

**PortSec: Port Operations Modeling for Risk Management and Resource Allocation**  
**Isaac Maya, N. Onur Bakir, Petros Ioannou, Michael Orosz, Jennifer Chen**  
 isaac.maya@usc.edu

- 1. Overview ..... 1
- 2. Research Accomplishments ..... 2
  - 2.1. The Risk Analysis Approach ..... 2
    - 2.1.1. Risk Dimensions ..... 2
    - 2.1.2. Port Critical Areas ..... 3
  - 2.2. PortSec Concept of Operations and User Interface ..... 4
- 3. Applied Relevance ..... 6
- 4. Collaborative Projects ..... 6
- 5. Research Products ..... 6

**1. Overview**

This project is developing a port security risk management and resource allocation system model (PortSec) of the Ports of Los Angeles (POLA) and Long Beach (POLB) for performing port security risk assessments and resource allocation analysis. The basic modules of the PortSec system include a port risk analysis component, a macro-micro simulation model of port operations, an robust resource/technology portfolio allocation model, and state-of-the-art user interfaces. The goal is to develop a system for performing risk-based analysis of security countermeasures to reconcile the seemingly opposing goals of minimizing the risk of terrorism while maintaining unimpeded flow of daily port activity.

The Ports of Los Angeles and Long Beach (POLA/LB) are facing the challenge of conducting daily port activities with maximum focus on homeland security efforts. Inspection of incoming cargo and protection of port perimeters and waterways are top priorities of port officials. There is a growing need to optimize allocation of resources on security investments and use technology effectively within the port complex to maximize the benefits of each dollar spent on homeland security missions.

We are developing a simulation modeling approach that incorporates detailed understanding of daily port operations to quantify the impacts of technological countermeasures on both risk and daily business operations. The novelty in our approach is in exploring optimal resource allocation strategies within a simulation model that will measure relative impacts of security activities and countermeasure on risk, business continuity and the pace of daily port activities.

A key objective of this project is the initial development of a user interface and the underlying middleware of PortSec. This system is targeted for use by port security and resource personnel to evaluate countermeasures, technologies and resource allocation policies for terrorism and economic impact on operations at POLA/LB. In addition, PortSec will allow for real-time monitoring of port security conditions (i.e., situational awareness) and allow “what-if” analysis to be undertaken to quantify resource allocation trade-offs to minimize risk from a possible terrorism event.

CREATE is working closely with POLA/LB port personnel to ensure experience-based security and operational issues of primary interest are accurately modeled, while providing flexibility to explore alternate security strategies and technology deployments. CREATE is also working closely with Coast Guard personnel to ensure the model is consistent with MSRAM approaches, models, and results.

"This research was supported by the United States Department of Homeland Security through the 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."

## 2. Research Accomplishments

Over the past year, the following efforts were undertaken in the initial development of the Port Security Risk Management and Resource Allocation project (PortSec):

- Risk analysis approach
- Macro/Micro system model developments (initiated late in the year, and not further described herein)
- Requirements analysis and development of initial concept of operations (ConOps) definition
- Development of the initial user interface and middleware functional requirements
- Resource allocation analysis (described in Kleinmuntz, et al., Risk-Based Allocation of Resources to Counter-Terrorism, CREATE Year 4 Executive Summary)

### 2.1. The Risk Analysis Approach

Our main approach concurs with the Department of Homeland Security's (DHS's) risk assessment methodology. This methodology separates risk into three components: threat, vulnerability and consequence. The functional relationship between risk and its three components is defined by the following formula:  $Risk = Threat \times Vulnerability \times Consequence$

Threat is defined as the likelihood that an attack occurs, whereas vulnerability is the likelihood of success to the adversary. Consequence is a measure of damage inflicted on the port as a result of the attack. Following this definition of risk, our approach is to identify the critical areas in the port complex and assess each component of risk in all the critical areas. In what follows, we present how these critical areas are identified and discuss our risk analysis methodology.

#### 2.1.1. Risk Dimensions

There are a variety of ways that an adversary could attack the port complex. Therefore, we identified eight different dimensions of risk for each critical area in the port complex. We assign scores for each dimension based on the likelihood of a successful attack employing a certain pathway to reach the terrorist goal and the consequence of such an attack. The risk dimensions are as follows: waterways – on water, waterways – underwater, air, road, rail, access between gates of entry, entry with fake documentation and insider attack. They do not identify a certain scenario under which each risk dimension could be exploited. However, the consequences of an attack should depend on the particular scenario considered.

Risk scores are assigned for each dimension in each critical area. The components of risk that are quantified with the scoring methodology are threat and vulnerability. Each risk score refers to a likelihood of an event occurring. However, it is very difficult if not impossible to assign a precise likelihood to the occurrence of an event. As such, the estimates are approximate measures of the likelihood of an event. The risk scoring approach is used to reduce the computational complexity as well. Both threat and vulnerability assessments are made using risk scores ranging from 1 to 7.

Threat scores represent a scale for the likelihood of a terrorist attack. Moving down the scale refers to multiplication of the threat level by two. In this regard, a threat score of 1 refers to the highest threat level, whereas a score of 7 is the lowest threat level. Similarly, an attack is judged to be twice more likely if a threat score of 3 is assigned instead of 4. These relative probabilities are converted to actual probabilities

based on the *anchor value* selected for the highest threat level. The *anchor value* will be selected based on our discussions with the port authority. For example, if we judge that the maximum daily likelihood of an attack upon a port facility is  $10^{-5}$  (i.e., if the *anchor value* is  $10^{-5}$ ), then each risk score is translated into actual probabilities.

These scores are assigned for each risk dimension at each critical facility. Although  $10^{-5}$  may seem a very low value for the daily likelihood of an attack at a certain facility, we should note that this low number refers to a 10 year likelihood of 0.035, which is quite high for a single critical facility in the port complex.

Vulnerability scores do not use the same scale idea. Nevertheless, they represent discrete assessments of a successful attack given an adversary makes an attempt to inflict damage. As in the case of threat scores, the vulnerability scores range from 1 to 7 where 1 refers to the highest level of vulnerability and 7 to the lowest. As in the case of threat scores, vulnerability scores are separately assigned for each risk dimension at each critical facility.

The third component of risk is consequence. Our approach for consequence assessment is quite different than the risk scoring approach used for threat and vulnerability assessment. We will use a macroscopic port simulator that accounts for flows in and out of the port complex. The macroscopic simulator has the capability to measure the economic consequence of an attack by estimating the direct loss of port output and the delays in terminal operations.

### 2.1.2. Port Critical Areas

The port of Los Angeles has 24 terminals, and the Port of Long Beach as 11 piers. We assigned risk scores for each POLA terminal. However, terminals do not cover the entire port area. There are critical facilities in the port that are outside the boundaries of terminals. We initially identified an additional 12 critical non-terminal areas in the port as well. However, based on risk scores assigned for each critical area, we clustered them based on a similarity metric which minimizes the difference assigned for the threat level on the total of 8 risk dimensions. A typical threat and vulnerability matrix for a terminal is illustrated in Table 3 above. We make a distinction on the threat level based on the activity taking place at the particular critical area on a given day. The threat level is assumed to increase if there is activity. For example, we believe the threat level at a cruise terminal depends heavily on whether there is passenger activity.

Clustering of critical areas helps reduce the computational complexity. In short, the similarity metric reduces the number of critical areas that should be considered for resource allocation purposes by more than half. Our goal is consult POLA/LB personnel to improve initial threat and vulnerability scores as well as the clustering results. A notional example threat and vulnerability matrix is illustrated in Table 4 below.

	Baseline Threat	Activity Threat	Vulnerability
Waterways - On Water	4	1.8	1
Waterways - Underwater	4	1.8	1
Air	5	1.2	1
Road	4	1.1	1
Rail	6	1	5
Access between the gates of entry	5	1.1	2
Entry with fake documentation	5	1.1	2
Insider threat	5	1.1	2

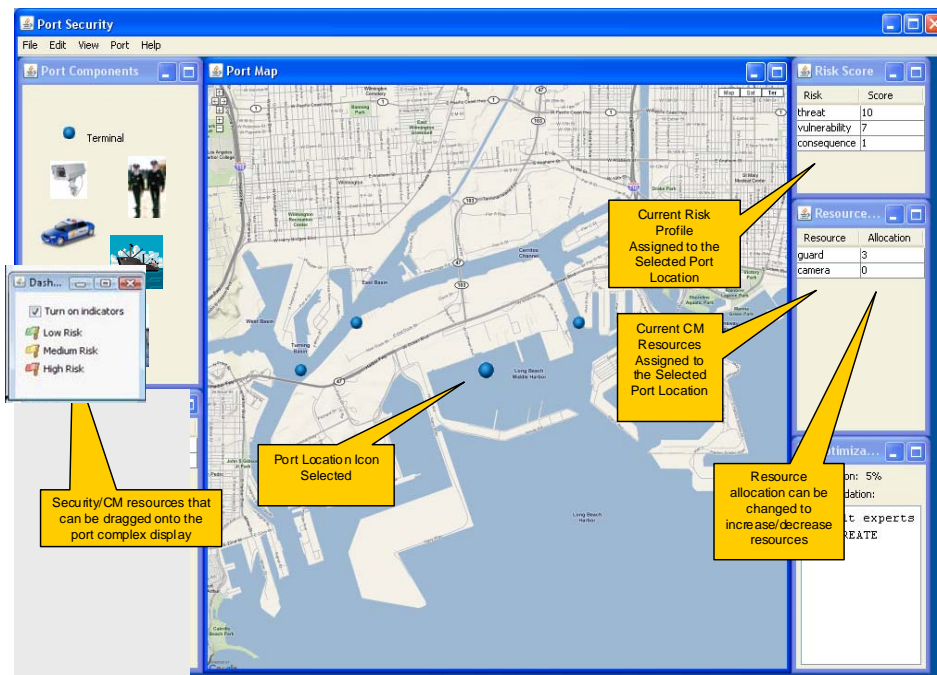
**Table 4 Threat and vulnerability score matrix for Pier B.**

## 2.2. PortSec Concept of Operations and User Interface

We envision two types of users of PortSec. These are described as:

- Port Security Officer – tactical responsibility for daily security arrangements, has 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

The notional User Interface for the Port Security Officer is shown in Figure 1.



**Figure 1: Prototype PortSec User Interface**

The Concept of Operations for conducting resource allocation what-if analysis would follow these steps:

1. Define/update port configuration/layout/infrastructure as in Figure 2
  - Select items from Control/Selection Area
  - Items include: bridges, highways, terminals, rail lines, watercraft operations, port perimeter, entry/exit portals, surveillance equipment locations, inspection locations, car patrols, foot patrols, watercraft patrols, warehouse locations
2. Define/update performance data (performance of components and links between them)
  - Specify performance for each port component (or accept defaults)
  - Performance values reflect risk/resource allocation analyses
    - For example: Add inspection station on highway entry portal
      - Will slow down throughput of incoming traffic
      - Will impact throughput of terminals
      - Will reduce risk of terminal or bridge from being destroyed by a truck bomb
      - Will cost X dollars to implement and maintain yearly
3. Simulate port operations
  - Select Run from Menu Bar
4. Collect performance metrics (note metrics in Status Area)
  - Port performance (cargo throughput)
  - Economic costs (security costs + normal port operation costs + anticipated costs if terrorism event occurs)
5. Save scenario definition and performance metrics
6. Repeat steps 1-5 for each desired scenario
  - First scenario is typically the current port operations (benchmark)
  - Second and subsequent scenarios are “what-if” options
7. Compare scenarios (examine performance differences) in Figure 3

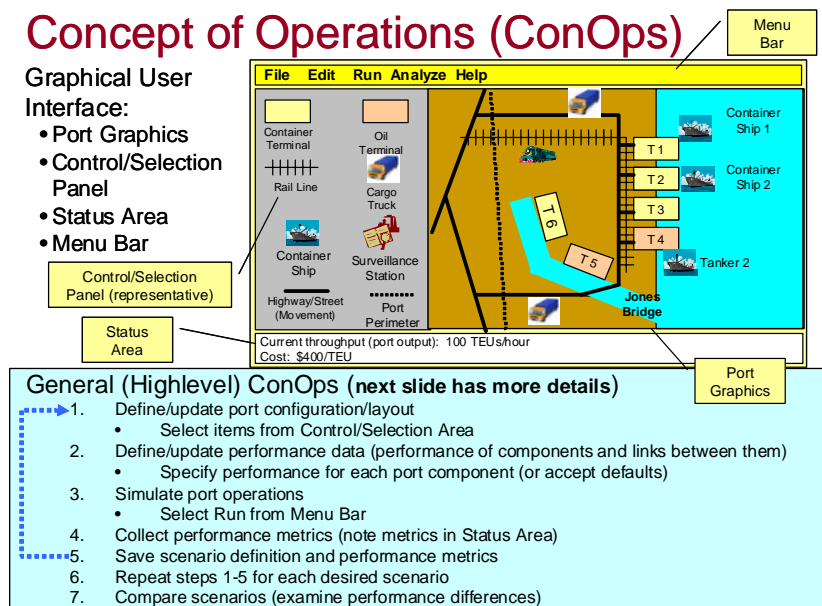


Figure 2. Establish Baseline Port Definition and New Features to be Evaluated

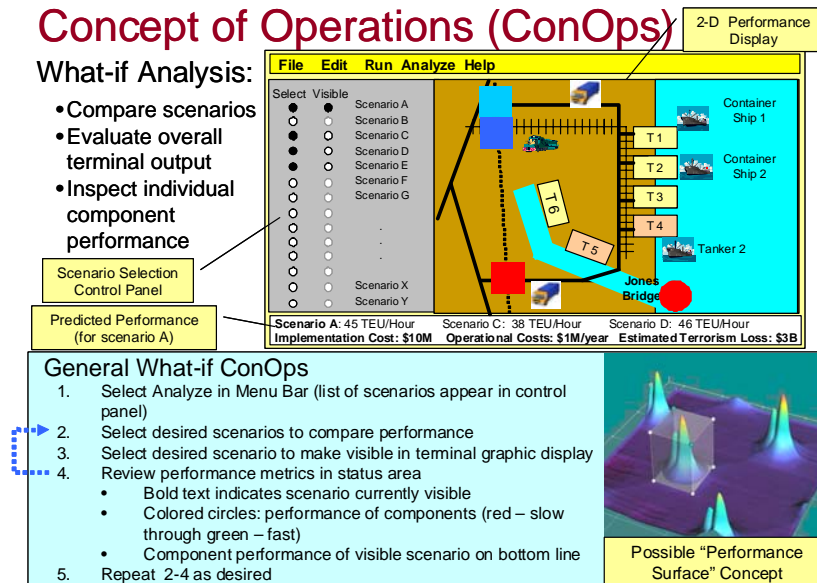


Figure 3. Results of Analysis

These results would then provide the input to the resource allocation analysis described in the Kleinmuntz project.

### 3. Applied Relevance

A major problem raised by the management of the Ports of Los Angeles (POLA) and Long Beach (POLB) is the lack of risk management resources to help them access the trade-offs in employing or integrating new or enhanced counter-terrorism methods and systems into their day-to-day operations. Such trade-offs include the benefit of implementing the methods and system – in terms of reduced risk of a terrorist event or reduced cost in recovery from such an event vs. the initial investment in the technology and the impact on day-to-day operations of the ports. In addition, port management expressed the need to evaluate day-to-day situational awareness for increased risk of a terrorism event and provide tools that will allow immediate resource re-allocation to help lower that risk (e.g., increase foot patrols near one of the terminals due to an unexpected gathering of a large number of people demonstrating against forced new work rules).

The PortSec system is being developed to address these requirements. In Year 4, in collaboration with the POLA and POLB authorities, we undertook an initial requirements analysis and system design. A prototype user interface and Concept of operations (ConOps) were developed. Effort on this project is on-going.

### 4. Collaborative Projects

We will be collaborating with the CA OHS port risk assessment effort, and the Coast Guard MSRAM effort to ensure consistency in the approach.

### 5. Research Products

This project expects to deliver prototypical code to the Port of LA/LB in Year 5.