2005

Modeling of Commercial Maritime Port Recoverability from Security Disruptions: Work-in-Progress

C. Ariel Pinto
Old Dominion University

Wayne K. Talley
Old Dominion University

Original Publication Citation

Pinto, C. A., & Talley, W. K. (2005). Modeling of commercial maritime port recoverability from security disruptions: Work-in-progress. *26th Annual National Conference of the American Society for Engineering Management 2005: Organizational Transformation: Opportunities and Challenges, ASEM 2005, October 26-29, 2005, Virginia Beach, Virginia* (pp. 470-474). American Society for Engineering Management.

© 26th ASEM National Conference Proceedings, October 2005

MODELING OF COMMERCIAL MARITIME PORT RECOVERABILITY FROM SECURITY DISRUPTIONS: WORK-IN-PROGRESS

C. Ariel Pinto, Ph.D., Old Dominion University
Wayne K. Talley, Ph.D., Old Dominion University

Abstract

This article describes active research in commercial maritime port's recovery from security disruptions which explores the synergy of economic and simulation models in investigating the recoverability of ports after security incidents. Previous study has identified decision variables and throughput simulation models of port operation. However, none of these models have been utilized to investigate port's recovery from a security disruption and in evaluating recoverability investments. The method of research includes analysis of recorded disruptions, identification of impediments to recovery and investment criteria for recoverability. This article provides managers insight into including security and continuity of operation in managing various types of systems.

Introduction

The U.S. Coast Guard has moved aggressively since 9/11 to provide for maritime security – e.g., the creation of the High Interest Vessel Boarding Program, the deployment of Coast Guard personnel as "Sea Marshalls" aboard certain ships entering and leaving ports, and the establishment of port security zones around ships and high-risk port facilities.

On November 25, 2002, the Maritime Transportation Security Act (MTSA) was signed into law and was designed to protect the nation's ports and waterways from a terrorist attack. The MTSA is based upon a risk-based methodology and focuses on those maritime industry sectors that have higher risks of incurring transportation security disruptions. The MTSA requires the establishment of committees in the nation's ports to coordinate the activities of port stakeholders, e.g., shipping lines, shippers, longshoremen, shipping agents, the recreational boating public and various port-related federal, state and local agencies. In essence, the focus of the MTSA is to prevent security disruptions in the maritime supply chain, i.e., in the movement of maritime cargo from shipper to consignee, with the emphasis on the port link of the chain.

The research community has also responded to the events of 9/11. A number of recent studies have investigated risk and security in general and in ports and the supply chain. Leung et al. (2004) emphasized the importance of a critical infrastructure such as a bridge to recover from failure incidents. Together with other properties such as redundancy and robustness, system recoverability is critical for system-wide risk management. Harrald et al. (2004) presented a framework for sustainable port security that includes port-security prevention (pre-attack) and mitigation and recovery (consequence) programs. The framework is based on two perspectives: the causal chain of events leading to security incident and the system of systems nature of ports. As such, ports are critical nodes in the complex economic inter-modal subsystems that move goods and cargo around the world. For example, a container facility is tightly coupled with the inter-modal rail yard and the tightly scheduled container vessels.

Chopra and Sodhi (2004) investigated the stress-testing of the supply chain by running exercises based on what-if scenarios. These exercises identify subsystems (or links) within the supply chain, the various risk scenarios the subsystems may experience and the effects to the overall chain. The study notes that one of the best defenses against a supply chain failure is a well-designed and communicated recovery process.

To date, there have been significant improvements in securing U.S. ports, i.e., the investigation of ex ante security disruptions since the events of September 11, 2001. However, there has been little or no investigation of ex post port security disruptions, i.e., the recoverability once a security disruption has occurred. Possibly, this is due to the absence of any major security-related disruption at U.S. ports.

However, port security disruptions cannot be prevented with certainty. An optimal port security disruption prevention and recovery strategy is one that maximizes the net benefits (i.e., benefits minus costs) of such a strategy, where the benefits are the cost savings to the port from the strategy and the costs are those attributed to the strategy -- thereby providing an efficient allocation of security-disruption resources among the competing activities of prevention and recovery. It is expected that law-makers, policy-makers and the maritime industry itself in the near future will place greater emphasis on recovery issues related to port security disruptions (Maritime and Port Security Summit, 2004). Thus, a potential high-yield study is one that contributes towards the analysis of recovery strategies after a security disruption.

Specific Aims

The focus of the research is to address port's recovery from security disruptions. The highly uncertain nature of security disruptions and the commercial orientation of maritime ports make this topic well suited from the fields of economics, logistics, and risk modeling, assessment, and management.

The particular aims of this research are embodied in a set of questions that will provide direction to research activities in a port's recovery from security disruptions. These questions are:

- What are the potential security disruptions to a port?
- What are the impediments to recoverability?
- How can we analyze recovery strategies?

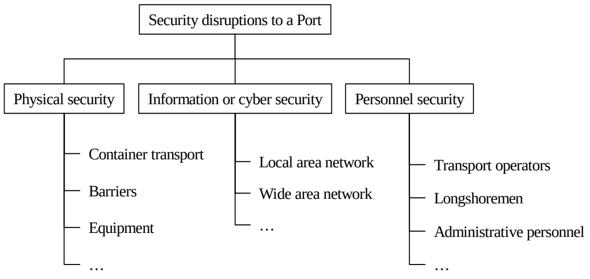
Accidental disruptions. Recovery strategies from any type of disruption depend highly on specific characteristics of the disruption, and are designed based on experience and analysis of event records. However, there has never been any recorded major security incident in a commercial port in the U.S. As such, describing a security disruption to a port is not a trivial exercise but will require an analysis of non-security related disruptions and an extension of the analysis to potential security-disruption scenarios.

An investigation of port accidents in 95 countries can help classify such accidents by type, origin and cause (Darbra and Casal 2004), and location (Ronza et al. 2003). The origins of the accidents are (a) transport of cargo (56.5%), (b) loading and unloading operations (14.9%), and (c) other origins (process plant, storage, waste and warehouse facilities) (28.6%). Among accidents originating from the transport of cargo, majority (65%) involve ocean-going vessels' movements in and out of port and ship maneuvering within port, followed by pipeline accidents (12%). The causes of the accidents were collision between ships or between a ship and dry land or between truck and rail vehicles (46%), mechanical failures (18.1%), Human error (15.9%), and external causes such as high winds and fires (17.0%).

Accidents can also be classified in terms of types such as releases and loss of containment (51%), fires (29%), and explosions (17%); and in terms of its location of occurrence such as the sea during approach and maneuver (40%), on land during storage, process and transport (21%), and at a sea-land interface during loading/unloading and maintenance (39%). The most common types of substances involved in port accidents are crude oil and other oil products. Port accidents that involve the handling and temporary storage of hazardous cargo in port areas originate from the nature of port activities – e.g., hardware failures of ship, inland and loading/unloading equipment and external events such as bad weather (Christou, 1999).

Potential security disruptions. Obviously, there are security disruptions that are not aptly represented by the accidents described above. In particularly, possible terrorism related disruptions such as nuclear attacks, poison gas attacks, dirty bomb explosions, or commandeered container trucks and ships have not been recorded yet. Using decomposition to facilitate the analysis of possible security disruptions to a port leads to three subsystems of analysis: physical security, information or cyber security, and personnel security, as suggested by Roberts (2004) as shown in Exhibit 2. These three subsystems provide technologist, security experts, and system analysts possible approaches to analyzing the port as a whole.

Exhibit 2. Decomposition of Port for Security Incident Analysis.



Decomposition of a recorded major accident into critical data elements may be performed using a method adapted from Lincoln et al. (2004). This method identifies six key data elements: activity area, task, contributing factor, precipitating mechanism, incident event and outcome. These elements are described in the tables below. This method facilitates extraction of data from narrative text of recorded incidents and aids in the development of the potential incident scenarios.

The following two cases of recorded vessel and port accidents are decomposed into key data elements:

Case I: Fire aboard the tug Scandia and the subsequent grounding of the tug and the tank barge North Cape on moonstone beach south Kingston, Jan 19, 1996.

Summary: On Friday afternoon Jan 19 ,1996 ,the U S tug Scandia had an engine room fire while towing the unmanned US tank barge North cape ,4.5 miles Off point Judith ,Rohde Island .All six crewmembers abandoned the Scandia and 10-foot 25-knot winds .The crew was unsuccessful in its attempts to release the anchor of the barge ,which rans around and spilled 828,000 gallons of home heating oil, causing the largest pollution incident in Rohde island history.

Sequence of events:

- Tug Scandia departed bay one enroute to providence, Rhode Island.
- Scandia was pushing an unmanned barge which contains 4,074 gallons of heating oil as soon as tug left New York harbor, it switched from pushing to towing the North Cape.
- Captain of tug Scandia requested and received a faxed whether forecast from fleet Whether.
- Friday noon, captain started losing visibility because of fog.
- He asked chief engineer for check up and chief engineer found everything fine .
- One of the crewmembers standing in the gallery and saw smoke coming from top.
- He Informed tanker man about smoke.Immdiatly sirens are activated, vessel monitoring system panel started.
- Crew bought portable (co2) fire extinguisher but unable to control fire
- Captain reported coast guard about uncontrollable fire on vessel and asked for help.
- Captain and crew members' wore sea suits
- Seaferrer vessel arrived to help crew members and rescued them

Case 2: - Ramming of the eads bridge by barges in tow of the M/V Anna Holly with subsequent ramming and near breakaway of the president casino on the admiral St. Louis Harbor, Missouri April 4, 1998.

Summary: On April 4, 1998 a tow of M/V Anna Holly, which was traveling northbound on the Mississippi river through the St. Louis Harbor, struck the Missouri-side pier of the center span of the Eads Bridge. Eight barges broke away and drifted back through the Missouri span. Three of these barges drifted toward the president casino on the admiral, a permanently moored gaming vessel below the bridge on the Missouri side of the river. The drifting barges struck the moored admiral, causing most of it's mooring lines to break .The admiral then rotated away from the Missouri riverbank .the captain of Anna Holly disengaged his vessel from the remaining barges in the tow and placed the Anna Holly's bow against the Admirals bow to hold it against the bank. Fifty people suffered injuries people were killed and an estimated damage $11 million.

Sequence of events:

- Anna Holly was traveling from northbound Mississippi river through St. Louis harbor.
- At about 18:30 got underway from fleeting area (upstream Minnesota, consists of 12 barges)
- Captain radioed and request for help at coast guard to assist Anna Holly through bridges.
- Captain asked chief engineer to do routine check ups Captain directed tow to the right of the eads bridge center span
- Steering light was not lit, so captain maneuvered Anna holly close to the middle of the arched center span and Vessel started to begin slow.
- Anna holly stalled (halted by water current)
- Headway stopped and current caused to drift sideways towards Missouri side pier of the edge bridge 8 barges broke away the tow
- The drifting barges struck moored caused most of its mooring lines to break
- Captain disengaged vessel and placed Anna holly's bow against Admiral's bow to hold it against the bank

Impediments to recovery. Ports are likely to experience a number of impediments to recovering from security disruptions. Impediments are factors that prevent the instantaneous recovery of a port from a security disruption. The identification of these impediments can provide critical information in the effective design and efficient implementation of recovery strategies.

For any particular security disruption, there can be more than one possible recovery strategy. Therefore, there is the need to differentiate among recovery strategies based on criteria (e.g. cost-benefit, throughput, etc.) that are acceptable to the various port stakeholders. This is particularly true in light of scarce resources.

Typical concept of recovery pertains to activities after real incident such as fire or equipment failure. However, the aversion from security related incidents and the layered security approach typical of many critical infrastructures have lead to the heavy use of technologies for early detection of incidents (Wolthusen 2001, Chen 2004). Nonetheless, any detection systems always have the possibility of false-positive alarms; wherein an apparent security incident actually turns out to be false-alarms. Thus, there are two types of recovery activities that will be looked at: recovery after a true security incident and recovery after a false alarm.

For a true security incident, expected impediments to a port's recoverability include rebuilding port infrastructure (berths); replacement of port mobile capital (cranes); federal, state and local government regulations; union labor restrictions; and replacement of inland-carrier infrastructure and mobile capital. The time required for a port to recover from a major port infrastructure disruption is in general expected to be greater than that from a major port mobile capital disruption. In general, regulations of federal agencies are expected to be greater impediments than regulations from state and local government agencies.

For a false alarm, the expected impediments to a port's recoverability will be inherently different from a true security incident. Instead of structural impediments as described above, impediments such as policies set forth by the port operator, the local law enforcement agencies, and other policy-based restrictions will be more evident.

Analysis of recovery strategies. Talley (1996) presented an economic model of port operation which identifies performance indicators for evaluating port's performance with respect to its economic objective over time. It considers demand functions for the port's throughputs; prices charged for various services; opportunity costs incurred by ocean carriers, inland carriers and shippers; port production functions; port resource functions; and the costs of port resources. The model uses economic objective that maximizes annual throughput subject to a profit constraint, equal to zero for a public port and some positive value for a private port.

Some of the port performance indicators include: ship and vehicle loading and unloading service rates by type of cargo; port channel accessibility and reliability; port berth accessibility and reliability; entrance and departure gate reliability; probabilities of ship, vehicle, and cargo damage in port; and probabilities of ship, vehicle, and cargo loss (or theft) in port. With these performance indicators, port management can evaluate the performance of specific services or service areas (e.g., the dock, gates and the port channel) of the port, thereby detecting where performance within the port has been improving or declining over time.

This model will be very useful for the analysis of security disruption if coupled with a throughput model of port operation during recovery. There are several recent throughput model of port operation: Leathrum et al. (2004) describes a simulation of port operation for military purposes; Luo and Grigalunas (2003) suggested a spatial-economic approach to modeling a port; and Demirci (2003) suggested a simulation of additional investment to port operation. However, none of these models clearly address the economics of recoverability

Preliminary Conclusion

The primary challenge of the research during the preliminary phases is the lack of information on security disruptions and recoverability in port operation. Nonetheless, records of accidental disruptions have been deemed very valuable in creating potential security disruptions. These records are also very valuable in identifying impediments to recoverability. Disruption due to false alarms is neglected in previous studies but may prove to be important for the case at hand. Lastly, models for analyzing port operation, both economic and throughput abounds. However, more detailed examination of the models is needed to determine their suitability for analyzing recoverability issues.

Overall, this article summarizes possible approach to including security and continuity of operation into the management of various types of systems.

Acknowledgements

This work was supported, in part, by the Office of Research and the Research Foundation at Old Dominion University through the Summer Experience Enhancing Collaborative Research (SEECR) Program.

References

Chadwin, Mark, Jim Pope and Waybe K. Talley, Ocean Container Transportation: An Operational Perspective. New York: Taylor and Francis, (1999).

Chen, Hsinchun, "Intelligence and Security Informatics for Homeland Security: Information, Communication, and Transportation," IEEE Transactions on Intelligent Transportation Systems, Vol. 5, No. 4, (2004), pp. 329-341.

Chopra, Sunil. and ManMohan S. Sodhi, "Managing Risk to Avoid Supply-Chain Breakdown," *MIT Sloan Management Review*, Vol. 46, No. 1, (2004), pp 53-61.

Christou, Michalis. D., "Analysis and Control of Major Accidents from the Intermediate Temporary

Darbra, Rose-Mari and Casal, Joaquim, "Historical Analysis of Accidents in Seaports," *Safety Science*, v. 42, (2004) pp. 85-98.

Demirci, Emrullah, "Simulation Modelling and Analysis of a Port Investment," *Simulation*, Vol. 79, No. 2, (2003) pp.94-105.

Harrald, John R., Hugh W. Stephens, and Johann Rene vanDorp, "A Framework for Sustainable Port Security," *Journal of Homeland Security and Emergency Management*, Vol. 1, No. 2. (2004).

Leathrum, James, Roland Mielke, S. Mazumdar, R. Mathew, Y. Manepalli, V. Pillai, R. Malladi, and J. Joines. "A Simulation Architecture to Support Intratheater Sealift Operations", *Mathematical and Computer Modeling*, Vol. 39, (2004) pp. 817-838.

Leung, Maria F., James H. Lambert, and Andrew Mosenthal, "A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks," *Risk Analysis*, Vol. 24, No. 4. (2004).

Lincoln, A.E., G.S. Sorock, T.K. Courtney, H.M. Wellman, G.S. Smith, P.J. Amoroso "Using

Narrative Text and Coded Data to Develop Hazard Scenarios for Occupational Injury Preventions”, *Injury Prevention*, 10, pp. 249-254, (2004).

Luo, Meifeng and Thomas A. Grigalunas, “A Spatial-Economic Multimodal Transportation Simulation Model For US Coastal Container Ports,” *Maritime Economics & Logistics*, Vol. 5, No. 2, (2003) pp. 158-178.

Maritime & Port Security Summit, 2004. Roundtable discussion at the Maritime & Port Security Summit, George Washington University, Washington, D.C., (November 16-17).

Roberts, Steven, “Tips and Trends for Homeland Security and Critical Infrastructure Protection,” *Journal of Homeland Security and Emergency Management*, Vol. 1, Issue 4, (2004) Article 405

Ronza, A., Felez, S., Darbra, R. M., Carol, S., Vilchez, J. A. and Casal, J., “Predicting the Frequency of Accidents in Port Areas by Developing Event Trees from Historical Analysis,” *Journal of Loss Prevention in the Process Industries*, Vol. 16, (2003), pp.551-560.

Storage of Dangerous Substances in Marshalling Yards and Port Areas,” *Journal of Loss Prevention in the Process Industries*, Vol. 12, (1999), pp. 109-119.

Talley, Wayne K., “Ocean Container Shipping: Impacts of a Technological Improvement,” *Journal of Economic Issues*, Vol. 34, No. 4, (2000) pp. 933-948.

Talley, Wayne K., “Performance Evaluation of Mixed-Cargo Ports,” a paper prepared for the Department of the Army Corps of Engineers Water Resources Support Center, Alexandria, Virginia, (1996).

United States Coast Guard, 2004. Factfile: Maritime Transportation Security Act of 2002, < www.uscg.mil>, most recent access: Dec 2004.

About the Author(s)

C. Ariel Pinto is an Assistant Professor of Engineering Management and Systems Engineering at Old Dominion University. His works focus on risk management in engineered systems and systems engineering. He has worked at Carnegie Mellon University’s Software Industry Center on software security and quality. He also worked at the Center for Risk Management of Engineering Systems at the University of Virginia on various projects with the US Army Corps of Engineers, Virginia Department of Transportation, and Comdial Corporation. He received his Ph.D. from the University of Virginia and his M.S. and B.S. from the University of the Philippines.

Wayne K. Talley is Professor of Economics at Old Dominion University where he is the Executive Director of the Maritime Institute and holds the designations of Eminent Scholar and the Frederick W. Beazley Professor of Economics. He is an internationally recognized transportation economist. He has held visiting domestic positions at the Woods Hole Oceanographic Institution, U.S. Department of Transportation, the Interstate Commerce Commission and the National Aeronautics and Space Administration and international positions at Oxford University (England), the University of Sydney (Australia), University of Wollongong (Australia), University of Antwerp (Belgium) and City University (England). He is the Editor-in-Chief of Transportation Research E: Logistics and Transportation Review.