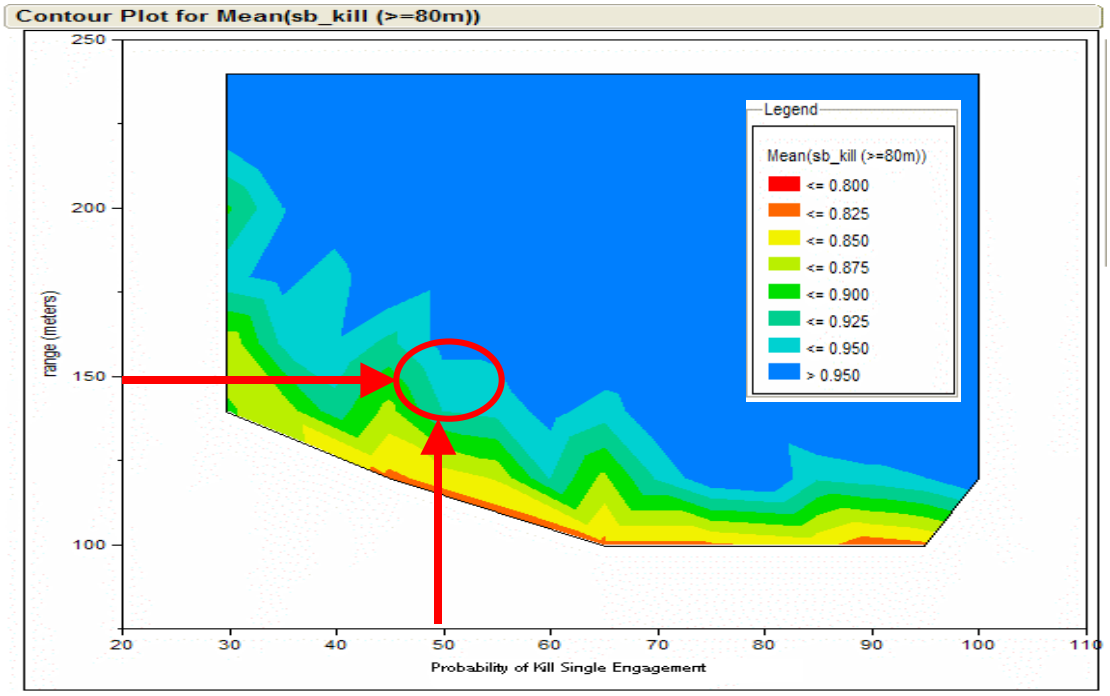

Figure 85. Force Model Results for Sea Marshal Escort in SBA Scenario

This figure shows the overall probability of kill that modeling determined for various engagement ranges and single engagement probabilities of kill (PKSE). This information was used to determine the required engagement range for a given PKSE and a desired overall probability of kill.

4.3.1.2 Ship As a Weapon Scenario

Figure 86 graphically depicts the performance (measured as probability of defeat) of the different Force alternatives against the SAW scenario.

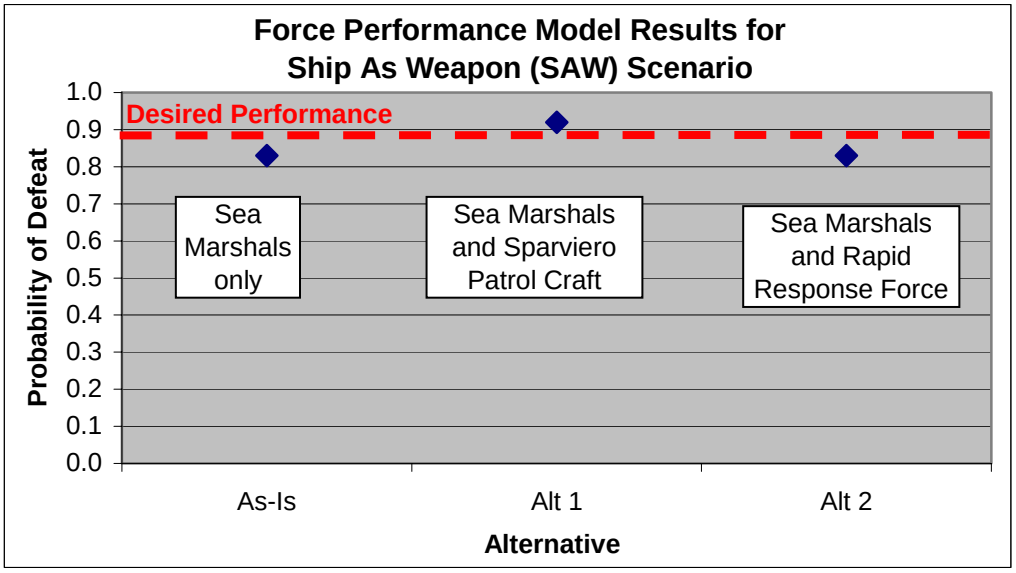

Figure 86. Force Performance Model Results Comparison of Alternatives for SAW Scenario

The Force Group model results for the SAW scenario show that the "As-Is" Sea Marshal team was the most effective, and could be improved by adding the Sparviero patrol craft. The Rapid Response Force showed no improvement over the existing system due to the limited response time to respond available in the SAW scenario description.

2005 "As-Is" Capability – Sea Marshals. Model results for the "As-Is" Force alternative showed that Sea Marshals on all HVUs entering Singaporean ports accounted for an 83% probability of defeat. This was under the assumption that the Sea Marshals would be loaded onboard the vessel at five NM with the harbor pilot, and each Sea Marshal was capable of a 2.2 Force Engagement Ratio (FER) (each Sea Marshal was capable of successfully defeating 2.2 terrorists).

Alternative 1 – Patrol Craft. With the addition of Sparviero patrol craft to counter the SAW threat by launching disabling fire at the incoming SAW vessel's propulsion and steering if the Sea Marshals were unsuccessful, the probability of defeat increased to 92%. The onboard Sea Marshals maintained their 2.2 FER proficiency.

Alternative 2 – Rapid Response Force. The addition of a helicopter-lifted assault team to aid the Sea Marshals in retaking the SAW vessel did not improve the probability of defeat. There were no successful helicopter interventions for the SAW model runs, but only because of the scenario limitations, which gave an average

of 22 minutes between the detection of hostile intent and pier impact. The scenario did not allow sufficient time, approximately one hour, to engage the helicopter and equip, brief, and transport the assault team to the SAW vessel. There were no successful helicopter interventions until the SAW vessel was identified outside of seven NM from Singapore.

4.3.1.3 WMD Scenario

2005 "As-Is" Capability - None. There were no "As-Is" Force transport capabilities since there was no "As-Is" Sea Inspection capability for the WMD scenario (see Figure 87).

Alternative 1 – Helicopter Transport. The use of SH-60B helicopters to lift the 12-man inspection teams allowed for not only a relatively short intervention time (just over 1½ hours), but also the staging of forces in a centralized location. This allowed for easier team rotation plans, as well as ease of repair for equipment needed by the inspection teams.

Alternative 2 – Patrol Craft Transport. Using the Sparviero hydrofoil as a high speed transport vessel, inspection teams could be ferried to COIs in 1½ hours (see Figure 87). In order to make this transport time, forward-located base stations were required.

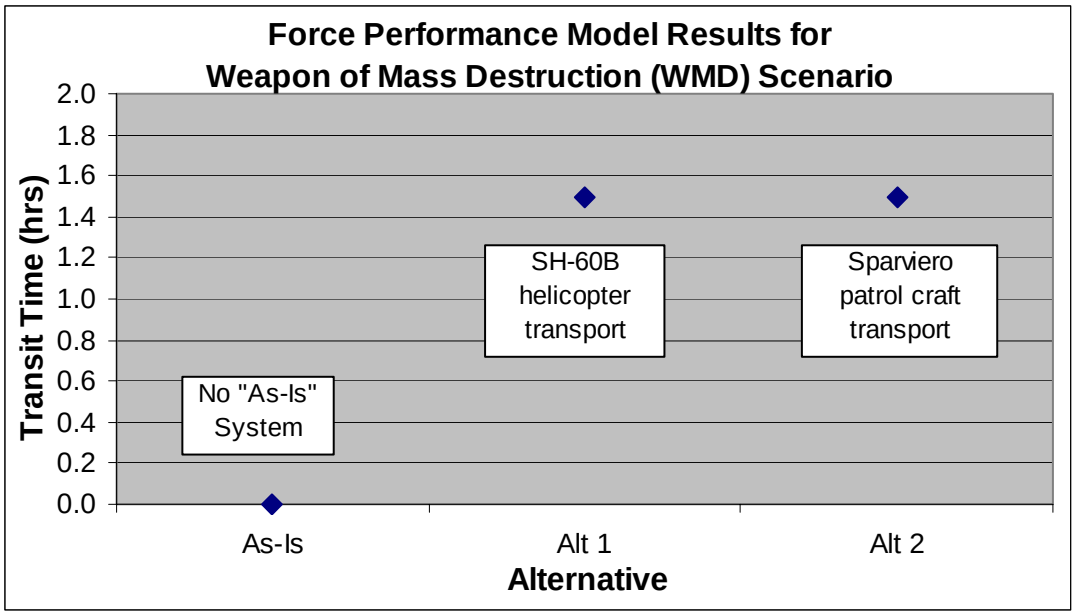

Figure 87. Force Performance Model Results Comparison of Alternatives for WMD Scenario

The Force Group model results for the WMD scenario show that, in order to transport the Sea Inspection team to a contact of interest at 250 NM from the critical area, helicopters and patrol craft alternatives were equally effective.

4.3.2 System Cost Model – Force Group

Approach: In order to translate the Force Group functional requirements into budget requirements, economic analysis used current data when possible, but primarily relied on historical data. Individual costs estimates were determined for each of the largest components of the Force System alternatives, which were combined to give a realistic view of the likely system cost.

The analogy methodology was used to find the O&S cost for the HSV-X1 and the Sparviero ships, quantifying relevant cost that should be incurred by those ships (subsystems) under the O&S conditions specified for the system (if assumptions regarding operating conditions changed, the cost reflected those changes). Extrapolation from actual was used to determine the O&S cost for the SH-60B helicopter and the annual cost of the Interdiction/Inspection teams.

MOEs: The MOE for all scenario alternatives was the MDP System Cost: the ten-year Procurement and O&S cost of the MDP System. There were no Commercial System or Delay costs associated with the Force System.

Assumptions: O&S for the HSV-X1 was found using the analogy method, using the O&S cost data for the MCM-1CL "Avenger."[72] The HSV-X1 was a new commercially developed ship (the first one was delivered to the U.S. Navy in August 2003), so O&S data was not yet available. The MCM-1 was chosen because of the similarities shown in Table 22.

	MCM-1CL	HSV-X1
Tonnage	1,312 T	1,102 T
Diesel Engines	4	4
Length	224 feet	321 feet
Draft	15 feet	12 feet

Table 22. Comparison of MCM "Avenger" to the High Speed Vessel (HSV)

The MCM "Avenger" was very similar to the HSV. Because of these similarities, O&S costs for the MCM were used as an analogy for the costs of the HSV.

O&S for the Sparviero was found using the analogy method, with the provided data for the PHM-1CL "Pegasus."[73] The PHM-1 is no longer in U.S. Navy service, but it was the closest (because of the characteristics: Hydrofoil, aluminum hull, small combat craft, small crew) to the Sparviero.

In the development of the personnel cost estimation, given the wide spectra of designators for military personnel, Navy and Marine Officers (O03), and Navy and Marine Enlisted (E06) were chosen as personnel employed for inspections/interdiction. The following are the characteristics that each one needed to fulfill the system's scenario requirements.

Navy Officer: Additional qualification QC1 (SEAL-qualified, fleet experience).

Marine Officer: Parachutist and Combat Diver.

---

[72] Sharpe, Richard, Captain, Royal Navy, Jane's Fighting Ships, 91st ed., 1988-89, Jane's Information Group Inc., 1340 Braddock Place, Suite 300, Alexandria, VA, p. 752.

[73] Ibid, p. 754.

Navy Enlisted: E6, General Duty, and Operations Specialist.

Marine Enlisted: E6, Infantry Assault, Parachutist and Combatant Diver.

Inputs: The inputs for the Force alternative cost model came from a number of sources. The procurement cost for the HSV-X1 came from the Marine Corps Combat Development Command.[74] For the O&S cost, the data came from the Navy Visibility and Management of Operating and Support Costs (VAMOSC) database;[75] and was provided by the Business Consulting Services Department. These include O&S data for the SH-60B helicopter, and Navy and Marine personnel cost elements. They also provided the O&S data for the MCM-1CL "Avenger," and the PHM-1CL "Pegasus," used in the analogy with the HSV-X1 and the Sparviero ships.

Description: In order to get the better cost estimation, given the different subsystems, the components' costs were statistically summed to derive the total system cost, instead of adding the best "guesses" for each component. Each of the components were quantified in terms of their statistical properties (mean, standard deviation, range, most likely, highest, lowest, etc.), and a Monte Carlo simulation was performed, varying each element in accordance with its statistical properties. A cost probability distribution was developed for each of the components.

Results

SBA Scenario: The resultant costs of the major components for the alternatives for the SBA scenario are shown in Table 23. A graphical depiction of the total expected costs for each alternative is shown in Figure 88.

[74] Marine Corps Combat Development Command, https://www.mccdc.usmc.mil/, (accessed 15 May 2005).

[75] Navy Visibility and Management of Operating and Support Costs, http://www.navyvamosc.com/, (accessed 10 May 2005).

	"As-Is"	Alternative 1			Alternative 2
	N/A	1 HSV-X1	9 Sparviero Patrol Craft	Total	85 Sea Marshals
High	**N/A**	301.4	937.6	**1,239.0**	**280.8**
Expected	**N/A**	263.2	657.9	**921.1**	**257.8**
Low	**N/A**	225.4	377.3	**602.7**	**240.1**

95% Confidence Interval
All in FY05$M
N/A = Not Applicable.

Table 23. Alternative Component Costs and 95% Confidence Interval for the SBA Scenario

The Force cost model results gave the expected value for the major components of each alternative and the high and low values for the 95% confidence interval.

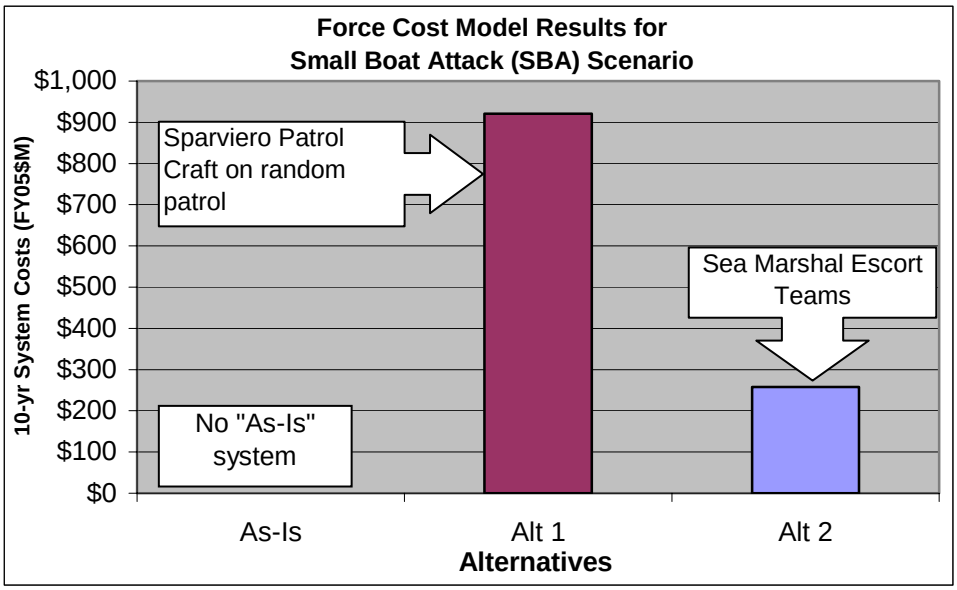

Figure 88. Force Cost Model Results Comparison of Alternatives for SBA Scenario

The Force Group cost model results for the SBA scenario show that the Sparviero patrol craft (Alternative 1) was the most expensive. The Sea Marshal Escorts (Alternative 2) were less than one-tenth as costly.

SAW Scenario: The resultant costs of the major components for the alternatives for the Small Boat Attack scenario are shown in Table 24. A graphical depiction of the total expected costs for each alternative is shown in Figure 89.

	"As-Is"	Alternative 1			Alternative 2			
	48 Sea Marshals	48 Sea Marshals	4 Sparviero Patrol Craft	Total	48 Sea Marshals	3 SH-60B Helicopters	36 Rapid Response Forces	Total
High	**34.8**	34.8	167.7	**237.3**	34.8	85.2	30.1	**150.1**
Expected	**37.6**	37.6	292.4	**367.6**	37.6	96.9	27.3	**161.8**
Low	**40.2**	40.2	416.7	**497.1**	40.2	108.6	24.4	**173.2**

95% Confidence Interval
All in FY05$M

Table 24. Alternative Component Costs and 95% Confidence Interval for the SAW Scenario

The Force cost model results gave the expected value for the major components of each alternative and the high and low values for the 95% confidence interval.

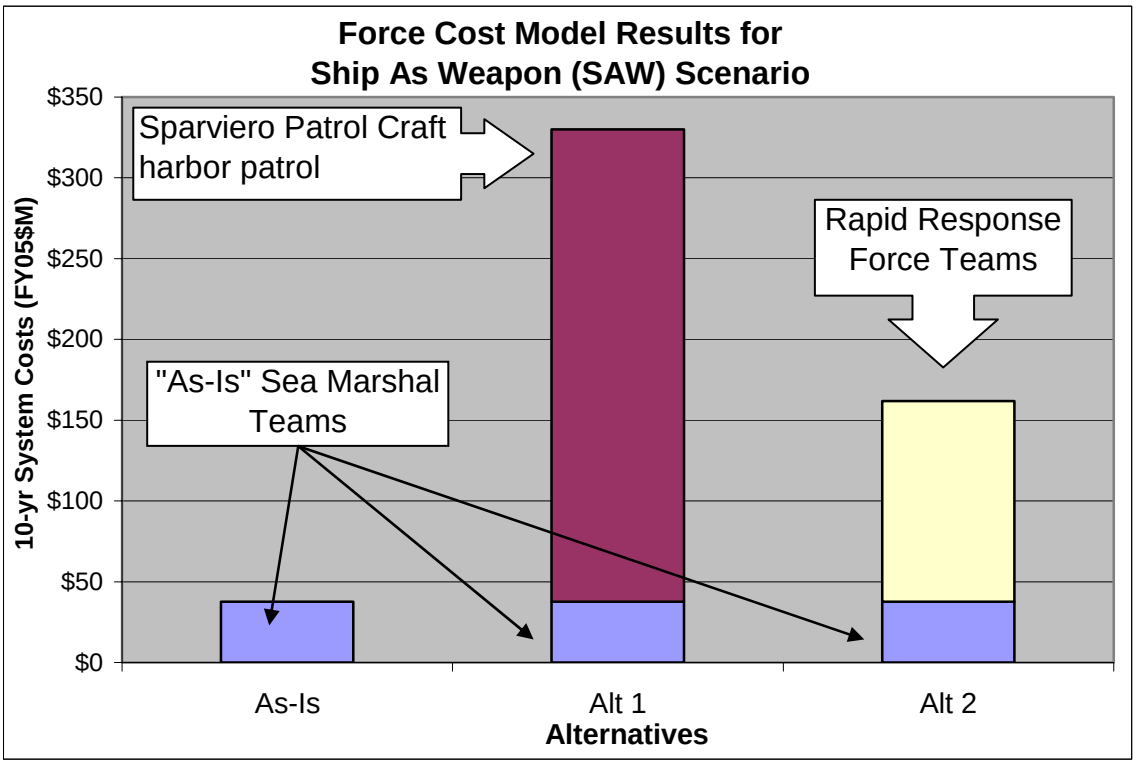

Figure 89. Force Cost Model Results Comparison of Alternatives for SAW Scenario

The Force Group cost model results for the SBA scenario show that the Sparviero patrol craft (Alternative 1) was the most expensive. The Rapid Response Force Teams (Alternative 2) added cost to the "As-Is" System, but were approximately half as costly as Alternative 1.

WMD Scenario: The resultant costs of the major components for the alternatives for the SBA scenario are shown in Table 25. A graphical depiction of the total expected costs for each alternative is shown in Figure 90.

	"As-Is"	Alternative 1			Alternative 2		
	N/A	4 SH-60B Helicopters	36 Sea Inspectors	Total	6 Sparviero Patrol Craft	36 Sea Inspectors	Total
High	**N/A**	144.8	30.1	**174.9**	715.6	90.5	**806.1**
Expected	**N/A**	129.2	27.3	**156.5**	520.5	81.9	**602.4**
Low	**N/A**	113.6	24.4	**138.0**	324.8	73.3	**398.1**

95% Confidence Interval
All in FY05$M
N/A = Not Applicable.

Table 25. Alternative Component Costs and 95% Confidence Interval for WMD Scenario

The Force cost model results gave the expected value for the major components of each alternative and the high and low values for the 95% confidence interval.

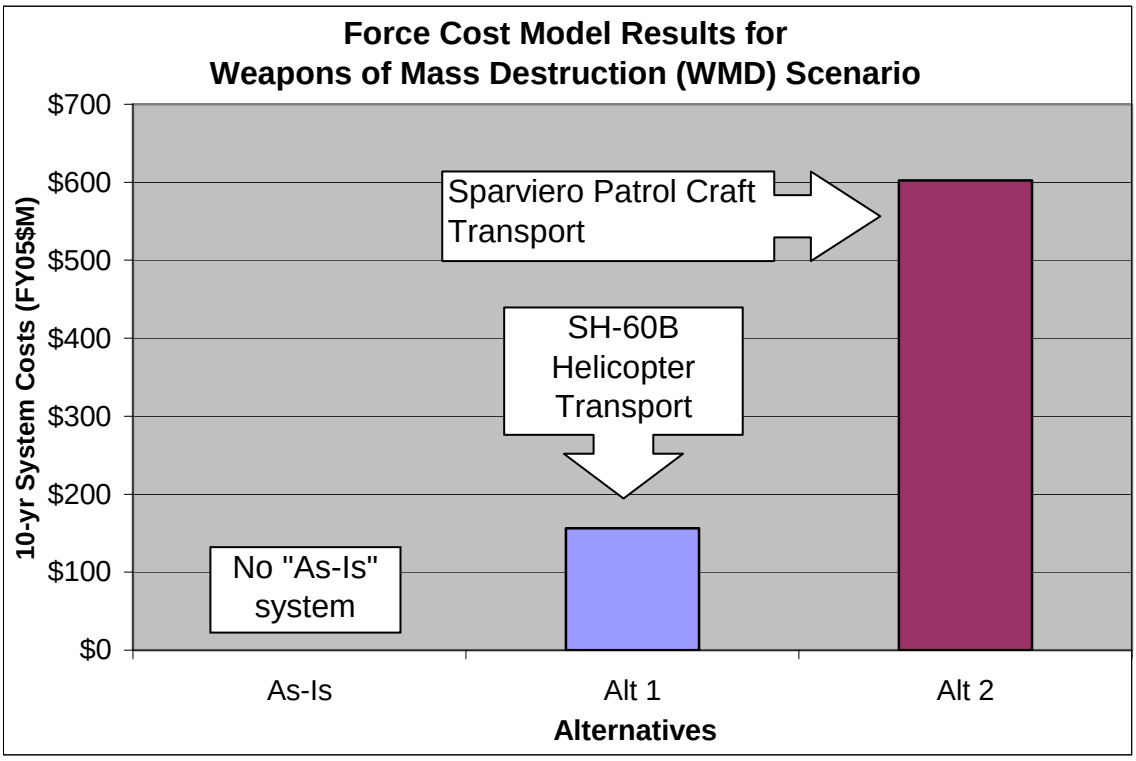

Figure 90. Force Cost Model Results Comparison of Alternatives for the WMD Scenario

The Force Group cost model results for the SBA scenario show that the Sparviero patrol craft transport (Alternative 2) was the most expensive. The SH-60B helicopter transport (Alternative 2) was approximately one-fourth as costly as Alternative 1.

4.3.3 Analysis – Force Group

The Analysis of the Force alternatives was done by plotting a benefit versus cost graph for the alternatives in each threat scenario. This methodology allowed the end

user to be able to graphically see the relationship between the different alternatives, and provided the leeway to select the option best suited to budgetary considerations.

Small Boat Attack Scenario: Figure 91 shows the performance of the Force alternatives with respect to their costs against the SBA threat. The Alternative 2 Sea Marshal Escort teams were over 90% effective, at a relatively low cost (around $250M over ten years). The Alternative 1 Sparviero Patrol Craft did not meet the desired performance, and had a ten-year system cost of almost $1B. Thus, Sea Marshal Escort Teams offered a cost-effective defense against the SBA threat.

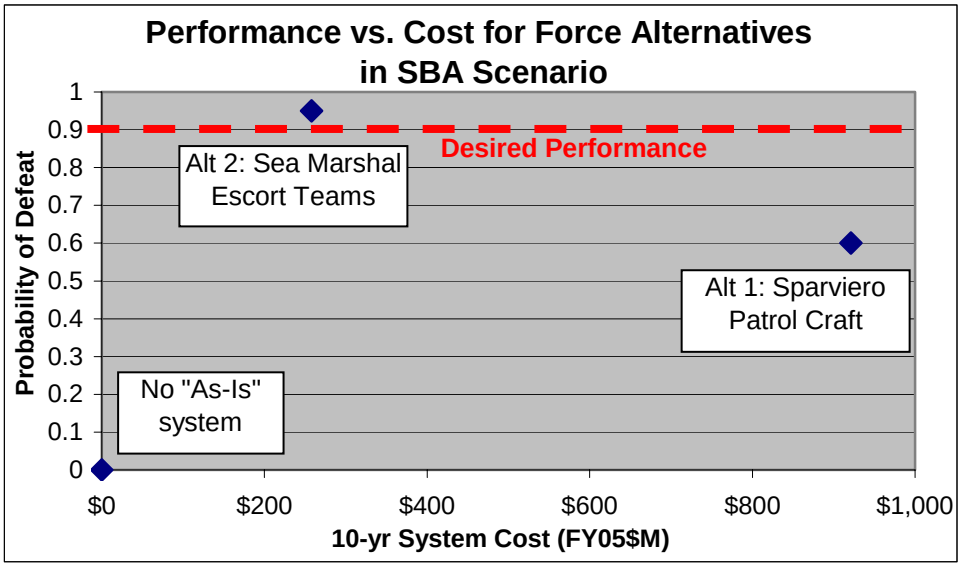

Figure 91. Performance vs. Cost for Force Alternatives in SBA Scenario

This graph shows the relative performance of each Force alternative with respect to the associated cost.

SAW Scenario: Figure 92 shows the performance of the Force alternatives with respect to their costs against the SAW threat. The "As-Is" Sea Marshal System was fairly effective, at a ten-year system cost of less than $50M. Although the Alternative 2 Rapid Response Force was found to cost almost four times more than the "As-Is" System, while giving no performance gain, the results garnished from the SAW scenario modeling were slightly biased due to the scenario limiting operations to within the harbor boundaries. Despite this artificial limit, this alternative was considered viable, and should remain within the system to counter longer lead-time threats. The

Alternative 1 Sparviero craft on harbor patrol did improve performance to over 90% probability of defeat, but at a ten-year system cost of almost $350M.

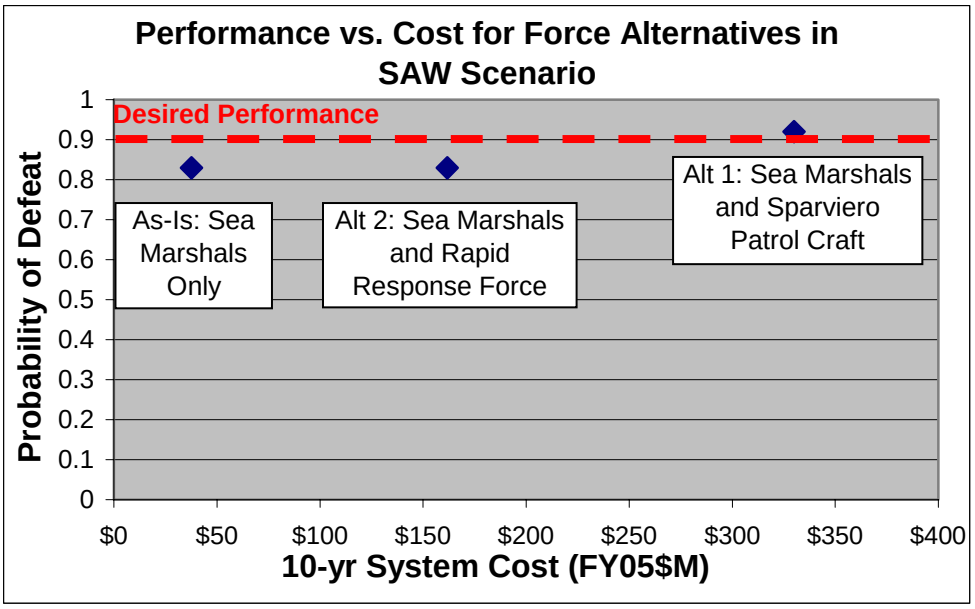

Figure 92. Performance vs. Cost for Force Alternatives in the SAW Scenario

This graph shows the relative performance of each Force alternative with respect to the associated cost.

WMD Scenario: Figure 93 shows the performance of the Force alternatives with respect to their costs in the WMD scenario. Both the Alternative 1 helicopter transport and the Alternative 2 Sparviero Patrol Craft transport transported the Sea Inspection teams to the 250 NM intercept point in 1½ hours. However, the Alternative 1 helicopters performed this task at a ten-year system cost of less than $200M, while the Alternative 2 Sparviero Patrol Craft cost over $600M.

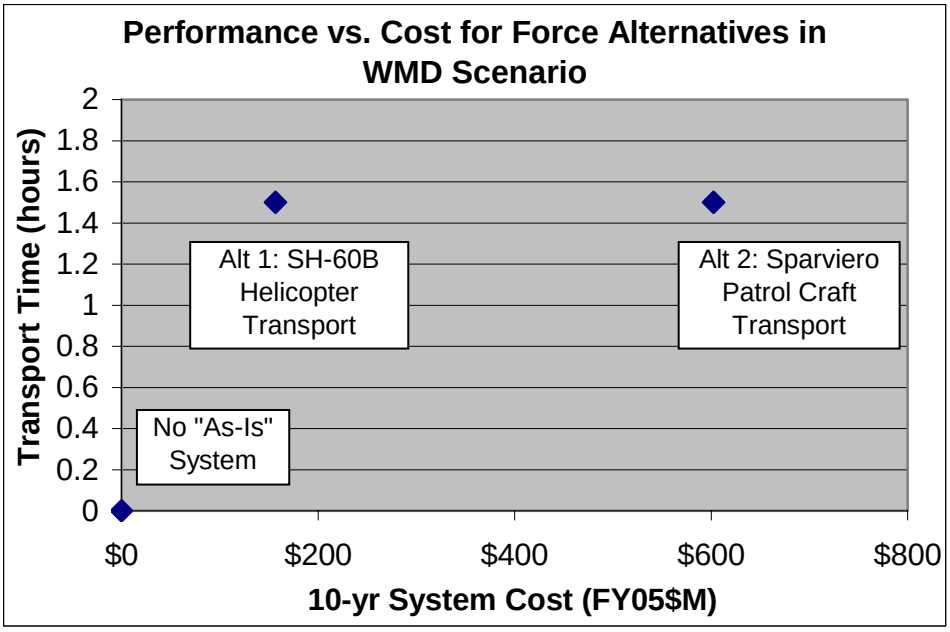

Figure 93. Performance vs. Cost for Force Alternatives in SAW Scenario

This graph demonstrates that the performance of the two Force alternatives is identical, with widely differing costs.

4.4 MODELING AND ANALYSIS – LAND INSPECTION GROUP

4.4.1 Performance Model

Approach: The Land Inspection System Team utilized EXTEND version 6.0 in order to create an interactive, dynamic process model to represent both the current "As-Is" Cargo Inspection System and the proposed improved alternatives for the Port of Singapore. Because of inherent differences in the processes, the "As-Is" System and the two alternatives were modeled as three similar, but distinct, Extend models. The two alternative models had similar architectures, but different inspection methodologies.

Measures of Effectiveness/Metrics: All of the models were designed to measure the effectiveness of the system and implications in terms of commercial impact/delay cost. System cost was tied to the alternative architectures, but was calculated separately from the model runs. The system performance MOE was "the probability that the system defeats an attack" (P_{def}). "Defeat an attack" was defined as the system discovered and quarantined a cargo container containing a nuclear weapon. This will be referred to as P_{def}. The commercial impact/delay cost metric is based on the amount of time a container

is delayed within the system because of a false alarm or search queue, and will be referred to as delay cost. A false alarm was defined as any time a sensor in the system alerted the presence of a nuclear weapon when there was not one present.

Assumptions: The assumptions made for the models were two-fold. First, assumptions were made to ensure the models were a valid representation of the current and envisioned alternative systems. Secondly, assumptions were required to ensure the model results would allow for comparison of the required performance and cost metrics.

The overarching assumption was that the model simulated the Inspection System at the Port of Singapore. The varying traffic volume and cargo types associated with the port's five large terminals were represented in the model as a single composite entity. Next, the throughput of the port was simplified based on the Free Trade Zone (FTZ) research compiled during the problem definition and alternatives generation phase. As stated in previous sections, because of Singapore's role as an international hub and cargo transfer port, most of the cargo container traffic throughput goes through customs-exempt FTZs, while a small amount enters and exits the port into Singapore proper. Our models assumed imports to Singapore accounting for 10% of daily throughput, and daily exports of 5%.

The 2004 port statistics, provided by the Maritime and Port Authority of Singapore[76] (MPA), were the baseline throughput used in the model. At 21.34 million Twenty Feet Equivalent Units (TEUs) through per year, volume alone exemplified the challenge of cargo security. This was a common baseline for both the Land Systems and Sea Inspection Groups. All assumptions for the port capabilities, such as number of cranes, number of container movers, and number of operating terminals were also based on the 2004 port statistics provided by the MPA.

Additionally, common sensor assumptions were created to facilitate accurate alternative scoring and comparison. Due to a wide variation in sensor technologies and their respective capabilities and performance, a simplified and common sensor capability

[76] Singapore Maritime Port Authority, *Total Container Throughput*, http://www.mpa.gov.sg/infocentre/pdfs/container-throughput.pdf, (accessed 10 May 2005).

was assumed. For the "As-Is" System, an optimistic, best-case sensor probability of detection (P_d) of 0.99 was assumed. The probability of detection was defined as the chance an inspection will discover a nuclear weapon if it is present. The small amount of cargo inspected and sensors used allow for thorough and intrusive inspections. If a container was searched, it was previously classified "suspect" and the inspection would lead to discovery of an intended weapon if it was present.

The overarching assumptions were consistent for all three models. The "As-Is" System-specific assumptions are based on Port of Singapore operations in 2004. The pivotal "As-Is" assumption was the method and percentage of cargo inspected by the system. Besides the inspections done by Singapore Customs on the imports and exports of Singapore (which was previously stated as a negligible amount of cargo), the only container security procedures in place are by a team of six U.S. Customs and Border Patrol (CBP) agents stationed at the Port of Singapore.[77] Their job is to identify cargo that is U.S.-bound, and inspect 100% of cargo identified as suspect. The number of U.S. CBP inspectors was modeled at six. Throughput statistics from 2002 and 2004 were assumed still valid for the model. Using these statistics, the number leaving annually from the port that were U.S.-bound was 330,000 TEUs.[78] Of these U.S.-bound containers, 6% were considered "suspect" and therefore inspected by the CBP team.[79]

For the Alternative 1 and Alternative 2 models, the common alternative-specific assumption were that there was a 50% daily split between cargo destinations: half of the cargo was assumed transferred from pier side to the FTZ storage zones, and the other half was assumed to be "daily turn-around" cargo that was quick-on/quick-off transshipment cargo. The amount of cargo leaving and entering via Singapore proper followed the same

77 U.S. Customs and Border Protection, "Fact Sheet," Cargo Container Security, http://www.customs.gov/xp/cgov/newsroom/fact_sheets/factsheet_container_security.xml, (accessed 10 May 2005).

78 U.S.Customs and Border Protection, "Singapore, the World's Busiest Seaport, Implements the Container Security Initiative and Begins to Target and Pre-Screen Cargo Destined for U.S.," http://www.customs.gov/xp/cgov/newsroom/press_releases/archives/cbp_press_releases/032003/03172003.xml, (accessed 10 May 2005).

79 U.S. Customs and Border Protection, "Fact Sheet," Cargo Container Security, http://www.customs.gov/xp/cgov/newsroom/fact_sheets/factsheet_container_security.xml, (accessed 10 May 2005).

percentage assumptions as the "As-Is" model. Additionally, the alternative models assumed a constant P_d for the for the passive and active system sensors.

The main difference between the two alternatives was the in-storage inspection scheme. For Alternative 1, the port-centric model seen in Figure 94, no intelligence or prescreening information was considered to decide if a stored container should be searched. All containers therefore had an equal chance to be searched. For Alternative 2, the trusted agent model seen in Figure 95, a container had a 2% to 3% chance of being randomly selected for search, and was inspected based on one the following three factors:

1. Was the container seal intact or had the seal been tampered with?
2. Did the container come from a certified shipper?
3. Was there a discrepancy on the electronic manifest?

The assumed values for these factors come from Wein, Wilkens, Baveja, and Flynn, and are as follows: 95% of containers are assumed properly sealed, 95% are assumed from certified shippers, and 95% of manifests are assumed discrepancy free.[80] The delay cost baseline was common between the two alternative architectures, and is discussed in depth in the follow-on "Individual Container Delay Cost Model."

[80] Alex Wilkens, Mena Baveja, and Steven Flynn, "Preventing the Importation of Illicit Nuclear Materials in Shipping Containers," http://www.gsb.stanford.edu/facseminars/events/oit/pdfs/Abstract.pdf, (accessed 15 March 2005).

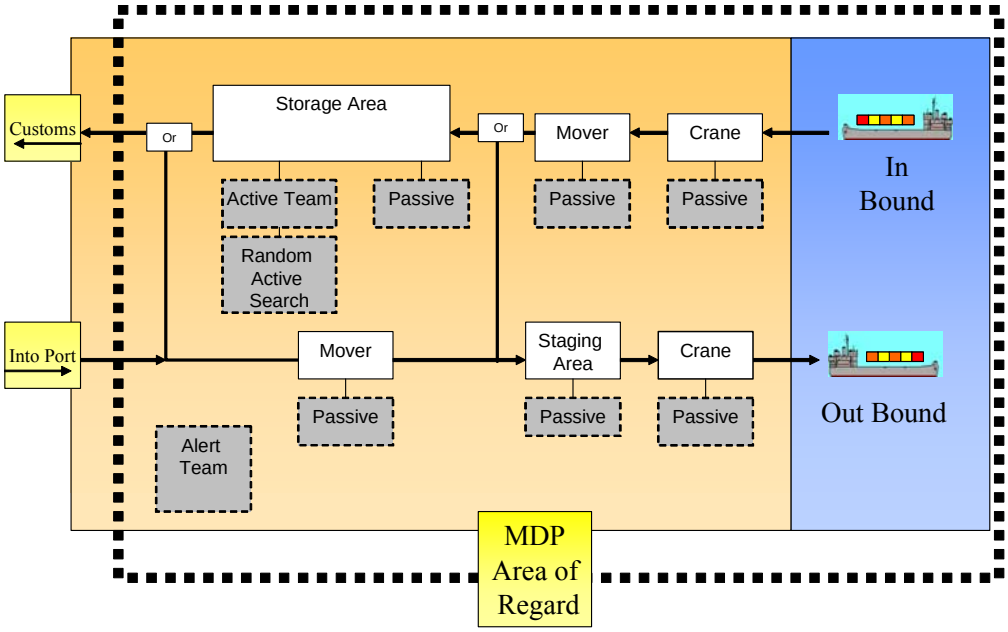

Figure 94. Alternative 1 Model Diagram

Alternative 1 establishes a network of sensors as a comprehensive in-port inspection system including as-is system sensors as well as new Sensor Systems and alert teams in order to achieve a higher Pd. Sensor placement is at the entrance and exit of ports, on cranes, movers, and storage areas.

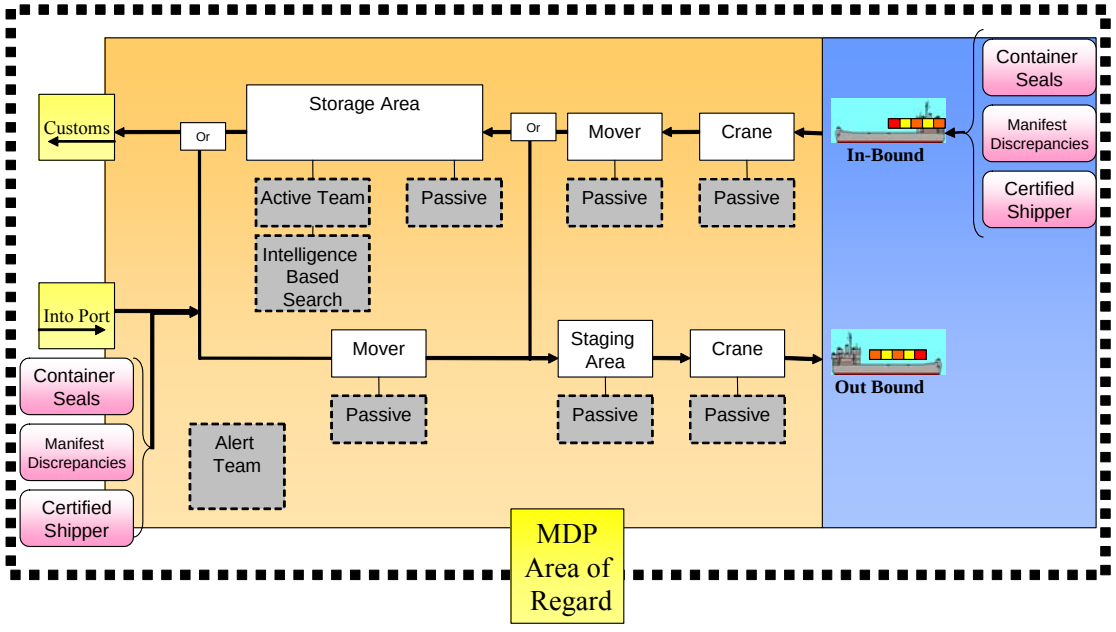

Figure 95. Alternative 2 Model Diagram

Alternative 2 follows the same process as Alternative 1. Additionally, Alternative 2 includes an intelligence-based search.

Inputs: The inputs for both the "As-Is" and Alternative performance models, the system's P_{def} was the conditional probability that, given there was an attack, the system would defeat it. To model "given an attack," all cargo containers sent through the model port contained nuclear material. The number of containers discovered by the inspection regimen in the model containing nuclear material represented the number defeated. Delay cost due to false alarms was not calculated in the performance model.

When measuring the delay cost portion of the performance models, the system's ten-year commercial impact cost was determined by sending every container through with no WMD material onboard, "given no attack," to measure the number of false alarms produced by the system. These false alarms then create a delay time for each container, based on the number of sensor teams used to scan containers that were detected by the passive system.

In addition to the assumed sensor values from the "Assumptions" portion, there are several architecture-specific input values that were varied. After optimization, pair-wise comparisons, and analysis of interactions, the sensor characteristics and number of teams were selected for each alternative. Table 26 summarizes the values evaluated and chosen for inputs.

Factors	Values Evaluated	"As-Is"	Alt 1	Alt 2
Number of Sensors	2 to 100	5	50	50
Active P(detection)	.3, .4, .5, .6, .85, .99	0.99	0.85	0.85
Active P(false alarm)	0.01	0.01	0.01	0.01
Passive P(detection)	.1, .6	0	0.6	0.6
Passive P(false alarm)	.01, .15	0	0.01	0.01

Table 26. Land Inspection System Variable Values

This table represents the values used in evaluating the system alternatives and their respective outputs from the model.

Flowchart: Figure 96 is a representation of the logic used to decide which containers are inspected in the current system. This logic was used in the model to determine the probability of detection of a nuclear weapon. After a container entered port, it was either sent to storage or not, classified "suspect" or not, and finally inspected.

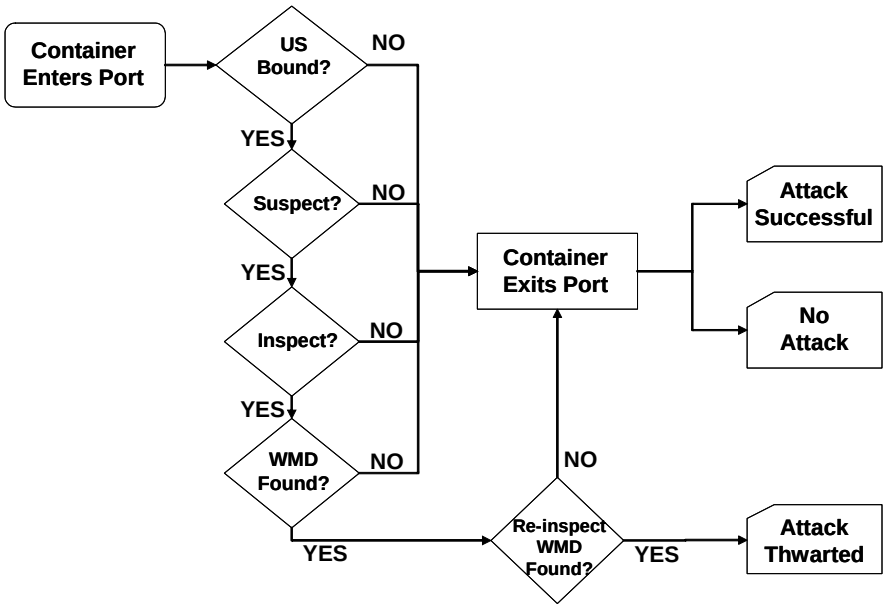

Figure 96. "Current" Model Flow Chart

"As-Is" System follows a sequential questioning process in order to find contraband in containers. As a result, there are three possible outcomes of that process.

Description: The three models are designed to represent a systems-level view of a single day in the Port of Singapore. Daily performance values were then extrapolated over a ten-year operating and support timeframe to determine both the effect of various security regimes on the flow of the large volume of commercial cargo container traffic and the ability of the system to defeat an attack.

4.4.2 System Cost Models- Land Inspection Group

4.4.2.1 Cost Breakdown Structure for Land Inspection System Alternatives

Ten-year O&S costs of the alternatives were estimated by calculating all direct and indirect incurring costs. These costs were analyzed by building a cost element structure, as shown in Figure 97, including: personnel, procurement of equipment, maintenance, supplies, services, and training. Applicable costs for the listed items in

each architecture were included, which were determined based on several sources for cost information.[81, 82, 83]

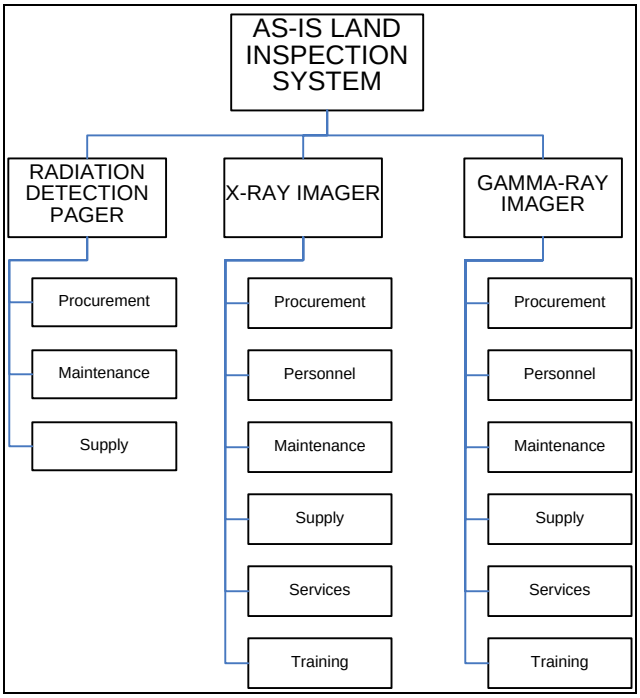

Figure 97. "As-Is" System Cost Breakdown Structure

The figure illustrates the cost breakdown structure for the "As-Is" alternative. The same breakdown was used for each item in the Port Centric and Trusted Agent alternatives.

The initial cost used the Port of Singapore infrastructure and operations. From the "As-Is" architecture in Singapore, the costs were scaled for implementation of the system in the top 16 ports by volumes and cargo value that export to Singapore[84] and is summarized in Table 27. The teams and ports were assumed to be equally efficient at all 16 ports in order to use a scaling factor determined by ratio of cargo throughput. A

[81] EDO Corporation, *Gamma-Cam*, http://www.edocorp.com/documentation/gammacam_overview.pdf, (accessed 14 April 2005).

[82] Berkley Nucleonics, *Radiation Detectors*, http://www.berkeleynucleonics.com/radiation-detectors-pager.htm, (accessed 14 April 2005).

[83] Physical Optics Corporation, *LEXID X-Ray Imagine Device*, http://www.poc.com/emerging_products/lexid/default.asp, (accessed 12 May 2005).

84 Nanyang Technological University Library, Stat-Link, Annual Report for Imports, http://www.ntu.edu.sg/lib/stat/tti40.htm, (accessed 17 May 2005).

ratio of total throughput of each port to Singapore[85] was used to compute how many sensors and operators were needed to inspect and process an equivalent percentage of containers. For the "As-Is" architecture, these ports had to also be CSI participants.[86] This was done for comparison of the cost effectiveness between implementing systems in Singapore alone and/or in the top exporters to Singapore. This addressed detecting threats before getting to the Port of Singapore.

The "As-Is" System included:

- Radiation Detection Pagers.
- X-ray Imagers.
- Gamma-Ray Imagers.

Cost Element	Cost($)
Radiation Detection Pager System	45,500
Mobile X-Ray Imager-Truck System	18,216,500
Mobile Gamma-Ray Imager-Truck System	18,361,500
Total "As-Is" Land Inspection System	**36,498,500**

Table 27. Ten-Year O&S Cost of "As-Is" Architecture

This table summarizes what it cost to continue operating the current Land Inspection System.

Alternative 1, Port Centric alternative included:

- One Hundred Radiation Detection Pagers.[28]
- Five mobile and Five fixed Gamma-Ray Imagers.[27]
- Five Pulsed Fast Neutron Analyzers.[87]
- Fifty High Purity Germanium Detectors.[88]
- Fifty Flow Cytometry Detectors.[89]

---

85 The Review of Network Economics, Vol. 3, Issue 2, (June 2004): p. 99.

86 U.S. Customs and Border Protection, Department of Homeland Security, "Ports in CSI," *Border Security*, http://www.customs.gov/xp/cgov/border_security/international_activities/csi/ports_in_csi, (accessed 19 May 2005).

87 Belbot, Michael, et al., Western Kentucky University, *A Commercial On-Line Analyzer Using Pulsed Neutrons*, www.wku.edu/API/publications/CAARI2000Coal.pdf, (accessed 25 May 2005).

88 Interview with Thomas Mcgrann, Lawrence Livermore Laboratories, site visit, (14 January 2005).

- Fifty Gas Chromatography/Ion Mobility Spectrometers.[90]
- Five Inspection Data Fusion and Analysis Rooms.
- Five Inspection Sensors and Facilities Communication Networks.
- Five Three-Person Alert Teams.[91]

The total cost for procurement and operation over ten years in the port of Singapore is summarized in Table 28.

Cost Element	Cost($)
Radiation Detection Pager System	166,000
Mobile/Fixed Gamma-Ray Imager System	29,871,500
Pulsed Fast Neutron Analyzer	34,182,500
High Purity Germanium Detector	305,000
Flow Cytometry Detector	405,000
Gas Chromatography/Ion Mobility Spectrometry	5,270,000
Inspection Data Fusion and Analysis Room	27,682,500
Communication Network	82,500
Alert Team	27,000,000
Total Alternative 1 Land Inspection System	**124,965,000**

Table 28. Procurement and Ten-Year Operating Cost for Port-Centric Architecture

The table summarizes the itemized cost of the Port-Centric alternative to include procurement and ten-year O&S.

Alternative 2, Trusted Agent Architecture, included additional costs. To be certified as a "Trusted Agent" there were standards and security measures that companies in the industry had to abide by similar to those required for C-TPAT certification[92] as indicated in the Alternative Generation section. The cost is based on certifying 10,000 companies. The containers were also sealed with a mechanical tamper

---

[89]Chemicon International, APO-BRDU™, http://www.chemicon.com/Product/ProductDataSheet.asp?ProductItem=APT115, (accessed 15 May 2005).

[90] Business Communications Company, *Biologic Detection Technologies: Pyrolysis-Gas Chromatography Mobile Spectrometer*, http://bcc.ecnext.com/coms2/summary_0279-17730_ITM, (accessed 10 May 2005).

[91] Defense Finance and Accounting Service (DFAS), *Military Pay Chart*, http://www.dod.mil/dfas/money/milpay/pay/paytable2005-rev1.pdf, (accessed May 2005).

[92] U.S. Customs and Border Protection, Department of Homeland Security, *C-TPAT Fact Sheet and Frequently Asked Questions*, http://www.customs.gov/xp/import/commercial_enforcement/ctpat/fact_sheet.xml, (accessed 23 May 2005).

lock. The cost reflects 1.75 million seals that can be reused over the ten-year time frame.[39]

Alternative 2 (summarized in Table 29) includes:

- One Hundred Radiation Detection Pagers.
- Five mobile and Five fixed Gamma-Ray Imagers.
- Five Pulsed Fast Neutron Analyzers.
- Fifty High Purity Germanium Detectors.
- Fifty Flow Cytometry Detectors.
- Fifty Gas Chromatography/Ion Mobility Spectrometers.
- Five Inspection Data Fusion and Analysis Rooms.
- Five Inspection Sensors and Facilities Communication Networks.
- Five Three-Person Alert Teams.
- Automated Inter-port Information and Targeting Systems.
- 1.7 Million Tamper Resistant Seals for Containers.[93]
- Ten thousand Shipper/Manufacturer/Portal/Ship Security Certifications.

[93] Schwartz Ephram, "GE Completes Trial of Smart Shipping," Inforworld.com, http://www.infoworld.com/article/05/01/11/HNge_1.html, (accessed 15 April 2005).

Cost Element	Cost($)
Radiation Detection Pager System	166,000
Mobile/Fixed Gamma-Ray Imager System	29,871,500
Pulsed Fast Neutron Analyzer	34,182,500
High Purity Germanium Detector	305,000
Flow Cytometry Detector	405,000
Gas Chromatography/Ion Mobility Spectrometry	5,270,000
Inspection Data Fusion and Analysis Room	27,682,500
Communication Network	82,500
Alert Team	27,000,000
Automated Inter-port Information and Targeting	19,500
Tamper Resistant Seal for Containers	52,500,000
Shipper/Portal/Ship Security Certification	17,500,000,000
Total Alternative 2 Land Inspection System	**1,767,748,450**

Table 29. Procurement and Ten-Year Operating Cost for Trusted Agent Architecture

The table summarizes the itemized cost of the Trusted Agent alternative to include procurement and ten-year O&S.

4.4.3 Analysis – Land Inspection Group

The "As-Is" model indicated very poor performance for defeating an attack. Using the variables from Table 29, the probability for defeating an attack is $P_{def} = 0.0011$. Combining the Customs and Port Inspection System indicates that 98.6% of cargo exiting the port will not be subjected to any sort of active or passive search regimen. The model was then run for all CSI participating ports exporting to Singapore instead of the United States. This resulted in the numbers shown in Table 30. The delay cost metric of the "As-Is" System was considered to be negligible, based on empirical research, because no significant delays were reported in the port of interest. Specifically, the increase in the false alarm rate of the passive sensor is the key factor in increasing delay cost, as seen in Figure 98. Additionally, passive sensor P(detection) is the primary factor concerning P(defeat), as also seen in Figure 98.

MOE / Metric	'As-Is'	ALT 1	ALT 2
Percent Cargo Inspected	6%	99%	99%
P(Detect I Inspect)	99%	87%	93%
P(Detect)	6%	87%	93%
Comm. Delay Cost ($M)	~0	1,921	1,688
Comm. Cost ($M)	0	0	1,753
Land System Cost ($M)	38	1,143	1,150
Total System Cost ($M)	38	3,064	4,591

Table 30. Summary of Results of MOEs for Alternatives

The table compares the results for the "As-Is" System and the two alternatives. The alternatives clearly outperform the status quo with respect to Pdetect, but come at a much higher cost.

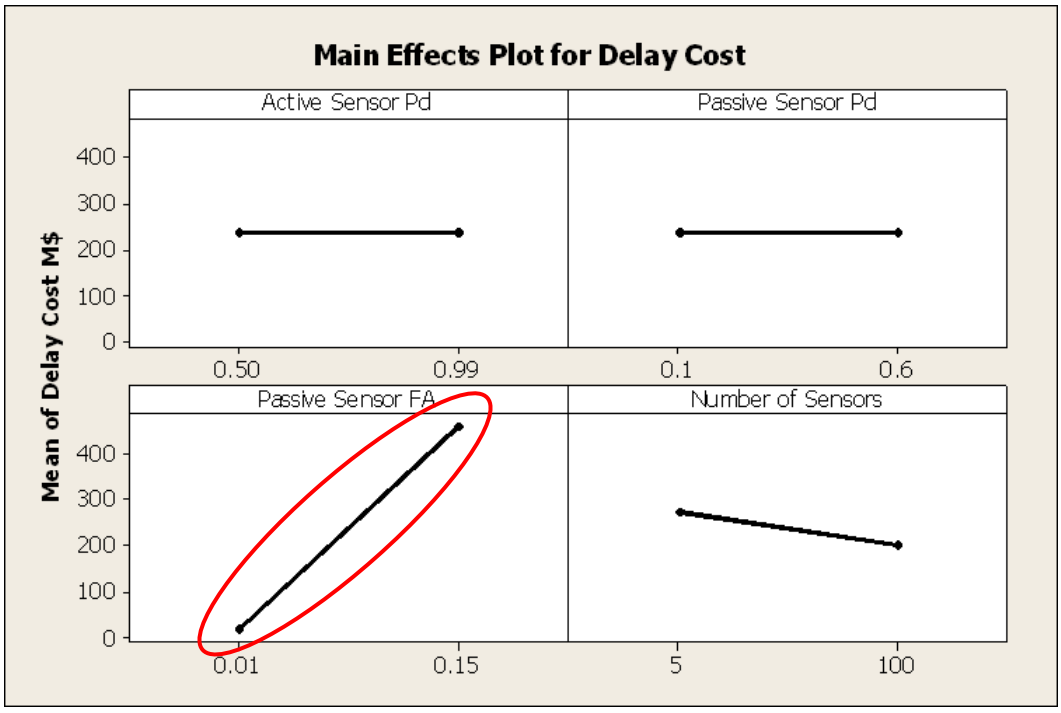

Figure 98. Main Effects Plot for Delay Cost

The active sensor Pd results indicate that the sensor Pd's have minimal influence on the delay cost, while the Passive False Alarm rate is a delay cost driver.

While analyzing the first model run for Alternative 1, it was apparent that the overall system performance is influenced most by the strength of the Passive System that was installed in the port, as seen in Figure 99.

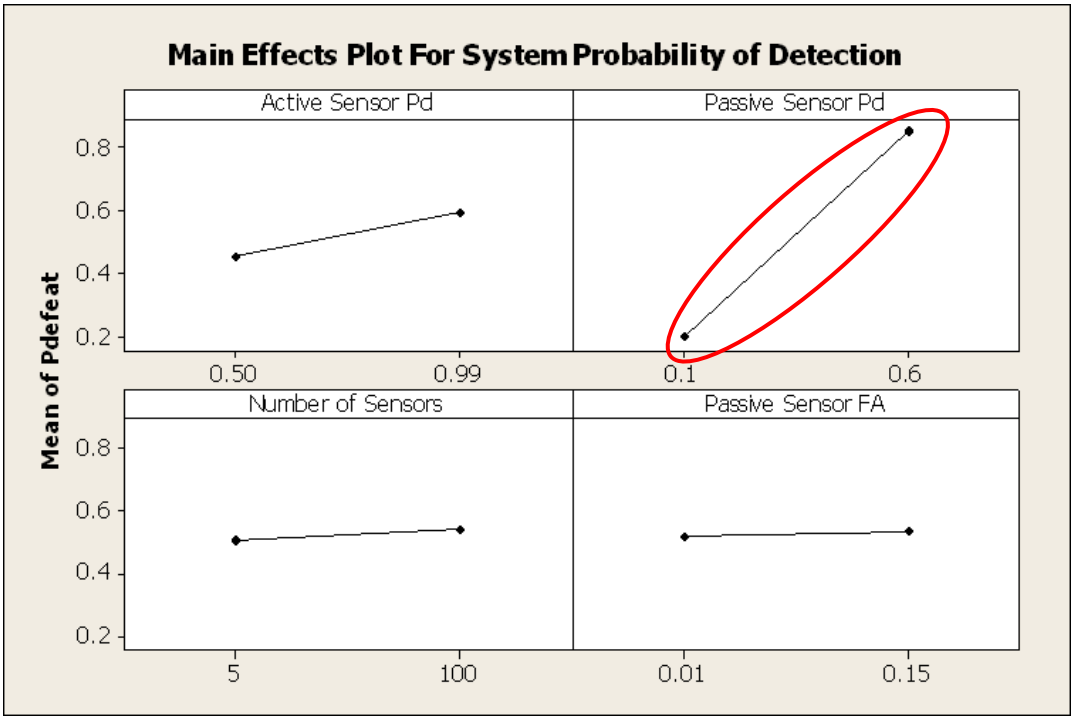

Figure 99. Main Effects Plot for System Pd

The Active Sensor Pd does appear to have some significance, but not the large influence that the Passive Pd has on the overall system Probability of Defeat.

Because of the overall systems perspective that the team took, it became beyond the scope of this project to delve into an intense analysis of an intrusive, "From Scratch" Passive Sensor System (but the team does recommend this as a focus for further study). The second iteration of Alternative 1 and the iteration of Alternative 2 instead focused on near-term, nonintrusive detection involving active search that does not require large commercial infrastructure changes.

After analyzing the various active Pd sensor values and the number of active sensors employed, a "best-case" treatment was chosen for each case to compare and score the alternatives. The value of 50 sensor teams was chosen based on the results seen in Figures 100 and 101, where the delay cost is minimized by reducing the queue wait to 0.

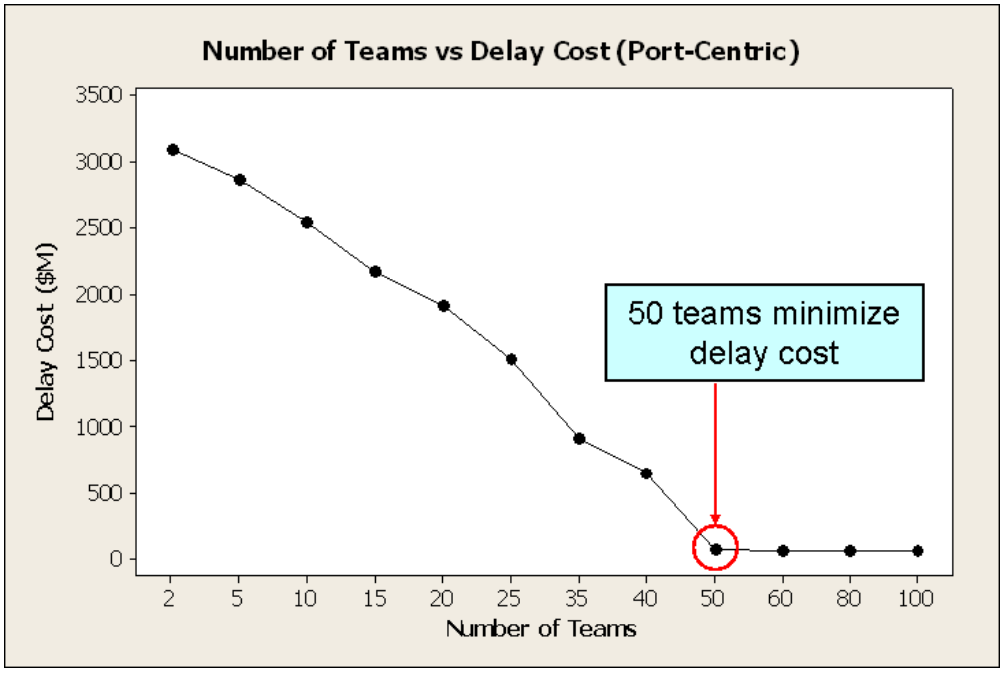

Figure 100. Alternative 1 Sensor Variation and Cost Results

Illustrates the point where the number of teams is sufficient to reduce the false alarm verification queue line to 0 wait.

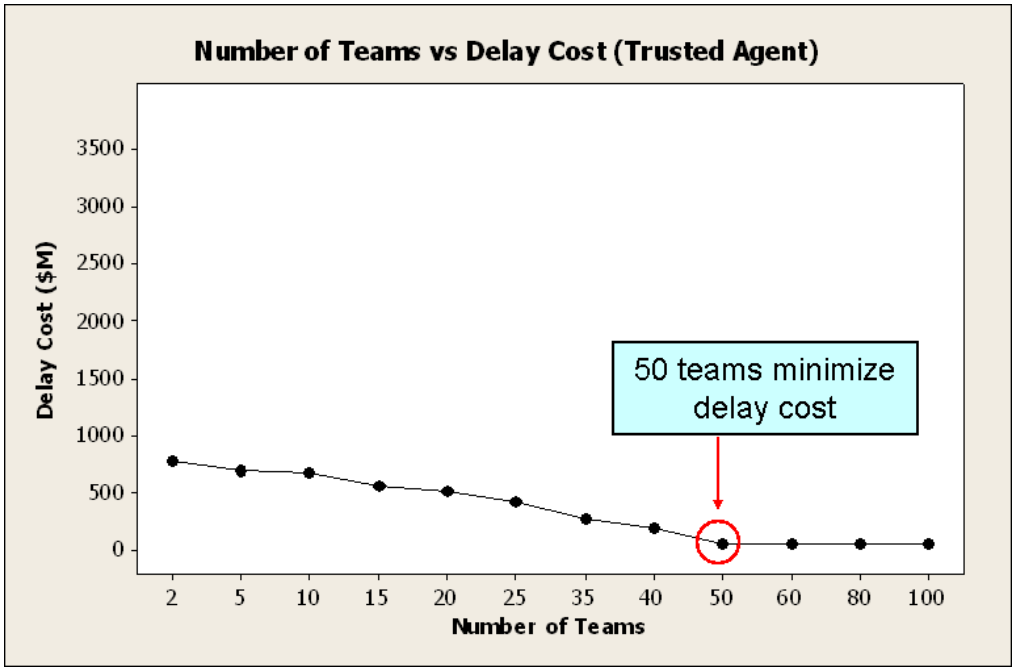

Figure 101. Alternative 2 Sensor Variation Cost Results

The "knee in the curve" is found as the point where the number of teams is sufficient to reduce the false alarm verification queue line to 0 wait.

The predicted probability of defeating an attack was raised significantly by installing a nonintrusive, hybrid passive/active Sensor Inspection System. The obvious price paid for the increased probability of detection was the large impact/delay cost on the shipping and commerce industry, based on the higher false alarm rate. There is also an additional commercial cost for the implementation of the Trusted Agent Certification System used in Alternative 2.

After initial modeling results were complete, there still remained a concern to address weapons that are detonated or released at a pier, before the Singapore Land Inspection System was able to be utilized. The system infrastructure was scaled to be placed in the top 16 exporting ports by volume into Singapore. This accounted for 47% of the cargo that is imported into Singapore. The results for implementing each alternative in those ports are summarized in Table 31.

MOE / Metric	'As-Is'	ALT 1	ALT 2
% Inbound Cargo Inspected	2%	47%	74%
P(Detect I Inspect)	99%	88%	94%
P(Detect) all inbound cargo	2%	41%	56%
Comm. Delay Cost ($M)	~0	30,730	27,019
Comm. Cost ($M)	0	0	1,753
Land System Cost ($M)	608	36,677	33,841
Total System Cost ($M)	608	67,407	62,613

Table 31. Results of Implementing the System in Top 16 Ports

The table compares the results for the "As-Is" System and the two alternatives for the 16-port expansion of the Land Inspection System. Once again, the alternatives clearly outperform the status quo as far as Pdefeat, but come at a much larger cost.

The cost model data and performance results were then combined to show a graphical representation of cost versus performance of the alternatives, both in Singapore and in the top 16 ports. Figure 102 and Figure 103 are graphical representations of the results. Through these figures it is apparent that Alternative 2 gives a higher Pdefeat over either the "As-Is" System or Alternative 1.

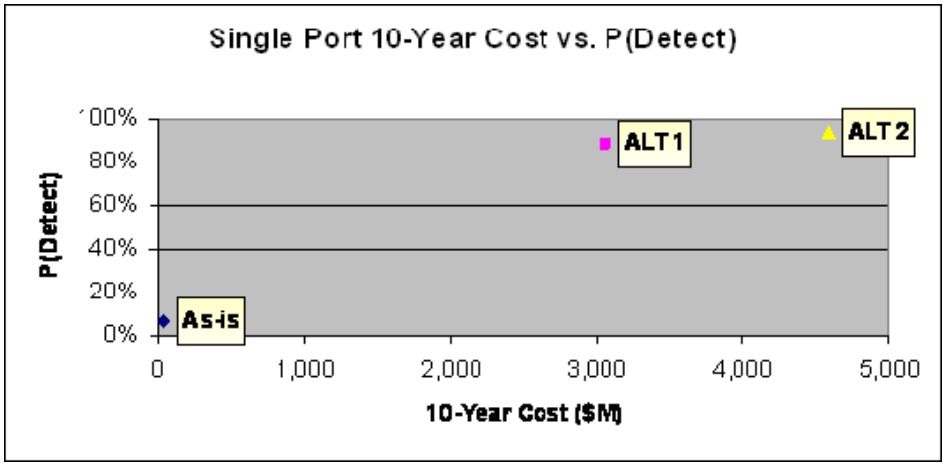

Figure 102. Cost vs. Performance for Single Port

The figure illustrates the cost versus performance for each alternative in the port of Singapore.

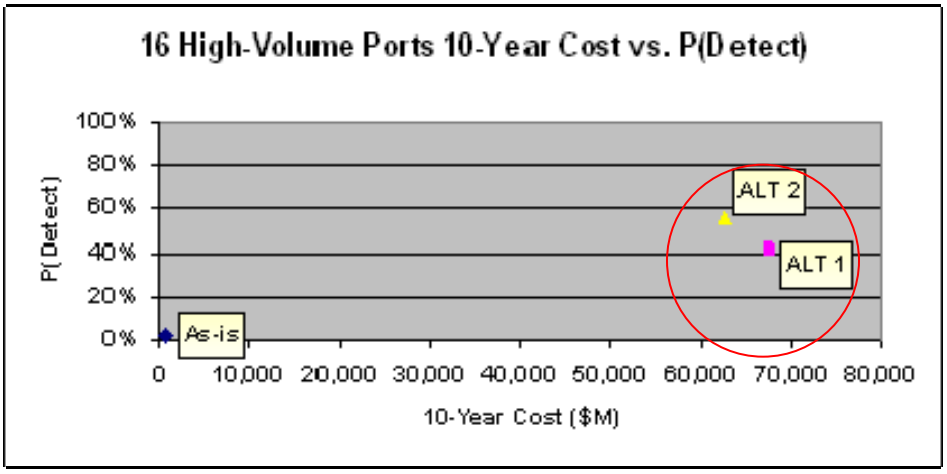

Figure 103. Cost vs. Performance for Top 16 Ports

The figure illustrates the cost versus performance for each alternative implemented in the top 16 exporting ports to Singapore.

4.5 MODELING AND ANALYSIS – SEA INSPECTION GROUP

4.5.1 Performance Model – Sea Inspection Group

Approach: The important goal for the Sea Inspection Group during the model-building phase was to generate a model that would be reusable for each alternative. The way in which the two alternatives were designed helped the team to

build this functionality. Specifically, the Honor System incorporates Smart container technology added to the boarding team.

For the performance runs, every ship was assumed to have hazardous material onboard and inspected by the system. This allowed the model to give the Sea Inspection Group an overall probability of detection for the system. After that, extra runs were performed using the generated probability of detection and false alarm to generate a queue length and time for analyzing the delay cost the alternative generated.

MOEs: One of the overarching MOEs of the model was the average percentage of inspections that were completed. Due to the limitations on the number of teams and inspection time used as treatments, the model generated an output of how much of each ship was inspected. In the performance runs, the overall average of the percentage of completed inspections was used as an MOE. The value of this MOE was used to estimate the system probability of detection against each type of threat.

Assumptions: For Alternative 1—the Boarding Team Inspection System—there were some key assumptions. In the model, ships arrived according to the exponential distribution with a certain mean time between arrival (MTBA). The total number of container ships per year was estimated as 10,000 for modeling purposes. To model the container ship sizes, values were obtained from Figure that showed the distribution of the number of ships versus ship sizes. This was taken from actual data over a span of 40 years.[94]

[94] www.manbw.com/files/news/filesof761/Propulsion%20container.pdf.

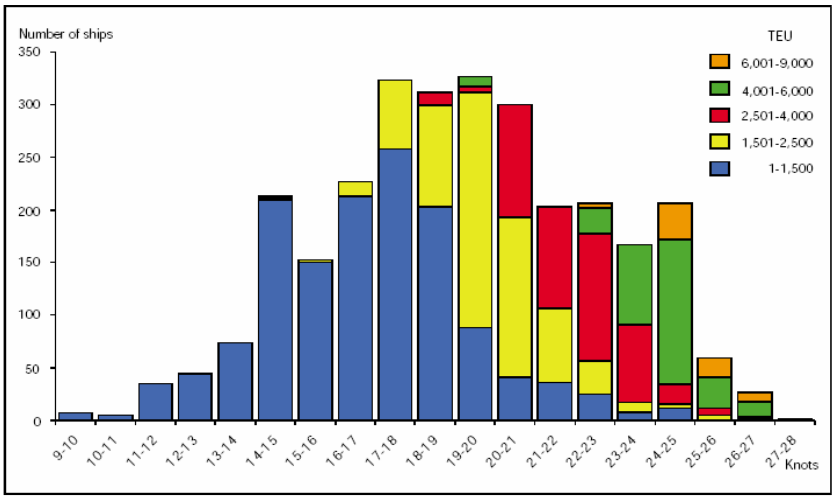

Figure 104. Distribution of Number of Ships vs. Ship Size

This graph was used to retrieve the number of ships for different ship sizes. It shows the number of ships built versus their speed. The different colors represent the different ship sizes built over the last 40 years. The Sea Inspection Group used the distribution to create Figure 104, which was then used in the Ship Generator function in the model to assign each ship generated a certain ship size.

Using Figure 104, the distribution was then curve-fitted and random ship sizes were generated using the curve that represented the distribution shown in Figure 105.

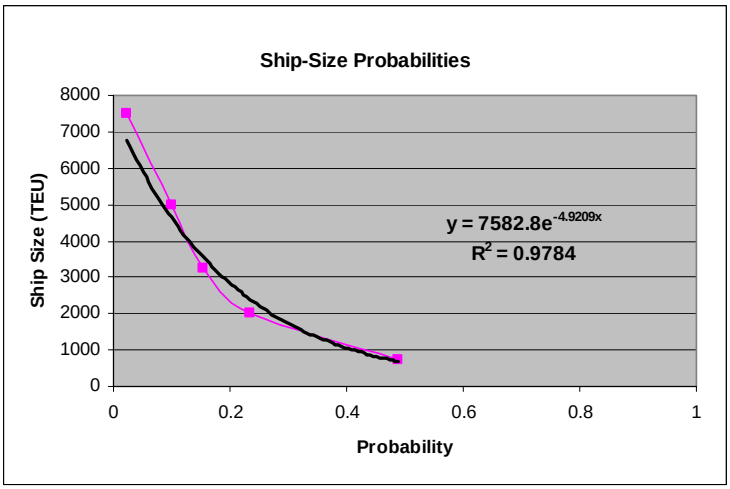

Figure 105. Ship-Size Probabilities

This plot of the ship size probability distribution gives the equation used in the Ship Generator function of the model. It allows the Ship Generator to produce a realistic number of ships with appropriate ship sizes for the model. The pink line is the actual curve generated by the data and the black line is a display of the equation to the right of the curves. The R^2 value represents how well the curve of the equation fits the curve from the data.

Boarding teams were then transported to the ship waiting to be inspected by helicopter or hydrofoil based on the Force Group's alternatives. After an inspection was finished, a one-hour delay was assumed for the teams to be ready for another inspection. This is based on an assumption of the boarding team returning to base or turning over to another boarding team.

In the model, ships need the required number of teams to be onboard before the inspection would start. The required number of teams were calculated and assigned to the ships by using the Ship Size Per Team (SSPT) variable in the model. SSPT values depended on different Soak Time values and the inspection time located in Table 32. Soak time is defined as the time allowed for sensor detection per container. The values in Table 32 were generated from the TDSI Land Systems Group inspection model results. The Land Inspection Group then provided the team with data that showed the effects of soak time to the maximum possible amount of cargo that a ten-man team could inspect, as shown by Figure 106. When the maximum number of teams available for that treatment did not meet the required number of teams for that ship, the maximum number of teams available was assigned to the ship for inspection. This assignment strategy resulted in some ships not being inspected completely.

		Soak Time (Minutes/Container)		
		1	**2**	**3**
Inspection Time (Hours)	**3**	1,250	700	275
	5	2,250	1,300	650
	6	2,650	1,300	800
	7	3,100	2,250	1,000
	8	3,750	2,250	1,150

Table 32. SSPT Table Using Inspection and Soak Times

The values in this table were used to calculate the required number of inspection teams to board the ship to be inspected. Each number represents the inspection capability of a single team in terms of TEUs per certain period of time given the first column.

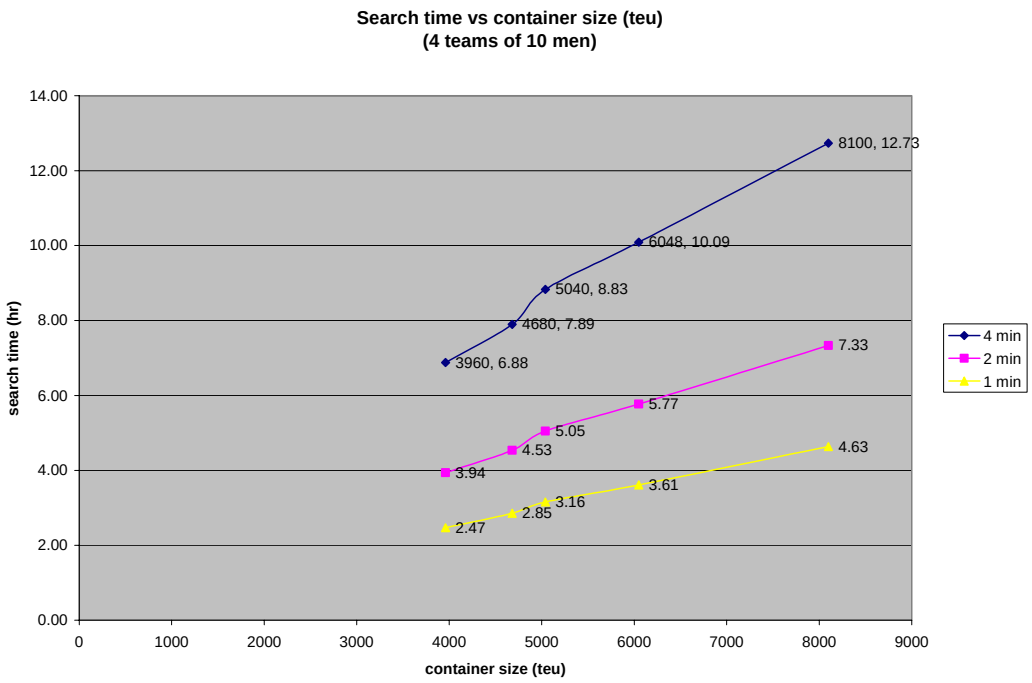

Figure 106. Effect of Inspection Time on Inspection Capacity (TEU) for Different Soak Times

This graph was provided by the Land System students' robotic search model modified to represent human search. Table was filled with the corresponding numbers out of this graph for use in the model.

It was also assumed that the false alarm rates of the individual sensor types needed to be combined together, as the false alarm of any type of sensor could cause the same results, as shown in Equation 5. The same calculation for the combined false alarm rates were done for both Smart containers and the boarding team's handheld devices.

$$P(FA)=1-[(1-P(FA_{Neutron})(1-P(FA_{Gamma}))(1-P(FA_{Chem/Bio}))(1-P(FA_{Explosives}))] \quad \textit{Equation 5}$$

This equation was used in the model for determining the overall false alarm rate for each system. The probability of false alarm was important because it was assumed that the false alarm rate of the Smart container devices would drive the queue size for the boarding teams.

Alternative 2 was similar to Alternative 1, but with the added layer of Smart containers on all shipping containers. Before the ships were targeted for inspection, the Smart containers provided the C3I System with a trigger that a container had detected hazardous materials. The model assumed that 95% of the container ships

were equipped with Smart container devices on their containers and that the AIS used in the area was able to detect those without Smart containers. The C3I System was also assumed to have a 99% probability of deciding to inspect a ship from a Smart container trigger. The detection probabilities and false alarm rates of the Smart containers played a significant factor in the output since a detection or a false alarm generated a boarding team response.

Inputs: The inputs that went into both alternatives were initially the same due to the layered approach, but with added inputs for Alternative 2. Both models had a MTBA and a SSPT input. Inputs also included whether or not hazardous materials were onboard (Boolean), the inspection time, and the number of teams. Alternative 2 included the added probabilities and false alarm rates for the Smart container devices.

Flowchart: The model flowchart, as shown in Figure 107, was developed to reflect each alternative as a function in separate swim lanes. The "alternative selector" decision block represents the model's ability to switch between alternatives for model runs.

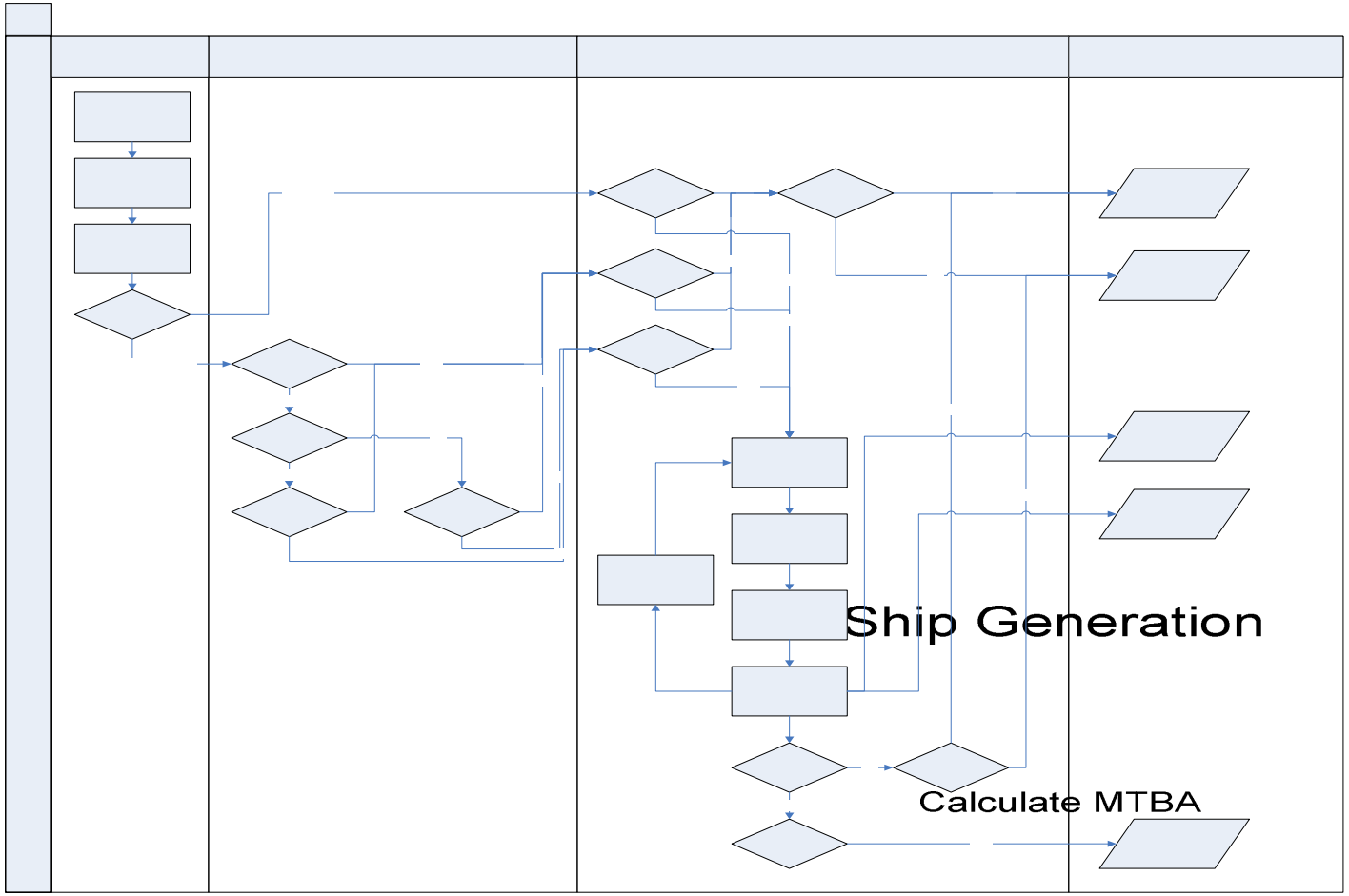

Figure 107. Model Flowchart

This flowchart represents the operation of the model. Each alternative modeled was represented in different swim-lanes to clearly identify each alternative's input and output variables. Features such as the "alternative selector" allow the model users to select which alternative to represent when running the model.

Description: The model began with the "Ship Generation" phase where every ship was generated using an exponential distribution with a calculated MTBA. During this phase, the ship size was assigned to the ships using the distribution shown in Figure Depending on the "Alternative Selector" decision block value, the model continued its execution for either alternative. This decision block acted as a router for the execution flow of the model.

A timer started whenever a ship entered the "Boarding Team" block. The required number of teams needed for the ship to be inspected in a certain amount of time (declared by "Inspection Time" variable) was calculated. The model then assigned that number of teams to the ship. If the required number of teams was not available at that moment, the ship waited until the required number of teams was available. If the required number of teams was more than the maximum number of teams (declared by "Num Teams" variable), then the maximum number of teams that were available were assigned to the ship. In this case, the ship could not be inspected thoroughly. In doing so, the number of teams assigned to each ship, ship size, and SSPT were used to calculate a percentage of the ship that could be inspected. Before the ship exited the "Boarding Team" block, this percentage value was accumulated in a block and then used to calculate an "Average Percentage Completed" value for each run.

After the team assignment, the ship and the teams (this number was varied in the model for different treatments) were batched and sent to an activity block that represented the inspection activity and delayed both the ship and the teams for a certain period of time (declared by "Inspection Time" variable). When the activity block ran out of associated time, an unbatching took place and the ship was back on its way (or pulled into a predefined place for detailed inspection in case of detection). After the unbatching, the teams went back to their original pool for the next inspection assignment, which was represented by a fixed amount of time (one hour). Because the inspection team was assumed to not cause the ship any delay during the inspection, the delay in the activity block was subtracted from the timer value of the ships. By doing this, the delay figure for the ship included only the queue time.

For Alternative 2, the ship was diverted to the "Smart container" block before the "boarding team" block. Then several decision blocks determined whether the ship had Smart container devices installed and the probability of detection for those Smart container devices. These blocks routed the ship through the model and determined whether the hazardous material was detected or not. It was assumed that the Smart container devices did not improve the detection capability of the handheld devices of the boarding teams, but did reduce the amount of the ship the boarding team needed to inspect due to device mapping. If a ship was diverted through "Cleared" tank of the model, but did, in fact, carry a hazardous material it was counted as a failure. Any ship directed to "Detected" tank proceeded to the "Boarding Team" block and received the same inspection procedures described in the boarding team model explanation.

The treatments used in both alternatives are listed in the "Values Evaluated" column in Table 33. This column represented the run plan of the model regarding the treatments and the values of those treatments. A combination of all treatments were generated and entered into the model via a text file, providing 30 results for each combination output to a separate text file. Then, each combination was analyzed and the team was then able to select the optimum treatment value set (listed in the "Value Chosen" column).

			Values Chosen	
Treatment		**Values Evaluated**	**Alt 1 (BT)**	**Alt 2 (HONOR)**
Number of Teams		1,3,5,7,9	3	9
Inspection Time		3,5,6,7,8	7	8
Soak Time		1,2,4	1	1
P(Random Inspection)		.01, .025, .05, .075, .1	0.05	0.01
P(FA) Smart Containers		0.155, 0.198, 0.241, 0.284	N/A	0.16
P(FA) Boarding Team		0.073, 0.088, 0.103, 0.107	0.117	0.07
Pd - Smart Containers	Neutron	0.5, 0.8	N/A	0.80
	Gamma	0.6, 0.7	N/A	0.70
	Chem/Bio	0.3, 0.4	N/A	0.40
	Explosive	0.1, 0.2	N/A	0.20
Pd - Boarding Team	Neutron	0.1, 0.25	0.25	0.25
	Gamma	0.1, 0.25	0.25	0.25
	Chem/Bio	0.2, 0.3	0.30	0.30
	Explosive	0.4, 0.5	0.50	0.50

		Alt 1 (BT)		Alt 2 (HONOR)	
Overarching MOEs		**Mean**	**Std Dev**	**Mean**	**Std Dev**
P(detect)	Boarding Team	0.25	0.007	0.24	0.004
	Smart Container	N/A	N/A	0.66	0.005
Commercial Delay Time (queue + false alarm)		0.21 hr/ship	0.03 hr/ship	0.53 hr/ship	0.05 hr/ship
Commercial Cost		0	0	12,680 B$	5,551 B$
System Cost		16.93 B$	0.2857 B$	100,76 B$	1.995 B$

Table 33. Treatments and Evaluated Results for Model Runs

This table provides a summary of the treatments and values tested for the alternatives and the values chosen to be optimum. The bottom half of the table summarizes the output of the alternatives using the treatment values chosen above.

4.5.2 System Cost Model – Sea Inspection Group

Approach: To obtain an accurate cost model, the Sea Inspection Group collected data on commercial equipment equivalent to what would be used in each alternative. For each alternative's list of gear, the group gathered three costs—a low, medium, and high. Using these three values, the triangular distribution was used to obtain a 95% confidence interval on the expected values of total costs for the different alternatives. However, for some gear, there was only one piece of equipment that was the best option or was the only option available. In these instances, that single cost value was used across all three values.

MOEs: The MOEs for the cost model were the MDP System acquisition cost and the MDP System Ten-Year O&S costs. Also included in the MOEs of the cost model were the Commercial Costs and Commercial O&S costs in Alternative 2. To start building the cost model, it was decided that all costs would be in FY05$. The group then needed to decide what the team size would be and what the sensor makeup for that team would be. The group decided the team size would be based on the Navy's boarding teams used in Visitation, Board, Search, and Seizure (VBSS). For this, there would need

to be 12 personnel per team, with two of them on the bridge for administration and external communications and the other ten conducting the inspection throughout the ship.

Assumptions: The requirements for the boarding team alternative meant that each person would carry a handheld radio for internal communication with the rest of the team. Additionally, each team would also carry five chemical detection kits, five explosive detection kits, ten gamma/neutron detectors, and five biological detection kits. For the Honor System alternative, all of the above requirements remained the same, but each team would also have a Gamma Camera Imager/Laptop. Figure 108 shows the Boarding Team Sensor costs for one team and Figure 109 shows the Honor System costs for one team. It should be noted that the costs to acquire and implement the Smart container technology were not listed in the Honor System Costs. It was assumed that this would be a commercial cost absorbed by the shipping companies, etc., and was listed in the overall Honor System Cost model, but was not added to the sensor costs. Also, the costs were gathered directly from manufacturer's Websites. Lawrence Livermore National Laboratories also supplied some cost data for their particular hardware and sensors.

Equipment Type	Low	Med	High	Expected Cost	Variance	Standard Deviation
Portable Radios (6 sets of 2)	$240	$420	$840	$500	$15,800	$126
Headsets for Radio (12)	$156	$180	$216	$184	$152	$12
Chemical Kits (5)	$1,200	$1,200	$1,200	$1,200	$0	$0
Explosive Detector Kit (5)	$575	$725	$135,000	$45,433	$1,002,774,410	$31,667
Gamma/Neutron Detector (10)	$86,000	$86,000	$86,000	$86,000	$0	$0
Biological kits (5)	$5,475	$5,475	$5,475	$5,475	$0	$0
			1 Team Total	$138,792	$1,002,790,362	$31,805

Figure 108. Boarding Team Sensor Cost (FY05$)

This chart displays the cost for sensors for one boarding team in the Boarding Team System (Alternative 1). This includes all handheld sensors used by the team. Three different sets (low, medium, and high) were used to a 95% confidence interval for the cost of the sensors.

Equipment Type	Low	Med	High	Expected Cost	Variance	Standard Deviation
Portable Radios (6 sets of 2)	$240	$420	$840	$500	$15,800	$126
Headsets for Radio (12)	$156	$180	$216	$184	$152	$12
Chemical Kits (5)	$1,200	$1,200	$1,200	$1,200	$0	$0
Explosive Detector Kit (5)	$575	$725	$135,000	$45,433	$1,002,774,410	$31,667
Gamma/Neutron Detector (10)	$86,000	$86,000	$86,000	$86,000	$0	$0
Biological kits (5)	$5,475	$5,475	$5,475	$5,475	$0	$0
Gamma Imager w/ Laptop	$180,000	$180,000	$180,000	$180,000	$0	$0
			1 Team Total	$318,792	$1,002,790,362	$31,667

Figure 109. Honor System Sensor Cost (FY05$)

This chart displays the cost for sensors for one boarding team in the Honor System (Alternative 2). This includes all handheld sensors used by the team. Three different sets (low, medium, and high) were used to a 95% confidence interval for the cost of the sensors. The difference between this alternative and the Boarding Team System is the use of a gamma imager for active interrogation of containers for radioactive sources.

In the final cost model spreadsheet, there are several columns for the total cost to support three, five, seven, or nine teams per shift. To calculate exactly how many teams would be needed to support inspections, the team assumed a certain number of shifts would be used. For example, if three teams per shift were used, there are three 8-hour shifts in one day. Therefore, nine teams total were needed to support inspections. This would be the "Gold" team and they would be in rotation for one week. The following week would be the "Blue" team, with another nine teams in rotation for the next week. To allot for leave, sickness, overloads, etc., another full team was added, making the total number of teams to support three teams/shift inspections to 27 teams. This logic followed for the other numbers of teams needed for ship inspections and the totals for all teams can be viewed in Figure 110.

Number of Teams/Shift Inspection	1	3	5	7	9
Total Teams Needed	9	27	45	63	81

Figure 110. Total Teams needed to Support Ship Inspections

This chart shows the total number of teams needed for the number of teams used per shift for inspections. This is based on eight-hour shifts and therefore three shifts per day. Each three-shift period lasts for one week when another three shift period starts with another set of teams. Given a third set of teams for back up and vacation time for the first two sets of teams, the total number of teams needed is derived.

Once the costs were calculated for the sensors needed for an individual team, those values needed to be integrated with the overall cost model. For the overall cost model, there were additional assumptions made for sensors, training, maintenance, etc. A basic assumption to start the sea inspection model was that the actual personnel used to man the teams would be included in the Force Group's cost model. Figure 108 and Figure 109 represent the sensors costs for one team for one year. These values were used in Figure 111 and Figure for the first year costs, as seen in the first row of these two tables. Each year thereafter, it was assumed that there would be a 30% replacement cost for the sensors due to the nature of the environment the sensors would be operating in. This higher replacement cost also took into account maintenance costs.

To have accountability of all the equipment, all gear would be checked in and out of an armory-type system. The personnel running the gear locker would be responsible for general maintenance only (i.e., replacing batteries, etc.). It was determined that the gear locker would be manned by the equivalent of two E-5s and would have four personnel on a yearly payroll.[95] Breakage of handheld sensors was accounted for in the replacement costs of the sensors. However, with the handheld radios that came with rechargeable batteries, back-up replacement batteries were still needed. It was determined that each radio needed to have two extra batteries per year for replacements, accounted for in consumables.

The training course was intended to train the teams for the threats they would be encountering and how to use the gear issued for inspections. This course was not intended to train the teams for ship boarding (that was taken into account in the Force

[95] http://www.dod.mil/dfas/money/milpay/pay/paytable2005-rev1.pdf.

Group's cost data). To obtain this, an analogy to an actual Army Radiological course lasting three weeks was used.[96] The 120-hour course would be taught by two qualified instructors, but to effectively train all the boarding teams for the model, there needed to be four instructors on hand, paid on a yearly basis. Their pay was based on the pay equivalent to an E-7 with 20 years in service.[97] For the treatments of more than five teams per shift for inspections, having four instructors would not be enough to train all teams, so for treatments above five teams per shift, eight instructors were included in the cost data.

While the group searched for comparative costs of equipment to be used in the inspections, several factors were considered. While the best gear was desired, the group wanted to try to reduce the amount of gear each team would be carrying. If there was a piece of gear that combined several tests, it was selected over others. Ruggedness was also a factor, given the nature of the environment in which the gear would be used.

Inputs: Inputs for the Boarding Team Alternative cost data for the handheld radio were obtained through the Motorola Website. Several versions of the Talkabout radio were available and were suitable for a shipboard environment.[98] To free up the inspectors' hands during the inspection, it was decided to have headsets for the portable radios and these figures were also obtained from the Motorola Website. For the chemical kits, the group decided to use only one—the M256 military kit (available online), as it was the most cost effective option. There were other kits available, but they were not capable of testing for blister, nerve and blood agents in the same kit.[99] For the Biological detection this was another situation where there were several kits available, but the group found the Biowarfare Agent Detection Device (BADD) Box that included tests for anthrax, ricin, and botulism all in one portable kit, so this was the selection for all three cost values.[100] The values for the explosive detection kits range from a simple swab kit

---

[96] http://www.wood.army.mil/84chem/hhc/ttd/radcrs.htm.

[97] http://www.dod.mil/dfas/money/milpay/pay/paytable2005-rev1.pdf.

[98] http://direct.motorola.com/ENS/NationalHome.asp?Country=USA&language=ENS&SelectedTab=5.

[99] http://www.ki4u.com/products1.htm.

[100] http://www.labsafety.com/store/product_group.asp?dept_id=31172.

for the low value to a handheld EVD 3500 detector. The swab kit tested for only several explosive traces, but was good if the inspector knew specifically where to look.[101] The handheld EVD 3500 was very costly but capable of detecting the presence of all threat explosives.[102] If cost was not a factor, this would be the ideal detector for inspectors. Another case where only one cost was used in the model was with the Gamma and Neutron detector. To keep a minimum on the amount of gear each team member was carrying, there was a piece of gear manufactured by Laurus Systems that was capable of detecting both gamma and neutron in one piece of gear, minimizing the gear being carried, so this was selected for the teams.[103] The only additional piece of equipment that the Honor System Alternative included was the portable Gamma-Ray Imaging System manufactured by EDO Electronic Systems Group.[104] Again, this was a situation where there was only one cost because there was only one piece of equipment that suited the exact needs of the inspection teams. The costs for the Smart-container technology were obtained from various sources, to include Savi, General Electric, and Lawrence Livermore. The team used these devices for cost data because each device is capable of having additional detectors added to detect chemical and biological agents as well as radiological devices. Other devices not included were tamper/intrusion detection only.

Description: For 2005, all teams would need all gear and equipment to conduct ship inspections. Therefore, the startup costs for the first year were to acquire all gear and equipment and all teams would be fully mission-capable the first year of implementation. In addition, the shipping companies would be responsible for implementing the Smart-container technology on all containers within the first year.

Alternative 1 was the Boarding Team System and one, three, five, and seven teams per shift inspection were the treatments for modeling. The cost breakdown can be viewed in Figure 111. Figure 112 shows the further breakdown of acquisition costs and total O&S costs for the ten years. Note that for the Boarding Team alternative there were no commercial costs because the Smart containers were not used in that alternative.

---

[101] http://www.meditests.com/exdetfieltes.html.

[102] http://www.securityprousa.com/poexdede35.html.

[103] www.laurussystems.com.

[104] Michael Vanwart, GammaCam Product Line Manager.

Fiscal Yr	Expected Sensor Costs/Team	Maintenance Costs	Consumables	Training	9 Teams	27 Teams	45 Teams	63 Teams
1	$138,792	$116,208	$912	$165,984	$1,539,528	$4,054,200	$6,568,872	$9,249,528
2	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
3	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
4	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
5	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
6	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
7	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
8	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
9	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
10	$41,638	$116,208	$912	$165,984	$665,138	$1,431,031	$2,196,924	$3,128,801
10 YR SYSTEM COST	$513,530	$1,162,080	$9,120	$1,659,840	$7,525,774	$16,933,481	$26,341,188	$37,408,735

Figure 111. Boarding Team Cost Model (FY05$)

This chart shows the ten-year cost for the boarding team alternative. Included on the right side is the total cost for each of the team size requirements (1 team/shift, 3 teams/shift, etc.).

# TEAMS	9	27	45	63
SYSTEM ACQUISITION COST	$1,539,528	$4,054,200	$6,568,872	$9,249,528
10 YR TOTAL O & S COST	$7,525,774	$16,933,481	$26,341,188	$37,408,735
10 YR TOTAL COMM COST	0	$0	$0	$0
10 YR TOTAL OPER COST	$7,525,774	$16,933,481	$26,341,188	$37,408,735

Figure 112. Boarding Team Cost Breakdown (FY05$)

This chart shows the ten-year costs for each total team numbers. The ten-year operational cost is displayed at the bottom.

Alternative 2 was the Honor System and three, five, seven, and nine teams per shift treatments were used for modeling. It was assumed that the shipping companies would implement the Smart-container technology on all shipping containers the first year. Each year thereafter, assumed a 5% replacement cost due to aging, etc. The cost breakdown can be viewed in Figure 113. Figure 114 shows the further breakdown of system acquisition costs, O&S costs, and total commercial costs.

Fiscal Yr	Expected Sensor Costs/Team	SMART Container	Maintenance Costs	Consumables	Training	27 Teams	45 Teams	63 Teams	81 Teams
1	$318,792	$5,972,120,000	$116,208	$912	$165,984	$8,914,200	$14,668,872	$20,589,528	$26,344,200
2	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
3	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
4	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
5	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
6	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
7	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
8	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
9	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
10	$95,638	$298,606,000	$116,208	$912	$165,984	$2,889,031	$4,626,924	$6,530,801	$8,268,694
10 YR TOTAL	$1,179,530	$8,659,574,000	$1,162,080	$9,120	$1,659,840	$34,915,481	$56,311,188	$79,366,735	$100,762,442

Figure 113. Honor System Cost Model (FY05$)

This chart represents the total system cost for the Honor System (Alternative 2). The light blue section shows the cost of the Smart container devices, which is the major difference between the two alternatives.

# TEAMS	27	45	63	81
SYSTEM ACQUISITION COST	$8,914,200	$14,668,872	$20,589,528	$26,344,200
10 YR TOTAL O & S COST	$34,915,481	$56,311,188	$79,366,735	$100,762,442
10 YR TOTAL COMM COST	$8,659,574,000	$8,659,574,000	$8,659,574,000	$8,659,574,000
10 YR TOTAL OPER COST	$8,694,489,481	$8,715,885,188	$8,738,940,735	$8,760,336,442

Figure 114. Honor System Cost Breakdown (FY05$)

This chart shows the ten-year costs for each total team numbers. The ten-year operational cost is displayed at the bottom.

Analysis: Figure 15 represents the main effects of each treatment. This plot allowed the Sea Inspection Group to determine if any of the individual factors significantly contributed to "percentage completed." It is apparent due to each curve being nearly horizontal that there is little impact on this MOE due to the change in any of the treatment values except for the number of teams. It was imperative to compare these values with the delay cost plots for each alternative. Without comparison, the treatment value from the performance run results looked like an optimum point, but would have inadvertently caused the maximum delay cost. By comparing two sets of output data, the group made a trade-off analysis between performance and cost.

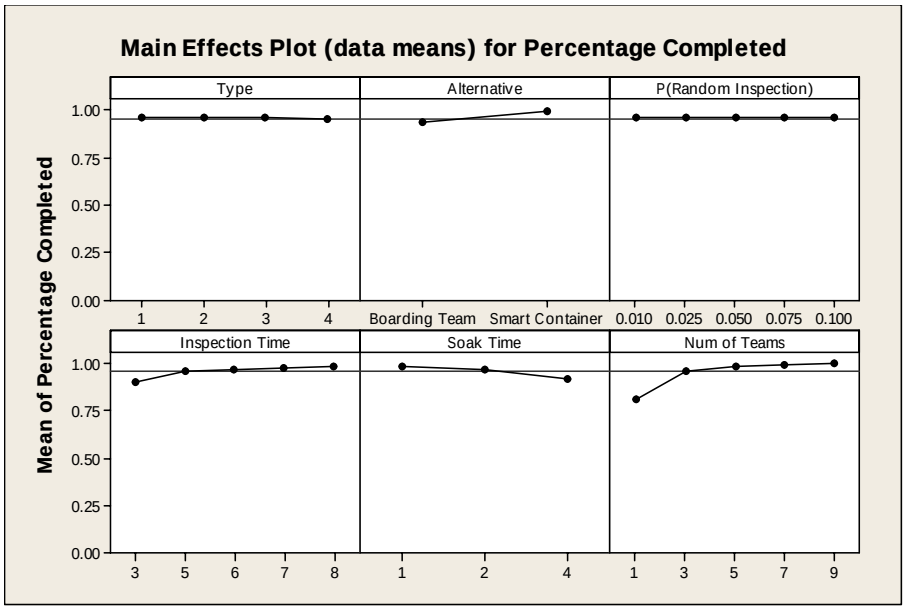

Figure 115. Main Effects for Treatments

This plot summarizes the effects of each treatment to the "Average Percentage Completed" value for both alternatives. The slope of the lines in each small plot represents the effect amplitude. More slope means more effect. For example, the main effects of the number of teams plot can be interpreted to mean that using more than three teams per shift does not affect the output in a significant way.

The main effects for the delay model from the treatments are shown in Figure 116. Outputs of the delay model helped the group complete the trade-off analysis and decide which treatment value was the optimum for each alternative.

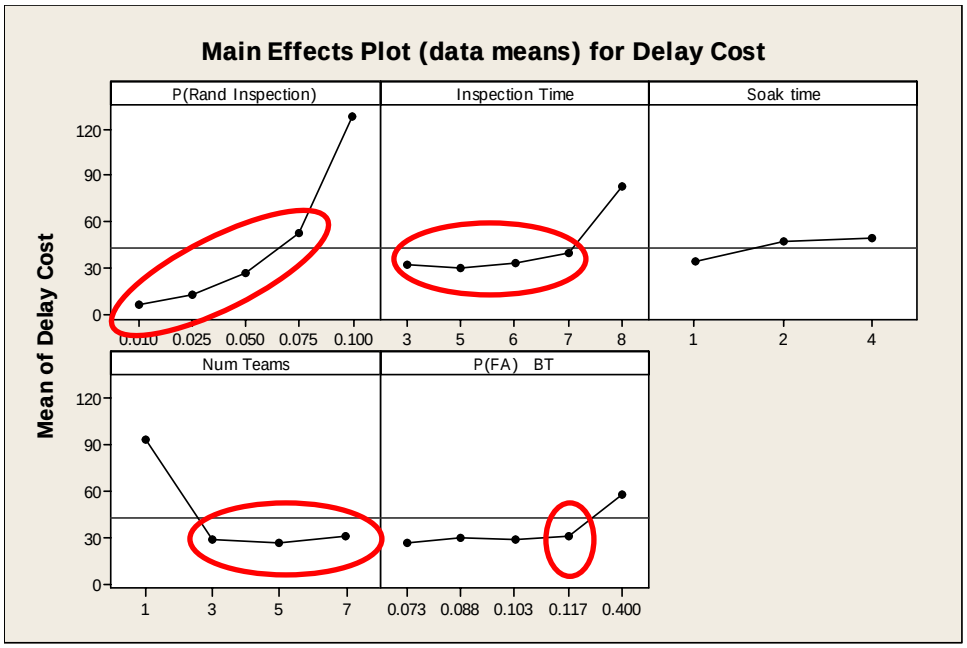

Figure 116. Main Effect Plot for Boarding Team System

This plot shows the relative impacts of each treatment on the delay cost of the alternative.

It was observed that the boarding team delay cost was not affected if the number of teams was at least three. The lowest delay cost was observed between three teams and five teams. Since the delay cost of three or five teams was almost the same, the group decided to have three teams in Alternative 1. It was also observed that the boarding teams could be allowed a maximum false alarm rate of 11% before significant delay cost was observed. Therefore, the Sea Inspection Group chose 11% as an alternative choice. Another finding from the main effects plot was that allowing the inspection teams seven hours to complete the inspection did not add any significant delay cost for the system. This seven-hour inspection period would also increase the amount of time each inspector could spend on each container and therefore was selected for the system. Finally, it was seen that the Boarding Team Inspection System could allow 5% of the ships to be randomly inspected without causing significant delay to commercial shipping. For this reason, 5% was chosen as a value for use in the overall model.

A similar approach was followed for the treatment selections in Alternative 2. The resultant plots for the Honor System (Alternative 2) are shown in Figure 117. From this graph it is easy to see that nine teams/shift reduced the delay cost far more than the other selections and the resultant minimal delay cost made up for the increase in cost due

to number of sensors and manpower. It can also be seen that the best value for Smart container false alarms was 15.5%. In our model, this means that as long as the C2 element can reduce the number of ships it sends inspection teams to down to 15.5% of the total number of ships that come into the port the system will not cause significant delay costs to shipping. The C2 element must be able to use the AIS information, Intelligence, and other resources to reduce the number of ships it sends inspection teams to. The Sea Inspection Group also selected eight hours for the inspection time in the Smart Container System. The delay cost incurred while allowing the inspection teams more time for inspection was not significant in our model. It was initially assumed that giving the inspection teams any more than six hours to inspect a ship would lead to much greater delay costs.

Finally, the Sea Inspection Group chose 1% as the value for probability of random inspections. It was felt that with the increased number of inspections, real or from false alarms, the need for random inspections was not necessary, but adding a small percentage to keep shipping companies honest was tolerable.

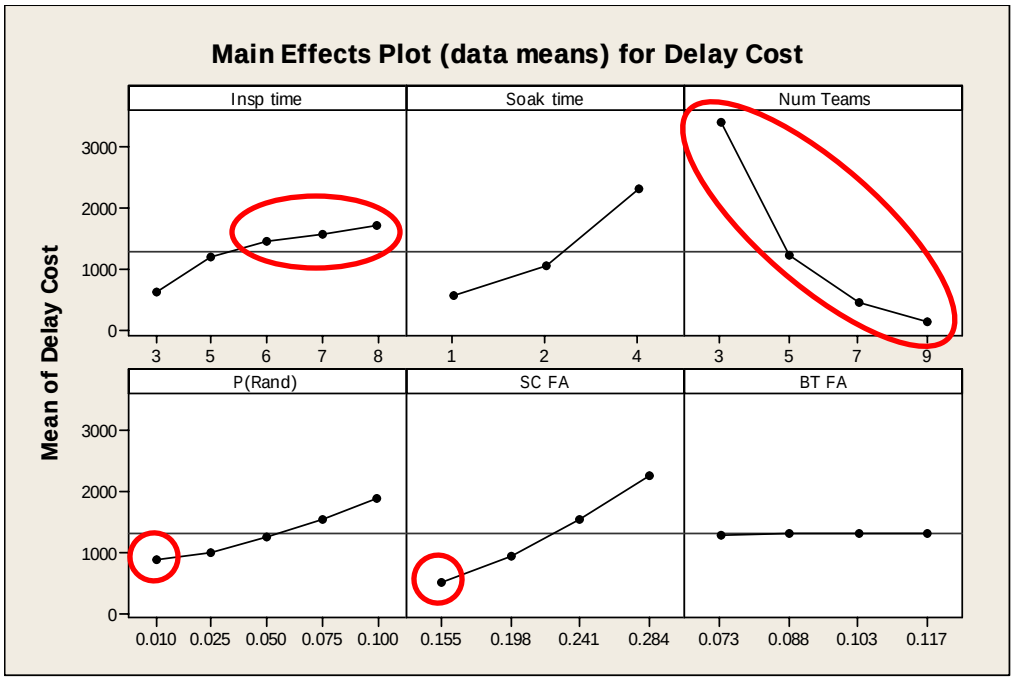

Figure 117. Main Effects Plot for Smart Container System

This plot shows the relative impacts of each treatment on the delay cost of the alternative.

As can be seen in Table 34, the delay cost for a single ship in a year for Alternative 1 (the Boarding Team System) was .01 million dollars. This means that, on average, the system caused $10,000 worth of delay to each ship. The delay cost for a single ship in Alternative 2 (the Honor System) was .02 million dollars and means that the cost to each ship in the system is approximately $20,000.

In order to fully understand the impact to commercial shipping, this per ship cost must be summed for each ship that gets inspected in each alternative as in Table 34. The total delay cost to shipping for Alternative 1 then becomes 130 million dollars and for Alternative 2 becomes 330 million dollars.

As can be seen in Table 35, the delay cost associated with at sea inspection is quite high when using these assumptions for either of the alternatives. A major difference that should be noticed is that in the Boarding Team Inspection System 5% of the total ships are being inspected by a human boarding team, whereas in the Honor System, over 16% of the ships are being inspected by humans.

MOE/Metrics	**"As-Is"**	**Alt 1**	**Alt 2**
Percent Cargo Inspected	0%	100%	100%
P(Detect | Inspect)	0%	25%	25%
P(Detect) WMD on Ship	0%	25%	25%
Commercial Delay Cost ($M)	0	.01	.02
Commercial Cost ($M)	0	0	10
MDP System Cost ($M)	0	17	100
Total System Cost ($M)	0	17	110

Table 34. Model Results for Each Alternative in Tabular Form

Table 34 shows the results of each model in tabular form. Of note, the commercial delay cost for Alternative 1 is $10K, while Alternative 2 is $20K; but total system cost is ten times higher due to the total number of teams involved. Also, these results are for one ship in the system.

MOE/Metrics	"As-Is"	Alt 1	Alt 2
Percent Inbound Ships Inspected	0%	5%	16.5%
P(Detect) WMD on Ship	0%	25%	25%
Overall Pd WMD Inbound	0%	1.2%	4.1%
Commercial Delay Cost ($M)	0	130	330
Commercial Cost ($M)	0	0	12,680
MDP System Cost ($M)	0	17	100
Total System Cost ($M)	0	147	13,110

Table 35. Model Results for Each Alternative

Table 35 shows the results of each model in tabular form. Of note, the commercial delay cost for Alternative 1 is $130M, while Alternative 2 is $330M. The total system cost is much higher for Alternative 2, but three times the amount of ships are inspected in Alternative 2. These results are for all ships entering the Port of Singapore.

4.6 DAMAGE MODELS

The SEA-7 Cohort developed damage models for each threat scenario to allow an evaluation and analysis of the performance, or level of defeat, that each integrated system architecture produced. The SBA damage model derived attack damage cost from the distance at which the response force defeated the explosives-laden attacking speedboat. The SAW damage model determined attack damage cost from the speed at which the tanker impacted the pier. The WMD damage model obtained damage cost from the distance at which the WMD device detonated from the pier; however, during simulation runs, a WMD attack was assumed to be either completely defeated due to detection at a safe distance, or the full damage occurred if the WMD was not detected. In all scenario damage models, damage cost was the result of a combination of the following costs, as applicable: structural repair, loss of life, environmental cleanup, and lost commerce.

4.6.1 Small Boat Attack Scenario Damage Model

The SBA damage model was designed to evaluate the overall performance model results. It was based on results garnered from the DOD Explosive Safety Board Blast Effects Computer, version 4,[105] which predicts the airblast from an amount of explosives at sea level. The DOD Blast Computer was used with the assumptions of a 1,000-lb TNT explosive, lightly cased and detonated at sea level. The relative over pressure at range

105 Air Force Safety Center, "Explosive Site Planning," Tools,.http://afsafety.af.mil/AFSC/RDBMS/Weapons/oteam_site_planning.htm#tools, (accessed 20 February 2005).

was then compared to known failure points of structures. With this information, it was determined that sheet metal panels would buckle if this explosion occurred at 65m, and oil tanks would rupture if the explosion was at 35m. These calculations lead to the distribution of damage from the modeling results.

The cost of the damage associated with the SBA was a compilation of the repair and salvage costs for the ship that was attacked, as well as the cost of environmental cleanup. For the purpose of this exercise, the HVU was assumed to be a crude oil tanker, similar to the French-flagged MV LIMBURG. The scenario HVU was assumed to be carrying in excess of 90,000 tons of crude oil in a single-hulled tanker. The Estimating Cleanup Costs for Oil Spills model,[106] Figure 118, was then used to compute estimated damages for the scenario.

[106] Dagmar Schmidt, "Estimating Cleanup Costs for Oil Spills," *1999 International Oil Spill Conference*, http://www.environmental-research.com/publications/pdf/spill_costs/paper6.pdf, pp. 1-10.

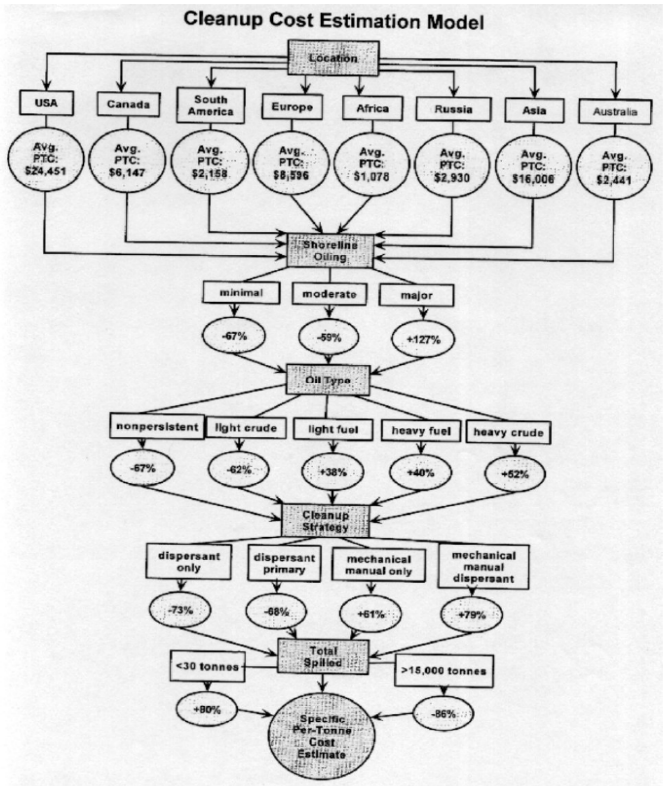

Figure 8: Per-Tonne Cost Estimation Model (based on data from the *OSIR International Oil Spill Database*). The per-

Figure 118. Oil Spill Intelligence Report Oil Spill Per-Tonne Cost Estimation Model

This model was used for the environmental cleanup costs for the spills associated with the MDP scenarios. This model takes into account the location of the spill, the amount of shoreline contamination, the cleanup methodology, the type of oil spilled, and the amount spilled. It does not include any environmental damage fines, or lost revenue, associated with a degraded fishing habitat.

With the spill occurring in Asia, with major shoreline oiling of heavy crude oil, and a mechanical manual cleanup strategy, the estimated cleanup cost was $39,054 per ton. With the spill occurring in Asia, with moderate shoreline oiling of light fuel oil, and a mechanical manual cleanup strategy, the estimated cleanup cost was $8,600 per ton. These represented the worst- and best-case scenarios for an oil spill in the Straits of Malacca. The damage was then equated to the cost through an equation linking the probability of successfully defeating the attack outside of 65m, between 65m and 35m, and inside of 35m to the cost of the damage associated with an explosion at that range. The environmental damage cost was computed for both a heavy crude spill and a light fuel spill, and the average was used for the damage model. Figure 119 shows the three levels of damage.

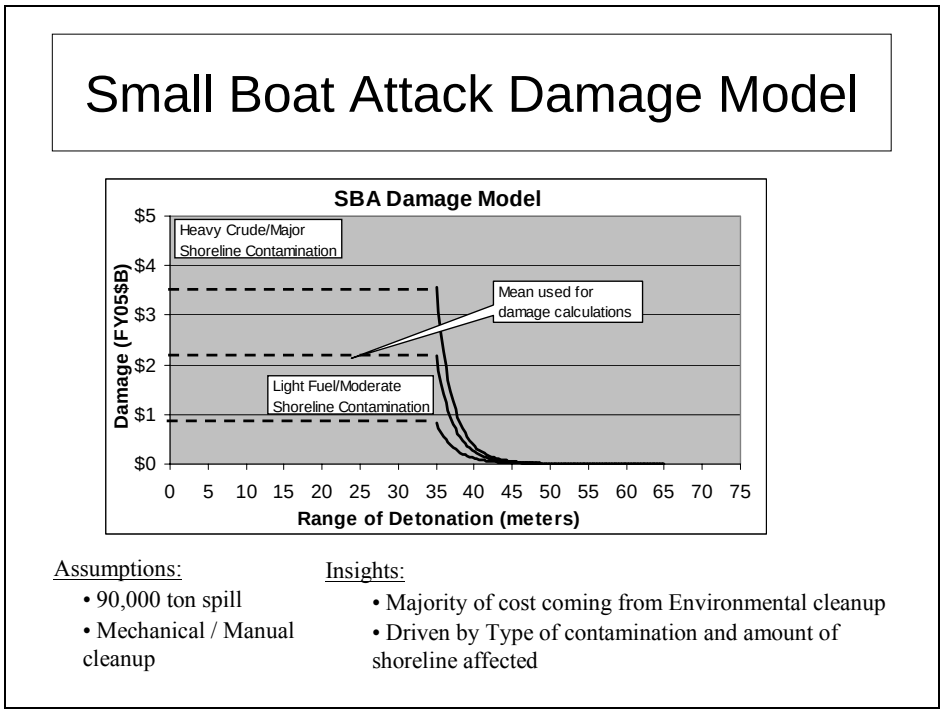

Figure 119. SBA Damage Model

The damage model for the SBA scenario assumed that the detonation of 1,000 lbs of TNT outside of 65m from the hull of an oil tanker would only cost $10,000 for paint and glass repair. Alternatively, the same blast occurring inside of 35m would cause full damage.

4.6.2 SAW Scenario Damage Model

The SAW scenario established the foundation of the myriad of assumptions utilized in the development of the SAW model. From the established scenario, the model was based on an 8,000-ton, 113-meter vessel loaded with 90,000 tons of raw crude oil. All calculations were established assuming an ambient air temperature of 82°F and 90% humidity. Initial pier damage calculations evaluated the relative energy of the ship at the following speeds: 5, 10, 15, and, 20 kts versus the strain rate of a modern pier. The pier strain rates were based on March 2001 construction data from the deep-draft pier at Changi Naval Base, Singapore. All calculations assumed the attack occurred at Mean Low Low Tide, the most widely accepted standard in the industry. The model assumed a direct collision, and reconstruction costs were based on analogy utilizing new construction costs interpolated per square foot, adjusted for economies of scale. The economic impact portion of the SAW model derived from the construction timeline, versus economic losses per day. The daily cost was based on Singapore's average daily

maritime commerce. The environmental cleanup costs surpassed all other costs associated with the SAW scenario, therefore special consideration was given to the accuracy of these cost estimates. Ship repair costs were evaluated using a direct analogy with the repair costs of the LIMBURG oil tanker. Figure 120 shows the results of the SAW damage model as a relationship of total damage cost to impact speed. The mean value was used for SAW damage calculations.

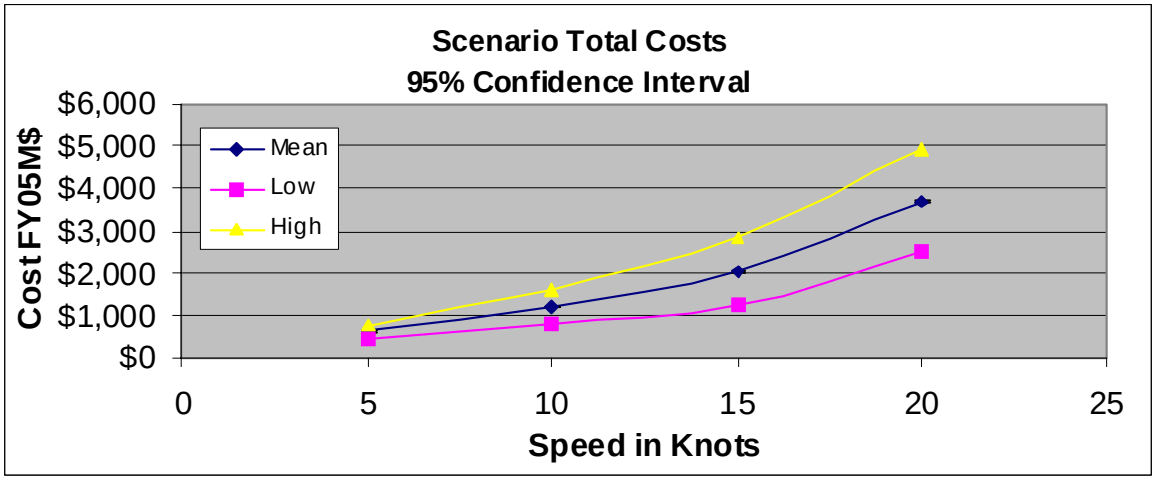

Figure 120. SAW Scenario Damage Model

The SAW damage costs assumed an 8,000-ton, fully loaded oil tanker rammed into a pier in Singapore. Damage costs included ship repair, pier reconstruction, economic impact, and environmental cleanup.

4.6.3 WMD Scenario Damage Model

In order to design a WMD model that would provide reasonably understandable outputs, limiting assumptions in addition to those established in Threat Scenario 3 (WMD), were established. The weapon utilized in Threat Scenario 3 was established as a 1970s-era, 20-KT, Soviet-made, nuclear device—the same yield as the weapon employed at Nagasaki.

This weapon was chosen primarily due to the following considerations: 1) This kind of nuclear weapon would be a relatively attainable nuclear device, with damage results significant enough to produce more harm than current conventional devices, and 2) destruction effects of 20-KT nuclear devices were more accurately documented than other nuclear detonation yields. The most important assumption was that the weapon was

ground-detonated. If terrorists were able to propel the weapon to 1,850 feet above sea level, the destructive effects would be enhanced significantly, resembling the destructive effects observed at Hiroshima.

The WMD damage model represented three categories of economic impact:

1. Destruction of structures.
2. Economic impact associated with the loss of productive capability.
3. Cost of life.

The model for the destruction of structures was based on the following standard destructive categories: Window Breakage, Wood-Framed Building Destruction, Multistory Brick, and Multistory Reinforced Concrete Offices. Destructive arcs were calculated at: the Port of Sembawang and at the following distances east of Sembawang, within the channel: ½, 1½, and 3½ miles. Portions of destructive effectiveness were interpolated, but no information was extrapolated. Reconstruction expenses ranged from $0 to $284 FY05M.

Economic impact was computed using the ratio of the area destroyed (modeled in section 1) to the total area of Singapore, per projected reconstruction period, versus the Gross Domestic Product (GDP). Estimated economic impact ranged from $0 to $400 FY05M.

Cost of life was the primary factor in the WMD damage model. Loss of life calculations utilized a ratio of the overall area established where overpressure would reasonably exceed 35PSI, and a stochastic model representing the conversion of objects into missiles due to the explosion, versus the corresponding population in the affected area. Each life below age 70 was valued at $3.7 FY05M referencing an Environmental Protection Agency (EPA) cost-benefit analysis conducted in 2002, which revised previous estimates of the economic feasibility of removing arsenic from drinking water.[107] These results were adjusted to reflect the current price index. Life cost estimates ranged from $0 to $193,584 FY05M, far surpassing the other two portions of

[107] OMB Watch, "Pricing the Priceless," http://www.ombwatch.org/article/articleview/616/1/134?TopicID=3, (accessed 15 February 2005).

the cost model, as seen in Figure 121. Integration of the three cost factors provides cost estimates ranging from $566 to $194,282 FY05M.

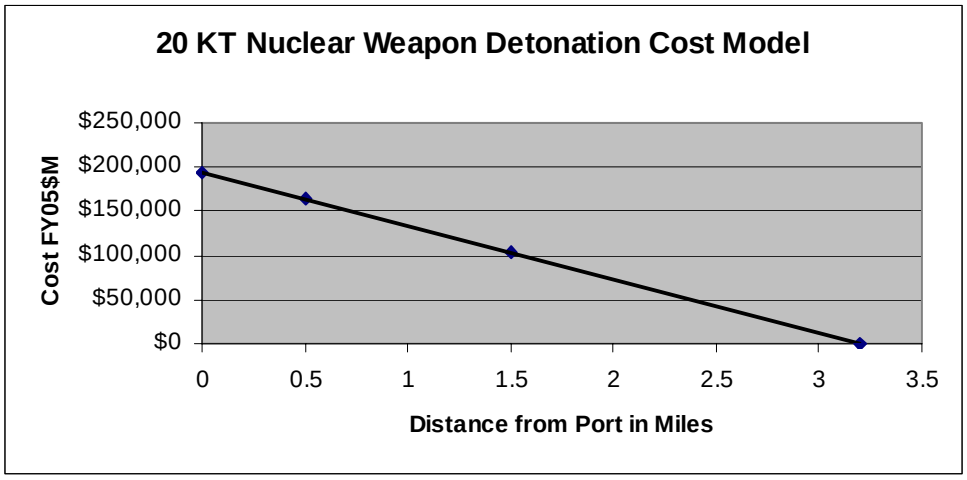

Figure 121. WMD Scenario Damage Model

The WMD Damage Model assumed a 20-KT, Russian-made, nuclear weapon detonated in Singapore harbor. The model included costs based on the destruction of structures, economic impact, and cost of life.

4.6.4 Integrated Architecture Models

The SEA-7 Cohort developed integrated system architecture models in order to obtain values for overarching MOEs and Metrics for each architecture combination of system alternatives (see Figure 122). The integrated architecture models, as represented in Figure , were specific to each threat scenario.

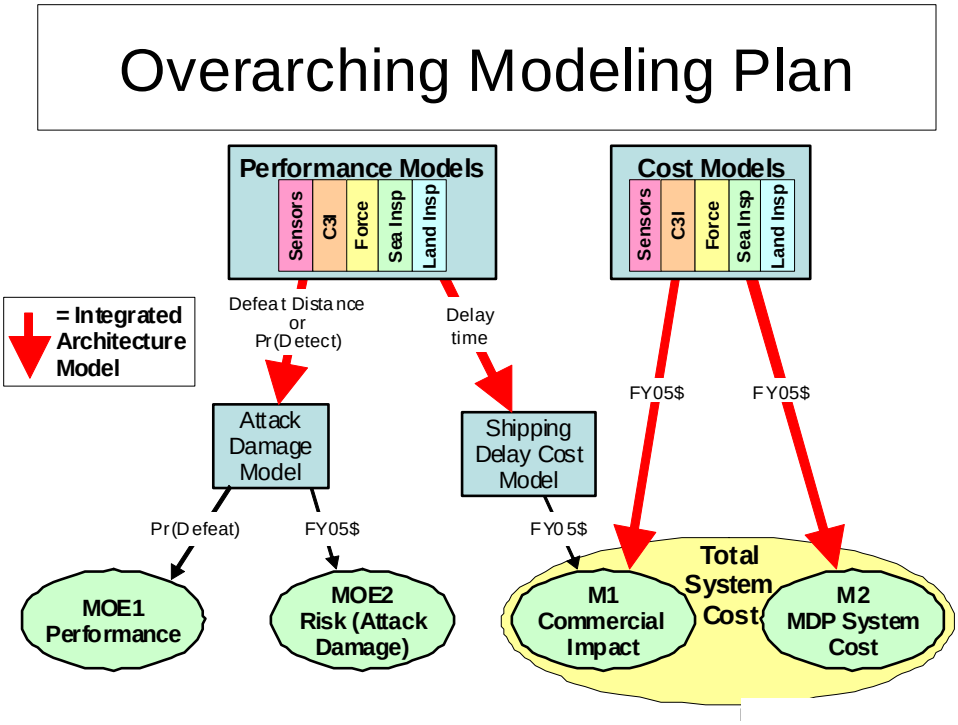

Figure 122. MDP Overarching Modeling Plan

The Overarching Modeling Plan pictorially showed the process of utilizing Integrated Architecture Models to transform inputs from individual system performance and cost models into the desired performance measure outputs.

For calculating MOE 1 (Performance) and MOE 2 (Risk) in the SBA and the SAW threat scenarios, the integrated architecture model used Time-To-Go (TTG) until the attack was complete as the common element passed between system models. The integrated architecture model for the WMD threat scenario used a Bayesian model in which probabilities of inspection and detection for the various systems were linked to give the final outcome. Metric 1 (Commercial Impact) and Metric 2 (MDP System Cost) were directly calculated as a summation of the system costs for all architecture system combinations, regardless of threat scenario. However, Commercial Impact (Metric 1) for the WMD threat scenario also included commercial delay costs that resulted from queue delays and false alarm delays in the cargo inspection process. These commercial delay costs were calculated by running the delay time output from the integrated architecture model through the Shipping Delay Cost Model to determine a cost estimate.

4.6.5 WMD Scenario Results

4.6.5.1 MOE 1 Performance

Approach: The performance model for Scenario 1 (WMD Attack) was designed to incorporate the overall performance values for WMD detection from each functional group within the MDP Group. The first task was to identify the performance output by creating a "probability tree" shown in Figure 123. The various paths of the tree represented the likelihood of finding WMDs in a container, or conversely not finding WMDs in a container (attack success), given that WMDs were in a container.

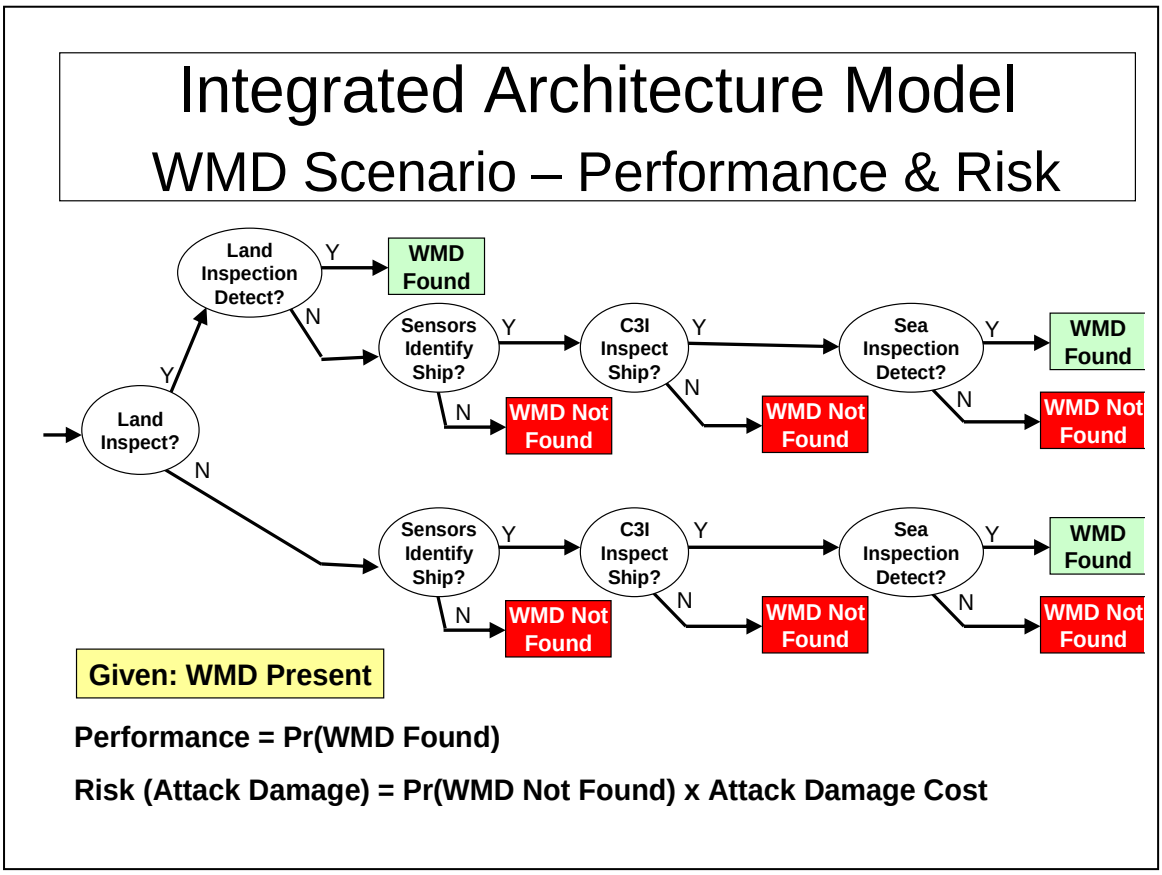

Figure 123. Probability Tree for Overarching WMD Performance Model

This figure shows the notional probability tree used in creating the overarching performance model for the WMD scenario. The overarching model incorporates all of the performance inputs from each group within the MDP Group.

Once the different system values were assigned to the model, a matrix was created in a Microsoft Excel™ spreadsheet to account for all 109 combinations of five

systems each with three alternative architectures. Using Bayes' theorem for conditional probability, a model representing Figure was developed. This model computed the various combinations of probabilities for "WMD found" and was built as an imbedded equation within the same spreadsheet. Performance values for each group's alternatives were then inserted into the equation for a particular combination. Thus, the performance value, or the overall probability of finding WMDs onboard a ship, was generated.

MOEs:

- The probability that WMD is found by the system given that a WMD is present.

Assumptions:

- Sensors can detect all high interest vessels. The Sensor Group Systems design assumes that all high interest vessels are using the AIS implemented in the region.
- C3I decision-making performance can be represented by a number (probability) – This allows the use of a probability for modeling purposes.
- All cargo can be separated by the Land Inspection System. The Land Inspection System is capable of searching each container individually instead of a mass of containers for more precise detection capabilities.
- Enemy possesses no ability to adapt to system. This is a simplifying assumption for modeling purposes.

Inputs (as seen in Figure 124):

- Probability of Land Inspection.
- Probability of Detection given a Land Inspection.
- Probability that the Sea Inspection System detects the WMD.
- Probability that the Sensors System detects the ship.
- Probability that C3I recommends appropriate vessels for Sea Inspection.

Scenario	Land	Land Pd	Land Insp	Sea	Sea Pd	Sensors	Sensors Pd	C3I	C3I Pd
WMD	As-Is	0.99	0.02	As-Is	0	As-Is	1	As-Is	0.2
	1	0.88	0.47	1	0.25	1	1	1	0.35
	2	0.94	0.74	2	0.25	2	1	2	0.68

Figure 124. Inputs to WMD Scenario Performance Model

This figure shows the performance inputs for the WMD scenario performance model from each group within the MDP Group.

Description: As seen in Figure , the Excel™ model for Land Inspection, "As-Is" and Alternative 1, the probability that a land inspection occurs and the probability that detection occurs given there was an inspection, constituted the first and second branches of the probability tree, respectively. The third branch contained the probability that the Sensor System identified the ship. Since the Sensor System was designed to have a probability of identification of 1.0, the outcome of this branch was always positive. The fourth branch was the probability that the C3I System recommended the appropriate vessel to the Sea Inspection System. The final branch was the probability that the Sea Inspection System detects the WMD.

The Extend model for Land Inspection Alternative 2 followed the same path above with a branch added before the probability of land inspection to account for the probability that cargo comes from a trusted shipper, and the probability that the trusted shipper would "find" or at least deter WMDs.

Results: Each combination of the WMD scenario Excel™ model performance values were plotted against the relative combination of system alternatives. Three distinct series groups of points with similar performance ranges were observed, as in Figure . These three regions were due to performance increases of the Land Inspection System. Within these groups, smaller spikes occurred in groups of eight. The smaller spikes were due to performance improvements in the C3I System.

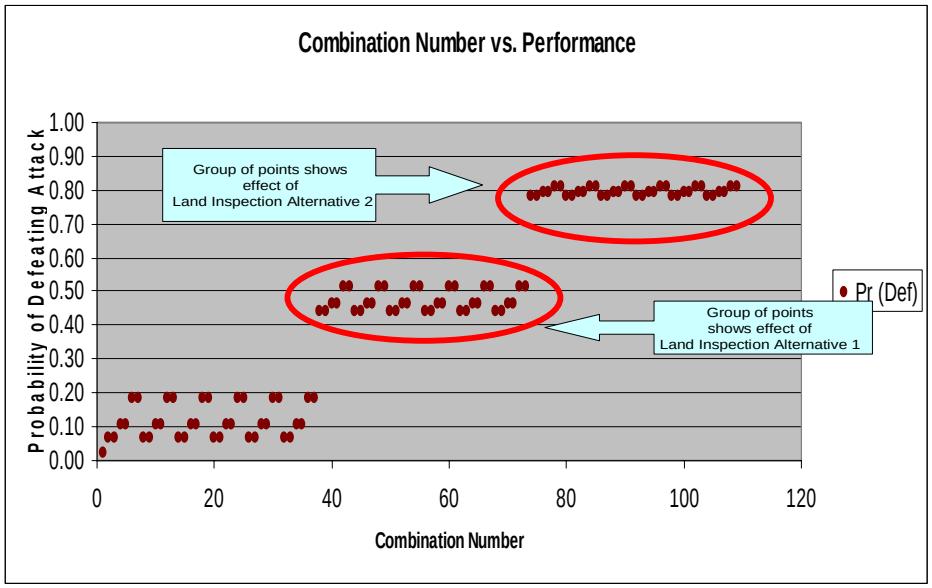

Figure 125. Plot Showing Increase in Performance Due to Land Inspection System Across Combinations

This figure shows the increase in performance of the MDP System as combination number changes. Note the three regions of similar performance due to the Land Inspection System alternatives. The smaller spikes within these regions represent performance improvements due to the C3I System alternatives.

4.6.5.2 MOE2 Risk (Attack Damage)

Approach: The risk model for Scenario 1 (WMD Attack) was determined from the complement of the performance model. Risk was calculated by multiplying the probability of failure (1 minus the probability of finding WMD) by the WMD scenario attack damage cost.

MOEs: The expected damage cost resulting from the system architecture failing to find WMD given that WMD is present.

Assumptions: Same as WMD scenario Architecture Performance Model.

Inputs: Same as WMD scenario Architecture Performance Model.

Description: Same as WMD scenario Architecture Performance Model.

Results: Each combination of the WMD scenario Excel™ model risk values were plotted against the relative combination of system alternatives (see Figure 126). Similar to the performance graph, three distinct series groups of points with

similar performance ranges were observed, due to performance increases of the Land Inspection System.

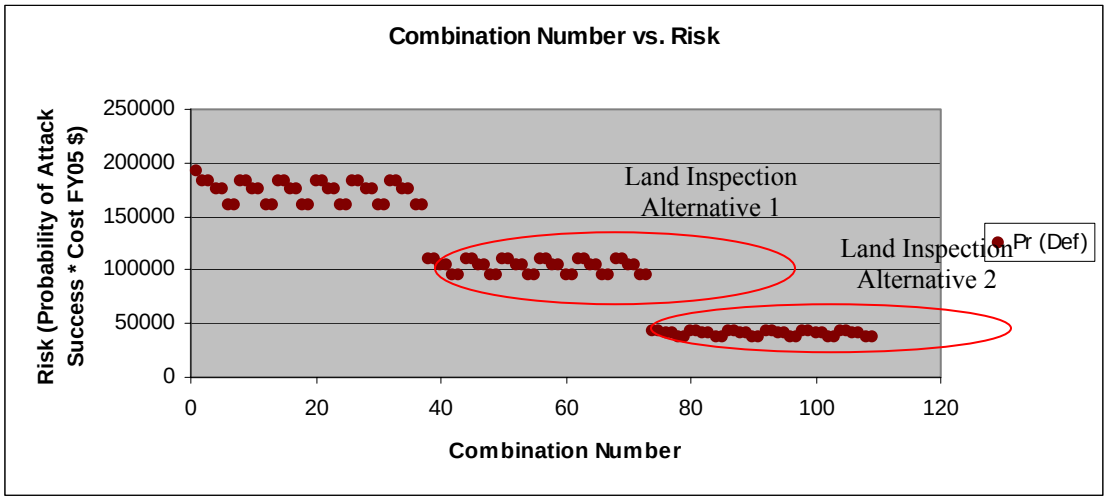

Figure 126. Plot of Combination Number vs. Risk

Risk was calculated by multiply the probability of attack success by the cost of failure. There were three regions of similar performance due to the Land Inspection System alternatives.

4.6.5.3 M1 Commercial Impact

The Commercial Impact Integrated Model estimated both of the separate costs incurred by the commercial maritime industry: system costs and delay costs. These costs are inversely related. Specific examples of commercial system costs included the cost to purchase and maintain Smart containers and the cost to maintain a "Trusted Shipper" certification. Delay costs were opportunity costs representing the lost revenue the commercial maritime industry forfeited in order to implement a specific alternative architecture. These costs have been determined in the Shipping Delay Cost Model. Both categories of commercial impact were evaluated for each combination of alternatives: "As-Is," Alternative 1, and Alternative 2. The resultant combination outputs denote the cost of each system alternative combination. There were 109 separate combinations (results shown in Figure 127, which represent 109 individual cost alternatives, for system costs and delay costs. The land alternatives represented in combinations 36 to 109 represented a majority of the shipping delay costs, while sea inspection Alternative 2 imposed the most serious cost fluctuations to the alternative combinations designed to prevent a WMD attack. The rise in both categories of

commercial costs differs from all other portions of the integrated model, but this anomaly is the result of differing concepts of accepted risks. Alternative 2 is clearly less risk-adverse than Alternative 1.

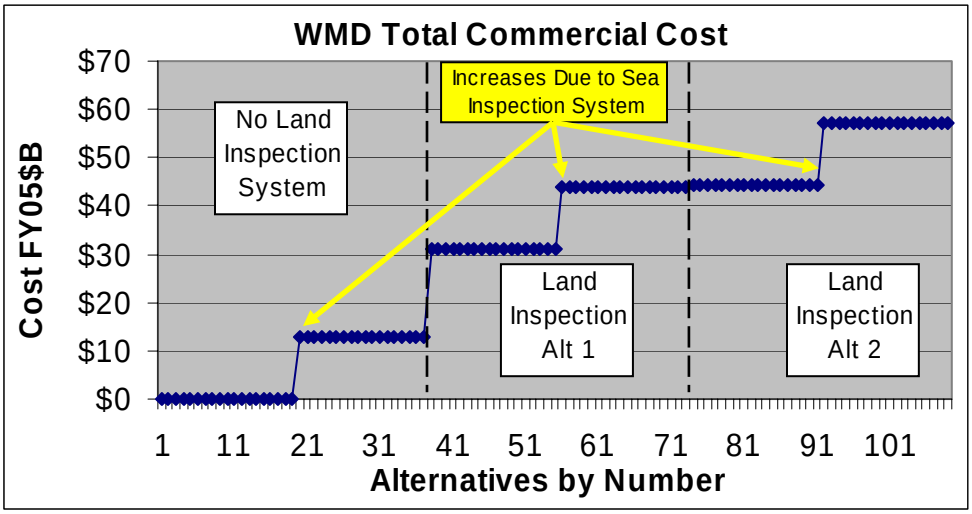

Figure 127. Commercial Impact for WMD Scenario

The Commercial Impact Costs for all 109 system architecture combinations shows the significant influence of the Land Inspection System alternatives, and the influence of the Sea Inspection System alternatives on Commercial System Costs.

4.6.5.4 M2 MDP System Cost

The MDP System Cost Integrated Model evaluated the MDP System Cost for all system architecture combinations. In keeping with the rest of this project, all figures were in FY05$M, and covered a time period of ten years. As previously discussed, there were 109 separate cost combinations the WMD System could utilize to combat WMD infiltration. Evaluation of these combinations clearly suggested that the Land Inspection system costs drove the overall system costs. The large changes seen in alternatives 36 represents the change from the land "As-Is" System, to the two Land Alternatives, as seen in Figure 128.

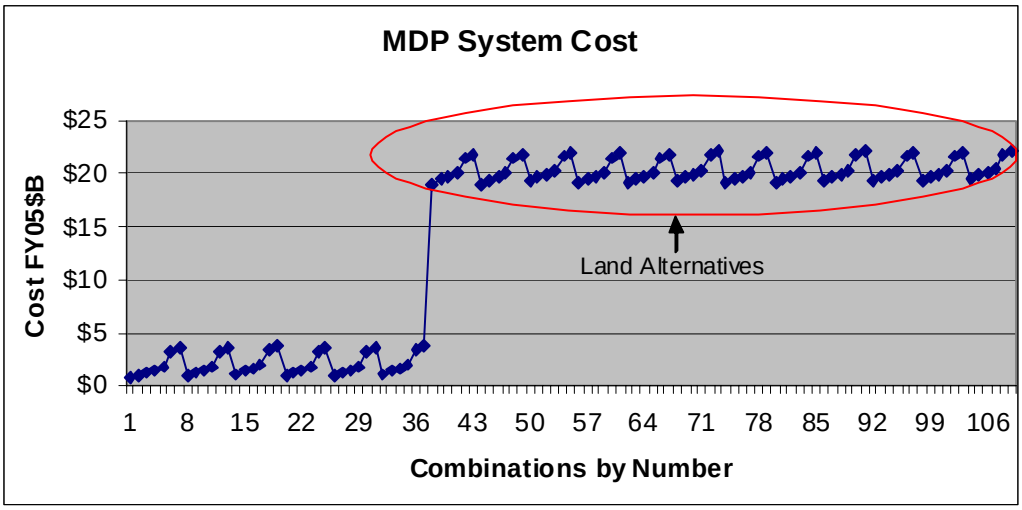

Figure 128. MDP System Costs for WMD Scenario

The MDP System Costs for all 109 system architecture combinations show the significant influence of the Land Inspection System alternatives. The large shift in the data indicates architecture combinations without a Land Inspection System to those with Land Inspection System Alternative 1 and Alternative 2.

Analysis: The graph in Figure 129 shows a comparison of performance and cost for the "As-Is" and Alternative Systems.

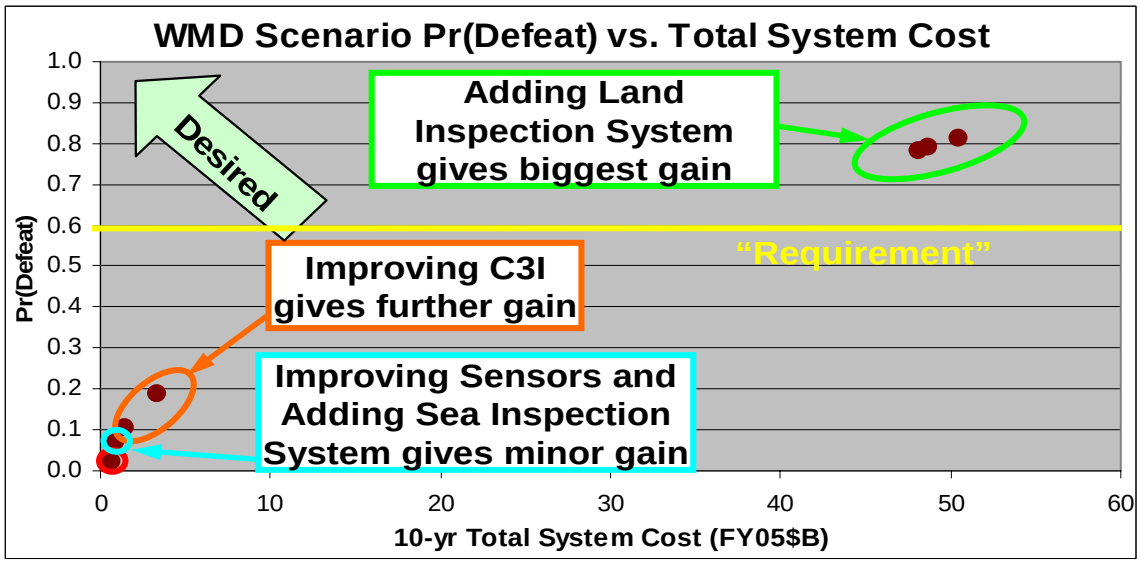

Figure 129. Alternative Performance vs. Total System Cost

The graph shows that Land Inspection gives the required performance, but at great cost. Total System Cost includes MDP and Commercial Cost and Commercial Delay Cost.

In the performance versus cost comparison, the desire was to have the highest performance with the least cost as indicated by the "desired" arrow in Figure 129. The improvements provided by alternatives to Sensor and Sea Inspection Systems improved performance over the current system. The improvements to C3I capabilities further increased performance, but did not meet the requirement threshold of 60%. Land Inspection, combined with improvements to C3I, increased performance well above the requirements threshold, but at a cost of over $50B.

The graph in Figure 130 shows a comparison of risk and cost for the "As-Is" and Alternative Systems.

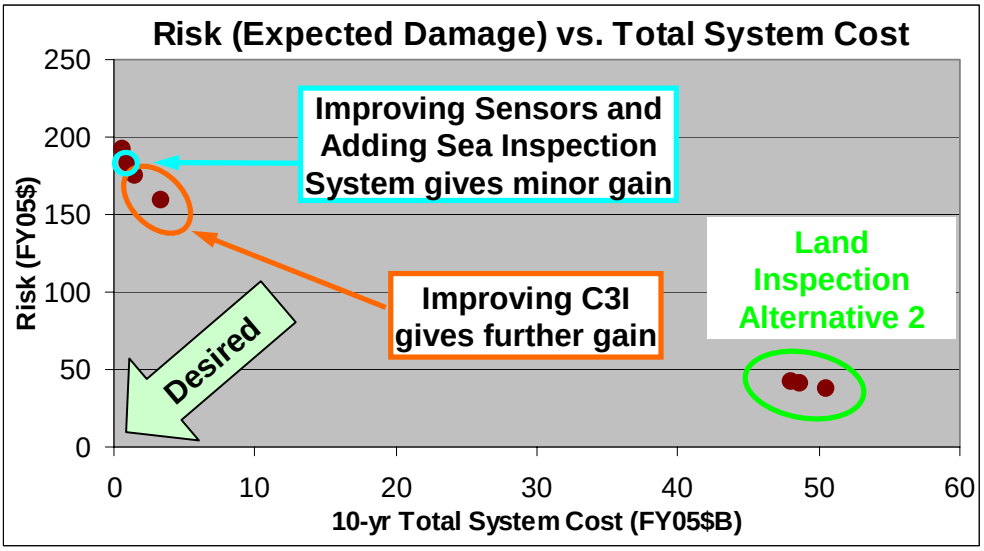

Figure 130. Alternative Risk vs. Cost

The graph above shows a low-cost gain from adding Sea Inspection and improving Sensors and C3I.

In the risk versus cost comparison, the desire was to have the lowest risk with the least cost as indicated by the "desired" arrow in Figure 131. As expected, the effects of each alternative on risk mirrored their effects on performance. The improvements to the Sensors and Sea Inspection Systems reduced risk the least. Land Inspection significantly reduced risk, but at a very high cost.

Land Inspections "Trusted Agent" System included implementation in 15 high volume ports of origin. Sensitivity analysis was performed by reducing the number of "Trusted Agent" ports. The results are shown in Figure 131.

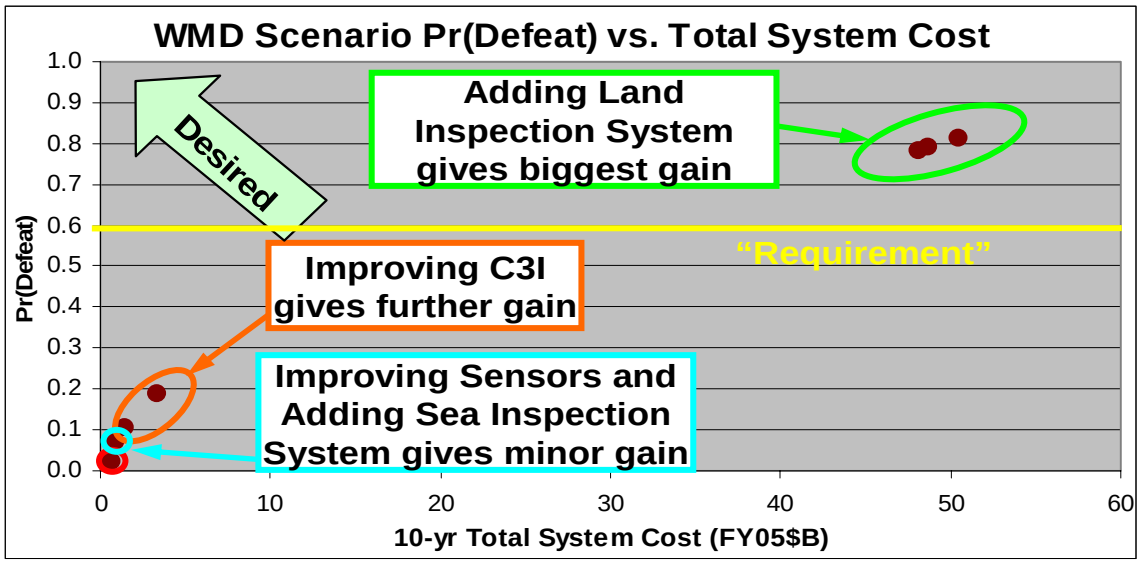

Figure 131. Effect Reducing "Trusted Agent" Land Inspection Alternative Implementation on Performance and Cost

Decreasing Highest-Volume ports of origin using Land Inspection System reduces cost, but performance stays above requirement. The series of numbers above the points (1, 5, 10, 15) indicated the number of ports where the Trusted Agent" System was implemented.

Decreasing the number of "Trusted Agent" ports moves performance versus cost toward the desired "high Performance/Low Cost" region of the graph in Figure . Yet, the decrease in performance is minimal, compared to cost reduction, when reducing the number of trusted agent ports from 15 to 1. However, it must be acknowledged that a "smart" enemy is not assumed. This means, as expected, the effects each reducing the number of Trusted Agent on risk mirrored the effect on performance, as shown in Figure 132. The combination of Coastal Radar Stations (X-band) + HFSWR (Sensor Alternative 1), a boarding team inspection (Sea Inspection Alternative 1), a network centric C3I System, and reducing the number of high volume "Trusted Agent" ports, provided minimum risk at the least cost. However, reducing the number of "Trusted Agent" ports does not consider an "Intelligent" adversary. Terrorists will simply not utilize ports that are considered "Trusted Agents."

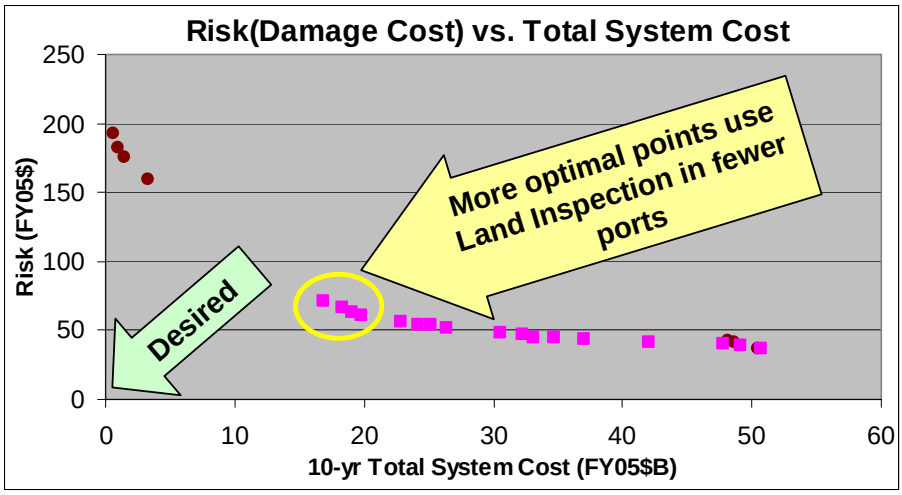

Figure 132. Effect Reducing Trusted Agent Ports on Risk and Cost

Decreasing Highest-Volume ports of origin using Land Inspection System reduces cost, but risk stays below the other alternatives.

4.6.5.5 SAW Scenario Results

For the SAW scenario the attack timeline used time to go for measuring the time of the scenario. The attack began at TTG0. The Sensors System detected the attack at TTG1. The C3I System decided to engage at TTG2 and the Force System responded and defeated the attack at TTG3. This TTG3 was evaluated against 0. If TTG3 was less than 0, the attack was successful with full damage. If TTG3 was greater than 0, the defeat distance was calculated from TTG3 and the attack damage was determined from the scenario Attack Damage Model. Luckily, the C3I System was capable of near instantaneous identification of intent, well outside of the harbor limits, therefore allowing the maximum engagement range for the Force alternatives of five miles.

For this threat there were 11 combinations of alternatives between the "As-Is" System and the alternative combinations developed by the Force, Sensor, and C3I alternative designs. These combinations were compared on the basis of performance against the attack, as well as the cost of the respective alternatives. It was discovered that C3I and sensors were severely limited by the scenario. Even the "As-Is" System was evaluated as adequate for the scenario selected as it met the requirement for 80% P(defeat) as seen in Figure 133. This shows that for close in altercations, the "As-Is"

System is functional and sufficient. However, this does not account for SAW engagements outside of the defined harbor area. If the scenario were to be expanded outside of the harbor limits, the results might differ dramatically. This is a possible realm for future work, as it was not addressed with this study.

The best performance of all of the alternatives came with the use of Force Alternative 2, using a combination of patrol craft and Sea Marshals. This allowed over 91% of all SAW attacks to be stopped with no damage to port facilities. Figure 133 shows the different combinations of alternatives and their respective probabilities of defeating the SAW threat.

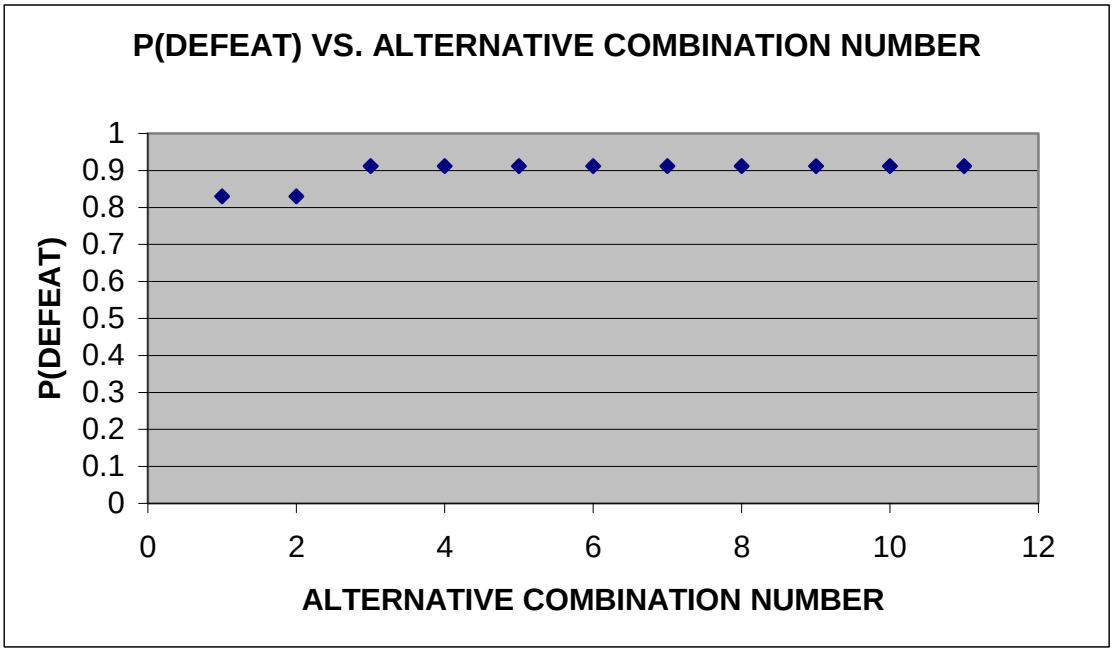

Figure 133. P(Defeat) vs. Alternative Combination

This graph shows the different P(Defeats) as associated with the combinations of C3I, Sensors, and Force alternatives. The first two points represent the "As-Is" System and the Force Alternative 2 System. The other points show the relative ineffectiveness of changing the C3I and Sensors alternatives.

Figure 134 shows the improvements that could be made by adding the harbor patrol craft to the existing Sea Marshal force. Because of the capabilities of both Sensors and C3I alternatives, the Force alternatives were allowed to engage at the maximum range, as defined by the scenario. Hidden behind this is the fact that it was the scenario

that restricted the findings. If the Force alternatives were allowed to engage beyond the harbor limits, the C3I and Sensors alternatives would have a much more noticeable impact on the results.

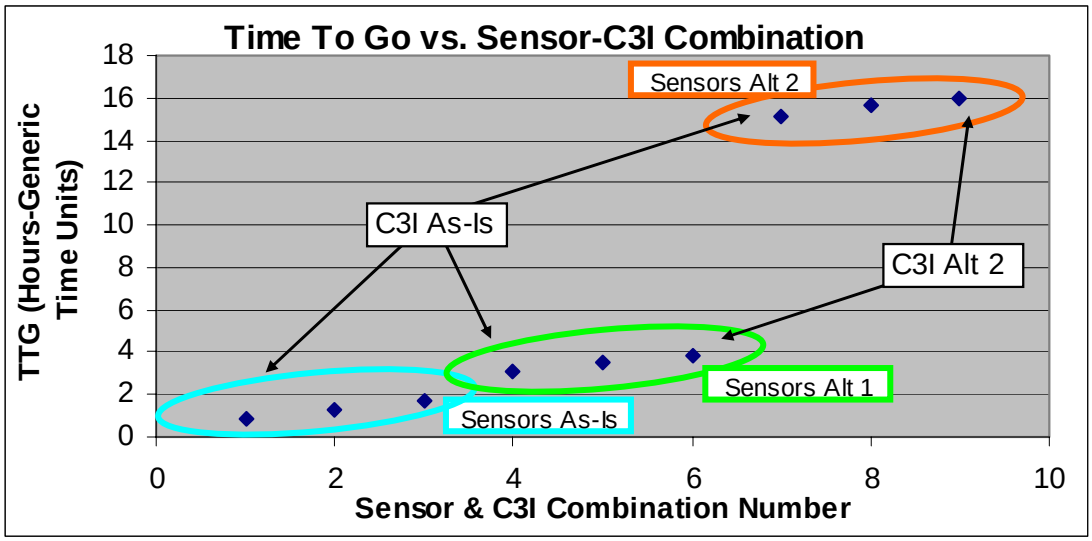

Figure 134. Time-To-Go vs. Sensor-C3I Combination

Time to go (TTG) following Sensor detection and C3I analysis/decision for the nine different Sensor-C3I System combinations. Sensors Alternative 2 has the biggest effect on giving the desired high TTG. C3I has a smaller effect.

4.6.5.6 MOE2 Risk (Attack Damage)

The risk associated with the SAW scenario was a compilation of the costs associated with both the reconstruction of the damaged port facility, the repair to the SAW vessel, the environmental cleanup costs, and the lost revenue to the port. It became apparent that the major cost driver was the environmental cleanup costs. Using the approved oil spill cleanup model, with a 90,000-ton spill within the port facility, the cost of cleanup would exceed $2.2B (FY05$).

To calculate the risk, the probability of successfully stopping the SAW attack was subtracted from one. The resulting probability was then multiplied by the cost of an attack. This was done for every combination of Sensor, C3I, and Force alternatives and can be seen in Figure 135.

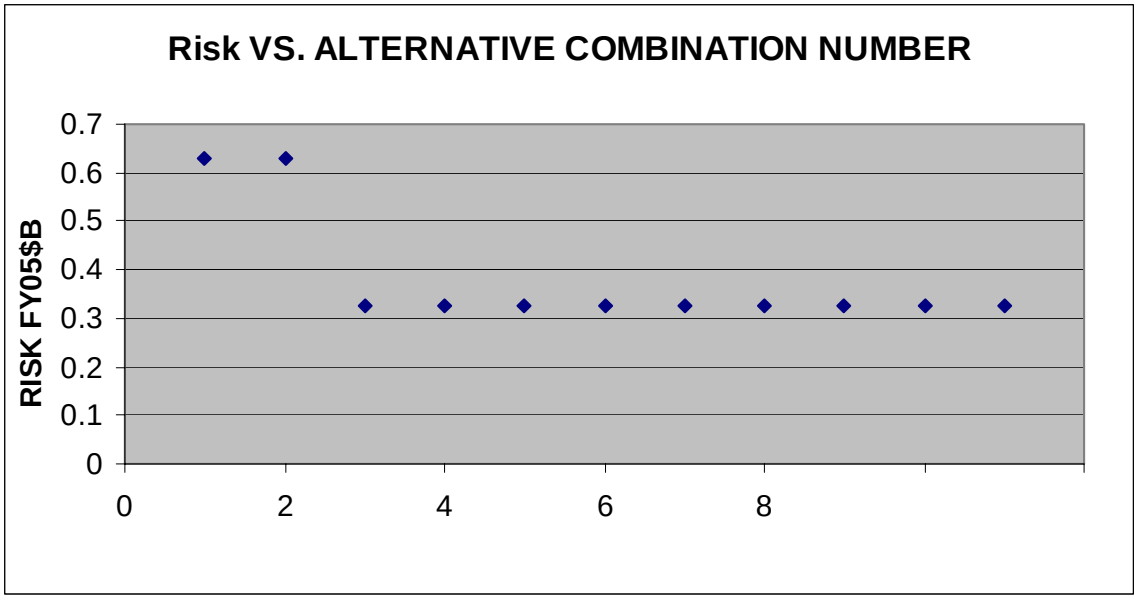

Figure 135. Risk vs. Alternative Combination Number

4.6.5.7 M1 Commercial Impact

There were no commercial impact costs associated with the SAW scenario.

4.6.5.8 M2 MDP System Cost

In the SAW scenario, Land and Sea Inspection did not actively participate so their costs were not considered in the evaluation of combinations. Because of their absence, C3I drove system costs, while Force and Sensor alternatives caused only fluctuations in the MDP System Cost, as seen in Figure 136. The three peaks in the cost combinations displayed in alternative combinations 5, 8, and 11 represented C3I Alternative 2. At a system cost of $ 2.9B, C3I Alternative 2 constituted at least 96% of the total costs in three combinations included in C3I Alternative 2. C3I Alternative 1 represented 65% of combinations 4, 7, and 10.

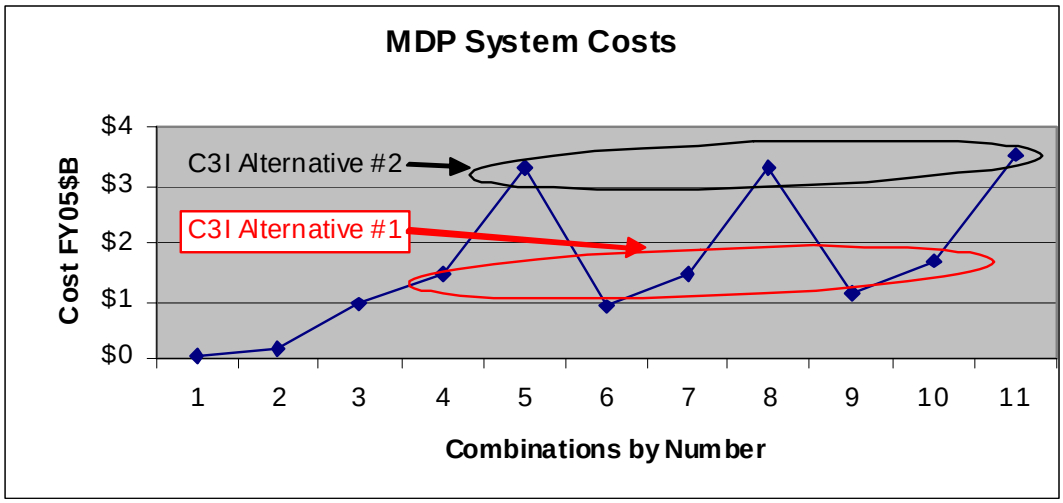

Figure 136. MDP System Costs for SAW Scenario

The C3I alternative drove the MDP System Cost for the SAW scenario. The three peaks in the data show that C3I Alternative 2 was by far the most costly.

4.6.5.9 SAW Analysis

The SAW scenario reflected several insightful findings. The major insight was that the scenario that was selected to test the system actually was a restriction to determining the full system capabilities. It was believed prior to modeling, that the performance of the system would be best tested by looking at the scenario that represented the smallest reaction time possible. This was determined to be an attack discovered within the port limits. However, C3I modeling showed that it was possible to determine an attack before hostile intent was shown, therefore allowing the Force alternatives the maximum engagement range of five NM. Figure 137 shows the performance of the alternative combinations with respect to their costs. This shows that it is possible to spend more money on C3I and Sensors alternatives, with no performance gain.

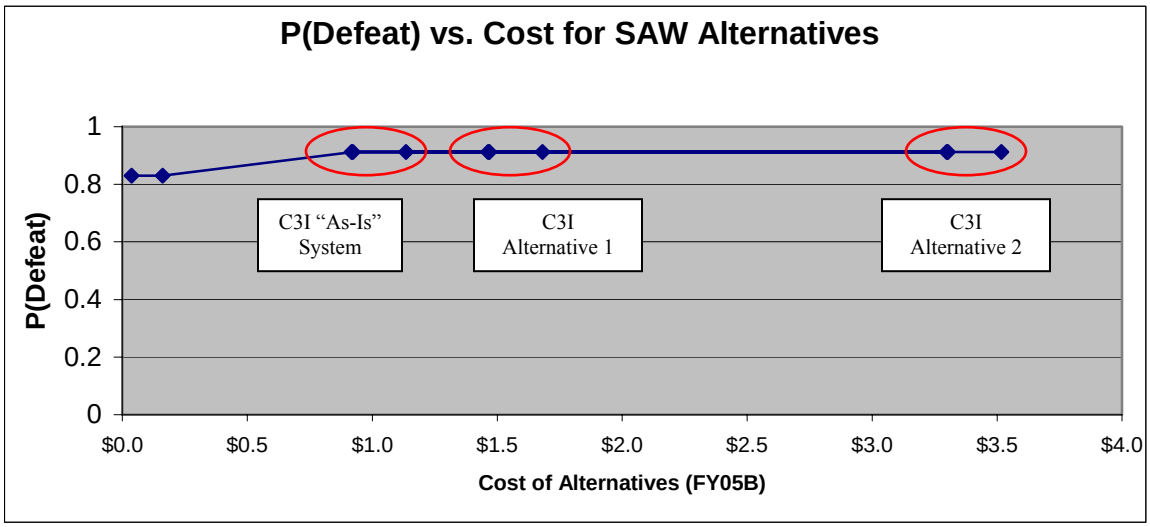

Figure 137. P(Defeat) vs. Cost for SAW Alternatives

This graph shows the nonexistent impact that C3I and Sensors had on the results of the SAW scenario. The major driver of performance was the Force alternative.

The risk followed a similar pattern. Very little risk was mitigated due to C3I or Sensor alternative manipulation. The majority of the risk was countered by the choice of Force alternative. Figure 137 shows the risk associated with the alternative combinations.

4.6.5.10 SBA Scenario Results

The SBA scenario was originally designed to test the systems against a small, fast-moving threat that gave very little warning. This was thought to be the hardest of the scenarios for all of the MDP Subgroups, because it required extensive amounts of detailed identification and analysis to accurately determine hostile intent. However, it was soon apparent that the amount of time given for a SBA scenario would restrict any type of reactionary force, except for a point defense force. The two alternatives that were developed by the Force Group included a Sparviero hydrofoil on random patrol and an embarked Sea Marshal option.

Both of these options were considered independently of the C2 and Sensors alternatives, as it would be overwhelming for sensors to attempt to track and identify all of the small boats in the AOR. Additionally, there were no C3I Systems

available that would meet the time restrictions imposed by the scenario. The C2 was assumed to be onboard the combatants, ether in the form of the Combat Information Center (CIC) on the Escort vessel, or as the Sea Marshal team leader on the HVU. It was assumed that the platforms would have to have sensor capabilities to identify the target, and would have the Rules of Engagement (ROE) in place to engage the target after identification.

4.6.5.11 MOE1 Performance

Overall, the Sea Marshals in Alternative 1 were able to completely defend 92.5% of all HVUs that they were deployed on, and mitigated the damage to another 2.5%. This allowed only 5% of all SBA attacks to be deemed a full success with the associated damage and environmental impact. The Sparviero random patrol option of Alternative 2 allowed for only a 60% success rate. These findings are reflected in Figure 138.

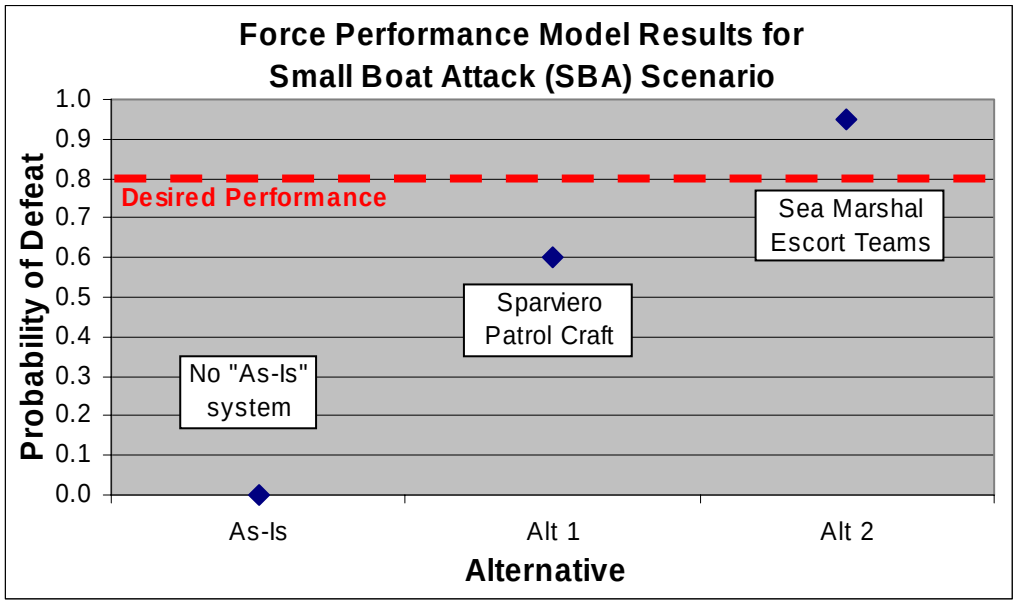

Figure 138. P(Defeat) vs. Alternative Combination Numbers for SBA

This chart shows the relative performances for each of the three Force SBA alternatives.

All of these results relied heavily on the assumption that hostile intent would be known with certainty, before the engagement commenced. This assumption was made on the initial belief that C3I would be able to determine hostile intent; however, as the modeling work progressed, this assumption became less valid.

The SBA scenario was an excellent test for the Force alternatives, but offered no insight as to the benefits gained by expending resources in either the C3I or Sensors alternatives. This was largely due to the time restriction placed on the study.

4.6.5.12 OE2 Risk (Attack Damage)

The risk associated with the SBA threat was calculated in a similar manner to the risk associated with a SAW scenario. The probability of the Force alternative stopping the attack was subtracted from one. The resulting probability, the probability of successful attack, was then multiplied by the expected cost of a small boat attack. The cost of an attack was based on the SBA Damage Model discussed previously. Figure 139 shows the risk associated with each Force alternative.

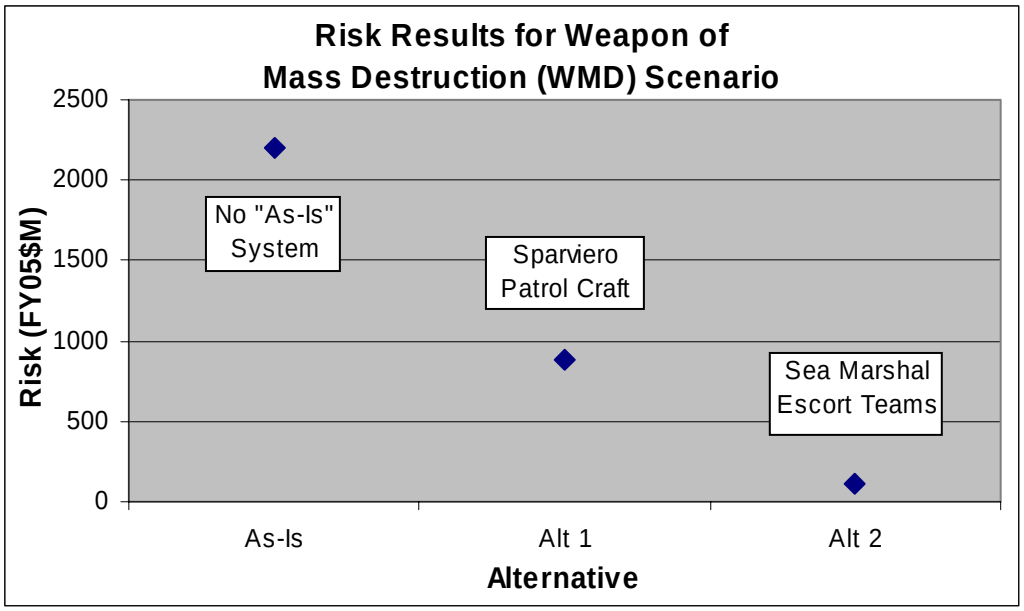

Figure 139. Risk vs. Alternative Combination Graph

This graph shows the risk associated with each of the Force alternatives given that there is an attack.

4.6.5.13 M2 MDP System Cost

Force was the only group that contributed system costs to the effort to thwart a SBA. There was no "As-Is" System. Alternative 1 set up a flexible system of reactionary forces, while Alternative 2 established a Sea Marshal Program that was less adaptive, but extremely cost efficient, as can be seen in Figure 140.

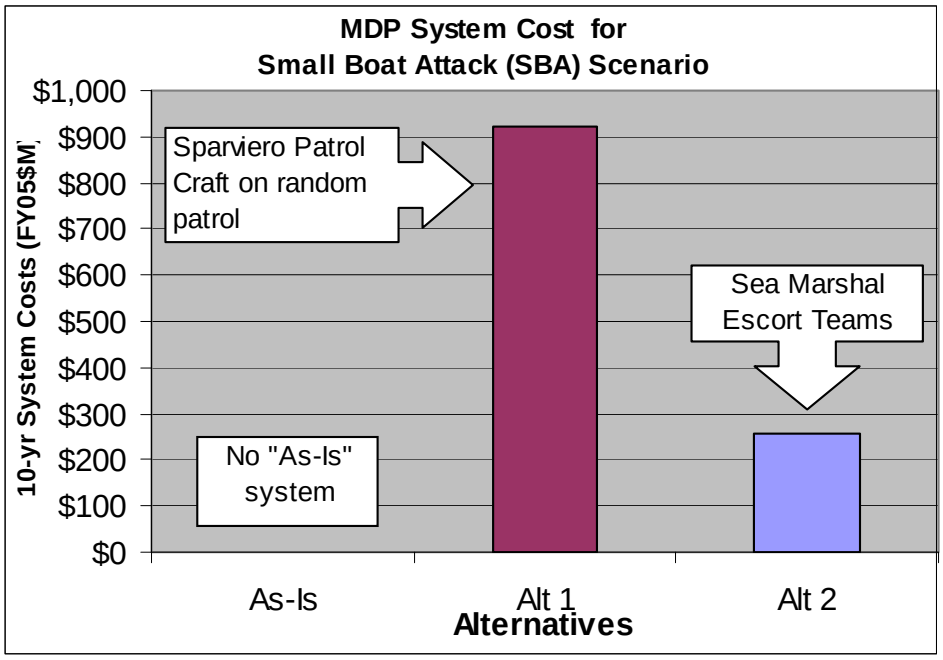

Figure 140. MDP System Costs are Represented Solely by the Force Group

This graph represents the MDP System Costs for the Force System alternatives, since they were the only system that contributed in the SBA scenario.

4.6.5.14 Analysis

Analysis of the SBA scenario showed that Alternative 2 (Sea Marshal escort) was the only alternative that was effective at countering the SBA threat (see Figure). The Sparviero hydrofoils used on random patrol only gave 60% probability of defeat. However, the patrol craft gave an additional potential gain in the realm of deterrence. The presence of armed hydrofoils patrolling the Straits would indicate that efforts were underway to counter terrorist threats; however, determining the deterrence gained was beyond the scope of this study.

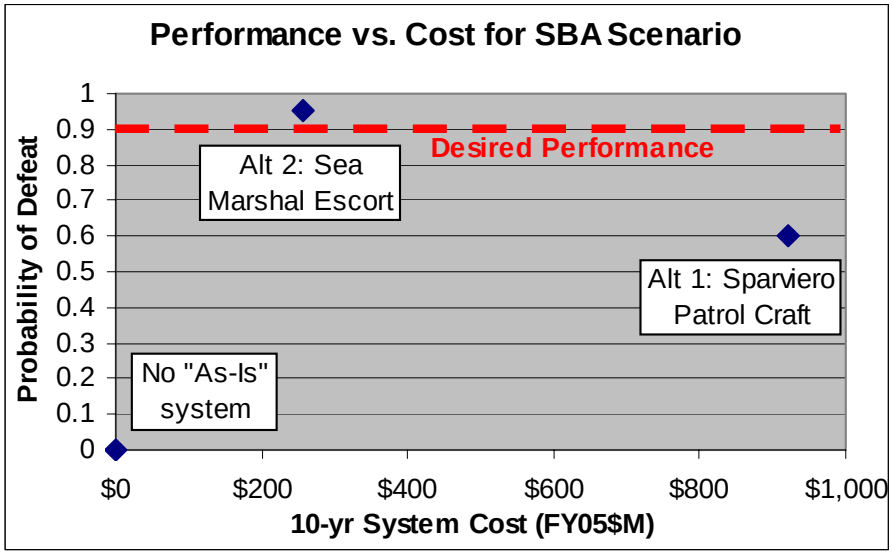

Figure 141. Performance vs. Cost for SBA Scenario

This graph shows the cost versus benefit for the Force System alternatives in the SBA scenario. The Sea Marshal escort was not only the sole alternative that met the desired performance criteria, but it was also cost-effective.