A Model For Standardizing Risk Assessment
For Port Security

Rashmi Jain
Associate Professor of Systems Engineering
Stevens Institute of Technology

Introduction
Risk assessment is the ability to understand the risk and plan in advance. It is a clear understanding of the awareness, prevention, response and consequence of the risks. The process of risk assessment involves risk identification, measurement, prioritization, management and mitigation. It is important to identify the main risk drivers so that the mitigation management can produce the most effect. Risk assessment is a more informative and quick “what-if” assessment of the impact on the risk estimate of a change in an individual parameter or a group of parameters. It is a continual process that should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives.

The benefits of risk assessment in the context of port security include identifying any risks and threats associated with the infrastructure and developing plans to mitigate these weakness, emphasizing problem prevention in a controlled, planned manner, rather than having to react to a crisis with little or no preparation and protecting the confidentiality, integrity and availability of assets while still providing functionality and usability.

Economics of security
Planning for security as well as facing the consequence of not planning for security both have their economic effects. A large attack in a port, especially a well-coordinated one, could have the result of shutting down the entire system as governments scramble to put in place appropriate security measures. These may be drastic, such as the complete closure of ports and inefficient, duplicative, and lengthy cargo checks in both originating and receiving ports. The volume of world trade conducted by sea magnifies the severity of the problem drastically. The United Nations Conference on Trade and Development (UNCTAD) estimates that 5.8 billion tons of goods were traded by sea at in 2001. This accounts for over 80% of the world trade by volume. The bulk of this trade is carried by over 46,000 vessels servicing nearly 4000 ports throughout the world. (OECD, 2003). The OECD report on “Security in Maritime Transport: Risk factors and economic impact”, has analyzed and estimated the effects of attacks and accidents in U.S ports. These are discussed below under four major categories of effects.
Port disruptions

The first obvious implication of any attacks or accidents on a port is the disruption of port activity. Such disruption can be in several different forms such as not having the critical mass (people) to operate the port as a result of a ‘strike’; a WMD threat like the ‘Palermo Senator’ incident; disruption of terminal operations due to an actual attack such as the ‘Limberg Tanker’ incident. Another example of port disruption of a different kind was the incident of storm damage to containerized cargo in Santa Clara I off the eastern coast of the United States in January 1992. In this incident storm caused several containers containing magnesium phosphide to spill their contents in the hold. The containers were improperly manifested thus hiding the dangerous nature of their contents. Cases of mislabeled containers is not a unique occurrence and, because of the constraints placed on hazardous compound handling and stowage both in ports and on ships, some unscrupulous shippers and forwarders ambiguously- and/or mislabel containers containing these compounds. (OECD, 2003).

Impact on the Economy

The cost of an attack in a port would likely be measured in the tens of billions of dollars (e.g. up to USD 58 billion). The initial burden on the ship operators is at least ~USD 1,279 million and USD 730 million per year thereafter. Estimated losses from cargo theft range from USD 30 to 50 billion per year. (OECD, 2003).

The October 2002 attack on Limberg tanker tripled insurance premiums to as much as $0.3 million for vessels calling in Yemeni ports. Many shipping lines cut Yemen from their schedule. About 3000 jobs were lost on Yemen port. Government estimated losses of $15 million per month sustained over 6 month period would account for nearly 1% Yemen’s 2001 GDP. (OECD, 2003).

The attack on world trade center on September 11th, 2001 resulted in the destruction of physical assets which accounts for $14 billion for private businesses, $1.5 billion for state and local government enterprises and $0.7 billion for federal government. Lower Manhattan lost approximately 30% of its office space and scores of businesses disappeared. Close to 200,000 jobs were destroyed or relocated out of New York City, at least temporarily. This, the consensus forecast for US real GDP growth was instantly downgraded by 05 percentage point for 2001 and 1.2 percentage points for 2002. The implied projected cumulative loss in national income through the end of 2003 amounted to 5% points of annual GDP, 0r half a trillion dollars. (OECD, 2003).

The losses from the terrorist attacks for the insurance industry (including reinsurances) are estimated at between $30 billion and $58 billion, with the main uncertainty deriving from payments on liability insurance. The attacks presented the largest insurance event in history, dwarfing the $21 billion of losses incurred when Hurricane Andrew hit Florida in 1992. (OECD, 2003).
Implementation of security measures

Besides the cost of the attack another major factor is the cost of implementation of security measures to the ship owners, terminal operators, Coast Guards, and businesses at large. Majority of the ship-related costs are related to management staff and security-related equipment expenditures. However, needless to say that the cost of “not–doing–anything” will be several times the cost of security measures. The OECD’s 2003 estimate of system-wide procedural changes such as those imposed by the United States 24-hour advance notice rule is approximately USD 281.7 million (using carriers’ data) significantly below the potential cost of inaction. Also the overall estimated port-related security costs of over USD 2 billion are substantially below the costs that might result from a major attack. The cost-benefit analysis of a new electronic customs manifest handling system proposed by Customs and Border Protection before September 11th, 2001, estimates the direct savings to the importers alone to be USD 222.2 billion over 20 years and to the government to be USD 4.4 billion over the same period. (OECD, 2003).

Consequence management

Another aspect of costs resulting out of major port disruption is the cost of managing the consequences of such disruption. In response to a dispute between labor and management, all American ports on the west coast of the United States Ports closed for 11 days in October of 2002. These ports handle approximately 60% of the United States maritime imports and exports by value and the losses from the lock-out were projected to reach in the billions of dollars. Port management estimated loss of $19.4 billion for 10 day lock out. The potential losses borne by American workers, consumers and producers accounted to $466.9 million. Property damage cost, costs related to port shut down in other countries, loss of life, insurance premiums, etc accounted for $32 million. Another example of consequence management is the cost related to the rescue and cleanup for September 11th attack. It amounts to at least $11 billion. (OECD, 2003).

Current state of port security

The US maritime border is 95,000 miles of shoreline and 3.4 million square mile of exclusive economic zone. Maritime transportation system and ports are an essential intermodal link in the international goods movement system and are very important to the economy and security. They are the most valuable and most vulnerable, low risk high payoff target. There are more than 1000 harbor channels and 25,000 miles of inland, intracoastal and coastal waterways in the United States serving 300 ports with more than 3,700 terminals that handle passenger and cargo movements. It also contains shipyard and repair facilities crucial to maritime activity. The other source of vulnerabilities to threats may also come from a large network of linkages such as 152,000 miles of rail, 460,000 miles of pipelines and 45,000 miles of interstate highways. (Report to congress, 1999).

U.S marine transportation moves more than 2 billion tons of domestic and international freight, imports 3.3 billion barrels of oil to meet U.S energy demands, transports 134 million passengers by ferry, serves 78 million Americans engaged in recreating boating,
hosts more than 5 million cruise ship passengers and supports 110,000 commercial fishing vessels and recreational fishing that contribute $111 billion. (Report to congress, 1999).

Port of New York and New Jersey spans over 2 states, 6 large port facilities and 4 smaller ones. It is the largest port of import in the United States and 10th largest in the world. It handles over 3 million containers in a year, including a broad range of liquid and dry chemicals and regularly handles more petroleum products than any other American port. New York being the financial capital becomes a potential target for terrorist groups. It is the main and immigration gateway of the Eastern seaboard of North America. (Rodrique, J., 2003).

**Risk Assessment Model for Network Centric Systems**

Risk management involves two primary steps each with three subsidiary steps. The first primary step is risk assessment which comprises of risk identification, risk analysis and risk prioritization. The second primary step involves risk control and comprises of risk-management planning, risk resolution and risk monitoring. (Boehm, B.W. 1991). Table 1 (Jain et al, 2003) below gives the list of existing risk models.

<table>
<thead>
<tr>
<th>Model</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barry Boehm’s Risk Model</td>
<td>Boehm, B. 1991</td>
</tr>
<tr>
<td>Software Risk Evaluation Model</td>
<td>Sista and Joseph, 1994</td>
</tr>
<tr>
<td>Three-dimensional Software Risk Model</td>
<td>Sherer, S. 1995</td>
</tr>
<tr>
<td>Risk Identification Model</td>
<td>Bass, T.; Robichaux, R. 2001</td>
</tr>
<tr>
<td>Total Risk Management/ Hierarchical Holographic Modeling</td>
<td>Haimes, Y.Y and Chittister, C. 1993</td>
</tr>
<tr>
<td>Rowe’s Causative Events</td>
<td>Rowe, W.D. 1977</td>
</tr>
</tbody>
</table>

Models proposed by Bass and Robichaux (2001) and by Haimes and Chittister (1993) for complex network-centric operations is based on the interactions of the three variables, namely, criticality, vulnerability and threat. Criticality is the degree of importance of the asset to the mission; vulnerability is ways in which it can be compromised, exploited, damaged or destroyed and threat is entities that can exploit vulnerability and capabilities that might be exploited. Risk is the greatest where vulnerability, threat and mission critically intersect in a Venn diagram. Haimes’s presents his Total Risk Management
(TRM) approach as a systematic, statistically based and holistic process that builds on formal risk assessment and management. It is built on Hierarchical Holographic modeling (HHM) framework. It identifies risk and uncertainties emerging out of exogenous and endogenous events. Exogenous events may include new regulations or legislation, acts of terrorism and other random events. Endogenous events may include likelihood and consequences of hardware, software, organizational or human failure. Haimes’s HHM representation for assessing risks related to systems integration comprises of seven visions, namely, software development, temporal, leadership, environment, acquisition, quality, and technology. The environment vision addresses five risk sources stemming from a range of failures such as hardware failure, software failure, organizational failure, and failure due to sources external to the system. (Haimes, Y.Y. and Chittiser, C., 1993). Haimes’s framework is very relevant to our context of risk assessment for network-centric systems as the systems integration risks are an integral part of such an assessment.

A review of the above discussed seven risk models/taxonomies reveals a common thinking on the sources or factors that contribute to risk of systems, products, and processes. Bass and Robichaux, Haimes, and Rowe’s models bring in a slightly different perspective. Bass and Robichaux model is different from other risk management models in that it identifies risks based on the characteristics of the entity/project rather than the factors impacting its functionality. Rowe’s model provides a four-stage sequential lifecycle approach to risk assessment and management. His model is comprehensive and generic at the same time, and as a result its application is not restricted to any specific domain. All the seven models include four common sources of risk, human, organizational, technical and environmental.

**Risk Assessment for port security**

Similar to the above discussion on existing risk models we have attempted at identifying a risk assessment model specific for port security. Based on our review of existing sources of literature and our understanding of maritime security the following are the factors impacting port security. Table 2 identifies these vulnerabilities to port security.
Some of the major maritime agencies and initiatives (including in our case NJ/NY agencies) that are responsible for identifying, mitigating and managing some/all of the above risks are International Maritime Organization (IMO), Department of Homeland security (merger of 21 federal agencies), U.S Coast Guards, Transportation Security Administration (TSA), Federal Bureau of Investigation (FBI), Federal Emergency Management Agency (FEMA), Bureau of customs and Border Protection (BCBP), Joint Terrorism Task Force (66 JTTFs), AMS committee, NY state office of public security, NY state emergency management office, NJ office of counter Terrorism, NJ office of emergency Management, NYC office of Emergency Management, Port Authority NY and NJ, Port Authority office of emergency management, NJ Domestic security preparedness Task Force, Local Government and law enforcement agencies, Area Maritime Security Committee, etc. These departments/agencies have in response to 9/11 initiated several programs and initiatives to secure the port of NY/NJ. Some of their major programs are discussed below:

**Mandatory Programs**

1. International Maritime Organization regulations (International Code for Security of Ships and Port Facilities-ISPS)


3. 96 hour Advance Notification of Arrival

4. 24 hour Advance Cargo Manifest filing
5. Navigation and Vessel Inspection Circular 4-02: Security for Passenger Vessels and Passenger


9. Immigration and Naturalization Service (INS) Crewmember Security Plans

10. Interim Final Rule for MTSA

Voluntary Programs

1. Container Security Initiative (CSI)

2. Operation Safe Commerce (OSC)

3. Customs-Trade Partnership Against Terrorism (C-TPAT)


Risk Assessment Model for Port Security:

Risk assessment of port security in terms of threats and vulnerabilities has been mandated by a few international maritime agencies, and federal agencies. We have analyzed and integrated most of these major regulations such as ISPS Code, MTSA, and various US Coast Guards Circulars. Our proposed risk assessment model as described below is based on such an analysis and integration.

Our risk assessment model for port security comprises of three major components, namely, Port Facility Threat and Vulnerability Assessments, Ship (also called vessel and facility) Vulnerability Assessments, and Foreign Port Assessments.

In general all risk/vulnerability assessments involve the following four steps:
• identification and evaluation of assets and infrastructure that are important to protect;

• identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;

• identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and

• identification of weaknesses, including human factors in the infrastructure, policies and procedures.

The *port facility security assessment* is fundamentally a risk analysis of all aspects of a port facility operation in order to determine which part(s) of it are more susceptible, and/or more likely, to be the subject of attack.

Security risk is a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack. Therefore, any port facility risk assessment must include the determination of perceived threat to port installations and infrastructure; the identification of potential vulnerabilities; and the calculation of consequences of incidents.

Similarly, *ship or vessel risk assessment* includes risk analysis of all aspects of the ship such as its structural integrity; backgrounds of its personnel; its radio, telecom, computer and network systems; level of skill and training of its personnel in providing security etc.

*Foreign ports risk assessment* is similar to the assessment of our own US ports except it is constrained by the regulations resources of the specific country where the port is located. However, the international community is coming together in the post-9/11 efforts to secure maritime trade and commerce.

Based on our above discussed analysis of threats and vulnerabilities the following risk assessment model is proposed for port security. This model covers and integrates all the different aspects of risks assessment mandated by the different regulatory authorities/agencies.
**A Proposed Risk Assessment Model for Port Security**

**Port Facility Threat and Vulnerability Assessment**

- Environment Factors
  - Assets/Infrastructure
  - Possible Threats
  - Vulnerability of Infrastructure

- Human Factors
  - Vulnerabilities in terms of human errors in intelligence, judgement, implementation etc.

- Organization Factors
  - Vulnerabilities in terms of inadequate and faulty policies and procedures
  - Measures to reduce vulnerabilities

- Technical Factors
  - Technical vulnerabilities in terms of inefficient inadequate technical solutions for securing the ports, and security and safety of such technologies

**Ships Threat and Vulnerability Assessment**

- Current security threats and patterns
- Possible Threats
- Vulnerability in terms of physical security, structural integrity, detection of dangerous devices, methods that can cause security incident etc.

- Human Factors
  - Vulnerabilities in terms of human errors in intelligence, judgement, implementation, personnel protection systems, recognising persons who are likely to threaten security

- Organization Factors
  - Vulnerabilities in terms of inadequate and faulty policies and procedures, ship/port interface business practices, contingency planning, emergency preparedness and response.
  - Measures to reduce vulnerabilities

- Technical Factors
  - Technical vulnerabilities in terms of radio and telecom systems, computer systems and networks, techniques used to circumvent security measures, marine engineering, effects of explosives on ship structures and equipment

**Foreign Ports Threat and Vulnerability Assessment**

- Measures to restrict access to cargo, vessels, and dockside property to authorized personnel only
- Additional security on board vessels

- Human Factors
  - Vulnerabilities in terms of human errors in intelligence, judgement, implementation etc. Background checking of cargo handling personnel

- Organization Factors
  - Licensing or certificate of compliance with appropriate security standards
  - Security management program of foreign ports

- Technical Factors
  - Technical vulnerabilities in terms of screening of containerized and other cargo and baggage

---

Some recommended preventions:
- Prevent harmful devices, substances to be introduced on port or ship
- Prevent unauthorised access to port facility, moored ships, and restricted facility
- Procedures for responding to threats while maintaining critical port interfaces
- Assign security responsibilities to personnel
- Procedures for interfacing with ship security activities
- Procedures for periodic review & auditing of Security Plan
- Measures for effective security of cargo and cargo handling at port
- Procedures for securing personnel movement in and out of ships
- Procedures for responding to a ship security alert system

Some additional prevention measures for vessels:
- Procedures for auditing the security activities;
- Procedures for training, drills and exercises associated with the plan;
- Procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
- Frequency for testing or calibration of any security equipment provided on board;
- Identification of the locations where the ship security alert system activation points are provided; and
- Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.
The above model is unique in two ways. First, it classifies all the different kinds of risks to port security based on its source. Based on the existing research and literature we believe that identifying the source of a risk is the first and important step in understanding a risk. Secondly, the model, by integrating regulatory requirements of the different bodies, provides a comprehensive view of risk assessment of port security. The model does leave out some other aspects of risk such as those coming from inland through highways and inland water ways connected to the ports. This aspect of port security has so far not received the attention of the maritime security and regulatory agencies.

Some potential areas of future research could be providing more detailed level analysis on the model. This paper has analyzed risk assessment at a fairly high level. Another area could be actually surveying the views of the ship-owners, terminal operators, Coast Guards on the completeness and effectiveness of the proposed model. In order to define effectiveness some metrics will have to be identified and this could be another area for further research.

References


U.S Coast Guard, “Navigational and Vessel Inspection Circular No. 402”.

U.S Coast Guard, “Navigational and Vessel Inspection Circular No. 902”.

U.S Coast Guard, “Navigational and Vessel Inspection Circular No. 1002”.

U.S Coast Guard, “Navigational and Vessel Inspection Circular No. 1102”.

U.S Department of Transportation, “An Assessment of the U.S. Marine Transportation System”, A report to congress, September 1999