PortSec: Port Security Risk Management and Resource Allocation System

Michael D. Orosz*, Carl Southwell,**
Anthony Barrett**, Onur Bakir**, Jennifer Chen*, Isaac Maya**

*Information Sciences Institute, University of Southern California, Marina del Rey, CA 90292
USA (Tel: 310-448-8266; e-mail: mdoros@isi.edu).
**Center for Risk and Economic Analysis of Terrorism Events, University of Southern California USA (e-mail: imaya@usc.edu)

Abstract: Ports are important to the US economy. This is particularly true with the Ports of Los Angeles and Long Beach (POLA/LB). Over 40% of all containers shipped in and out of the US flow through the two-port complex. In addition, the POLA/LB complex support large bulk cargo, tanker, and cruise ship operations. It is vital that these ports be protected from terrorist attack and/or from damage from natural causes. The DHS funded Center for Risk and Economic Analysis of Terrorism Events (CREATE) is developing a port security risk management and resource allocation system (PortSec). PortSec will support both tactical day-to-day security decision-making and long-term strategic security planning. An initial PortSec prototype (1.0) that supports tactical day-to-day risk assessment and resource allocation has been developed and demonstrated to the POLA/LB and the DHS Science & Technology Directorate.

1. INTRODUCTION

The DHS funded Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California was asked by the POLA/LB to develop a port security risk management and resource allocation system (PortSec). PortSec is being developed with the national mission of preventing port-related terrorism in mind. PortSec supports this mission by aiding in assessing terrorist intent and capability to focus resources to deter, interdict, and mitigate attacks, by assessing the ability of port/landlord, owner/operator, local law enforcement and security resources, and other security resources to protect targets, by assessing the ability of port/landlord, owner/operator, local first responders, and other security forces to respond to attacks that do happen, and by estimating the primary and secondary economic impacts of terrorist attack scenarios.

PortSec will support both tactical day-to-day security allocation decision-making and long-term strategic security planning. The system is intended to support two types of users:

- Port Security Officer – tactical responsibility for daily security arrangements with limited additional resources that can be reasonably reallocated on an as-needed basis
- Port Security Analyst – strategic analysis of potential long-term resource allocation investments for port security

For tactical usage, PortSec will provide up-to-date risk assessment for both identified areas of interest (AOIs) and for the overall port complex. These assessments reflect current counter-measure resource allocations, planned and unplanned events, and intelligence about possible threats. These assessments are frequently updated to reflect changing port conditions and assessed threats. The port security officer attempts to reduce overall risk by re-allocating available counter-measure resources. After each adjustment, the system calculates a new risk assessment score – providing instant feedback to the port security officer.

For strategic usage, PortSec will provide the port security analyst with tools to evaluate the cost-benefit of adding/modifying new counter-measures and the expected costs of adding/modifying an AOI to the port (e.g., adding or expanding a terminal).
This paper describes the PortSec project, the risk assessment and management approach taken, and current state of the project. Details about the terminal and port operations modeling can be found in a separate paper presented at this conference.

2. BACKGROUND

Ports are major contributors to the national economy through the large value of maritime import and export trade. In addition, ports are a major provider of both direct and indirect jobs locally and nationally, and any impact on the daily operations of these ports ripples through the various layers of the economy. This is particularly true with the Ports of Los Angeles and Long Beach. Approximately 40% of the US container trade flows through the two-port complex. In addition, the POLA/LB complex supports large bulk cargo, tanker, and cruise ship operations.

To address the vulnerabilities of ports to terrorist and other catastrophes, the US government unveiled several initiatives to secure incoming cargo. Customs-Trade Partnership against Terrorism (C-TPAT), which is administered by Department of Homeland Security (DHS), was announced in November 2001 in an effort to leverage the private sector and its global suppliers to address security concerns en route to the ports. In 2002, the Container Security Initiative (CSI) was launched by Customs and Border Protection (CBP) with the goal of identifying and pre-screening containers that pose risks of terrorism at the port of origin, as well as promoting the development of smart (tamper-resistant) containers. Use of technology such as state-of-the-art inspection equipment, electronic tags, smart seals, and in-box sensors have been encouraged through these initiatives to minimize the risk of arrival of a container with harmful cargo at a US port of entry.

Despite these efforts to introduce extra layers for defending the home front, POLA/LB is facing the challenge of conducting daily port activities with maximum focus on homeland security efforts while minimizing its impact on the free flow of trade. Realizing that terrorists have an array of options to deliver harm through seaports, various security measures have to be undertaken. Inspection of incoming cargo and protection of port perimeters and waterways have become top priorities to port officials. There is a growing need to optimize allocation of resources on security investments and to use technology effectively within the port complex to maximize the benefits of each dollar spent on homeland security missions.

Most security experts agree that applying countermeasures to reduce terrorism risks are likely to introduce unintended bottlenecks and additional trade costs. This risk is particularly present at POLA/LB where an average of 12,000 twenty-foot equivalent containers (TEUs) arrive every day. Efficient design of port facilities is vital to reduce bottlenecks in the system. Poor design of inspection operations will certainly compound traffic flow problems in the port complex, and risk-based optimization of cargo inspections can help minimize the impact of security missions on daily business activity.

Port officials and the US Coast Guard (USCG) are also grappling with the difficulty of protecting port perimeters and critical facilities surrounding the port complex. The large number of critical facilities around seaports and the vast size of the areas that need protection augment the risk of an attack on port infrastructure. Responding to waterborne threats can be difficult at POLA/LB due to the length of the waterfront and number of cargo terminals as well as the numerous facilities processing hazardous materials. USCG and POLA/LB officials have to exercise continuous vigilance to monitor the waterways’ traffic. It is our intention to expand our computer model to capture the complexity of daily activities land-based activities and for port perimeter protection and provide insights on how to optimally deploy technology and human resources to further reduce the risk of an attack.

Another area of concern is responding to emergencies in the case of an attack or other catastrophe at the port. Minimizing the consequences of a terrorist attack or other disaster depends largely on in-depth coordination between first responders, state-of-the-art equipment for communications interoperability, and a plan for diverting commercial traffic from affected areas of
the port with minimal delay. Design of daily port operations should be undertaken with an emphasis on building modularity and redundancy into the system to reduce the likelihood of a full port shutdown in the case of an attack. If a port shutdown is inevitable, the port system should be resilient to minimize economic consequences. Many just-in-time companies have minimal redundancy in their supply-chains and will have difficulty responding to port shutdowns or finding alternative suppliers for parts needed for manufacturing. Therefore, continuity of port operations means US business continuity.

3. APPROACH

Currently, maritime counterterrorism professionals have few software tools with which to perform scenario-based risk analysis, and port security professionals have a need for robust security resource allocation tools. The USCG’s Maritime Security Risk Analysis Model (MSRAM) serves as a terrorism risk analysis software tool and is used to perform scenario risk assessments on critical infrastructure and key resources. MSRAM aggregates its assessments and provides analyses to support risk management. Its methodology captures the security risk facing different targets spanning industry sectors and allows comparisons among different targets and geographic areas at the local, regional, and national levels.

MSRAM assesses risk based on scenarios—combinations of targets and attack modes—in terms of threat, vulnerability, and consequence.

- **Threat** is the intent and capability of terrorists to deliver an attack on a specific target.
- **Vulnerability** is the probability of a successful attack based on attack difficulty, ability of the owner/operator, local law enforcement, and the USCG to interdict an attack, and ability of the target to withstand the attack.
- **Consequence** is the negative impact of a successful attack on the US in terms of deaths/injuries, primary economic impact, environment, national security impacts, symbolic impacts, and secondary impacts to the US economy.

MSRAM also considers the response capability of the owner/operator, local first responders, and the USCG and other Federal agencies to mitigate the consequences of an attack. MSRAM also produces separate evaluations of primary and secondary economic impacts of an attack to improve understanding of response and recovery capabilities, a dynamic analysis and reporting center to review assessment results, an “as if” case module to assess and compare the impact of alternative strategies, and a three-tiered (local, regional, and national) review of risk assessments.

PortSec and MSRAM share the same underlying risk analysis concepts and framework. PortSec aims to complement MSRAM, but with a focus directed toward port usage and a level of detail that addresses port-specific needs. PortSec will incorporate information from MSRAM and other Port-related homeland security assessments, as available.

The complex operations and interactions within and between the various physical and non-physical components that make up a port complex are difficult to model and make risk assessment and management difficult. This is particularly true when the interactions between these “system of systems” are dynamic – constantly changing both day-to-day and long-term. The purpose of the PortSec project is to capture this dynamic “system of systems” environment and provide the port authorities with a risk assessment and management system that can be used for both tactical and strategic risk management and resource allocation.

4. PORTSEC

A major challenge faced in developing the PortSec system is how to model risk assessment and resource allocation in a port complex composed of many different areas of interest (AOIs) such as cargo-handling terminals and rail systems, business entities, and various local, state, and federal law enforcement agencies – each with its own priorities, operations, and concerns. Compounding this problem is the ability to model – with a specified degree of accuracy – the predicted impact that various terrorism-based scenarios will have on the overall operation of the port complex. Specifically, what are the predicted
disruptions to operations that ripple throughout the port complex resulting from a terrorist attack? In addition, for each of these attack scenarios, what countermeasures can be implemented to prevent or reduce these impacts (both direct and indirect), but simultaneously minimize impact to day-to-day operations (i.e., throughput) of the port complex?

We recognize that the framing of countermeasure use at various AOIs in terms of relative versus absolute risk may have profound effects on choices among AOIs and options. As such, PortSec will attempt to display risk in terms such that absolute and relative measures may be observed. For example, the absolute risk of a terrorist attack might be measured as a constant derived from a function of threat, vulnerability, and consequence. This would express the actual number of people and costs of property losses and trade flow disruptions as experiencing an actual negative outcome. Relative risk, quite differently, might be revealed as ratios (risks for a given scenario divided by the risks for hypothetical base state). Thus, in relative risk terms, those terminals that choose not to employ countermeasures A, B, and C might be described as twice as likely as terminals that employ these countermeasures to experience a terrorist attack; using countermeasures A, B, and C would be described as cutting the risk of attack in half. However, such relative risks do not reveal the actual rates or consequences of occurrence. Doubling a 0.01% risk is very different in its consequences from doubling a 4% risk. Thus, a relative risk presentation can produce errors in perceptions of risks and benefits. (Relative risks do not conform to normative Expected Utility (EU) theory assumptions.) These perceptual errors violate the assumption that individuals who make “rational” choices should prefer options with the highest expected utility relative among all options being considered. (Kahneman and Tversky, 1979)

In addition, we recognize that aggregating the risks calculated for individual AOIs into an overall port complex risk assessment is a daunting task. The aggregate risk of a port is a combination of the vulnerability of the port (wherein the port can be seen as a relative prospective target, a primary prospective target, or a collection of prospective targets) the perceived flexibility in terrorists’ specific attack modes and targets, the expected consequences of specific attacks, and the perceived ability to reproduce the attack types as well as countermeasures, alone or in concert and their efficacy and effectiveness in neutralizing the advantages of any specific mode of attack, whether by water, air, road, rail, perimeter intrusion, deceptive action, pipeline, or insider activity.

Another challenge is modeling and estimating the costs of business continuity associated with AOIs. In PortSec, business continuity modeling starts with the modeling of traffic and container delays and movements. These business interruption costs will then be compounded with delay costs associated with rebuilding damaged infrastructure and with the replacement of labor.

Finally, an overarching and continuing challenge is attempting to answer the question, “How do we communicate risk to the stakeholder?” PortSec intends to communicate risk through a combination of a traffic light model utilizing data from multiple sources guided by “smart” transparency (by this, we mean the use of publicly available data supplemented by confidential data only when necessary and in a manner that shields the input while increasing the validity of the output.)

As reiterated by the 9/11 Commission, “[h]ard choices must be made in allocating limited resources. The U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (federal, state, regional, and local) and to private stakeholders.” (National Commission on Terrorist Attacks Upon the United States. Page 391) Efforts at improving security should include enhanced information technology, automated targeting systems, non-intrusive inspection technologies, and radiation inspection technology. “No single security measure is foolproof. Accordingly, …[w]e must have multiple layers of security in place to defeat the more plausible and dangerous forms of attack against public transportation. The plan must take into consideration the full array of possible enemy
tactics, such as use of insiders, suicide terrorism, or standoff attack. Each layer must be effective in its own right. Each must be supported by other layers that are redundant and coordinated.” (National Commission on Terrorist Attacks Upon the United States. Page 392).

In addressing these challenges, two simultaneous parallel efforts are being undertaken: 1) model the port complex as a “system of systems” where each terminal, pier, rail line, and other identified AOIs of the port is treated as a system with its own operations and interfaces to other systems and 2) undertake the necessary research and develop the underlying risk assessment and resource allocation algorithms for each of these “systems” as well as the overall port complex.

4.1 System of Systems

The overall PortSec system architecture consists of a user interface, modeling infrastructure, and data stores (Figure 1). The graphical user interface (Figure 2) provides the user with access to either the tactical or strategic components of the PortSec environment.

4.2 Risk Assessment Methodology

Terrorism risk analysis of the Ports of Long Beach and Los Angeles enables decision analysis of port security alternatives. Critical issues to address include potential attack scenarios, and potential countermeasures such as infrastructure hardening.
and tactical defenses. Such analyses begin with assessment of the multiple layers of security directed at reducing the potential exposure to and consequential severity of conditions that may induce potential targeting by terrorists—the threats that induce the selected security activities, the vulnerabilities to these threats, the flexibility in terrorists’ potential attack modes and targeting, the consequences of attacks, and the ability to reproduce attacks—and in neutralizing the advantages of any specific modes of attack, whether by water, air, road, rail, perimeter intrusion, deceptive action, pipeline, or insider activity. This can be accomplished by expert elicitation or by using an analytic hierarchy process (Saaty, 2001) that subjectively weighs the targeting selection criteria and the specific target preferences based on pair-wise comparisons of these characteristics to create more efficient allocations of the ports’ security resources.

After delineating factors involved in targeting—the existence of viable targets, potential vulnerabilities in these targets, flexibility in attacking these targets—and eliciting target categories—inbound maritime, road, rail, pipeline, insider threat, deceptive activity, and air—and locations within the ports, we can make judgments by ranking expert elicitations or based on pairs of target characteristics and pairs of target categories and locations by individual target characteristic to determine whether both criteria are of equal importance, whether one is weakly more important than the other, whether one is moderately more important than the other, whether one is strongly more important than the other, or whether one is absolutely more important than the other. Numerical weights or ranks can be derived for each characteristic within the hierarchy, and diverse and otherwise potentially incommensurable characteristics can be compared to one another in a rational and consistent way (In this analysis, inputs were selected by the authors. More representative inputs can be obtained by expert solicitation. For example, distribution of a survey form to various military, security, maritime, technical, and administrative port personnel familiar with Ports of Long Beach and Los Angeles security concerns could be conducted. The results of this survey could be aggregated by use of median scores for each of pair-wise selection, or the results could be systematically aggregated and re-solicited in a Delphi format. In such a manner, the inputs would be more representative of an expert consensus). From these inputs, an implied allocation of security resources by port area-type to be defended based on specific scenarios can be calculated.

Security cost-effectiveness can be analyzed using decision trees. Decision trees can be crafted for each representative attack scenario. For example, a “bomb hidden in an inbound container scenario” decision tree follows a four-stage decision that occurs when the container ship approaches the Ports of Long Beach and Los Angeles. First, a decision is made with respect to the ship and its containers if the U.S. Coast Guard wishes to board the ship and inspect containers while the ship is still at sea. The tree assigns probabilities and costs to this contingency. The next decision is made once the containers are off-loaded at the port. In this decision, a sample of containers is passed through a nuclear/radiation portal. Based on a negative result (i.e., no detection of radiation), containers are then either physically inspected or scanned with personal radiation detectors. Finally, those containers that successfully pass the radiation detector screening are either physically inspected or not.

Based on the specific attack scenarios, simple cause-and-effect models can be utilized. In order to evaluate the likeliest course of action by possible terror cells, we can perform a range of decision sensitivity analyses to explore the outcomes of various decisions. Decision trees can include the choices involved in attacks assuming employed countermeasures and, given these choices, the attacks’ probabilities of success or failure. Plotting of expected consequence versus conditional additional expected costs based on various countermeasure and defense options can identify Pareto-optimal port security options from dominance relationships.

Scenarios may include targeting or exploiting a cruise ship, a container ship, a tanker ship, a harbor truck, a barge, a rail yard, port industrial facilities, and a bridge. Other scenarios may include terrorist stowaways on an inbound hazardous cargo vessel,
an explosion at a fuel receiving terminal, a suspicious package at a port facility, surveillance of petrochemical terminals, an improvised explosive device (IED) attached to the hull of a freighter, the theft of gasoline tanker truck, an explosives attack on a chlorine storage tank, hostage-taking and executions aboard a vessel in port, underwater explosive devices planted on multiple vessels in port, a nuclear device aboard an incoming vessel in a 55-gallon drum, an attack on hostage-taking and executions aboard a vessel in port, underwater explosive devices planted on multiple vessels in port, a nuclear device aboard an incoming vessel in a 55-gallon drum, an attack on

4.3 Concept of Operations

4.3.1 Tactical Operations

The port complex is divided into user definable AOIs (Figure 2). For each AOI, the PortSec software automatically and periodically calculates a risk assessment based on assessed threat, vulnerability and consequences of various operations and zones in the AOI and reflects current counter-measures (CM) allocated to the AOI. In addition, an overall port complex risk assessment is calculated based on the various AOI risk assessments. If a user makes a resource allocation adjustment, the PortSec software automatically recalculates the assessed risk of each AOI as well as the overall port complex. Areas of interest are painted green (low risk), yellow – moderate, red – high) and are based on current counter-measures deployed and on assessed threat to the AOI.

Figure 2 – Tactical User Interface – PortSec 1.0. Regions in green, yellow, and red represent areas of interest (AOI) and are user defined. Colors represent assessed level of risk (green – low, yellow – moderate, red – high) and are based on current counter-measures deployed and on assessed threat to the AOI.

The port security officer can allocate port resources by either “dragging” a resource to a desired AOI or adjusting sliders allocated to each available port resource. After each adjustment the PortSec software recalculates the assessed risk and repaints the various AOIs to reflect those assessments. The system can also use optimization algorithms to suggest allocations.
4.3.2 Strategic Operations

The concept of operations for strategic security and planning operations differs from the tactical in that in addition to re-allocating existing countermeasures (resources), the user can also evaluate new countermeasures as well as create new infrastructure components - such as terminals, channels, and rail lines. As with tactical operations, the PortSec software periodically re-calculates the risk assessment for all AOIs. In addition, when a resource has been re-allocated, a new resource (i.e., counter-measure) added, or the port complex infrastructure has been modified (i.e., expanded), the PortSec software automatically updates the risk assessment scores for each AOI.

As with the tactical user, the port security analyst can allocate port resources (counter-measures or infrastructure components) by either “Dragging” a resource to a desired AOI or adjusting the sliders allocated to each available port resource.

4.4 PortSec 1.0

The current version of PortSec (1.0) is an initial prototype that supports tactical day-to-day use only. This prototype has been demonstrated to the POLA/LB and to DHS Science & Technology Directorate. In both cases, the prototype and concept of operations were well received.

5. NEXT STEPS

Work has begun on PortSec 2.0 which will support both tactical and strategic security risk assessment and management. In addition, after an extensive evaluation period, the plan is to insert PortSec into the new Port of Long Beach Joint Command and Control Center (JCCC).

6. CONCLUSION

Ports are important to the US economy. This is particularly true with the Ports of Los Angeles and Long Beach. Over 40% of all containers shipped in and out of the US flow through the two-port complex. It is vital that these ports be protected from terrorist attack and other disasters. The DHS funded Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California is developing a port security risk management and resource allocation system (PortSec). PortSec supports both tactical day-to-day decision-making and long-term strategic security planning.

An initial PortSec prototype (1.0) that supports tactical day-to-day risk assessment and resource allocation has been developed and demonstrated to the POLA/LB and the DHS Science & Technology Directorate.

6. ACKNOWLEDGEMENTS

The PortSec project team would like to acknowledge the help and support of John Holmes, Director of Port Operations, Port of Los Angeles, George Cummings, Director of Port Security, Port of Los Angeles, Cosmo Perrone, Director of Port Security, Port of Long Beach, and the US Coast Guard. We also like to thank Dr. Petros Ioannou, Mithun Baphana, and Afshin Abadi at the University of Southern California for their constant support and input.

This research was supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security.

REFERENCES


