Evaluation and Enhancement of Port Security and Efficiency using Mathematical Techniques

Marco A. LARA GRACIA
Department of Engineering, University of Southern Indiana
Evansville, Indiana 47725, USA

Danielle ECKERT
Department of Engineering, University of Southern Indiana
Evansville, Indiana 47725, USA

ABSTRACT
In this paper, progress and challenges in US homeland security are discussed, and security and efficiency, two important aspects of the operation of maritime ports, are addressed. Specifically, this paper describes the application of Data Envelopment Analysis to assess port efficiency and the application of Fault-Tree Analysis and Risk Analysis to enhance port security. Use of high technology and marine animals to enhance port security are also discussed.

Keywords: Port security, Data Envelopment Analysis, Fault-Tree Analysis, and Risk Analysis.

1. INTRODUCTION
The progress that the US has achieved in terms of homeland and supply chain security since 9/11 is remarkable. The US Department of Homeland Security has successfully implemented numerous security initiatives with a favorable result: No terror attack since September 11, 2001. However, there is evidence that one of the areas less investigated in homeland and supply chain security is related to sources of risk at sea level and underwater. A self-propelled semi-submersible, a small vessel, an improvised explosive device, and divers are examples of threats to cargo ships and to maritime ports.

1.1 Facts
Some facts that magnify the risks and help justify research on underwater port security are:

- The United States has 95% of its trade relying on the maritime transportation.
- 90% of the war materials go by sea.
- 6.5 million Cruise passengers every year in the US.
- 200,000 mariners that come to US ports every year.
- 75,000 foreign ships per year stop at US port every year.
- 11,000,000 cargo containers enter the US every year, which is about 32,000 containers a day.
- 95,000 miles of open shore line. Assuming 10 miles into the ocean results in 950,000 square miles that need to be protected by the US Coast Guard (USCG).
- In the US there is an estimated 17 million small boats and about 3 million of those are not registered.

About 42,000 US Customs Border Protection (CBP) officers and 37,000 USCG members are responsible for protecting the US borders and ports. As a reference, there are 85,000 law enforcement officers that make up the New York Police Department.

1.2 Challenges
The threat and risk associated to small boats are significant. There are three incentives making small vessels appealing to terrorists:

1) Small vessels (i.e., boats) can be used as launching platforms for short range missiles.
2) Small vessels can be used in suicide attacks, for example, running the vessel into cargo or military vessels.
3) Small vessels can be used to transport weapons of mass destruction (WMD).

4) Small vessels can be used as diving platform for divers wanting to cause some form of damage or destruction.

Self-Propelled Semi-Submersibles (SPSS) are used to smuggle drugs to the US. They are water vessels that are partially submerged in the water and a very hard to spot in the open waters of the ocean, even from an aerial view. They are typically manned with 3 or 4 persons.

SPSS are constructed of steel and fiber glass and can cost up to 1 million dollar to build. Even with such a large amount of money put into the vessels, they are not meant to return. They are used for a one way trip (criminal organizations using the SPSS’s are well funded and have no problem with building the vessels for a one time use). In October of 2008 a SPSS was intercepted by the USCG. It had over 7 metric tons of cocaine on board with a market value of over 166 million dollars.

Improvised Explosive Devices (IED) can be used by terrorists to cause destruction and hurt/kill people. They (IEDs) can be placed on rivers, open sea, or navigation channels to float around in order to hit and destroy a vessel or part of a maritime port. Examples of IEDs are the bombs used in the 2013 Boston Marathon.

Divers can attach explosive devices on the bottom of vessels, legs of oil rigs, etc. with a single goal: inflict damage, cause destruction, and destroy lives.

Self-propelled semi-submersibles, small vessels, improvised explosive devices, and divers are examples of means that can be used by terrorists to perpetrate deadly terror attacks. It is quite likely that they (terrorists) are continuously developing new and creative ways of terrorism.

Security experts emphasize the need to concentrate on technological development to supply tools to law enforcement agencies to allow them to effectively detect and inspect in a timely manner suspicious devices and individuals.

1.3 Port security, technology and animal life

Technology is expected to play an important role in the development of advanced port security systems to be established to maximize the protection of US ports and vessels. For instance, to increase security at US major maritime ports, transponders could be installed on registered, privately-owned small vessels. This would allow the USCG to:

a) Watch the waters using Global Positioning System (GPS)

b) Track boats around the waterways to protect cargo vessels and ports

c) Identify non-registered boats

An unmanned underwater vehicle (UUV) has been tested by the USCG. The name of the UUV is the “Slocum Glider”. The UUV is a 1.5 meter long torpedo-shaped vehicle that moves in an up and down pattern as it moves forward. It has blades on the side of the vehicle to help drive the vehicle. Once the vehicle comes to the surface it transmits information back to receiving computers. The UUV can also accept new instructions once it reaches the surface without coming back to shore. The Slocum Glider can patrol for weeks at a time.

One of the most known and successful post 9/11 security initiative implemented by the US Department of Homeland Security is the Container Security Initiative (CSI) [4]. CSI allows for the screening of containers 24 hours before they will be shipped to a US port. US Customs and Border Protection officers physically located that foreign ports where shipping of US bound container takes place, are in charge of the screening of containers [5].

Other successful supply chain security initiatives implemented by the US Department of Homeland Security are the Megaports Initiative, C-TPAT, and the Secure Freight Initiative [5].

Manufacturers of cranes and container handling equipment used at maritime ports are active implementing security devices (i.e. sensors) on equipment that can help detect illegal cargo on containers. Cargotec Oy, a European manufacturer of container handling
equipment installs security-related accessories on new equipment.

Marine animals have been also used in the war against terror. A few years ago, the Port of San Diego, CA experimented with various types of underwater surveillance using marine animals to detect underwater threats. Sea lions and dolphins were trained as part of the Navy’s Marine Mammal Program in San Diego to actually locate an intruder and snap a locking clamp on to the limbs of the intruder and leave. The intruder will then have to wait for the Navy to show up and pick him/her up. Research has shown that: 1) Sea lions are not afraid of confrontation and 2) Dolphins become sluggish in warmer temperature, whereas sea lions don’t seem to be affected by changing water temperatures.

2. MODELING PORT SECURITY USING MATHEMATICAL TOOLS

Fault-Tree Analysis and Risk Analysis are applied in this research to enhance port security.

A Fault-Tree Analysis, developed by Bell Laboratories in the early 1960s to assist the U.S. Air force in examining missile failures, is a probabilistic process based on a graphical model of parallel and sequential combination of events, or faults, leading to the overall undesired event, for example, an accident or a terror attack. These events can be of various types and identified by different symbols. There are two main event categories: fault events, identified by rectangles, that are to be expanded further and basic events, identified by circles, at the bottom of the fault tree that cannot be developed any further.

The development of a fault tree starts with identifying all the events that are deemed undesirable for normal operation of a given system [3]. Figure 1 shows the outcome of a Fault-Tree Analysis applied to port security.

According to Figure 1, an outcome of the Fault-Tree Analysis conducted in this research indicates that a terrorist attack can develop from many different scenarios.

Although there are many ways an attack can be carried out, the terror attack needs two key pieces to occur:

1) Timing – Terrorist will look at what time the port is the busiest which would make it the most vulnerable; narrowing it down to the year, month, day, and hour.

2) Opportunity - The opportunity will be pinpointed down to:
   – Lack of security procedures for prevention of terror attacks
   – Lack of trained personnel
   – Lack of technology to protect infrastructure and personnel
   – Procedures not followed by personnel, which may be at fault of training

Even though it is impossible to prevent the terrorist from the planning of an attack or even from knowing the ports’ busiest time focused should be on eliminating the opportunity. The “Opportunity” is where more research needs to be developed as there are not many prevention standards or technologies in place for underwater threats and at sea level.

From the perspective of Risk Analysis, potential risk increases with increased likelihood or probability that the hazardous event will occur, increased exposure to the hazardous condition, and increased possible consequences of the hazardous event [3].

To verify the vulnerability to terror attacks at sea level and underwater a Risk Analysis has
been conducted to compare the likelihood of an attack to its effect on maritime ports. The risk value is a product of the likelihood, exposure, and possible consequences:

Figure 2 shows the outcome of a Risk Analysis conducted to enhance port security. Table 1 contains the data used to compute the risk values.

![Figure 2. Application of Risk Analysis in port security.](image)

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Values</th>
<th>Exposure</th>
<th>Values</th>
<th>Possible Consequences</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Rare</td>
<td>1</td>
<td>Submarine</td>
<td>10</td>
<td>Catastrophe</td>
<td>100</td>
</tr>
<tr>
<td>Rare</td>
<td>0.9</td>
<td>Small Vessel Attack</td>
<td>7</td>
<td>Disaster</td>
<td>75</td>
</tr>
<tr>
<td>Unusual</td>
<td>0.7</td>
<td>Floating IED’s</td>
<td>4</td>
<td>Very Serious</td>
<td>60</td>
</tr>
<tr>
<td>Occasional</td>
<td>0.5</td>
<td>Land Attack</td>
<td>1</td>
<td>Serious</td>
<td>45</td>
</tr>
<tr>
<td>Frequent</td>
<td>0.3</td>
<td></td>
<td></td>
<td>Important</td>
<td>30</td>
</tr>
<tr>
<td>Continuous</td>
<td>0.1</td>
<td></td>
<td></td>
<td>Noticeable</td>
<td>15</td>
</tr>
</tbody>
</table>

Table 1. Risk calculation values.

Using the example illustrated in Figure 2 in conjunction with the values shown in Table 1, would yield a risk index of 210 (0.5 × 7 × 60 = 210). The interpretation of the risk index would state that the threat is high risk and would require immediate correction to promptly improve and repair infrastructure and procedures to improve security.

Port efficiency is also addressed in this research. Data Envelopment Analysis (DEA), a technique based on linear programming, is the primary tool used to evaluate the performance of a maritime port in order to increase its efficiency. The way DEA works is rather simple. It:

- Allows for multiple inputs and multiple outputs.
- Compares unit-to-unit efficiencies; a unit can be a maritime port, hospital, factory, warehouse, airports, etc.
- Compares unit output in terms of productivity.
- Is used to benchmark underperforming units against best practices.
- Can be used to perform a gap analysis to determine infrastructure needed to reach the desired output.

Some approaches, for instance Regression Analysis, use central tendency, usually the mean, as the basis of their measures. DEA estimates a “Best Practice Frontier” and uses this frontier as a benchmark set for underperformers.

The application of DEA involves complex computations [2]. In this research, specialized software is used in a case study conducted to illustrate the application of DEA in the evaluation of a group of US maritime ports in term of efficiency (i.e., productivity). In this context, the basic concept of efficiency measurement is the ratio of total outputs (production) to total inputs (infrastructure) [1]. Each of the eight ports considered in the case study has three inputs (number of ship-to-shore cranes, number of berths, and number of container terminals) and one output (number of TEUs). A TEU (Twenty Equivalent Unit) is a 20’ cargo container. Therefore, a 40’ cargo container is equivalent to 2 TEUs. Data used in the case study was obtained from the official web sites of the maritime ports in question. Figure 3 shows the DEA-based efficiency scores.

![Figure 3. Efficiency scores.](image)
Efficiency scores for each of the ports were obtained using the specialized DEA software and the most efficient port was identified. Underperforming units (i.e., ports) were identified and a gap analysis was conducted to move the underperforming units (ports) to the efficiency frontier, which basically means to increase their efficiencies.

3. OPERATION OF SECURITY DEVICES ON CONTAINER HANDLING EQUIPMENT

An additional layer of defense can take place at terminals around the world where cargo containers are stored before they are loaded on vessels bound for the US. Sensors or portable x-rays / scanners can be attached to spreaders and mast of container handling equipment to detect illegal cargo and to send in real time information about security related incident or just to notify the US law enforcement agencies about suspicious cargo containers.

Figure 3 shows how high tech sensors can be mounted on a spreader to detect illegal / dangerous cargo being transported in a container. The green dots in Figure 3 represent high tech sensors. The figure in yellow is a spreader, which is normally mounted on cranes and container handling equipment to handle containers.

Figure 3. A spreader equipped with high tech sensors.

Figure 4 shows a container handling equipment (Reachstacker) equipped with a spreader to handle containers.

Figure 4. Reachstacker.

4. FUTURE RESEARCH

The next step in this project is the combined application of Fault-Tree Analysis, Risk Analysis, and DEA along with other applicable tools to enhance different areas of homeland security, for instance airport security, border protection, underwater security, etc.

5. REFERENCES


