2006-04

An Integrated Systems Architecture to Provide Maritime Domain Protection

McCarthy, Chris

þÿJDMS, Volume 3, Issue 2, April 2006 Pages 63 75, 2006 The Society for Simulation International

An Integrated Systems Architecture to Provide Maritime Domain Protection

Chris McCarthy
Special Assistant to the Commander
USNAVEUR and Allied JFC, Naples
chris.mccarthy@cne.naples.navy.mil

Russ Wyllie
Office of the Chief of Army Reserve
Crystal City, VA
russ.wyllie@us.army.mil

Ravi Vaidyanathan
Eugene P. Paulo
Department of Systems Engineering
Naval Postgraduate School
Monterey, CA
[rvaidyan, eppaulo]@nps.edu

The focus of this research is to address the criticality and vulnerability of commercial shipping in the Straits of Mallacca by designing and evaluating competing systems architectures that could provide sufficient maritime domain protection. The category of primary concern was the introduction of a weapon of mass destruction (WMD) in a cargo container. The Maritime Domain Protection (MDP) physical architecture alternatives combined five separate systems: 1) a land-based cargo inspection system, 2) a sensor system, 3) a C3I (command and control, communications, and intelligence) system, 4) a force response system, and 5) a sea-based cargo inspection system. Individual models for each system were developed and combined into an overarching integrated architecture model to evaluate overall performance. Study results based on current technology showed that while solutions were found to effectively reduce risk in the WMD threat scenario, effective suppression came at great expense and included the participation of commercial shipping companies. A range of alternative cost-effective solutions were also found, but with limited performance. Future work involves using the developed architecture as a test bed for evaluating the overall impact and effectiveness of new technologies and research (such as “smart containers”) on MDP and homeland security.

Keywords: Maritime domain protection, maritime defense, systems engineering and architecting, systems simulation

1. Introduction

Commercial shipping is characterized by a blend of dense traffic through straits and along coasts accompanied by long-distance, open-ocean transit. Global economic growth is contingent on this free flow of commerce along Asia-Pacific trade routes. A critical sector of this trade route is the Straits of Mallacca, which provides passage to nearly 700 ships per day, 135 large transport vessels per day, and two-thirds of the world’s liquefied natural gas (LNG) shipments [1, 2]. 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 [8, 9, 11, 12].

Therefore, the focus of this research is to address the criticality and vulnerability of commercial shipping in the Straits of Malacca by designing and evaluating competing systems architectures that could provide sufficient maritime domain protection. While this is an extremely broad problem, several assumptions were made to assist in bounding the problem space. First, any design architectural solutions would remain outside

JDMS, Volume 3, Issue 2, April 2006 Pages 63–75

of the political and diplomatic realms, assuming full international cooperation in the Southeast Asian region. Second, 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 time frame. Thus, only technologies with a Technical Readiness Level of 4 ("technology component and/or basic technology subsystem validation in laboratory environment") or greater were considered [3].

The category of attack that provided the specific focus of this research was the introduction of a weapon of mass destruction (WMD) in a cargo container. 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 to the target region.

2. Overview

2.1 Architectural Constructs

The overall systems architectural construct used in this research follows the "architectural views" methodology described in general by Maier and Rechin [13], but more specifically by Buede [4]. This architectural model follows Buede's model of a functional architecture, physical architecture, and operational architecture.

The functional architecture describes what the system must do, under what conditions it must perform these functions, and how the achievement of these functional capabilities is met using appropriate metrics. The physical architecture represents partitioning of physical resources, specifically the technological components and subsystems, which must be synthesized into an integrated grand system that performs the system's functions. The operational architecture maps the physical architecture and its resources to the system functions in a manner suitable for quantitative analysis within a discrete-event simulation or other suitable simulation or analytical modeling tool.

2.2 Architectural Focus: Land Inspection System

The proposed architecture included a broad look at a maritime domain protection system of systems that addressed sensing of potential targets through a series of radar systems in the Strait, command, and control nodes and variations, force response to perceived threats, and ship inspections, both at sea and on land, of suspect commercial carriers. However, for the sake of brevity and the desire to focus on the most significant aspect of the systems design, the bulk of discussion in this report will be on the land inspection system.

3. Functional Architecture

The functional architecture consisted of two primary components. The first was the functional hierarchy, which described the functions of the overall system of systems, as well as the relationship of these functions. The second was the Concept of Operation (CONOPS), which served as the conditions under which the system of systems would perform.

3.1 Concept of Operation (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. In this WMD scenario a legitimate merchant vessel inadvertently transported a forty-foot container containing a 20 KT Russian-made nuclear weapon. The container housing the weapon was loaded in an unknown port, with an ultimate destination of Singapore. 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 acquired a WMD they would not hesitate to use it.

3.2 Functional Hierarchy

The functional hierarchy was composed of top-level functions that had to be met in order for the system to perform as intended. These functions were sensing, command and control, force response, and maritime inspection. The maritime inspection function was addressed with two modes, a sea-based inspection and a land-based inspection system.

3.2.1 Sensors

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 tons). This information is fed into the C3I network, and its accuracy contributes to minimizing both force and inspection response time.

3.2.2 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 local 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.

3.2.3 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 non-destructive reaction options. Consideration was also given to cutting off the source of terrorist attacks by forcibly or non-forcibly taking out terrorist bases of operation and supply chains when intelligence or other means located them. The response forces also conducted more detailed active WMD inspections when directed, as a response to WMD detections or intelligence.

3.2.4 Maritime Inspection Systems: Sea Based and Land Based

Two cargo inspection systems were envisioned that were capable of searching bulk and container cargo for WMD. Nuclear, biological, chemical (NBC), and conventional explosives were seen as possible threats. A "ship" system inspected both 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 probability ship inspections. A "port," or land, inspection system inspected cargo either in port or as it is loaded onboard a ship. The land inspection system is discussed in more detail here.

The overall land inspection objective was to detect hazardous materials while minimizing impact on the economy. The challenge for the land inspection group was simplified 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 to a data fusion and analysis center as well as a command and control unit. Figure 1 illustrates the top-level functional decomposition for the land inspection system.

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.

4. Physical Architecture

Competing physical architectures were developed for each of the top-level functions described in the functional architecture section. Since each integrated architecture consisted of up to five system components, the number of overall architecture variables was substantial: each of the five top-level systems (sensors, C3I, force response, sea inspection, and land inspection) had either two or three alternatives that would be assessed in one or more of

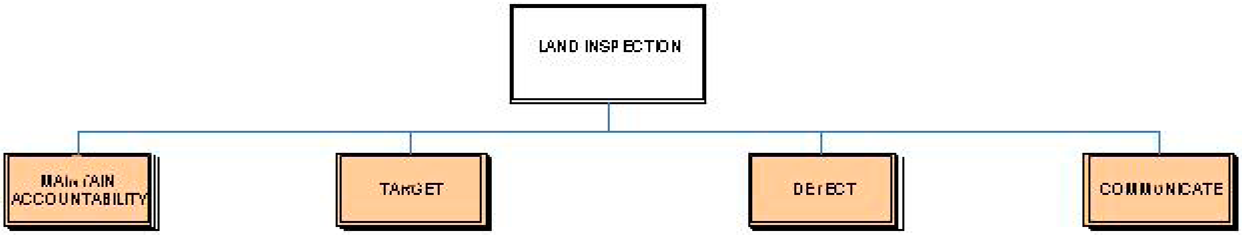

Figure 1. Land inspection system top-level functions

three different scenarios. This resulted in 109 different architecture combinations that were evaluated. However, the focus of this paper is the land inspection and its impact on overall results. Therefore, only the land inspection physical architecture is discussed.

4.1 Design Space

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. Insight from the Port of Oakland, Lawrence Livermore National Laboratory, and U.S. Customs and Border Protection were important in finalizing our alternatives. With the large number 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.

The driving factor for inspecting cargo was the volume of containers that ports had to process. 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.

4.2 Alternatives Generation Considerations

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 generating alternatives, an assessment of current or developing technologies was necessary to determine what was available to address the threats.

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 was 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.

4.3 Alternative Architecture 1

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 2.

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

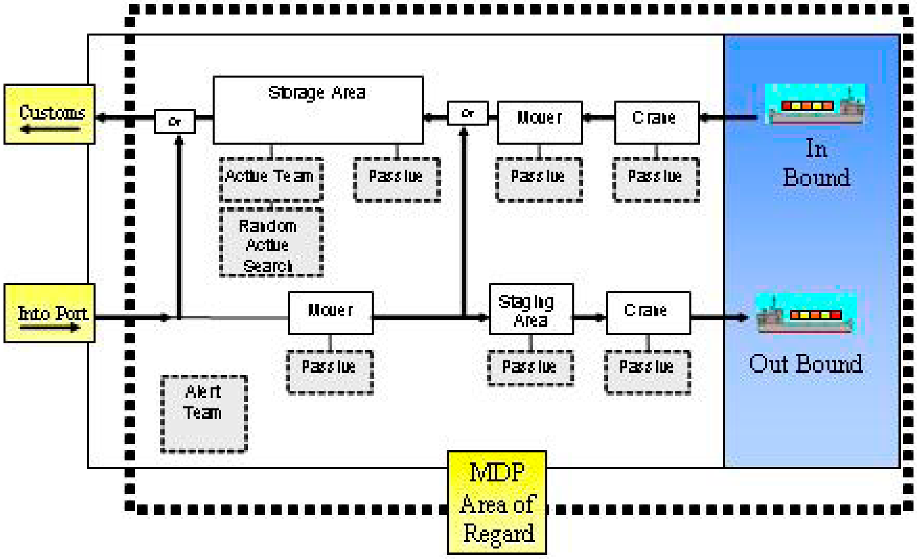

Figure 2. Land inspection system alternative 1: Port-centric inspection system

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 percent 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.

4.4 Alternative Architecture 2

Alternative 2, as seen in Figure 3, 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) [5]. 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. Cargo containers arrived at the port and were assessed as to whether or not they were from a certified shipper. There were then three inspection triggers warranting an active inspection.

As containers were filled 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.

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. Examples of additional data the maritime industry requires to make manifest data more relevant are more specific and precise cargo

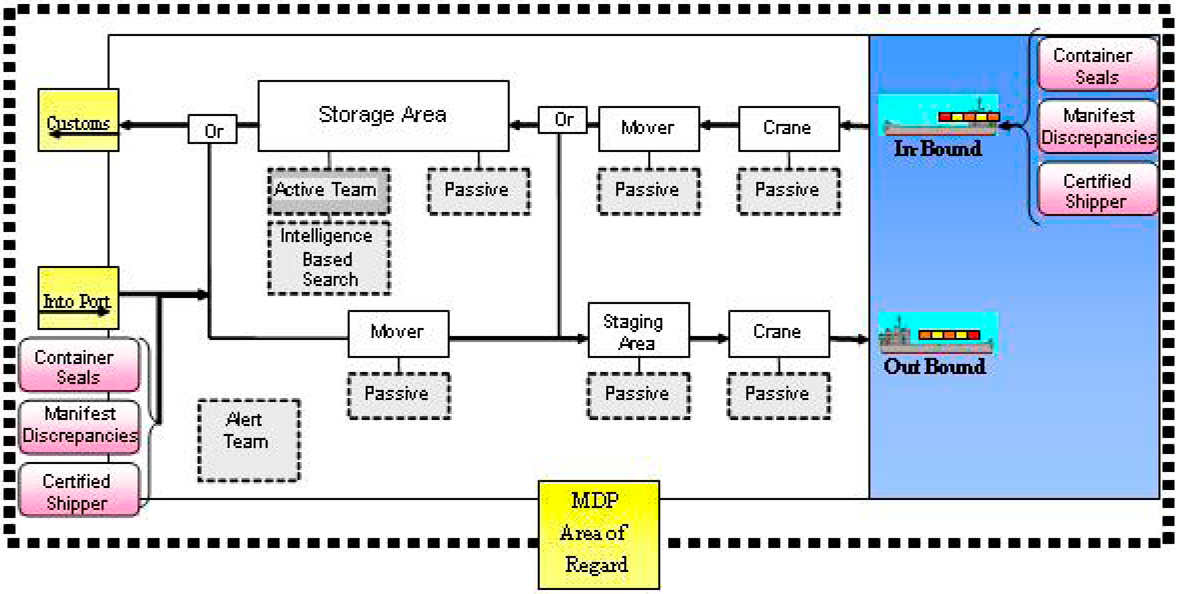

Figure 3. Land inspection system alternative 2: Trusted agent inspection system

descriptions, point of origin of the goods, and final recipient.

In addition to the three triggers that warranted an inspection, a small percentage of containers 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, in what environment the sensor would be working, 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.

5. Operational Architecture

A comprehensive modeling plan served as the centerpiece in the development of an operational architecture, linking system functions with proposed physical architectures and allowing for quantitative evaluation. This plan allowed for the transformation of system parameter inputs from each system group into values for the overall architecture measures of effectiveness (MOEs) and metrics. As stated earlier, 109 different architecture combinations were evaluated.

The team chose a modular approach that combined the results from smaller-scale group system models (produced separately by the 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 such 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, and 4) this approach allowed different modeling tools to be used in order to best model the system, allowing more in-depth analysis and a better understanding of system performance, as each system model was tweaked and analyzed to see which inputs and assumptions had the biggest effect on its local outcome. Additionally, the modular approach allowed for more rapid progress both as a result of parallel model development and because the end product was relatively smaller scale and less complex.

5.1 Overarching Modeling Plan

A graphical depiction of the MDP Overarching Modeling Plan is shown in Figure 4. 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.

Integrated architecture models were developed, which converted outputs from the individual group performance and cost models into values for the following:

- 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 (MDP System Cost: The combined total of MDP system procurement cost and ten-year operating and support cost).

In order to determine the performance and risk, *attack damage models* were designed, which allowed the conversion of the distance at which a given attack was defeated into a damage cost in dollars. If the defeat distance was far enough away, the attack was considered unsuccessful, and it counted positively toward the architecture's performance, 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. The system cost models divided the ten-year acquisition, operating, and support costs into systems required by industry, which contributed to commercial impact, and the MDP system itself, which contributed to MDP system cost. Since costs were viewed as somewhat fungible between commercial impact and MDP system cost, a total system cost was determined by simply summing these two costs.

5.2 MOE 1 Results

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 team. The first task was to identify the performance output by creating a "probability tree" shown in Figure 5. The various paths of the tree represented the likelihood of finding WMD in a container, or conversely not finding WMD in a container (attack success), given that WMD was in a container.

Once the different system values were assigned to the model, a matrix was created in a Microsoft Excel

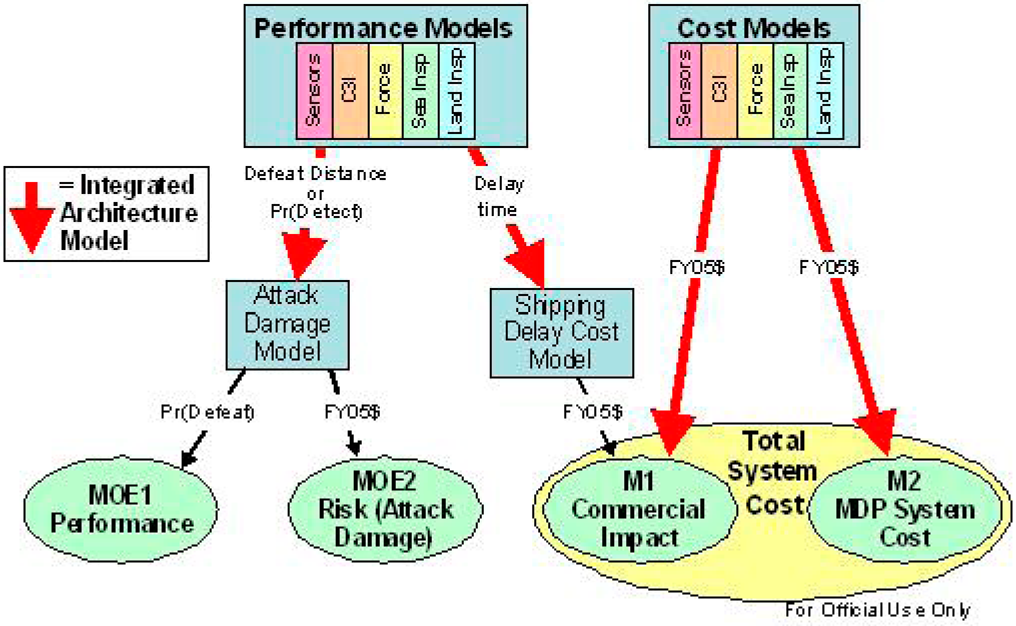

Figure 4. MDP Overarching Modeling Plan

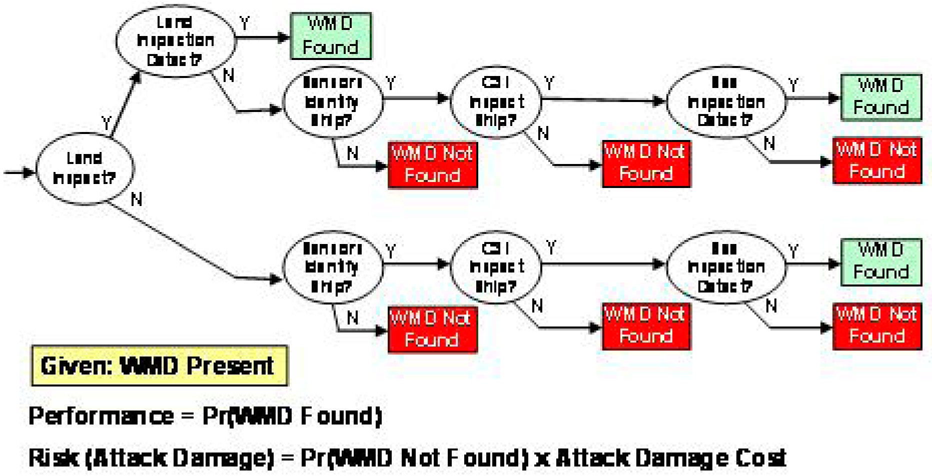

Figure 5. (Integrated architecture model: WMD scenario - performance and risk) Probability tree for overarching WMD performance model

Table 1. Inputs to WMD scenario performance model

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	0.20
	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

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 5 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 WMD on board a ship, was generated. The table representing the results from these models is seen in Table 1 below.

As seen in Table 1, 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 that 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 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 WMD.

Each combination of the model performance values was plotted against the relative combination of system alternatives. Three distinct series groups of points with similar performance ranges were observed as in Figure 6. 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.

5.3 MOE2 Risk (Attack Damage)

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.

Each combination of the WMD scenario Excel model risk values were plotted against the relative combination of system alternatives (see Figure 7).

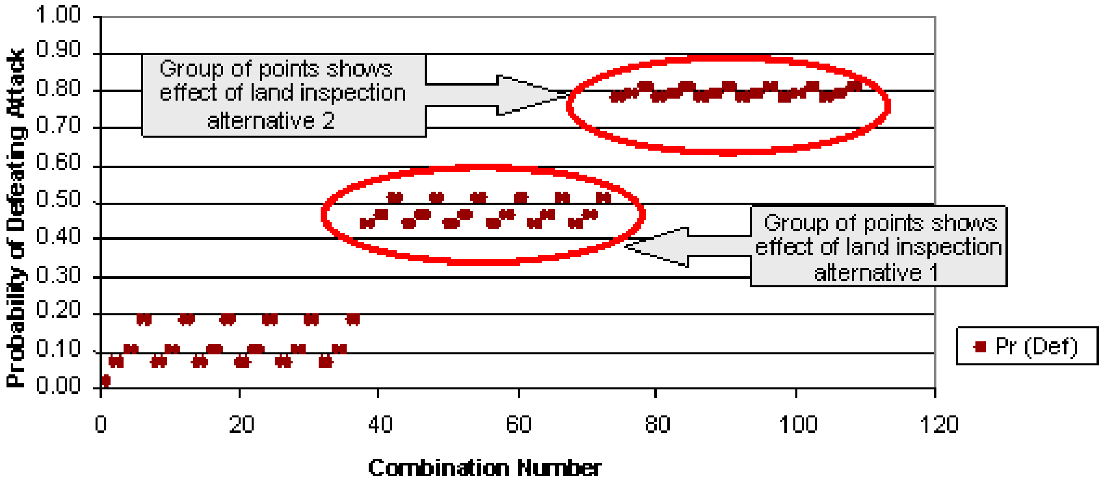

Figure 6. (Comination number versus performance) Plot showing increase in performance due to land inspection system across combinations

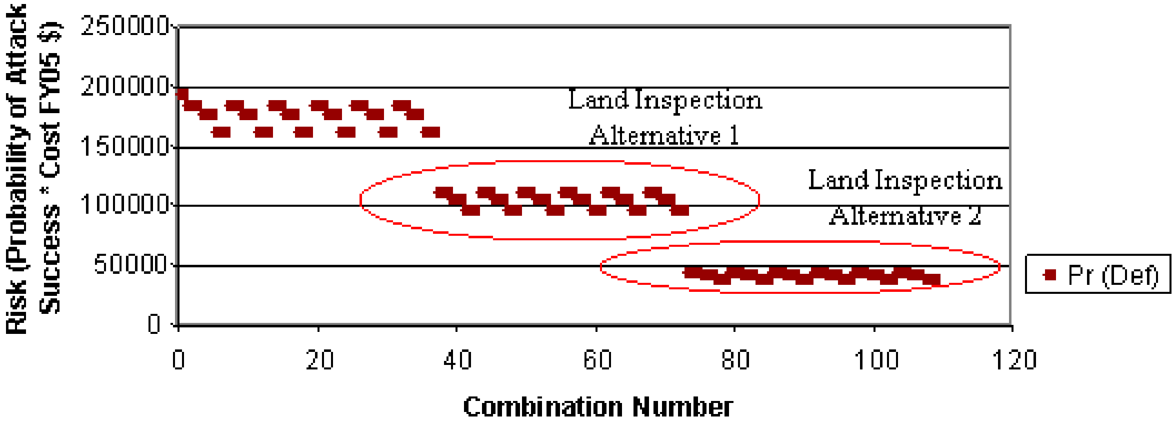

Figure 7. Plot of combination number versus risk

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.

5.4 M1 Commercial Impact

The commercial impact integrated model estimated both of the separate costs incurred by the commercial maritime industry, which were 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 a shipping delay cost model, which is not described in this paper. Both categories of commercial impact were evaluated for each combination of alternatives.

The resultant combination outputs denote the cost of each system alternative combination. As seen in Figure 8, the land alternatives represented in combinations 36–109 represented a majority of the shipping delay costs, while implementation of a sea inspection, to include stopping and boarding suspected ships, imposed the most serious cost increase in the effort to thwart a WMD attack.

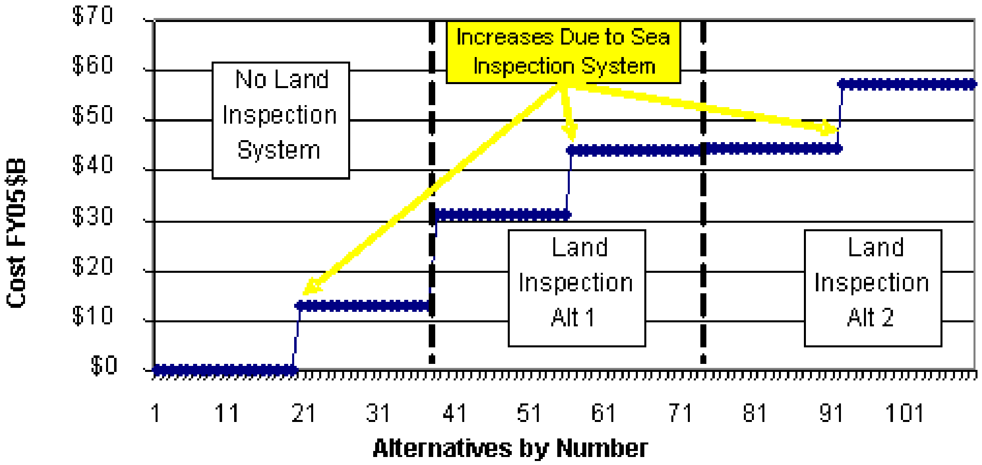

Figure 8. (WMD Total Commercial Cost) Commercial impact for WMD scenario

5.5 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$B, 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 at alternatives 36 and higher represent the change from the land "as-is" system, to the two land alternatives, as seen in Figure 9.

5.6 Analysis

The graph in Figure 10 shows a comparison of performance and cost for the proposed integrated architectures. 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 10. 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.

Land inspections "trusted agent" system included implementation in fifteen high-volume ports of origin. Sensitivity analysis was performed by reducing the number of "trusted agent" ports. The results are shown in Figure 11.

Decreasing the number of "trusted agent" ports moves performance versus cost toward the desired

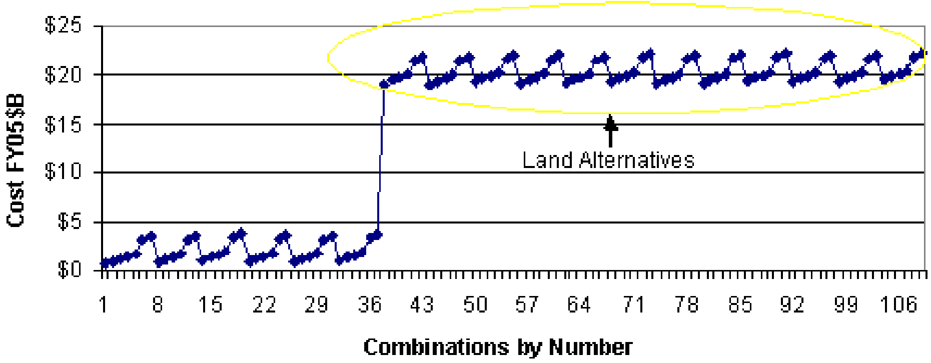

Figure 9. MDP system costs for WMD scenario

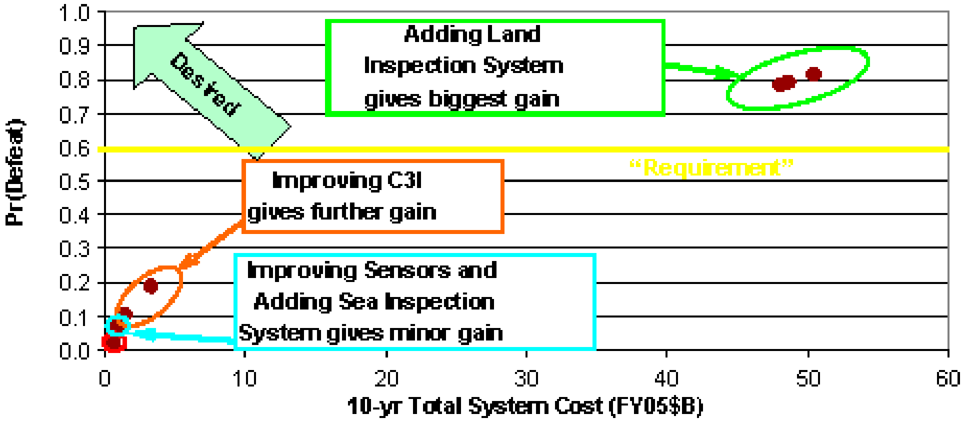

Figure 10. (WMD scenario pr. (defeat) versus total system cost) Alternative performance versus total system cost

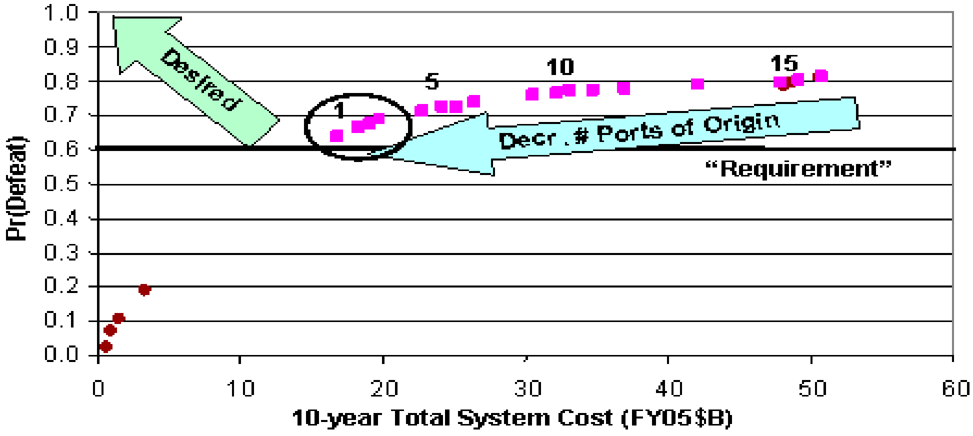

Figure 11. (WMD scenario pr. (defeat) versus total system cost) Effect of reducing "trusted agent" land inspection

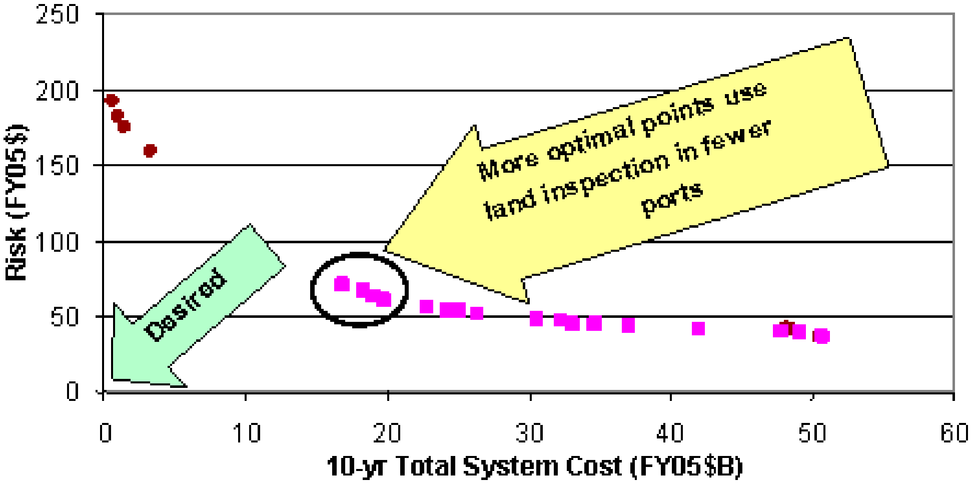

Figure 12. Effect of reducing trusted agent ports on risk and cost

"high performance/low cost" region of the graph in Figure 11. Yet, the decrease in performance is minimal, compared to cost reduction, when reducing the number of trusted agent ports from fifteen to one. However, it must be acknowledged that a "smart" enemy is not assumed. This means, as expected, that the effects of reducing the number of trusted agents on risk mirrored the effect on performance, as shown in Figure 12.

6. Recommendations and Conclusions

6.1 MDP Architecture

One insight gained in the NPS MDP study was the recognition of the extreme difficulty in designing a system to sufficiently address the maritime domain protection problem. Despite keeping the political and legal considerations out of the problem space, there were a myriad of variables resulting from various international participants in a largely unregulated, vulnerable industry that was simultaneously critical to the worldwide economy. The interconnected nature of the commercial shipping industry also held challenges, as any improvement or enforcement that was made across the entire industry would lead to significant shipping costs, especially due to delays. On the other hand, if improvements or enforcement were only made in a few areas by cooperative players, this could lead to either those players disproportionately assuming the cost burden or those areas being avoided altogether by nonconforming shippers.

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, instead of focusing on "stovepipe" or point solutions, although this had historically been the problem-solving method. There could be no lasting solution to the MDP problem, as technology, public attitudes, and threats would continuously change. Although the NPS MDP study focused on three specific threat scenarios, a continuous reassessment of the threat capabilities and intentions versus industry and infrastructure vulnerabilities would be required to determine the direction of future resource focus.

6.2 Conclusions

The largest gain in architecture performance in the WMD scenario came with the addition of a land inspection system installed in the highest volume ports of origin for cargo destined for the Straits of Mallacca. The land inspection alternative that was evaluated also relied on industry participation, using qualified "trusted agent" shipping companies to help find or deter WMD from being loaded in their shipping containers. This allowed resources to be focused on non-participating shippers, since they should be more likely to transport illegal cargo. Unfortunately, the cost to the shipping industry was significant for this land inspection alternative due to the worldwide extent of the industry, and the vast number of containers that were loaded and transported each day. Also, there was a trade-off that occurred between the number of ports that actively inspected for WMD, thereby reducing the opportunity for WMD shipment, and the high cost to install the land inspection system in those ports—in order to install land inspection systems in a meaningful number of ports, significant resources would be required.

Modeling analysis showed that passive sensor probability of detection drove the system and was instrumental in identifying suspect containers as they moved through the port infrastructure. The false alarms associated with passive detectors also impacted the delay cost of containers. The best architecture performance was achieved through a layered defense of port-centric (alternative 1) and trusted agents (alternative 2).

6.3 Recommendations

More effective defense against the WMD scenario could only be accomplished by installing land inspection systems in high-volume ports. These systems would take advantage of cargo delay times and close contact with transportation equipment in order to detect illegal cargo. Additionally, establishing a program to certify and randomly test "trusted agent" shipping companies would be required to deter the shipment of WMD.

Investment in passive sensor technologies would help maintain a constant flow of commerce that would be slowed down by intrusive, active inspections. Also, continued development of sensors with better penetration capabilities would help prevent harmful materials and potential WMD from being placed into containers. In the existing system, only moderate levels of shielding would permit successful passage of WMD through the supply chain. When active search was required, a method to decrease the amount of time it would take to actively search a container could minimize delay cost.

7. References

[1] Noer JH, Gregory D. Chokepoints – maritime economic concerns in Southeast Asia. Center for Naval Analyses, 1996.

[2] United States Pacific Command. Asia-Pacific economic update, vol 2; 2002.

[3] U.S. Department of Defense technology readiness assessment (TRA) deskbook, 2003 Sep.

[4] Buede D. The engineering design of systems. New York: John Wiley and Sons; 2000.

[5] U.S. Customs and Border Protection. C-TPAT fact sheet and frequently asked questions. [cited 2005 May 20]. Available from: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/fact_sheet.xml

[6] Armed Navy escorts for suspect ships. The Straits Times Interactive. 2005 Feb 28.

[7] Coalition for Secure Ports. Improving port security. [cited 2005 May 15]. Available from: http://www.secureports.org/improving_security/factsheet_screening.html.

[8] Kreil E. World oil transit chokepoints. Country Analysis Briefs. Available from: http://www.eia.doe.gov/emeu/cabs/choke.html

[9] Luft G, and Korin A. Terrorism goes to sea. Foreign Affairs. 2004; 83(6): 62.

[10] McCarthy C, Wyllie R, Ferraris G, et al. Maritime domain protection in the Straits of Mallacca. [integrated graduate project final report]. Monterey (CA): Naval Postgraduate School; 2005.

[11] Rodriue J-P. Straits, passages and chokepoints: a maritime geostrategy of petroleum distribution. Hofstra University; 2004.

[12] Vertzberger Y. The Malacca-Singapore Straits: the Suez of the South-East Asia. The Institute for the Study of Conflict.

[13] Maier MW, and Rechin E. The art of systems architecting. New York: CRC Press; 2002.

Author Biographies

Christopher J. McCarthy *is a Commander in the U.S. Navy and graduated from Naval Postgraduate School in June 2005 with an MS in systems engineering and analysis. He earned the Northrup-Grumman award for excellence upon his graduation.*

Russ Wyllie *is a Major in the U.S. Army and graduated from Naval Postgraduate School in June 2005 with an MS in systems engineering and analysis. He earned the Northrup-Grumman award for excellence upon graduation. MAJ Wyllie is currently the Strength Management Analyst for the Office of the Chief of Army Reserve, Human Resources Department.*

Ravi Vaidyanathan, Ph.D., *is an Assistant Professor of Systems Engineering at the Naval Postgraduate School. His research interests include robotics, unmanned aerial vehicles, and biological systems.*

Eugene P. Paulo, Ph.D., *is a Senior Lecturer of Systems Engineering at the Naval Postgraduate School. His research interests include modeling, simulation, and analysis of combat systems, systems engineering and architecting, and experimental design.*