12-13-2019

A discrete event simulation-based approach for managing cyber vulnerabilities in a full-service deep waterway port

Hebah Mohammed Mimesh

A discrete event simulation-based approach for managing cyber vulnerabilities in a full-service deep waterway port

By

Hebah Mohammed Mimesh

A Thesis
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Industrial and System Engineering
in the College of Bagley College of Engineering

Mississippi State, Mississippi

December 2019

A discrete event simulation-based approach for managing cyber vulnerabilities in a full-service deep waterway port

By

Hebah Mohammed Mimesh

Approved:

_____

Mohammad Marufuzzaman
(Major Professor)

_____

Junfeng Ma
(Committee Member)

_____

Linkan Bian
(Committee Member / Graduate Coordinator)

_____

Jason M. Keith
Dean
Bagley College of Engineering

Name: Hebah Mohammed Mimesh

Date of Degree: December 13, 2019

Institution: Mississippi State University

Major Field: Industrial and System Engineering

Major Professor: Mohammad Marufuzzaman

Title of Study: A discrete event simulation-based approach for managing cyber vulnerabilities in a full-service deep waterway port

Pages in Study: 32

Candidate for Degree of Master of Science

Deepwater sea ports are considered to be gateways for global trade and susceptible to a diverse range of risks, including natural disasters such as hurricane, storm, drought, as well as a course of events ranging from human error to malicious cyber-attack. To deal with cyber vulnerabilities, this study examines how cyber-attack to a given technology (e.g., Programmable Logic Controllers (PLC), Radio Frequency Identification Tags (RFID), Navigation Technologies, and others) impacts the overall port operations. We use Port of Pascagoula as testbed to visualize and validate the modeling results utilizing FlexSim software. Several sets of experiments are conducted to provide important managerial insights for decision makers. Results indicate that cyber-attack on technologies used by the port may significantly impact the port operations. In overall, cyber-attack has meaningful impacts on ports systems that may result in significant economic and operational loss as well as long-term security and sustainability for overall ports performances.

DEDICATION

First, I give thanks to God for the knowledge and abilities He has blessed me with, which made it possible to complete this thesis. I would like to dedicate this dissertation to my family, especially my parents Mohammed Mimesh and Faiqah Sarhan. They are the driving force behind my education as well as my success. I also dedicate this to my husband Rabeea Bazuhair without whose tireless support and understanding of the late hours and periods of seclusion this degree would not have been completed. I would also like to dedicate this thesis to my sons Eiad and Waheed. May your Father and I be a guiding example to you of what you can achieve, always believe it can be done and never give up!

ACKNOWLEDGEMENTS

The author expresses sincere gratitude to several people for assisting the completion of this dissertation. First and foremost, sincere thanks are due to Dr. Mohammad Marufuzzaman, my advisor and committee chairman, and to my committee: Dr. Junfeng Ma, and Dr. Linkan Bian. The author thanks the Saudi Arabia government for financial support to this process.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Seaports significantly contribute to the overall economy of a nation because they are key components on a nation's transportation system. In the United States and its territories, approximately 3,200 passenger handling facilities are located within 360 commercial ports. Among them, about 150 are deep water seaports, administered by 126 public seaport agencies (Homeland Security, 2016). The primary role of seaports is to facilitate the movement of trade of both foreign and domestic markets. In 2013, more than 1.1 and 1.2 billion short tons of domestic and foreign trade, respectively, moved through United States ports (Homeland Security, 2016). There are more than 80% of the capacity of total goods is handled by ports and carried by sea worldwide (U.S. Department of Transportation, 2015). Convenient, effective transportation ports have the potential to significantly increase economic growth and success of a nation (Sleeper, 2012). The United State spend annually a total of $33 billion due to the delays in several areas, such as vessel technical malfunction, technical faults in port, failure in feeder schedule, or navigational hazards. Several ports not prepared for any attack or risk like cyber-attack. A cyberattack can be consider extremely harmful for a port system because it may cause significant damages and losses. The decisions makers should be aware of these consequences and understand the risk of the cyberattack to limit the impact on the system.

Nowadays, the adaption of technology is increasing rapidly and the critical infrastructures gradually become more reliant on them (Lewis, 2002). As the complexity and size of a network

increases, managing the security of a given critical infrastructure also increases. Among others, The World Economic Forum raised cyber-attacks as the third top global risk in 2018 (Insight Report, 2019). Different types of cyber-attack can occur in a given critical infrastructure and is difficult to detect them in the early stages. Cyber-attacks could be treated unknowingly or have some prompting behind them (Saini et al., 2012). Further, United States government fund more than $15 billion in 2019 for cybersecurity (The white House, 2018). The limitation of cybercrime depends on the appropriate analysis of their conduct and understanding of their effects at different levels of the organization.

Unfortunately, most of the medium to small-sized businesses are not well prepared against a possible cyber-crime. Every enterprise has the risk of system hack, ransomware attack, data breach, or malware, access to the processing power of their network. These risks can include financial losses, theft of cargo or information, and strikes or malfunctions in security, which can lead to the shutdown of a port (Ho and Ho, 2006; Loh and Thai, 2015). Concerns due to cyber risks are increasing since the transportation network is increasingly dependent on the technology in their operation. Moreover, the nation's reliance on global mobility, international supply chains, and overseas markets need consideration of the threats to the vital worldwide transport infrastructure. Several federal department and privet organization contribute to developing security protocols through regulatory bodies and international agreements (U.S. Department of Homeland Security, 2015). The damages from cyber-attack on transportation could be in profit, trademark, competitive position, reputation, and operating efficiency. Cyber security is very important for the maritime industry. According to the Naval Institute Proceedings, the shipping on maritime moves between 90 to 94 percent of world trade (CyberKeel, 2014). The value of goods is approximately $500 billion, or the goods worth more than $1.3 billion per day through

United States ports (Sands, 2004). The maritime transportation system is the most targeted in the world and suffers cyber-attacks recurrently (Belmont, 2015). Recently, the cyber-attack on maritime has been increase due to undetected and unreported attacks (Hayes, 2016). Also, there consequences impact from cyber-attacks on critical infrastructure and operators of the system. In addition, the United States has more than 25,000 miles of inland waterways and there is a delay in the system by 49% (Infrastructure, 2017). Recently, Port of San Diego experiences a cyber-attack on their system. Port of San Diego considers as one of the largest port in the United States. According to San Diego Reader News, the attack costs them approximately $30 million in losses and damages (Senzee, 2019). Another attack in control the cargo movement, between 2011 and 2013, group of attackers' breach information technology (IT) systems that controlled the location and movement of containers at the Port of Antwerp, Belgium. First, attackers send malware to employees in port to gained access to IT system. That access allows them to obtain the containers location and security details so they could change the container location and send drivers to steal the cargo before the legitimate owner arrived (Jones et al., 2016; Bateman, 2014; Homeland security, 2016; Daum, 2019).

According to International Convention for the Safety of Life at Sea (SOLAS), Automatic Identification Systems (AIS) became compulsory for all ship starting 2004. Also, since 2012 under the same chapter, depend on the vessel type, they are required the vessels to provide information system and electronic chart display for navigation charts instead of the paper-based system as adopted earlier (Daum, 2019). Therefore, nowadays, most of the maritime system depend on Global Positioning System (GPS) and that create many vulnerabilities into the system. By using GPS, the system could have spoofed (send a false information) or jammed (lost the GPS signals) and if the GPS signals are blocked that will affect the other technologies such as

AIS, Voyage Data Recorder (VDR), Electronic Chart Display and Information (ECDIS), Vessel traffic services (VTS). One of the most prominent example of cyber-attack in maritime is the A.P. Moller-Maersk in 2017. Cyber-attack affected the systems caused disruption in loading and unloading of containers because of the impossibility to correctly identify the shipments that caused acute delays in the shipment in numerous ports, including Jawaharlal Nehru Port, Port of Rotterdam, and terminals in the United States with losses and damages of approximately $300 million (Moerel and Dezeure, 2017; Daum, 2019). Further, cyber-attack on the maritime sector causes a lot of damages and losses because of the ignorance about the possible vulnerabilities in a given port system. Till now, numerous researches attempted to detect a cyber-event in a given system. In the domain of a maritime sector, there are several anomaly detection approaches currently available in the literature, such as signature-based anomaly detection (Roy, 2008), Norm-based anomaly detection (Riveiro et al., 2008), GEMASS (Genetic algorithm knowledge discovery for Maritime Security System) (Chen et al., 2014), and many others. Such detection mechanisms can detect threat on real-time and can alert the vessels. Further, Signature-based NIDS (Network Intrusion Detection System) technologies detect cyber-attack by realizing exact patterns in system data steams (Chiappetta and Cuozzo, 2017). According to BIMCO (2017), to detect cyber-attack on the system, the industry should update techniques for reporting non-conformities, hazardous, and accidents conditions that relating to a cyber-event. Then, if a cyber-attack occurs in the system, automatically protective measure should repulse the cyber-attack effectively (Daum, 2019). Also, BIMCO (2017) provides some other solution if the system has a cyber-attack, such as check for the shore-based support and adequate resources are obtainable to help the DPA in answer to the critical system loss and update the processing of the implementing remedial activity to prevent recurrence that include cyber events. Recently, there are diversity of

cyber-attack on maritime infrastructures and vessels. Most of the cyber-attacks occur publicly; however, the information and details related to a cyber-attack are very limited. Botnet malware could provide the attacker some of the systems commends that could use with other system and with manufacturing cyber-event the attacker would control disruption or destruction of the equipment (Fischer, 2014). Maritime sector still has lack in the necessary incentives to improve their overall cyber security posture (Cimpean et al., 2011). Similar to other modes, maritime business experiences threats because of the dependence on technology associated with the vessel navigation needs. The vulnerability contains losing the vessel control or cargo that could lead to profit loss or consequences resulting from its use in acts of terrorism (Caponi and Belmont, 2014).

Deepwater seaport connected heavily with inland waterways ports, are increasingly becoming the cynosure of attention of the cyber-related attacks. Deepwater seaports are usually used for heavily and large loaded ships because the water depth helps the ship to enter the waterway. Further, deep water seaports are equipped with different equipments such as pipelines and pumping stations, cargo, service platforms, and berth buoys to help loading and unloading commodities faster. Essentially, ports play an important role in the economies of a country and their effectiveness can lead to significant economic benefits or failures (Dwarakish and Salim, 2015). Some of the failures could happen from cyber-related attacks. These potential attacks may attempt to get unauthorized access to a computer system in order to compromise its data, information and resources, install malicious viruses or codes to harm the computer security system, and/or infect the system in such a way that resources become unavailable to provide any kind of services (Ahokas and Kiiski, 2017). Attackers may potentially hack different navigation vessels systems such as AIS, ECDIS, or GPS to change or control the vessels route for attack by

smugglers or pirates (Barnes, 2018; Homeland security, 2016). A prior study shows that ECDIS was not been designed securely, for example, accepting dangerous network methods, and that systems on these ships are often outdated and therefore lacking in some security patches (Jones et al., 2016). Security researchers also found ways to abuse the AIS, such as generating valid commands, changing ship courses, replaying commands, and tracking ships for potential physical attacks (Balduzzi et al., 2013). Researchers at the University of Texas at Austin (2013) managed to exploit the lack of authentication of satellite GPS signals, and successfully divert the course of a $80 million yacht with a GPS spoofing device. As the GPS receivers of the vessel did not authenticate incoming signals, it was possible to slowly overpower the authentic ones, and eventually gain control of the vessel's navigational system without being detected or raising any alarms (Jones et al., 2016). Few deepwater seaport cyber vulnerabilities include: limited cybersecurity training and preparedness, errors in software, inadequately protected commercial off-the-shift technologies and legacy systems, network connectivity and interdependencies, software similarities, foreign dependencies, GPS jamming or spoofing, and insider threats (Homeland security, 2016).

Most of the prior studies focused on identifying the vulnerabilities of a system and some recommendations of the appropriate way to protect the system from a cyber-attack. However, there is lack of information about the impact of cyber-attack in a deepwater seaport. To fill this gap in the literature, this study provides a simulation model to show the impact of cyber-attack on a deepwater seaport. The impact of a critical infrastructure depends on which deep water seaport are disrupted. The results or consequences of cyberattacks can be difficult to define, precisely because the damage can be greater than expected or known (Sanger et al., 2014). Cyber-attackers usually target port operators inside the port area because operators tend to have

fewer security controls than the port itself and are therefore easier to attack (Shackleford, 2015). Thus, this study covers both sea area and inland operation to visualize better understanding of the impact of cyber event.

In summary, this study examines how a cyber-attack to a given technology (e.g., PLC, RFID, OCR, GPS, AIS, and others) impacts the overall port operations. We use Port of Pascagoula as a testbed to visualize and validate the modeling results. Several set of experiments are conducted to provide important managerial insights for the decision makers, including cyber vulnerabilities on PLC, RFID OCR, GPS, and AIS which significantly impact the ship and barge waiting time, loading and unloading time at the terminals and the overall delay in the system.

This thesis is organized as follows. Section 2 described the problem and introduces the modeling issues considered to simulate the case port operations. Section 3 presents the experimental results. Finally, Section 4 concludes with a summary of the research conducted in this study and a set of future research directions.

CHAPTER II

AN ILLUSTRATIVE CASE STUDY FOR MODEL VALIDATION

This study introduces a discrete event simulation model capable of detecting the realistic physical dynamics in a complex system. This model is utilized to estimate and provide better understanding of the extensive impact of cyber-attack on deep water seaport system. We utilize Port of Pascagoula as a testbed to visualize and validate our simulation model results. This port is located on the southeastern coast of Mississippi. The port is important due to proximity to the Gulf of Mexico, where a large carrier of shipping and exporters are performed. The port has 12-14 miles' sea channel with a depth of 42 feet of mean water level. Further, it is the largest port in Mississippi and ranks the top 20 ports nationally with respect to the volume of foreign cargo that it carries. Port of Pascagoula is classified as a *full service deep water seaport* that handles cargo from worldwide. The port has two harbors with private and public terminals. Chevron utilizes the largest private terminal for processing, handling, and exporting chemicals. Additionally, this port annually handles approximately 32 million tons of cargo and is capable of professionally handling a wide variety of materials due to the availability of manpower, facilities, and technologies that belongs to this port. Port of Pascagoula serve both barges and ships in harbors. The right side of the harbor is utilized for handling oil with pipelines and tanks while the left side includes pallet (cargo) with crane and yard to move and store pallet as shown in **Figure 2.1**. The port has a narrow channel with 350` in width; thus, only one vessel can enter into the channel at a time as illustrated in **Figure 2.2**) (Jackson County Port Authority).

Figure 2.1 Loading and unloading zone in the Port of Pascagoula (Available from: www.portofpascagoula.com)

Figure 2.2 Visualizing the channels in Port of Pascagoula (Available from: www.portofpascagoula.com)

2.1 Simulation Model

A simulation model of the port of Pascagoula is developed using FlexSim software. The business hours of the port in the simulated model is Monday through Friday from 8 AM to 5 PM. **Figure 2.3** shows the operation flow of the port of Pascagoula system. Operation and processing are classified into three major activities: 1) sea area, 2) yard operations, and 3) gate operations as illustrated in **Figure 2.3a**, **2.3b**, and **2.3c**, respectively. Both the sea area and yard operations (**Figure 2.3a** and **2.3b**) are simulated in this study; however, gate operations (**Figure 2.3c**) are not included in this study, and it is utilized in **Figure 2.3** to show the overall operation and processing of the port of Pascagoula. After a vessel arrives in a berth, it has two sides to go through. The first side is for vessels (barge) loaded with pallet while the other side is for vessels (ship) loaded with oil. The operation processes for the barges loaded with pallets are: crane operation, cargo loading, and yard empty, respectively (**Figure 2.3b**). For ships loaded with oil, the operation processes are: pier, hose pipeline, tank, discharge, and fuel loading, respectively (**Figure 2.3b**). Note that the numbers shown in **Figure 2.3** represent technologies used for different port operations and are elaborated in details in **Table 2.1**. The main focus on this study is to simulate and illustrate the impact of a cyber-attack on the port operation. Variety of scenarios regarding cyber-attack that may potentially affect these infrastructures and operations (e.g., pipelines, crane, berth, and many others) are described later.

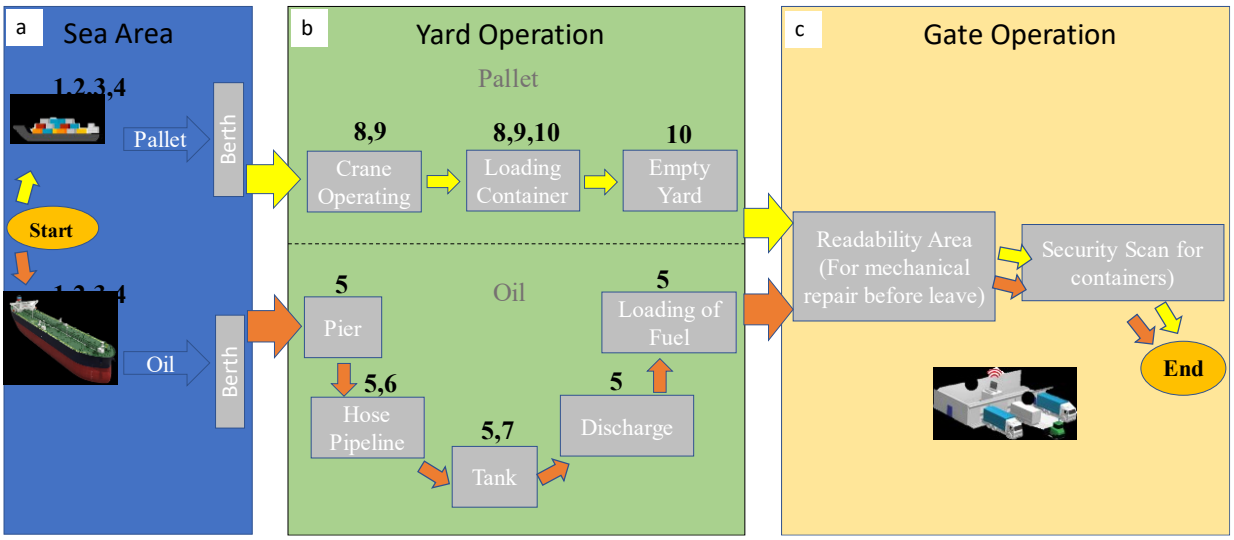
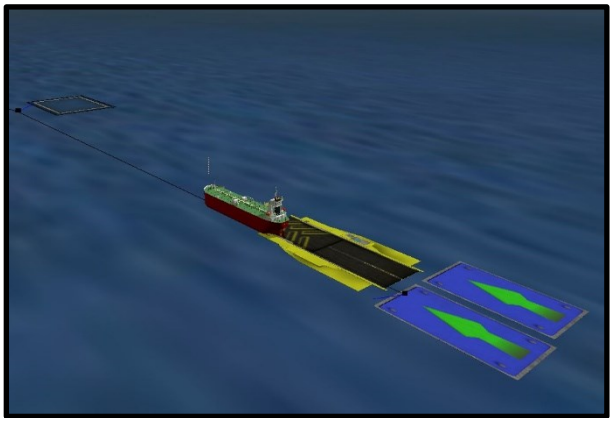


Figure 2.3 Operation flow of the Port of Pascagoula

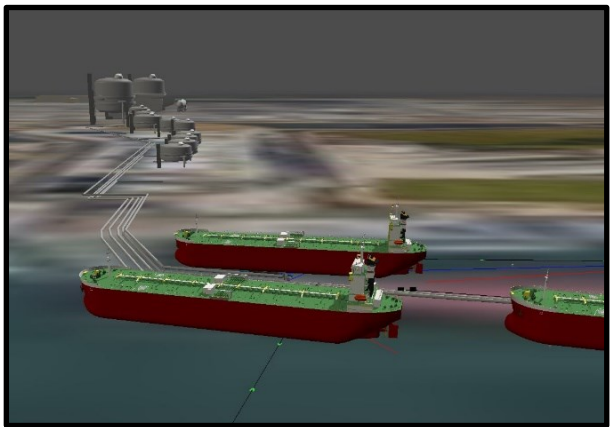
2.1.1 Ship and pipeline processing

In the simulation model, berth can handle up to seven ships at the same time. Ships only handle oils in this port and enter randomly into the system in every 4.5 to 5.5 hours. The length of a ship is 500 feet and can handle up to 113,800 barrels (18,090 m^3) of oil. Each ship generally requires approximately 2 hours to reach to the berth area from the initial waiting area (shown in **Figure 2.4a**), while it takes two to five days for each ship to perform all unloading operations (**Figure 2.4b**). Note that turning maneuver with the channel is difficult; therefore, it is not possible for two ships to move within the channel at the same time due to the narrow channel as shown in **Figure 2.2**. Arrival of the vessels (both ships and barges) to the berth usually requires the vessels to utilize the following technologies: Global Positioning System (GPS), Automated Identification System (AIS), and Electronic Chart Display and Information ECDIS as discussed in details in **Table 2.1**. GPS usually controls the other two technologies (i.e., AIS and ECDIS). These technologies allow the ship to send and receive information regarding location, speed, destination, and unloaded time on berth. When ship arrive to berth (**Figure 2.4**), radios,

Programmable logic Controllers (PLC), and Remote Terminal Units (RTU) technologies, as discussed in **Table 2.1**, are utilized to unload oil form ships through pipelines to the tanks. After completing the unloading operations, the ship exits the port utilizing again the GPS, AIS, and ECDIS technologies. It shall be noted that the technologies descried in **Table 2.1** are very common technologies utilized in different port operations and the most candidate to be cyber-attacked.



(a) Ships waiting area prior to departure for leading operations



(**b)** Loading operations of the ships

Figure 2.4 Simulated waiting area and loading operations for the ships at the Port of Pascagoula

Table 2.2 Technologies utilized in the Port of Pascagoula.

ID[1]	Category	Technology	Purpose
1	Vessel	Automated Identification System (AIS)	Identify ship as they come into the port.
2		Global Positioning System (GPS)	Provides geolocation and time information.
3		Radar	Determine the range, angle, or velocity of objects
4		Electronic Chart Display and Information (ECDIS)	Integrate position information from position, heading, and speed.
5	Fluid	Radios	Pump gasoline from ship to the fuel manifold.
6		Programmable logic Controllers (PLC)	Control pipeline meters and pumps.
7		Remote Terminal Units (RTU)	Monitor tank gauges and detect leaks.
8	Cargo	Optical Character Recognition (OCR)	Identify cargo.
9		Radio Frequency Identification Tags (RFID)	Identify cargo.
10		Terminal Operating Systems (TOS)	Help orchestrate the location and movement of cargo from ship, to yard, to truck.

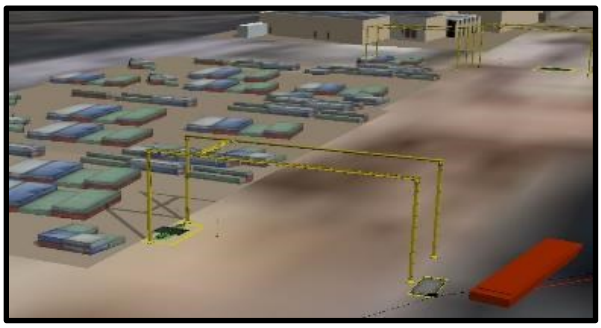
[1]The IDs use for clarification in **Figure 2.3**.

2.1.2 Barge and crane processing

The simulation modeling can handle up to four barges at the same time. A barge always transferring pallet and enters the system randomly on every 2.5 to 3.5 hours. The usual size of the barge is 195 feet without any compartment facility. The average capacity for barge 1,500 tons. Each barge requires 8 to 10 hours for unloading depending on the type of commodities carried by the barges. Our simulation model includes four cranes to load/unload pallets from barges to yards as shown in **Figure 2.5**. Like ships, barges also utilize the same technologies (GPS, AIS, and ECDIS) to arrive at the berthing places from the initial waiting areas as shown in **Figure 2.2**. Once a barge arrives to a berth, cranes are used to load/unload the pallets from a

barge to a yard by using the following technologies: Optical Character Recognition (OCR), Radio Frequency Identification Tags (RFID), and Terminal Operating Systems (TOS) as described in **Table 2.1**. Then, OCR and RFID identify the destination containers of the pallets. TOS technology receives information from the OCR and RFID regarding the pallet location and then provides updated information, regarding pallet movement from ship to yard and then to truck. After the unloading operations are performed, the barges exit into the system by utilizing the similar technologies as described for the ships (i.e., GPS, AIS, and ECDIS).

(a) Real port crane operation (Available from: www.portofpascagoula.com)



(b) Simulated crane operation

Figure 2.5 Real and simulated crane operations for the Port of Pascagoula

CHAPTER III

EXPERIMENTAL AND RESULTS

This section discusses four sets of experiments to illustrate the impact of cyber-attack on a full-service deep waterway port. By assuming that a cyber-attack may occur in any specific type of technology, four different experiments are conducted, namely, cyber vulnerabilities on Programmable Logic Controllers (PLC), cyber vulnerabilities on Radio Frequency Identification Tags (RFID) and Optical Character Recognition (OCR), and cyber vulnerabilities on navigation technologies (e.g., Global Positioning System (GPS), Automated Identification System (AIS)) for ships and barges. The following measures are used to assess the performance of these experiments: total number of vessels (i.e., ships or barges) (i) waiting time, (ii) ideal time, (iii) processing time, and (iv) fluid level on the reservoirs (i.e., tank level). There is a total of 15 replications simulated for each experiment and for a period of three weeks.

3.1 Experiment 1: Cyber Vulnerabilities on Programmable Logic Controllers (PLC)

The first set of experiments illustrate the impact of cyber vulnerabilities on PLC over the entire port operations. Essentially, pipelines are utilized to transfer fluid from ships to tanks, and PLC controls these pipelines (i.e., controlling pipeline meters and pumps). As described earlier, the simulation model can handle up to seven ships in berth, and each ship usually takes 2-5 days to unload. Cyber-attack on PLC usually affects the process of transferring the oil from ships to tanks. The performance measures in this experiment are: waiting time for ships to enter the channel and the total number of ships exiting the simulation model. Four scenarios are created,

namely, delay of 1 day, 2 days, 4 days, and 6 days on the oil transferring process, respectively, to assess the impact of cyber vulnerabilities on PLC.

Table 3.1 summarizes the results from this set of experiment. **Figure 3.1** represents the difference between normal scenario with the other scenarios (e.g., 1 day, 2 days, 4 days, and 6 days) with respect to waiting time for ships and total number of ships exiting the system with statistical analysis. A *t*-groping test was conducted on these scenarios to show if there is any statistically significant difference at 95% confidence that shown in **Table 3.2**. For illustration, each scenario has different letter means that they are statistically significant different (i.e., waiting time of ships for scenario of 1 day and 2 day that assigned to letters "A" and "B", respectively). If two scenarios assigned to the same letter, that means they are statistically similar (i.e., waiting time of ships of normal and 1 day scenarios assigned to letter "A").

Table 3.1 Test results of cyber vulnerabilities on PLC Experiment

Scenario	**Waiting Time of Ship (hr)**	**Throughput (No. of Ships)**
Normal	0	29
1 Day	0	23
2 Days	13	20
4 Days	46	17
6 Days	57	14

Results indicate that the cyber-attack on PLC may not significantly impact the waiting time of ships in the port on the very first day, even though there would be a significant decrease in the total number of ships exiting the system by approximately 19%. Results further indicate that for a delay of 2 days due to cyber-attack on the PLC, ship waiting time significantly increases by 13 hours while exits of ships into the system is dropped by 39%. For a delay of 4

and 6 days, there is significant increase in the ship waiting time by approximately 46 and 57 hours, respectively while the total number of ships decreases by 42% and 52%, respectively. Finally, results in **Figure 3.1** illustrate that the cyber-attack on PLC resulted a 6 days delay can reduce the performance of the port by approximate 50% and increase the waiting time of ships in the ports for 7 business days.

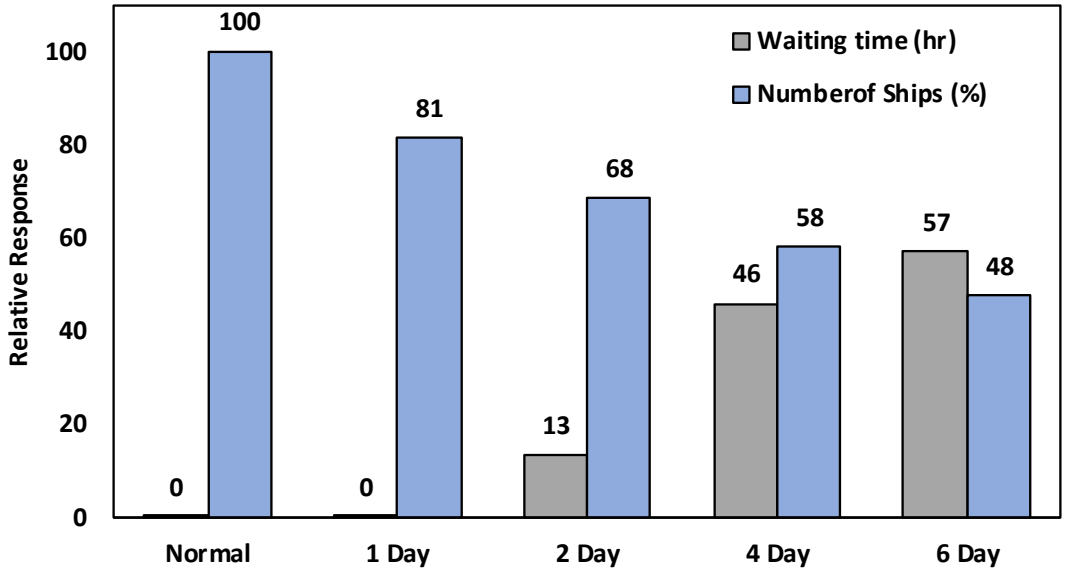


Figure 3.1 Scenario comparison of cyber vulnerabilities on PLC

Table 3.2 *t*-groping statistical analysis of cyber vulnerabilities on PLC

Scenario	Waiting Time of Ship (hr)	*t*-test	Throughput (No. of Ships)	*t*-test
Normal	0	A	29	A
1 Day	0	A	23	B
2 Days	13	B	20	C
4 Days	46	C	17	D
6 Days	57	D	14	E

3.2 Experiment 2: Cyber Vulnerabilities on Radio Frequency Identification Tags (RFID) and Optical Character Recognition (OCR)

The next set of experiments illustrate the effect of cyber vulnerabilities on both of RFID and OCR and their consequences to a given port. More specifically, this experiment focuses on cyber-attack that effect pallets harbor. In the simulation model, four cranes are used to transfer the pallets from barges to the yard. RFID and OCR technologies are usually used to manage cranes activities while transferring and identifying pallets. Six scenarios are simulated in this experiment to see the impact resulted from delays of the cranes process for up to 16 hours (2 business days). The performance measures utilized in this experiment are: waiting time to identify pallets and move them to the right location in yard and the total number of pallets processed.

The results from this experiment are shown in **Table 3.3**. **Figure 3.2** represents the difference between normal scenario with the scenarios (e.g., 0.5 hr, 1 hr, 2 hrs, 4 hrs, 8 hrs and 16 hrs) with respect to waiting time of pallets and the total number of pallets processed in the system. **Table 3.4** summarizes a *t*-grouping test that is conducted on these scenarios to show if there is statistically significant difference at 95% confidence similar to the previous experiment.

Table 3.3 Test results of cyber vulnerabilities on RFID and OCR

Scenario	Waiting Time of Pallets (hr)	Throughput (No of pallets)
Normal	4	179
0.5 hr	22	173
1 hr	116	104
2 hr	180	58
4 hr	216	30
8 hr	249	15
16 hr	255	8

Results indicate that if cyber-attack is taken place into the system that results in delay the cranes processes for 0.5 hours, the waiting time of pallets will significantly increase 18 hours and number of pallets significantly decrease by 4%. For scenario of 1 hour delay of cranes processing, the waiting time of pallets will significantly increase 111 hours (approximately 14 business days) and number of pallets significantly decrease by 42% (almost half of the number of pallets). For cyber-attack that results in delay the cranes processes for 2 hours, the waiting time of pallets significantly increase to 176 hours (22 business days) and the total number of pallets processing are dropped by 68%. Further, for a scenario of 4 hours delay of cranes processing, the waiting time of pallets significantly increases to 212 hours (26 business days) while the number of pallets processed by the crane significantly decrease by 83%. Delays in cranes processing of 8 hours (one day of work) would result in significant increase of waiting time of pallets by 244 hours (30 business days) and significant drops the pallets handling quantity by 92%. In case where cyber-attack results in delay the cranes processing for 16 hours (2 business days), the pallets waiting time significantly increases to 251 hours (31 business days) and the total number of pallets processed by the crane dropped by 96%. The impact of cyber-attack on RFID and OCR for two business days would results in increasing waiting time of pallets to 31 business days and decreases the processing of pallets by 96%.

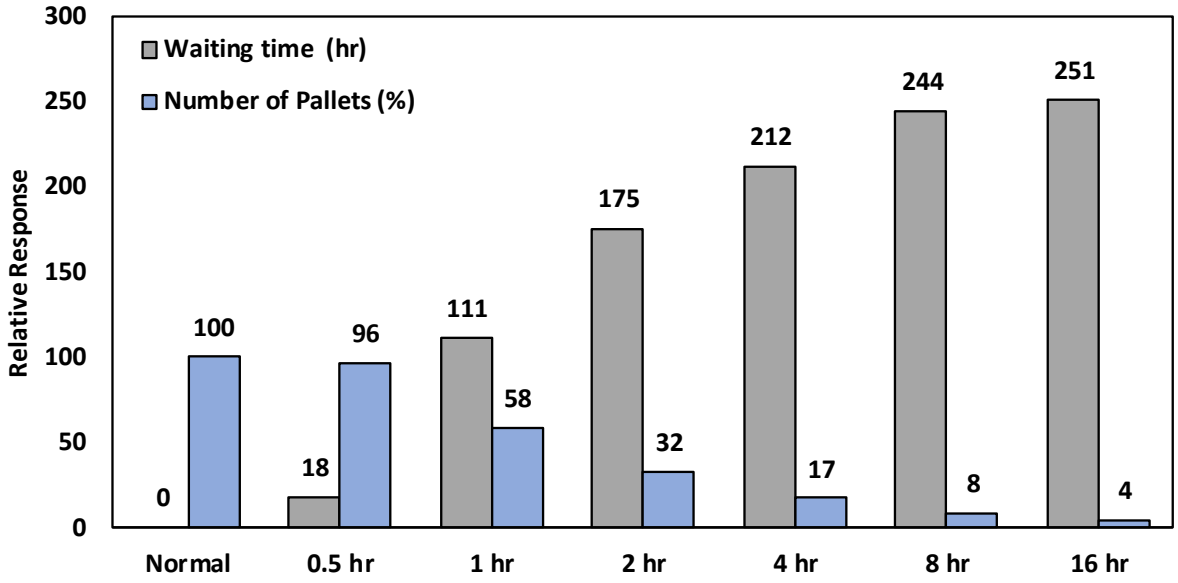


Figure 3.2 Comparison of scenarios of cyber vulnerabilities on RFID and OCR

Table 3.4 *t*-groping statistical analysis of cyber vulnerabilities on RFID and OCR

Scenario	Waiting Time of Pallet (hr)	*t*-test	Throughput (No of pallet)	*t*-test
Normal	4	A	179	A
0.5 hr	22	B	173	B
1 hr	116	C	104	C
2 hr	180	D	58	D
4 hr	216	E	30	E
8 hr	249	F	15	F
16 hr	255	G	8	G

3.3 Experiment 3: Cyber Vulnerabilities on Navigation Technologies for Ships

This set of experiments illustrate the impact of cyber-attack on navigation technologies (i.e. GPS, AIS, and ECDIS technologies) that utilized to identify vessels location and directions. The experiment focuses in cyber-attack on navigation technologies that impacts the fluid side of berth. There is a total of seven berths for vessels that located in two sides. The first one (berth A)

includes four berths with up to nine tanks and the other one (berth B) includes three berths with six tanks as shown in **Figure 3.3**. GPS, AIS, or ECDIS technologies manage ships entrance to channels until arriving to berth. Thus, cyber-attacks on navigation technologies would affect the number of ships coming to ports. To simulate this impact, four scenarios are conducted in this experiment as following: one of the seven berths does not receive any ship, two of the seven berths do not receive any ship, berth B side that includes three berths do not receive any ship, and berth A that includes four berths do not receive any ship. Performance measures in this experiment are: waiting time for ships to enter the channel, number of ships exiting the system, processing time, idle time, and tanks status.

Figure 3.3 Simulated fluid side berthing for the Port of Pascagoula

Table 3.5 summarizes the test results of this experiment. For clarification, normal scenario represents the normal condition of the port where all 7 berths functions, and 6 berths scenario represents the case that one of the seven berths does not work and the like. **Figures 3.4** and **3.5** represent the difference between normal scenario with the other scenarios (e.g. 6 berths,

5 berths, 4 berths, and 3 berths) with respect to waiting time of ships, total number of ships, processing time, idle time, and tanks status. Statistical *t*-grouping analysis is conducted to identify if there is a statistical difference between scenarios as shown in **Table 3.6** (described in section 3.1).

Table 3.5 Test results of cyber vulnerabilities on navigation technologies for ships

Scenario	Waiting Time of Ship (hr)	Throughput (No. of Ship)	Processing (Min)	Idle (Min)	Tanks (Empty)
Normal	0	23	20	7.0	83
6 berths	6	22	20	3.6	87
5 berths	32	19	17	2.1	88
4 berths	64	16	14	1.4	83
3 berths	100	12	11	0.8	96

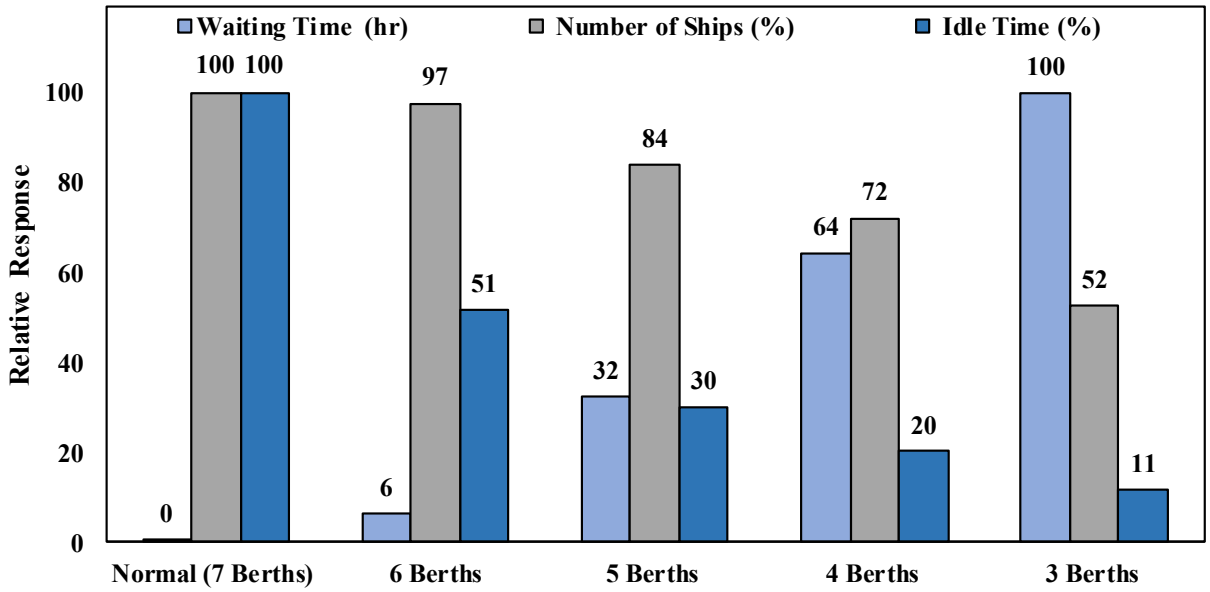


Figure 3.4 Comparison of waiting time of ships, number of ships, and idle time.

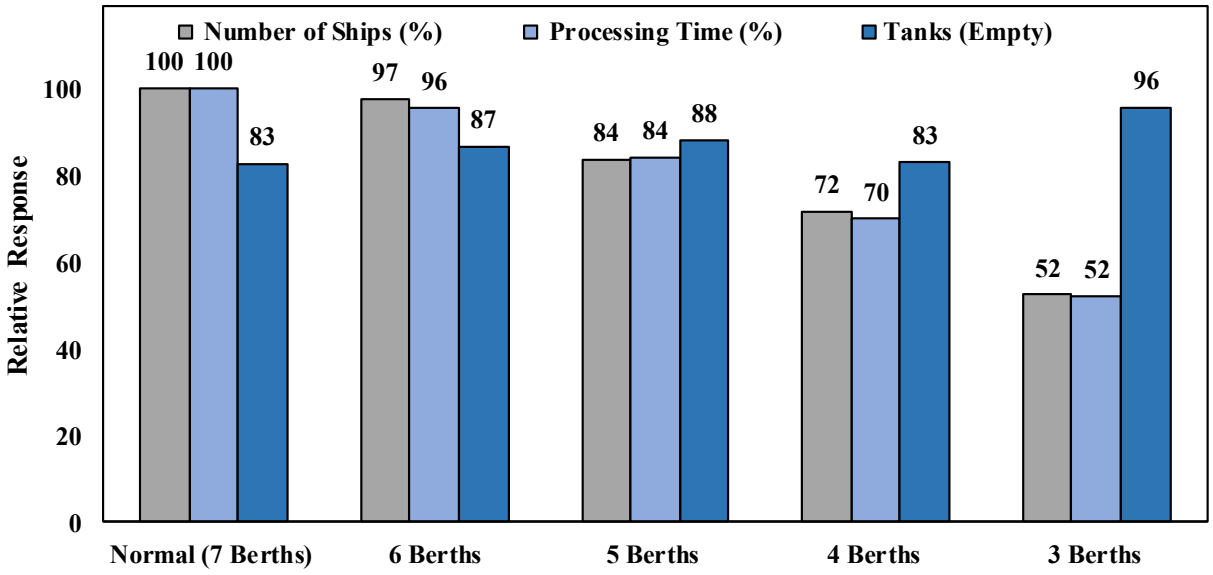


Figure 3.5 Comparison of number of ships, processing time, and tanks status.

Table 3.6 *t*-groping analysis of cyber vulnerabilities on navigation technologies for ships

Scenario	Waiting Time of Ship (hr)	*t*-test	Throughput (No. of Ship)	*t*-test	Processing (Min)	*t*-test	Idle (Min)	*t*-test	Tanks (Empty)	*t*-test
Normal	0	A	23	A	20	A	7.0	A	83	A
6 berths	6	B	22	B	20	B	3.6	B	87	B
5 berths	32	C	19	C	17	C	2.1	C	88	C
4 berths	64	D	16	D	14	D	1.4	D	83	A
3 berths	100	E	12	E	11	E	0.8	E	96	D

In **Figure 3.4**, the waiting time of ships significantly increase from normal scenario to 6 berths, 5 berths, 4 berths, and 3 berths by 6, 32, 64, and 100 hours, respectively. This shows that the cyber-attack on navigation technologies would results in delay the ships for approximately 1 to 13 business days. Results indicate that the total number of ships reduced significantly for each scenario with respect to the base/normal scenario, such as 6 berths scenario reduced 3%, 5 berths scenario reduced 16%, 4 berths scenario reduced 28%, and 3 berths scenario reduced 48%. Total

number of ships decreases up to around 50%. Further, the idle time reduced for each scenario with respect to the normal scenario. For 6, 5, 4, and 3 berths scenarios, the idle time reduced by 49, 70, 88, and 89%, respectively. Note that the idle time is reduced significantly even in the case of 6 berths (reduced 49%).

Figure 3.5 shows performance measures of total number of ships in the system, processing time, and tanks status. The total number of ships are described in the previous paragraph but included in **Figure 3.5** for clarification with processing time and tanks status. Processing time of berths decrease significantly for each scenario with respect to the normal scenario. This is expected as the total number of ships also significantly decreased. The processing time reduced by 4 ,16, 30, and 48% for 6, 5, 4, and 3 berths, respectively. The tanks status increased for all scenarios with respect to the normal, except the scenario of 4 berths that has similar value as the normal case. This is because the simulation model includes a total of seven berths for vessels that located in two sides, the first one (berth A) includes four berths with nine tanks and the other one (berth B) includes three berths with six tanks as shown in **Figure 3.3**. The difference in tanks number between berth A and B led to the tank status of the scenario of 4 berths value to be similar to the normal scenario. In overall, cyber-attack on navigation technologies for ships can affect the ports operations significantly with respect to delaying the port operations and processing time and the number of ships handled by the port.

3.4 Experiment 4: Cyber Vulnerabilities on Navigation Technologies for Barges

This experiment shows the impacts of cyber-attack on navigation technologies (i.e. GPS, AIS, and ECDIS technologies) that are utilized to identify vessels location and directions. Basically, it similar to the experiment of cyber-attack on navigation technologies for ships; however, the experiment focuses in cyber-attack on navigation technologies that impacts the

pallet side of berth which includes a total of four berths for barges. Navigation technologies manage barges entrance to channels until arriving to berth. Thus, cyber-attack on navigation technologies would affect the number of vessels coming to ports. To simulate this impact, two scenarios are conducted in this experiment as following: one of the four berths does not receive any barge, and two of the four berths do not receive any barge. Performance measures in this experiment are: waiting time for barges to enter the channel, number of barges exiting the system, processing time, and idle time.

Table 3.7 summarizes the test results from this experiment. For clarification, normal scenario represents the normal condition of the port where 4 berths work, and 3 berths scenario represents the case that one of the four berths does not receive any barge, and 2 berths scenario represents the case that two of the four berths do not receive any barge. **Figure 3.6** represents the difference between normal scenario with the other scenarios (e.g. 3 berths, and 2 berths) with respect to waiting time of barges and total number of barges, processing time, and idle time. **Table 3.8** provides statistical *t*-groping analysis to identify if there is a statistical difference between scenarios (described in section 3.1).

Table 3.7 Test results of cyber vulnerabilities on navigation technologies for barges

Scenario	Waiting Time of Barges (hr)	Throughput (No. of barge)	Processing (Min)	Idle (Min)
Normal	0	44	20	8
3 Berths	26	39	18	4
2 Berths	85	26	12	2

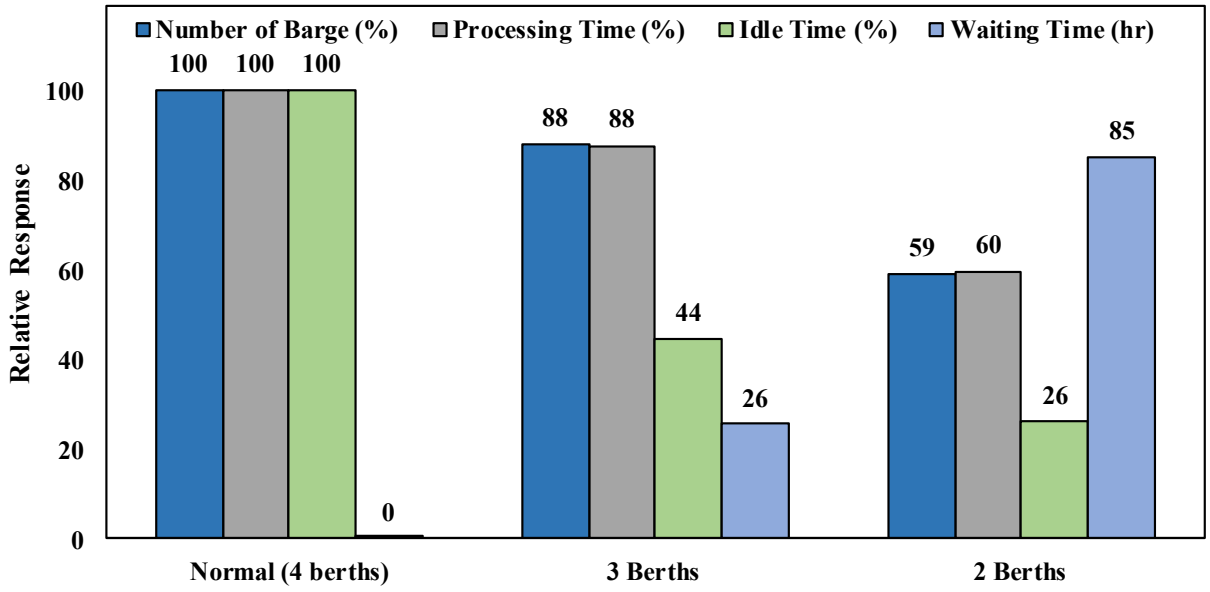


Figure 3.6 Comparison of scenarios of cyber vulnerabilities on navigation technologies for barge

Table 3.8 *t*-groping analysis of cyber vulnerabilities on navigation technologies for barge

Scenario	Waiting Time of Barges (hr)	*t*-test	Throughput (No. of barge)	t-test	Processing (Min)	*t*-test	Idle (Min)	*t*-test
Normal	0	A	44	A	20	A	8	A
3 Berths	26	B	39	B	18	B	4	B
2 Berths	85	C	26	C	12	C	2	C

Figure 3.6 clearly demonstrates that such attack can significantly drop the total number of barges handled by the port over the base case scenario, such as 3 berths scenario reduced 12%, and 2 berths scenario reduced 41%. In overall, the total number of barges handled by the port decreases by almost the half. Processing time of berths decreases significantly for each scenario with respect to the base scenario. This is expected as the total number of barges also decreased significantly. For instance, the processing time of barges is reduced by 12% and 40% for 3 berths and 2 berths scenarios, respectively over the base case scenario. Further, the idle time reduced

for each scenario with respect to the normal scenario. For 3 and 2 berths scenarios, the idle time is reduced by 56, and 74%, respectively. The idle time is reduced meaningfully even in the case of 3 berths (reduced 56%). The waiting time of barges significantly increases from normal scenario to 3 berths and 2 berths by 26 and 85 hours, respectively. In overall, the results show that the cyber-attack on navigation technologies for barges would result in delay the barges by approximately 1 to 11 business days.

CHAPTER IV

CONCLUSION AND FUTURE WORK

A full-service deep waterway port, even though carefully designed, is vulnerable to cyber-attack. This study examines how a cyber-attack to a given technology (e.g., PLC, RFID, OCR, GPS, AIS, and others) impacts the overall port operations. The author uses Port of Pascagoula as a testbed to visualize and validate the modeling results. Several sets of experiments are conducted to provide important managerial insights for the decision makers.

cyber vulnerabilities on PLC, RFID OCR, GPS, and AIS which significantly impact the ship and barge waiting time, loading and unloading time at the terminals and the overall delay in the system. Some key findings obtained from this study are summarized below:

- Cyber-attack on PLC, if not recovered up to 6 days, can reduce the overall system performance of the port by approximately 50% and increase the waiting time of ships in the ports for around 7 business days.
- The impact of cyber- attack on RFID and OCR, if not recovered up to two business days, would result in increasing waiting time of pallets to 31 business days and decreases the processing of pallets up to 4%.
- Cyber-attack on navigation technologies (i.e., GPS, AIS, and ECDIS technologies) for ships can affect the ports significantly resulting in delays of ships for up to 13 business days reducing the total number of ships handled by the

port approximately 50% and increases the idle time and processing time by approximately 89%, and 48%, respectively.

- Cyber-attack on navigation technologies (i.e., GPS, AIS, and ECDIS technologies) for barges would results delays for barges approximately for 11 business days, drops the total number of barges handled by the ports by 40%, and increases the idle time by approximately 74%.
- Cyber-attack has meaningful impacts on ports systems that resulted in reducing the overall ports performance.

This study can be extended in several research directions. First, our study ignores the interconnections of the reference ports with their sources/destinations. This is important since the cyber-attack will not only impact the base port but also to all of its connecting ports. Further, appropriate economic and risk models need to be incorporated with this simulation model to capture a realistic financial loss that a port experiences due to a cyber-attack. These issues will be addressed in future studies.

REFERENCES

Ahokas, J., and Kiiski, T. (2017). Cybersecurity in ports. *Publication of the HAZARD Project, 3*.

Balduzzi, M., Wihoit, K., and Pasta, A. (2013). Hey Captain, Where's Your Ship? Attacking Vessel Tracking Systems for Fun and Profit. *Hack in the Box (HITB) Security Conference in Asia*.

Barnes, B., Marla, L., Salo, G., Sandone, R.,Weaver, G. (2018) Assessment and Measurement of port Disruption. *Critical Infrastructure Resilience Institute*, *Department of Homeland Security Center of Excellence*.

Bateman, T. (2013). Police warning after drug traffickers' cyber-attack. *BBC News.*

Belmont, K. B. (2015). Maritime Cyber Attacks: Changing Tides. *Maritime Executive, November, 16.*

BIMCO, C., ICS, I., and Intertanko, O. C. I. M. F. (2017). IUMI, "Guidelines on cyber security onboard ships," *BIMCO*.

Caponi, S. L., and Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. *Intellectual Property & Technology Law Journal, 27*(1), 16.

Chen, C. H., Khoo, L. P., Chong, Y. T., and Yin, X. F. (2014). Knowledge discovery using genetic algorithm for maritime situational awareness. *Expert Systems with Applications, 41*(6), 2742-2753.

Chiappetta, A., and Cuozzo, G. (2017). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. *In 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)* (pp. 206-211). IEEE.

Cimpean, D., Meire, J., Bouckaert, V., Vande Casteele, S., Pelle, A., and Hellebooge, L. (2011). Analysis of cyber security aspects in the maritime sector.

CyberKeel, (2014). Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas.

Daum, O. (2019). Cyber Security in The Maritime Sector. *Journal of Maritime Law & Commerce, 50*(1).

Dwarakish, G. S., and Salim, A. M. (2015). Review on the Role of Ports in the Development of a Nation. *Aquatic Procedia, 4*, 295-301.

Fischer, E. A. (2014). Cybersecurity issues and challenges: In brief. *Congressional Research Service.*

Hayes, C. R. (2016). *Maritime cybersecurity: the future of national security*, Doctoral dissertation, Monterey, California: Naval Postgraduate School.

Ho, M. W., and Ho, K. H. D. (2006). Risk management in large physical infrastructure investments: The context of seaport infrastructure development and investment. *Maritime economics & logistics*, 8(2), 140-168.

Homeland Security. (2016). Consequences to Seaport Operations from Malicious Cyber Activity. *Operational Analysis Division. National Protection and Programs Directorate.*

Homeland security. (2015). Transportation System Sector-Specific Plan". *United State Department of Transportation*.

Infrastructure Project Card O. A. S. (2017). A Comprehensive Assessment of America's Infrastructure. *American Association of Civil Engineering*.

Jackson County Port Authority (2019). Port of Pascagoula. https://www.portofpascagoula.com/.

Jones, K., Tam, K., and Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. *IET Engineering & Technology Reference*

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies.

Loh, H. S., and Thai, V. V. (2015). Management of disruptions by seaports: preliminary findings. *Asia Pacific Journal of Marketing and Logistics, 27*(1), 146-162.

Moerel, L., Dezeure, F. (2017). Cyber Security in Ports. *The Vlaams Nederlandse Delta (VNDELTA).*

Polatidis, N., Pavlidis, M., and Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces, 56*, 74-82.

Riveiro, M., Falkman, G., and Ziemke, T. (2008). Visual analytics for the detection of anomalous maritime behavior. *In 2008 12th International Conference Information Visualisation* (pp. 273-279). IEEE.

Roa Perera, I., Peña, Y., Amante García, B., and Goretti, M. (2013). Ports: definition and study of types, sizes and business models. *Journal of industrial engineering and management (JIEM), 6*(4), 1055-1064.

Roy, J. (2008). Anomaly detection in the maritime domain. *In Optics and Photonics in Global Homeland Security IV* (Vol. 6945, p. 69450W). International Society for Optics and Photonics.

Saini, H., Rao, Y. S., and Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202-209.

Sands, J. N. (2004). TRB Special Report: Cybersecurity of Freight Information Systems: A Scoping Study. *TR News*, (230).

Sanger, D. Barboza, D., and Pelroth, N. (2014) *Cyber Security*. United States Coast Guard.

Senzee, T. (2019). What happened in ransomware attack on Port of San Diego. *San Diego Readers News*.

Shackleford, D. (2015). Combatting cyber risks in the supply chain. *SANS. org*.

Sleeper, D. M. (2012). Port Significance Contributions to Competitiveness in Latin America and Asia, Journal *for Global Business and Community*, Volume 3, Issue 1, 22-28.

The white House. (2018). Cybersecurity Funding. *Homeland Security (DHS) and* Department *of Defense. (DOD).* (PP: 273:287)

U.S. Department of Transportation. (2015). *Bureau of Transportation Statistics,* Transportation Statistics Annual Report 2015, Washington, DC.

Wallischeck, E. Y. (2013). *ICS security in maritime transportation: a white paper examining the security and resiliency of critical transportation infrastructure* (No. DOT-VNTSC-MARAD-13-01). John A. Volpe National Transportation Systems Center (US).

Insight Report. (2019). *The Global Risks Report 2019*. 14th Edition. World Economic Forum.