BACHELOR THESIS & COLLOQUIUM – ME184841

# A BAYESIAN NETWORK MODEL FOR PIRACY AND ROBBERY ASSESSMENT OF A PORT: A CASE STUDY OF TANJUNG PERAK PORT

I PUTU GEDE BAGUS PARTA SAPUTRA
NRP. 04211541000033

SUPERVISOR :
Raja Oloan Saut Gurning, ST, M.Sc., Ph.D.
Prof. Dr. Ketut Buda Artana, ST., M.Sc.

DOUBLE DEGREE PROGRAM
DEPARTMENT OF MARINE ENGINEERING
FACULTY OF MARINE TECHNOLOGY
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2019

"This page intentionally left blank"

**BACHELOR THESIS & COLLOQUIUM – ME184841**

# A BAYESIAN NETWORK MODEL FOR PIRACY AND ROBBERY ASSESSMENT OF A PORT: A CASE STUDY OF TANJUNG PERAK PORT

**I PUTU GEDE BAGUS PARTA SAPUTRA**
**NRP. 04211541000033**

SUPERVISOR :
**Raja Oloan Saut Gurning, ST, M.Sc., Ph.D.**
**Prof. Dr. Ketut Buda Artana, ST., M.Sc.**

DOUBLE DEGREE PROGRAM
DEPARTMENT OF MARINE ENGINEERING
FACULTY OF MARINE TECHNOLOGY
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2019

"This page intentionally left blank"

**SKRIPSI – ME184841**

# MODEL BAYESIAN NETWORK UNTUK PENILAIAN PADA KASUS PEMBAJAKAN DAN PERAMPOKAN DI PELABUHAN: STUDI KASUS PELABUHAN TANJUNG PERAK

**I PUTU GEDE BAGUS PARTA SAPUTRA**
**NRP. 04211541000033**

DOSEN PEMBIMBING :
**Raja Oloan Saut Gurning, ST, M.Sc., Ph.D.**
**Prof. Dr. Ketut Buda Artana, ST., M.Sc.**

PROGRAM DOUBLE DEGREE
DEPARTMEN TEKNIK SISTEM PERKAPALAN
FACULTAS TEKNOLOGI KELAUTAN
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2019

"This page intentionally left blank"

## APPROVAL FORM

## A BAYESIAN NETWORK FOR PIRACY AND ROBBERY ASSESSMENT OF A PORT: A CASE STUDY OF TANJUNG PERAK PORT

### BACHELOR THESIS

Submitted to Comply One of The Requirement to Obtain a Bachelor Engineering Degree
On
Reliability, Availability, Management, and Safety (RAMS)
Bachelor Program Department of Marine Engineering
Faculty of Marine Technology
Institut Teknologi Sepuluh Nopember

Prepared by:
**I PUTU GEDE BAGUS PARTA SAPUTRA**
NRP. 04211541000033

Approved by Supervisor:

Raja Oloan Saut Gurning, ST, M.Sc., Ph.D. ( ) 30/1/2019

Prof. Dr. Ketut Buda Artana, ST., M.Sc. ( )

"This page intentionally left blank"

## APPROVAL FORM

## A BAYESIAN NETWORK FOR PIRACY AND ROBBERY ASSESSMENT OF A PORT: A CASE STUDY OF TANJUNG PERAK PORT

**BACHELOR THESIS**

Submitted to Comply One of The Requirement to Obtain a Bachelor Engineering Degree
On
Reliability, Availability, Management, and Safety (RAMS)
Bachelor Program Department of Marine Engineering
Faculty of Marine Technology
Institut Teknologi Sepuluh Nopember

Prepared by:
**I PUTU GEDE BAGUS PARTA SAPUTRA**
NRP. 04211541000033

Approved by
Head of Department of Marine Engineering

Dr. Eng. Muhammad Badrus Zaman., ST., MT.
NIP. 197708022008011007

"This page intentionally left blank"

# APPROVAL FORM

## A BAYESIAN NETWORK FOR PIRACY AND ROBBERY ASSESSMENT OF A PORT: A CASE STUDY OF TANJUNG PERAK PORT

**BACHELOR THESIS**

Submitted to Comply One of The Requirement to Obtain a Bachelor Engineering Degree
On
Reliability, Availability, Management, and Safety (RAMS)
Bachelor Program Department of Marine Engineering
Faculty of Marine Technology
Institut Teknologi Sepuluh Nopember

Prepared by:
**I PUTU GEDE BAGUS PARTA SAPUTRA**
NRP. 04211541000033

Approved by
Representative of Hochschule Wismar in Indonesia

Dr.-Ing. Wolfgang Busse

"This page intentionally left blank"

## DECLARATION OF HONOR

I hereby who signed below declare that:
This bachelor thesis has written and developed independently without my plagiarism act, and confirm consciously that all data, concepts, design, references, and material in this report own by Reliability, Availability, Management, and Safety (RAMS) in Department of Marine Engineering ITS which are the product of research study and reserve the right to use for further research study and its development.

| | |
|---|---|
| Name | : I Putu Gede Bagus Parta Saputra |
| NRP | : 04211541000033 |
| Bachelor Thesis Title | : A Bayesian Network Model for Piracy and Robbery Assessment of A Port: A Case Study Tanjung Perak Port |
| Department | : Marine Engineering |

If there is plagiarism act in the future, I will fully responsible and receive the penalty given by ITS according to the regulation applied.

Surabaya, 2019

I Putu Gede Bagus Parta Saputra

"This page intentionally left blank"

# A BAYESIAN NETWORK MODEL FOR PIRACY AND ROBBERY ASSESSMENT OF A PORT: A CASE STUDY OF TANJUNG PERAK PORT

Name : I Putu Gede Bagus Parta Saputra
NRP : 04211541000033
Department : Marine Engineering
Supervisor I : Raja Oloan Saut Gurning, ST., M.Sc., Ph.D
Supervisor II : Prof. Dr. Ketut Buda Artana, ST., M.Sc.

## ABSTRACT

International Ship and Port Facility Security (ISPS) Code was developed by International Maritime Organization (IMO) to provide procedures and measures to prevent piracy, robbery, terrorism, and other criminal acts in international trade. Terrorism and criminal acts such as cargo theft, smuggling, piracy/armed robbery, etc. that happen in ships and ports will crippled operation and portray a bad image. 14 years after it came into force, the implementation of International Ship and Port Facility Security (ISPS) Code in Indonesia is still a poor one. Proven by the most recent crimes happened in Port Belawan at 10th July 2018 and in Terminal Marunda Centre at 13th August 2018 that was caused by armed robbery.

The Intensity of criminal acts especially piracy, armed robbery, and petty theft in Indonesia is quite high. Based on ICC International Maritime Bureau annual report of Piracy and Armed Robbery 2014-2018, Indonesia has the highest crime rate in Southeast Asia. In order to tackle this issue, a model using Bayesian network for predicting the likelihood of a ship being attacked by pirates and robbers is proposed in this research. Bayesian Network Model in this research is developed and tested using NETICA Software. A sensitivity analysis is done to the model created to provide a certain degree of confidence that the model creating is working properly. From the model created it was found that Situation hold a significant impact on the likelihood of an attack happened in Port of Tanjung Perak. A well-guarded situation of the port can reduce the likelihood of an attack up to 26.6% reducing the likelihood of an attack to 0.315 from the current situation 0.585. Based on this finding, suggestion for improvements of security protection to reduce number of piracy and robbery attack in the future.

Key Word: ISPS Code, Piracy and Robbery Assessment, Bayesian Network Model, Sensitivity Analysis

"This page intentionally left blank"

# MODEL BAYESIAN NETWORK UNTUK *RISK ASSESSMENT* PADA KASUS PEMBAJAKAN DAN PERAMPOKAN DI PELABUHAN: STUDI KASUS PELABUHAN TANJUNG PERAK


Nama : I Putu Gede Bagus Parta Saputra
NRP : 04211541000033
Jurusan : Teknik Sistem Perkapalan
Dosen Pembimbing I : Raja Oloan Saut Gurning, ST., M.Sc., Ph.D
Dosen Pembimbing II : Prof. Dr. Ketut Buda Artana, ST., M.Sc.


## ABSTRAK


Kode Keamanan Kapal dan Fasilitas Pelabuhan Internasional (ISPS) dikembangkan oleh Organisasi Maritim Internasional (IMO) untuk menyediakan langkah-langkah dan prosedur untuk mencegah pembajakan, terorisme, dan tindakan kriminal lainnya, yang mengancam keamanan penumpang, awak kapal, keselamatan kapal dan pelabuhan fasilitas yang digunakan dalam perdagangan internasional. Terorisme dan tindakan kriminal seperti pencurian kargo, penyelundupan, pembajakan / perampokan bersenjata, dll. Yang terjadi di kapal dan pelabuhan akan melumpuhkan operasi dan menggambarkan citra yang buruk. 14 tahun setelah diberlakukan, penerapan Kode Keamanan Kapal dan Keamanan Pelabuhan Internasional (ISPS) di Indonesia masih sangat buruk. Terbukti oleh kejahatan terbaru yang terjadi di Port Belawan pada 10 Juli 2018 dan di Terminal Marunda Center pada 13 Agustus 2018 yang disebabkan oleh perampokan bersenjata. Intensitas tindakan kriminal terutama pembajakan, perampokan bersenjata, dan pencurian kecil di Indonesia cukup tinggi. Berdasarkan laporan tahunan ICC International Maritime Bureau tentang Pembajakan dan Perampokan Bersenjata 2014-2018, Indonesia memiliki tingkat kejahatan tertinggi di Asia Tenggara. Untuk mengatasi masalah ini, sebuah model menggunakan jaringan Bayesian untuk memprediksi kemungkinan kapal diserang oleh bajak laut dan perampok diusulkan dalam penelitian ini. Bayesian Network Model dalam penelitian ini dikembangkan dan diuji menggunakan Perangkat Lunak NETICA. Analisis sensitivitas dilakukan untuk model yang dibuat untuk memberikan tingkat kepercayaan tertentu bahwa pembuatan model berfungsi dengan baik. Dari model yang dibuat ditemukan bahwa Situation memiliki dampak yang signifikan terhadap kemungkinan serangan yang terjadi di Pelabuhan Tanjung Perak. Situasi pelabuhan yang dijaga dengan baik dapat mengurangi kemungkinan serangan hingga 26,6% mengurangi kemungkinan serangan menjadi 0,315 dari situasi saat ini 0,585. Berdasarkan

hasil tersebut, saran untuk perbaikan perlindungan keamanan untuk mengurangi jumlah pembajakan dan serangan perampokan di masa depan.

Kata kunci: ISPS Code, Pembajakan dan Perampokan, Model Jaringan Bayesian, Analisa Sensitivitas

# PREFACE

Above all, the author gave thanks and praise to the Almighty God, Ida Sang Hyang Widhi Wasa who has given me strength and wisdom so that the author can complete his studies and this bachelor thesis. Hopefully with the completion of this research study, authors gain more perspectives, information, and knowledge for the future career.

The author owed sincere and earnest appreciation for those who had helped, guided through and provided the author vital suggestion in the completion of this bachelor thesis.

1. Author's beloved family, especially author's mother and brother who always give their prayer, support emotionally and financially, love, encouragement and inspiration to the author to pursuit a better life.
2. Dr. Eng, M. Badrus Zaman, ST., M.T. as Chairman of Marine Engineering Department, Marine Technology Faculty of Institut Teknologi Sepuluh Nopember
3. Raja Oloan Saut Gurning, ST., M.Sc., Ph.D as 1st Supervisor for his incessant support, encouragement and the enlightenment in the supervision of this bachelor thesis and provided him with vital suggestions and advice.
4. Prof. Dr. Ketut Buda Artana, ST., M.Sc as 2nd Supervisor who through his fruitful of knowledge, encouragement, and guidance supervised the author through his bachelor thesis work.
5. A.A.Bagus Dinariyana Dwi P., ST., MES., Ph.D as Head of RAMS Laboratory who provide a warm working milieu and enlightening life advice.
6. Taufik Fajar Nugroho, ST., M.Sc as Guardian Lecturer of the author who has given the author advice throughout college.
7. Dr. I. Made Ariana, ST., MT. who has given the author the opportunity to study and prepare the author for his future career.
8. Dr. Dhimas Widhi Handani, ST., M.Sc. as Lecturer in RAMS Laboratory who provide the author knowledge during study period in college
9. Fadilla Indrayuni Prastyasari, S.T., M.Sc as Coordinator Lecturer of Bachelor Thesis who has provided supervision, suggestion and information regarding bachelor thesis.
10. Mr. Luqman Sariful Hidayat, ST. as ISPS Code Auditor of Harbour Master Tanjung Perak for granting the author information regarding the issue in this bachelor thesis.

11. Mr. Huda from Pelabuhan Indonesia III Tanjung Perak who has provided the author information regarding the issue in this bachelor thesis.
12. Dit. Polair Tanjung Perak for providing and granting the author information regarding the issue in this bachelor thesis.
13. Emmy Pratiwi, Putri Dyah Setyorini and Thariq Aqbar as senior in RAMS Laboratory who has provide the author with vital suggestion, advice, and enlightenment through bachelor thesis work.
14. Mirah, Kitto, Ira, Firman, Tata, Prajna, Haidar, Dira, Fadil, Amel and Okta as fellow bachelor thesis colleague of the author that were always there in bitter sweet conditions.
15. To the author's friends and roommates, thank you for the thoughts, well-wishes, calls, texts, editing advice, and presence whenever he needed a friend.

The author concerns for the imperfection in this thesis. Therefore, any criticism and suggestion are expected. The author hoped this thesis will provide benefits primarily for the readers.

Surabaya, 2019

Author

# TABLE OF CONTENT

# TABLE OF FIGURES



# LIST OF TABLES

# CHAPTER I

# INTRODUCTION

## 1.1. Background

As a crucial part of global business, shipping industry conveys almost 90 % of the world trade volumes. Meaning, that number of ships have to carry cargoes between ports is very large. As it is so crucial, any threat or accident happened in this cycle will affect global economics. With the tendency of ships or ports having the likelihood of getting caught in an unwanted situation regarding security issues.

Security issues such as piracy, terrorism, and other criminal activities in shipping business is not a new concern. It already is a concern since the first-time ship introduced. But the issues had not been taken into a serious note until the attack on passenger vessels *Achille Lauro* and *City of Poros* in 1985 and 1989 respectively. The accident happened made International Maritime Organization (IMO) adopted a Convention on the Suppression of Unlawful Acts (SUA) which embody advices regarding security for ships in 1986.

Then, the horrific event of terrorist attack at the World Trade Centre on 11$^{th}$ September 2001 happened. It shocked the world with a graphical demonstration of what terrorist attack will go to an extraordinary extent. The horrific event of which involving aircraft, changed the perspectives dramatically as ship cargoes, and ports are perceived that they can be used as a targets, weapon or locations of attacks. It then triggered International Maritime Organization (IMO) to held The 22$^{nd}$ session of the assembly in November 2001 to create an instrument in order to deter and prevent piracy, terrorism, and other criminal acts against maritime target.

The assembly later on became International Ship and Port Facility Security (ISPS) Code consisted in amendment of SOLAS 1974 Chapter XI-2. International Ship and Port Facility Security (ISPS) Code came into forces 1$^{st}$ July 2004. The code was developed to provide measures and procedures to prevent piracy, terrorism, and other criminal acts, which threaten the security of passengers, crew, the safety of ships and port facilities used in international trade. Terrorism and criminal acts such as cargo theft, smuggling, piracy/armed robbery, etc. that happen in ships and ports will crippled operation and portray a bad image.

Implementation of International Ship and Port Facility Security (ISPS) Code will help to curb these criminal activities and in turn improve operations in ship and port. As one of the member states of International Maritime Organization (IMO) Indonesia has to implement the code. 14 years later after it came into force, the implementation of International Ship and Port Facility Security (ISPS) Code in Indonesia is still a poor one. Proven by the most recent crimes happened in Port Belawan at 10th July 2018 and in Terminal Marunda Center at 13th August 2018 that was caused by armed robbery.

The Intensity of criminal acts especially piracy, armed robbery, and petty theft in Indonesia is quite high. Based on ICC International Maritime

| Location | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|
| **SE ASIA** Indonesia | 47 | 54 | 24 | 19 | 25 |
| Mallaca Straits | 1 | 3 | | | |
| Malaysia | 9 | 11 | 4 | 3 | 2 |
| Philipphines | 2 | 4 | 3 | 13 | 3 |
| Singapore Straits | 6 | 6 | | 1 | |
| Thailand | | 1 | | | |

*Table 1. 1 Actual and attempted attack in January - June 2014 - 2018*

Bureau annual report of Piracy and Armed Robbery 2014-2018, Indonesia has the highest crime rate in Southeast Asia.

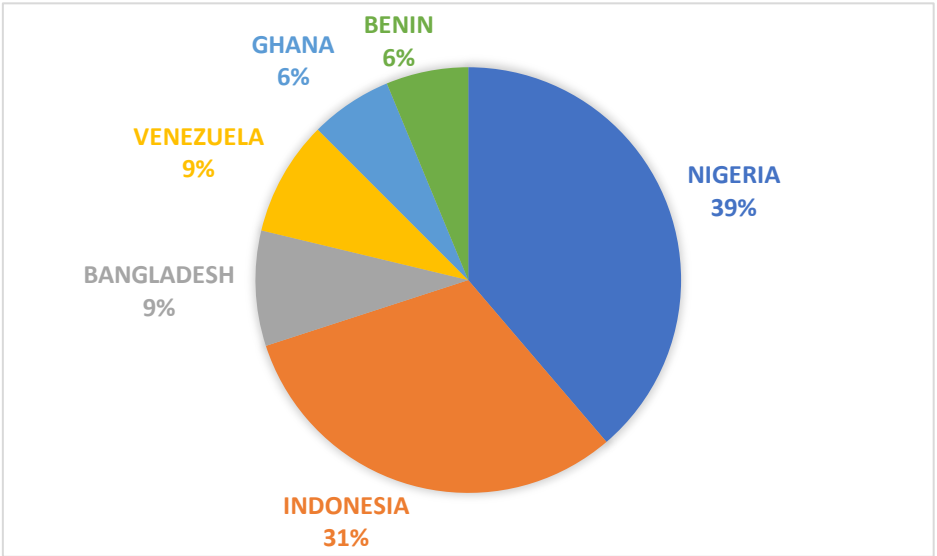



*Figure 1. 1 Country contributed to 75% of the total of 106 incidents reported in January – June 2018*

*Source: ICC annual report of Piracy and Armed Robbery 2014-2018*

From figures 1.1 we can see that Indonesia is the 2nd most frequent piracy and robbery attack happen. With such numbers of security threat happen in Indonesian ports it will cause trading-partner feeling unsafe and portray a bad image. This will affect Indonesia's economies especially local economies of the port industry.

In order to tackle this issue, a model using Bayesian network for predicting the likelihood of a ship being attacked by pirates and is proposed robbers in this research, due to characteristics of piracy and robbery threat is, to some extent, predictable depending on sea areas (Low Risk Areas or High Risks Area), weather conditions, and security measures in place. Model produced will be tested using NETICA Software to identify sensitivity of the model to provide a degree of confidence that the model has been built correctly and is working as intended. This model will predict the best scenario that leads to successful attacks given by the characteristics of the ship, environment conditions and the maritime security measures in place. From this scenario, improvements for future security protection complementing ISPS Code could be addressed more effectively to reduce number of piracy and robbery in Indonesia.

## 1.2. Research Problem

1) How to determine variables that potentially leads to successful attacks of piracy and robbery.
2) How to develop a model to estimate the likelihood of success attack of piracy and robbery in Port Tanjung Perak.
3) How to make a recommendation anti-piracy and anti-robbery decision by maritime stakeholders in operation.

## 1.3. Research Limitation

1) Port assessed in this research limited in Port Tanjung Perak (Terminal Jamrud, Terminal Gapura Surya Nusantara, and Terminal Petikemas Surabaya).
2) Ships assessed in this study is ships with international voyage and flag.

## 1.4. Research Objectives

1) Determine variables that potentially leads to successful attacks of piracy and robbery.

2) Develop a model to estimate the likelihood of success attack of piracy and robbery in Port Tanjung Perak.
3) Make a recommendation anti-piracy and anti-robbery decision by maritime stakeholders in operation.

## 1.5. Research Benefits

1) The model proposed can be used as a standalone technique to update the estimation of the probability of ships being attack by pirates and robbers in Port Tanjung Perak when a there is a new available information.
2) The model proposed can also be used to make operational security-based decision by maritime stakeholders.
3) The results of the research provided will be additional advice in making decisions on service operations at the port regarding security issues.

# CHAPTER II

# LITERATURE STUDY

## 2.1 ISPS CODE

International Ship and Port Facility Security (ISPS) Code is an amendment result of International Maritime Organization (IMO) 22nd sessions assembly in November 2001 to the Safety of Life at Sea (SOLAS) Convention (1974/1988). The amendment is carried out in Chapter V Safety of Navigation and additions to Chapter XI become Chapter XI-1 concerning special measures to improve shipping safety (special measures to enhance maritime safety) and Chapter XII-2 steps - special measures to improve shipping security (special measures to enhance maritime safety), known as the International Ship and Port Facility Security Code (ISPS Code) or International Code for Ship Security and Port Facilities. The purpose of this code is to establish an international and national framework focusing on protection of ship and port facility security from terrorism, piratical and other criminal activities, and increase awareness of preventive action against unlawful acts. ISPS Code is applied to ports and ship with a criterias:

- Passenger ships, including high-speed passenger craft;
- Cargo ships, including high-speed craft, of 500 gross tonnage and upwards;
- Mobile offshore drilling units;
- Port facilities serving such ships engaged on international voyages.

ISPS Code is divided into 2 parts, part A and part B. Part A regulates mandatory requirements of which consist of 19 subsections concerning goal of the code and demands on ships and in port facilities. Meanwhile part B is a guidance regarding the provisions of part A such as contracting governments responsibilities. It also concerns about establishing the vital issues of the code which is security levels. The ISPS code serves in building a framework that involves cooperation between the governments of signatory countries, government agencies, local governments and the shipping and port industries to identify security threats and take precautionary measures against security events that affect ships and or port facilities used for international trade (Budiyanto & Gurning, 2015). The other concern of the code is establishing the respective roles and

responsibilities of signatory governments, government agencies, local government, shipping industry and port industry, at the national and international level to ensure maritime security. The code also ensures early and successful collection of information and exchanges related to security by providing a method for security assessment for which the plan must exist and the procedure for responding to changes in security level.

2.1.1 Obligation of Contracting Governments

Contracting governments has a critical responsibility to the successful implementation and enforcement of the Code. Contracting Government is the authority decides maritime security level for the ships with their flag-state and ports within their jurisdictions. Flag states have the responsibility to provide guidance for protection from security incidents for the ships flying their flag and where to heightened security measures and levels. Appropriate security information related to shipping industry both the ships and port facilities also have to be provided. Contracting government also has the responsibility to ensure implementation on appropriate maritime security culture within its nation. Creating complimentary rules to support security practices in the region is also a part of obligation by contracting governments. Below are several various responsibilities of contracting government, amongst others include the following:

- Establish the Designated Authority (DA)
- Appoint Recognized Security Organization (RSO)
- Establish the level of security (Security Level)
- Endorsement of Port Facility Security Assessment (PFSA) and Port Facility Security Plan (PFSP)
- Ratification of the Ship Security Plan (SSP)
- Verification and certification
- Establish requirements for the Security Declaration or Declaration of Security (DoS)
- Convey information to International Maritime Organization (IMO) and to shipping industries port
- Supervision

2.1.1.1. Designated Authority (DA)

Designated Authority (DA) is a known organizer within the government who entered into an agreement as responsible institution for ensuring the implementation of the provisions of International Ship and

Port Facility Security (ISPS) Code which pertains to the security of port facilities and ship or port relations from the point of view of port facilities. Designated Authority in Indonesia is Director General of Sea Transportation.

2.1.1.2. Ship Security Plan (SSP)

Ship Security Plan is a plan made to ensure the application of steps or actions on ships designed to protect humans on ships, cargo, cargo transportation units, supplies of ships or their own ships from the risk of security events.

2.1.1.3. Port Facility Security Plan (PFSP)

Port Facility Security Plan is a plan that is built to ensure the application of the steps or actions planned to protect port facilities and ships, humans, cargo, cargo transportation units and ship supplies in port facilities from the risk of security events / events.

2.1.1.4. Ship Security Officer (SSO)

Ship Security Officer is personnel on board, who are responsible to the captain for the security of the ship, including the implementation and maintenance of the ship's security plan and to coordinate with company security officers and port facility security officers.

2.1.1.5. Company Security Officer (CSO)

Company Security Officer is the personnel assigned by the company to ensure that the ship's security assessment has been carried out. That the ship's security plan is strengthened, delivered for approval, and then implements and maintains it. Company Security Officer also responsible for dealing with port facility officers and ship security officers.

2.1.1.6. Port Facility Security Officer (PFSO)

Port Facility Security Officer is personnel assigned to be responsible for the development, implementation, change and maintenance of port facility security plan and for dealing with ship security officers and company security officers.

2.1.1.7. Declaration of Security (DoS)

Declaration of Security is an agreement reached between a ship and a port or other ship facility with which it interacts. The Declaration address

security requirements that could be shared between a port facility and a ship, or between ships, and states the responsibility for each. Declaration of Security can also set security measures that will be implemented.

2.1.1.8. Recognized Security Organization (RSO)

Recognized Security Organization is an organization with appropriate expertise in the field of security and with appropriate knowledge in the field of ship and port operations. The duties and authorities of RSO are determined by the Director General of Sea Transportation based on the provisions, capacities and applications submitted by each RSO candidate, but do not exceed the following limits:

- Carry out a security assessment (SSA and PFSA)
- Development of security planning (SSP and PFSP)
- Validation of assessment and planning ship security (SSP)
- Verification of planning implementation ship security (SSP)
- Issuance of International Ship Security Certificate (ISSC)

In Indonesia, Recognized Security Organization is Kesyahbandaran dan Otoritas Pelabuhan (Harbour Master).

2.1.1.9. Port Security Committee (PSC)

Port Security Committee is an organization consisting of the Port Administration Office with the Port Office as the coordinator, Head of the Guard and Rescue as Implementing Coordinator and Agency Representative. Port Security Committee in general has the responsibility such:

- Preparation of port communication, information and intelligence networks.
- Identify the threat and vulnerability of the port
- Develop procedures and port security systems to minimize security threat.

2.1.1.10. Port Security Officer (PSO)

Port Security Officer is the official of the Head of the Division of Security and Rescue as the Port Security Coordinator. PSO is personnel responsible for the development, implementation, revision, and maintenance of the port facility security plan and for dealing with the port authorities and Ship Security Officers (SSO) and Company Security Officer (CSO).

2.1.1.11. Verification

Verification is the act of inspection or audit of Ship Security Plan (SSP), and or Port Facility Security Plan (PFSP) and all related provisions and procedures in ship and port security plan that must be fulfilled in compliance to International Ship and Port Facility Security (ISPS) Code.

2.1.2 Security Level

Maritime security level established into 3 different levels of which every level has a specific procedures and standards. Certain security level operated on ships will be instructed from Flag-state Administration or as determined by master. For port facility, it will operate at certain Security Level as determined by the Port Facility Security Officer (PFSO) or instructed by Designated Authority (DA) of Contracting Government.

- Level 1
  Security level 1 defined as condition where minimum appropriate protective security measures shall be maintained at all times.
- Level 2
  Security level 2 defined as condition where appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.
- Level 3
  Security level 3 defined as condition where Further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

2.1.3 Shipping Company Responsibility

Shipping company must posses International Ship Security Certificate for each operating vessel and ensure it is available onboard at all times for inspection. According to the ISPS Code the following measures are mandatory for shipping company:

- Appointment of Company Security Officer;
- Appointment of Ship Security Officer (SSO);
- Ship Security Assessment (SSA) and install proper Ship Safety Alert System (SSAS) onboard;
- Approved and fully educated crew of Ship Security Plan (SSP) on board
- Ensure appropriate security training, drills, and exercises;
- Provide appropriate resources for ship in compliance with security plan.

### 2.1.4 Port Authority Responsibility

ISPS Code required port authority to have following mandatory measures in compliance with the code:

- Appointment of Port Facility Security Officer (PFSO);
- Approved Port Facility Security Assessment (PFSA);
- Approved Port Facility Security Plan (PFSP);
- Provide appropriate education, training, drills, and exercise for port facility personnel;
- Establish good communication and information flow towards the ships entering the port via a ship security officer (SSO), through a port facility security officer (PFSO) and to the responsible government handling the ISPS Code related issues within the country.

## 2.2 Maritime Piracy and Robbery

Maritime Security is defined as "the advancement and protection of a nation's interests, at home and abroad, through the active management of risks and opportunities in and from the maritime domain, in order to strengthen and extend nation's prosperity, security, and resilience and to help shape a stable world" (HM Government,2014). Maritime security issues include terrorism, piracy and robbery attacks, transportation of illegal items, people smuggling, and human trafficking. As one of the concerns of maritime security issues, maritime piracy and robbery is regulated under International Ship and Port Facility Security (ISPS) Code. Due to its effect, maritime piracy and robbery can cause not only disruption in supply chain but it also leads to economic consequences, loss of lives, short and long terms health problem of seafarers and passengers. Maritime piracy and robbery attacks to some extent is predictable depend on sea areas (piracy low risk area and high risks area), weather conditions and or Best Management Practices (Schneider P, 2012).

### 2.2.1 Maritime Piracy and Robbery Pattern

International organizations and shipping industry have made enormous effort to overcome piracy and robbery attacks. But piracy and robbery attack evolve within years. Modern pirates use state-of-the-art equipment in their operations (Psarros G, 2011). With crimes ranging from simple robbery to murder and entire ship hijacking. A significant

threat from maritime piracy came in the late 1990s. Based on IMO monthly piracy reports in 2000-2009 data it was found that incident of piracy In South China Sea and Malacca Strait led to more death compared to African continent.

*Table 2. 1 All incident of piracy and armed robbery from 1 July 1994 - 1 December 2014 (Source: IMO GISIS database)*

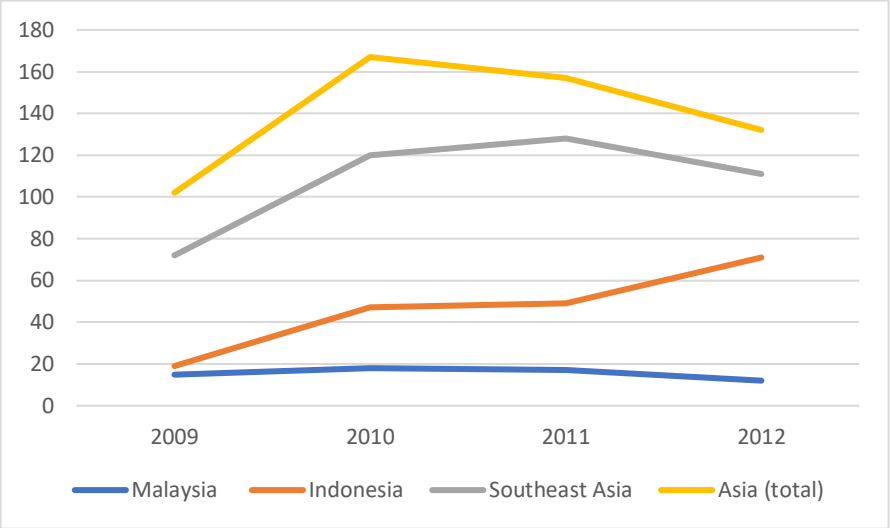
| Ship type | Total number | Ship type | Total number |
|---|---|---|---|
| Bulk carrier | 1425 | Gas tanker | 169 |
| Tanker | 1228 | Reefer | 95 |
| General cargo ship | 949 | Ro-Ro | 75 |
| Container ship | 933 | Car carrier | 38 |
| Chemical tanker | 580 | Passenger ship | 21 |
| Special purpose | 406 | Ferry | 13 |
| Small craft | 381 | Barge | 49 |
| unspecified | 275 | | |
| **Total:** | **6637** | | |

Figures above shows ship type that is mostly attacked is bulk carriers followed by tankers and general cargo ships. Based on data shown, characteristic of ship having slow speed and low freeboard having more tendency of becoming a piracy victim (Sascha P, 2016).

2.2.2 Maritime Piracy in Southeast Asia

Piracy threat in this region usually aiming to ransack ship limited to ship stores and crew valuables. Many cases of attack are happening when ships were at anchor with robbers were lightly armed, often with knives. Robbers often flee out of scene without being spotted and attack crew. However, violent attack causing crew seriously injured also occurred. In this region ReCAAP was signed in 2004 as a mechanism to quickly organize assistance when vessel under attack. ReCAAP was issued after the accident occurred in Malacca Strait. Indonesia and Malaysia are the only two ASEAN states that remain outside ReCAAP. Indonesia's reason regarding the agreement stem primarily comes from concerns that it would undermine the country's sovereignty. This results Indonesia is limiting their cooperation with ReCAAP to sharing information with the

ISC and its Focal Points in various ReCAAP member countries (RECAAP, 2018).




| | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|
| Malaysia | 15 | 18 | 17 | 12 |
| Indonesia | 19 | 47 | 49 | 71 |
| Southeast Asia | 72 | 120 | 128 | 111 |
| Asia (total) | 102 | 167 | 157 | 132 |

*Figure 2. 1Comparison maritime piracy and robbery incidents in the waters and ports of Indonesia, Malaysia, Southeast Asia, and Asia as a whole, 2009–2012*

*Source: ICC Annual Report 2018*

Based on graphic shown it can be confirmed that there is a rising number trend of robbery and theft incident in Southeast Asia. Despite geographically limited multilateral initiatives, both Indonesia and Malaysia prefer to view the piracy problem as a domestic issue that best be addressed by strengthening its law enforcement agencies and navy, as well as by addressing some of the underlying causes of piracy, such as poverty and a lack of economic opportunities.

## 2.3 Indonesia's Maritime Piracy

Indonesia has the highest piracy crimes rate compared to other countries in Southeast Asia and the 2nd in the world based on annual report of Piracy and Armed Robbery Against Ships published by ICC International Maritime Bureau in 2018. According to a 2017 report by the International Maritime Bureau the number of attacks in Indonesia in 2017

was higher than in other piracy-prone areas in the seas off West and East Africa. 43 violent in the sea were reported. These include one hijacking, five attempted attacks and 33 incidents at berth or at anchor, when ships were not underway. Based on the report, Indonesia was the most piracy-prone country in the world from 2012. Between 2000 and 2014 the average number of piracy events each year within Indonesia waters is 100, it is one of the highest totals of any country in the Asia-Pacific region (Morris & Paoli, 2018).

Indonesian-style piracy is closer to sea-thieves. The act is carried out on the high seas, while these armed robberies occur in territorial waters. Sea-robbers usually steal salaries in cash, mobile phones, laptops and shipping equipment (Frécon, 2018). Based on Frécon research in 2000-2010 about how the piracy act in Indonesia works, he found that there were two different types of categories. The first category consists of local taxi-boat drivers and fishermen who know the area well. They usually hid themselves in mangroves along straits and steal valuables from boats passing close to the shores. This category usually are amateurs who strike at night and put on masks and use their own household machetes (*parang*). They are led by either a violent or generous chief, one of whom considered himself a sea Robin Hood who provided funds to build a village and a mosque.

The second category consists of young people from remote Indonesian islands who are struggling to find proper jobs. This group works when they have job order from a foreign bad-intentioned businessperson to hijack a ship. The ship crew are either taken hostage or left at sea on a lifeboat during their operation. Once on board, they take over to sell the cargo.

To provide more about the recent statistics and characteristics from piracy and robbery attack in Indonesia, several tables are presented in this chapter. This tables are obtained from the recent International Maritime Bureau report of 2018.

*Table 2. 2 Actual and Attempted attack in Southeast Asia*

| | | Actual attacks | | Attempted attacks | |
|---|---|---|---|---|---|
| **Location** | | Boarded | Hijacked | Attempted | Fired Upon |
| **SE ASIA** | Indonesia | 19 | | 6 | |
| | Malaysia | 1 | | 1 | |
| | Philippines | 1 | | 1 | 1 |

Table 2.2 show the number of actual and attempted attacks happened in the South East Asia region during the first semester of 2018. This table give a clear comparation between number of events happening in Indonesia, Malaysia, and Philippines. From this table known that the attacks in South East Asia region only happened in these three countries. Without adding up the number of actual and attempted attacks, it is clearly shown that Indonesia in this year leads as the country with highest number of piracy and robbery attacks in South East Asia region.

*Table 2. 3 Port and anchorage with three or more reported incidents*

| **Country** | **Location** | **January – June 2018** |
|---|---|---|
| Bangladesh | Chittangong / Kutubdia | 7 |
| Benin | Cotonou | 5 |
| Ghana | Takoradi | 4 |
| Haiti | Port Au Prince | 3 |
| Indonesia | Muara Berau | 11 |
| Indonesia | Pulau Bintan | 3 |
| Nigeria | Lagos | 14 |
| Peru | Callao | 3 |
| Venezuela | Puerto Jose | 4 |
| Venezuela | Puerto La Cruz | 3 |

Table 2.3 present a more precise comparation of attacks of the countries with leading the number of attacks worldwide. Two of the most attacks in Indonesia take place on Muara Berau and Pulau Bintan. 11 attacks happened in Muara Berau make the location 2$^{nd}$ prone area of piracy and robbery attack.

*Table 2. 4 Ship status during actual attacks January - June 2018*

| **Location** | Anchored | Berth | Steaming | Not Stated |
|---|---|---|---|---|
| **SE ASIA** Indonesia | 10 | | 3 | |
| Malaysia | | | 1 | |
| Philippines | | | | |

10 out of 13 the actual attacks in Indonesia are happened while the ships anchored at the port shown by Table 2.4. While 3 of them are happened while ships steaming. The reason might of the attack happened during ships anchoring is due to the mobilization of the ship is limited, and most of the crew are not on guard.

*Table 2. 5 Ship status during attempted attacks January - June 2018*

| **Location** | | Anchored | Berthed | Steaming |
|---|---|---|---|---|
| **SE ASIA** | Indonesia | 6 | | |
| | Malaysia | | | 1 |
| | Philippines | | | 2 |

Table 2.5 shows that even most of the attempted attack in Indonesia operated while ships are anchored and there is no attempted attack happened during steaming. Meanwhile in Malaysia and Philippines attempted attack happened during steaming. For the attempted attacks, the status of the ship in Indonesia, Malaysia, and Philippines are different.

*Table 2. 6 Violence type to crew January - June 2018*

| **Location** | | Hostage | Kidnap | Threatened | Injured |
|---|---|---|---|---|---|
| **SE ASIA** | Indonesia | 1 | | 2 | |

The types of violence the robbers usually done to the crew in Indonesia are presented in Table 2.6. From the table we can assume that the robbers are likely armed. They also do take hostages of the crew and asked for cash in return to release the crew.

*Table 2. 7 Armed used January - June 2018*

| **Location** | | Guns | Knives | Not stated | Other Weapons |
|---|---|---|---|---|---|
| **SE ASIA** | Indonesia | | 4 | 21 | |
| | Malaysia | | 1 | 1 | |
| | Philippines | 1 | | 2 | |

Types of armed used to attack by the robbers mainly are not stated in the report. But, from the table information obtained are that the robbers are most likely arm themselves before doing the action and use the arm when they only need it.

From all tables attached, it provides a verification of research done by Frécon about the characteristics of piracy and robber attack in Indonesia. As an additional information regarding the characteristics of piracy and robbery attacks in Indonesia, a note cited from International Maritime Bureau Report stated that the robbers are normally armed with guns or

knives or machetes. And there is still many of attacks that have gone unreported. Pirates or robbers normally attack vessel during the night. When spotted and alarm sounded, they usually escape without confronting the crew.

## 2.4 Port Tanjung Perak

Due to geographic characteristics where most of the territory is in the form of the sea, sea transportation has become a dominant and important tool to facilitate inter-island relations throughout Indonesia. The means of sea transportation also affect the social relations and distribution channels for Indonesia's international trade. To support this, ports are needed as a gateway to support the economic growth. Port has undergone development in accordance with human needs and time. Port nowadays has various functions, namely as a passenger port, as an access point for inter-island trade routes (domestic) and foreign trade (international) and other economic activities. Indonesia currently has 5 main trade support ports. One of them is Port of Tanjung Perak.


*Figure 2. 2 Port of Tanjung Perak*
*Source: Pelindo.co.id*

Port of Tanjung Perak is the second largest and busiest port in Indonesia after the port of Tanjung Priok, Jakarta. This is because, in addition to being a gateway for eastern Indonesia, it is also due to increasing economic growth in the East Java Province. The situation affected the increasing flow of goods distribution to and from the East

Java region both for domestic goods and international trade. Domestic and international goods distribution activities continue to increase from year to year. Due to its criticality, the security and safety of this port is a critical concern for Indonesia's economic growth. Therefore, this port is chosen to be assessed in this research study.

Port of Tanjung Perak has varied depth depend on TEUs of ships; 14 metres depth to serve 10,000 TEUs 5th generation ships to be finished in mid-2015, while 16 metres (52 ft) depth with width 200 metres (660 ft) can serve 15,000 TEUs or 7th generation ships to be finished in mid-2016. Tanjung Perak has 6 main terminals, multi-purpose terminals for conventional cargo handling, passenger terminal, RoRo and an international container terminal. In 2015 port activities in Tanjung Perak are supported by Teluk Lamong Port Terminal, which is one of the most sophisticated port terminals in the world with fully automated operating system. Due to one of its function serving international voyage, 10 of its terminals including TUKS implement ISPS Code. Belows are the information regarding International Ship and Port Facility Security (ISPS) Code of the three terminals in Port of Tanjung Perak that already comply with the code.

| Facility Details | |
|---|---|
| Port facility name | Terminal Jamrud |
| IMO Port facility number | IDSUB-0011 |
| Alternative names for this port facility, if applicable | |
| Port facility description | General cargo, container, tanker, Ro-ro |
| Latitude | 1° 11.49` S |
| Longitude | 112° 43.25` E |

| Security Plan | |
|---|---|
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent security arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 11/06/04 |

| | |
|---|---|
| Date of most recent review or approval of the port facility security plan (PFSP) | 13/07/14 |
| Date of most recently issued Statement of Compliance, if applicable | 02/12/14 |
| Has this port facility security plan (PFSP) been withdrawn | No |

Figure 2. 3 Port Facility Security of Jamrud Pelindo III
*Source: IMO GISIS*

Figure 2.3 issued the Port Facility Security of Terminal Jamrud in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. Terminal Jamrud serves General Cargo, Container, Tanker, and Ro-Ro.

| Facility Details | |
|---|---|
| Port facility name | Terminal Petikemas Surabaya |
| IMO Port facility number | IDSUB-0015 |
| Alternative names for this port facility, if applicable | |
| Port facility description | Container terminal |
| Latitude | 7° 11.44` S |
| Longitude | 112° 42.05` E |

| Security Plan | |
|---|---|
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent securit arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 21/10/04 |
| Date of most recent review or approval of the port facility security plan (PFSP) | 03/10/16 |

| | |
|---|---|
| Date of most recently issued Statement of Compliance, if applicable | 27/10/14 |
| Has this port facility security plan (PFSP) been withdrawn | No |

*Figure 2. 4 Port Facility Security of Terminal Petikemas Surabaya*
*Source: IMO GISIS*

Figure 2.4 issued the Port Facility Security Note of Terminal Petikemas Surabaya in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. Terminal Petikemas Surabaya only Container.

| Facility Details | |
|---|---|
| Port facility name | Terminal Teluk Lamong |
| IMO Port facility number | IDSUB-0018 |
| Alternative names for this port facility, if applicable | |
| Port facility description | Multi-Purpose Terminal |
| Latitude | 7° 12.00` S |
| Longitude | 112° 40.00` E |

| Security Plan | |
|---|---|
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent securit arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 01/04/15 |
| Date of most recent review or approval of the port facility security plan (PFSP) | 01/04/15 |
| Date of most recently issued Statement of Compliance, if applicable | 25/07/18 |
| Has this port facility security plan (PFSP) been withdrawn | No |

*Figure 2. 5 Port Facility Security Terminal Teluk Lamong*
*Source: IMO GISIS*

Figure 2.5 issued Port Facility Security Note of Terminal Teluk Lamong in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. Terminal Teluk Lamong serves as a multi-purpose terminal. This terminal is the most recent terminal built. The operation in this terminal started at 2015 and is the first green port in Indonesia. These three terminals will be assessed and selected in this research study. The rest of the terminals mentioned below will not be assessed in this study.

| Facility Details | |
|---|---|
| Port facility name | Berlian Jasa Terminal Indonesia |
| IMO Port facility number | IDSUB-0008 |
| Port facility description | General cargo, container, tanker |
| Latitude | 7° 12.10` S |
| Longitude | 112° 43.32` E |
| Security Plan | |
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent securit arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 11/06/04 |
| Date of most recent review or approval of the port facility security plan (PFSP) | 14/10/14 |
| Date of most recently issued Statement of Compliance, if applicable | 20/11/14 |
| Has this port facility security plan (PFSP) been withdrawn | No |

Figure 2. 6 *Port Facility Security Berlian Jas Terminal Indonesia*
*Source: IMO GISIS*

Figure 2.6 issued the Port Facility Security Note of Berlian Jasa Terminal Indonesia (BJTI) in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. Berlian Jasa Terminal Indonesia (BJTI) were used to facilitate general cargo, container, and tanker.

| Facility Details | |
|---|---|
| Port facility name | Dermaga Terminal Nilam Utara Bag. Barat |
| IMO Port facility number | IDSUB-0029 |
| Port facility description | Bulk Liquid Cargo |
| Latitude | 7° 11.00` S |
| Longitude | 112° 42.00` E |
| Security Plan | |
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent securit arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 21/12/17 |
| Date of most recent review or approval of the port facility security plan (PFSP) | |
| Date of most recently issued Statement of Compliance, if applicable | 05/03/18 |
| Has this port facility security plan (PFSP) been withdrawn | No |

*Figure 2. 7 Port Facility Security Terminal Nilam Utara Barat*
*Source: IMO GISIS*

Figure 2.7 issued the Port Facility Security Note of Dermaga Terminal Nilam Utara Bagian Barat in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. Dermaga Terminal Nilam Utara Bagian Barat were used to facilitate bulk liquid cargo.

| Facility Details | |
|---|---|
| Port facility name | Semampir – PT. Pertamina (Persero) |
| IMO Port facility number | IDSUB-0028 |
| Port facility description | Unloading Avtur, Kerosene, Solar and Ido |
| Latitude | 7° 11.38` S |
| Longitude | 112° 44.46` E |
| Security Plan | |

| | |
|---|---|
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent securit arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 15/06/04 |
| Date of most recent review or approval of the port facility security plan (PFSP) | 09/06/14 |
| Date of most recently issued Statement of Compliance, if applicable | 03/09/14 |
| Has this port facility security plan (PFSP) been withdrawn | No |

*Figure 2. 8 Port Facility Security Terminal Semampir PT. Pertamina*
*Source: IMO GISIS*

Figure 2.8 issued the Port Facility Security Note of Terminal Semampir of PT. Pertamina (Persero) in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. Terminal Semampir of PT. Pertamina (Persero) were used to facilitate unloading avtur, kerosene, solar and ido.

| Facility Details | |
|---|---|
| Port facility name | PT. AKR Corporindo Tbk. |
| IMO Port facility number | IDSUB-0014 |
| Port facility description | Bulk, Liquid |
| Latitude | 7° 11.58` S |
| Longitude | 112° 43.10` E |
| Security Plan | |
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent securit arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 14/06/04 |
| Date of most recent review or approval of the port facility security plan (PFSP) | |
| Date of most recently issued Statement of Compliance, if applicable | 21/10/14 |
| Has this port facility security plan (PFSP) been withdrawn | No |

*Figure 2. 9 Port Facility Security PT. AKR Corporindo Tbk*
*Source: IMO GISIS*

Figure 2.9 issued the Port Facility Security Note of PT. AKR Corporindo Tbk in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. PT. AKR Corporindo Tbk. were used to facilitate bulk and liquid.

| Facility Details | |
|---|---|
| Port facility name | PT. ISM Bogasari Flour Mills |
| IMO Port facility number | IDSUB-0010 |
| Port facility description | Bulk |
| Latitude | 7° 12.07` S |
| Longitude | 112° 43.19` E |
| Security Plan | |
| Port facility has alternative security agreements | No |
| Port facility has approved equivalent securit arrangements | No |
| Port facility has approved port facility security plan (PFSP) | Yes |
| Date of port facility security plan (PFSP) approval | 11/06/04 |
| Date of most recent review or approval of the port facility security plan (PFSP) | 14/11/16 |
| Date of most recently issued Statement of Compliance, if applicable | 13/11/14 |
| Has this port facility security plan (PFSP) been withdrawn | No |

*Figure 2. 10 Port Facility Security Terminal Teluk Lamong*
*Source: IMO GISIS*

Figure 2.10 issued the Port Facility Security Note of PT. ISM Bogasari Flour Mills in regards to International Ship and Port Facility Security (ISPS) Code. It is registered to International Maritime Organization as Port Facility that has already comply to International Ship and Port Facility Security (ISPS) Code. PT. ISM Bogasari Flour Mills were used to facilitate bulk.

## 2.5 Engineering Statistics

A common attitude among engineers are to consider statistics as a tool in their toolbox. It can be of great help in a number of cases and having a general idea of how it works and use it whenever the problem under study requires it. One of the basic and fundamental theory known and used by engineers in their research study is probability. Probability

concept pervade many aspects of human activities. Probability is a loosely defined term employed in everyday conversation to indicate the measure of one's belief in the occurrence of a future event when this event may or may not occur.

Probabilities near 1 indicate that the event is extremely likely to occur, probabilities near 0 indicate that the event is almost not likely to occur and probabilities near 0.5 indicate a fair chance, that the event is just as likely to occur as not. In the context of system engineering, these two absolute conditions are a failed system and a successful system (Artana & Dinariyana, 2013). In this context the chances of success and failure can be interpreted as follows:

$$P(success) = \frac{number\ of\ successful\ events}{the\ number\ of\ all\ possible\ events} \quad 2.1$$

$$P(failure) = \frac{number\ of\ failed\ events}{the\ number\ of\ all\ possible\ events} \quad 2.2$$

If,

s = number of successful events

f = number of failed events

then the chances of success and chance of failure are:

$$P(s) = \frac{s}{s+f} \quad 2.3$$

$$P(f) = \frac{f}{s+f} \quad 2.4$$

2.5.1. Venn Diagram

An understanding of some rules for combining opportunities will be made easier with the help of the Venn agency. Venn diagrams are generally represented by a rectangle that represents the total opportunities available. There are two or more events in which the opportunities for each event will be combined.

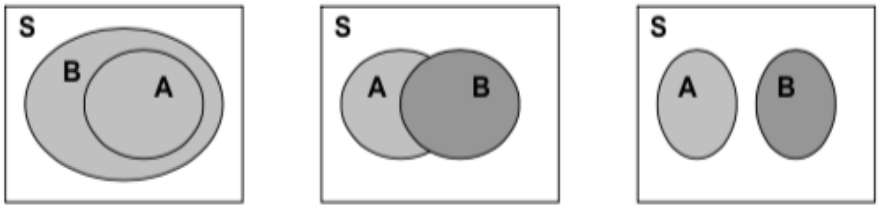



*Figure 2. 11 Venn Diagram*

*Source: Theory of system reliability and its application the first edition*

2.5.1.1. Independent Events

If the occurrence of event *B* has no effect on the probability of event *A*, then *A* and *B* are said to be independent and we can express this fact in terms of conditional probability as

$$P(A|B) = P(A) \qquad 2.5$$

or, equivalently, since we expect symmetry (if *A* is independent of *B* then *B* is independent of *A*)

$$P(B|A) = P(B) \qquad 2.6$$

2.5.1.2. Conditional Events

Conditional events are events that occur if another event has occurred. Opportunity for occurrence A occurs if event B has already occurred written with P (A | B) read event A if B, or opportunity with the condition A if B has occurred.

$$P(A|B) = \frac{the\ number\ of\ events\ A\ and\ B\ can\ occur\ together}{the\ number\ of\ event\ B\ occur} \qquad 2.7$$

Then,

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \qquad 2.8$$

2.5.2. Bayes Theorem

The concept of conditional probability is presented in this chapter on equation 2.8 . It is noted that the conditional probability of an event is a probability obtained with the additional information that some other event has already occurred.

$$P(A_k|B) = \frac{P(A_k)P(B|A_k)}{\sum_{j=1}^{n} P(A_j)P(B|A)} \qquad 2.9$$

Conditional probability in Bayes theorem used for revising a probability value based on additional information that is later obtained. One key to understanding the essence of Bayes theorem is to recognize that we are dealing with sequential events where a new additional

information is obtained for a subsequent event. Terms prior probability and posterior probability are commonly used in Bayes Theorem. A prior probability is an initial probability value originally obtained before any additional information is obtained. A posterior probability is a probability value that has been revised by using additional information that is later obtained.

## 2.6 Bayesian Network

Bayesian networks (BN) also known as belief networks is one of probabilistic graphical models (GM). Bayesian networks (BN) are graphical models for reasoning under uncertainty, where the nodes represent variables (discrete or continuous) and arcs represent direct connections between them. These direct connections are often causal connections. Bayesian Network (BN) model the quantitative strength of the connections between variables, allowing probabilistic beliefs about them to be updated automatically as new information becomes available. Nodes in Bayesian network represent a set of random variables, X = $X_1$,..$X_i$,...$X_n$, from the domain. A set of directed arcs connects pairs of nodes, $X_i \rightarrow X_j$ , represent direct dependencies between variables. Assuming discrete variables, the strength of the relationship between variables is quantified by conditional probability distributions associated with each node. The only constraint on the arcs allowed in a BN is that there must not be any directed cycles. Such networks are called directed acyclic graphs, or simply dags.

Graphical structures in this method are used to represent knowledge about an uncertain domain. Bayesian networks consist of nodes. Each node in the graph represents random variable, while the edges between the nodes represent probabilistic dependencies among the corresponding random variables. These conditional dependencies in the graph are often estimated by using known statistical and computational methods. Hence, BNs combine principles from graph theory, probability theory, computer science, and statistics.

Bayesian network modelling is used in this research due to its functionality fit for this case of which has multiple various variables contributes to success attacks of piracy and robbery. Those multiple variable relation to each other is also unknown (limited information), this characteristic is one of the reasons why Bayesian network is used due to mathematical analysis used in Bayesian is conditional probability

### 2.6.1 Nodes and Value

In this research study nodes that will be discussed is nodes that takes discrete values. The values should be both mutually exclusive and exhaustive, which means that the variable must take on exactly one of these values at a time. Common types of discrete nodes include:

- Boolean nodes, which represent propositions, taking the binary values true(*T*) and false (*F*). In a medical diagnosis domain, the node *Cancer* would represent the proposition that a patient has cancer.
- Ordered values. For example, a node *Pollution* might represent a patient's pollution exposure and take the values {*low, medium, high*}.
- Integral values. For example, a node called *Age* might represent a patient's age and have possible values from 1 to 120.

### 2.6.2 Structure

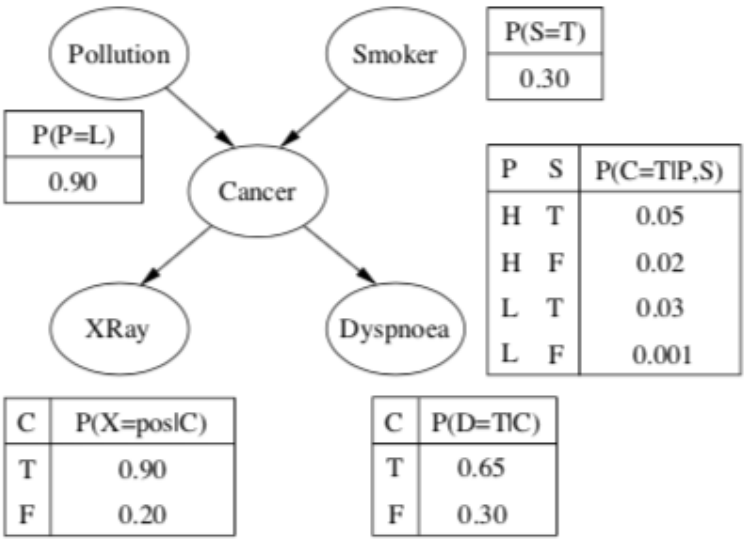



*Figure 2. 12 Bayesian Network Structure*
*Source: Introduction of Bayesian Network Book*

Structure or topology of Bayesian Network (BN) should capture qualitative relationships between variables (nodes). Nodes should be connected directly if one affects or causes the other, with the arc indicating the direction of the effect. It is useful to employ a family metaphor For Bayesian Network (BN) structure. This family metaphor is

well known used in creating Bayesian Network (BN) structure. Parent node is a node where the arc are coming from towards the other node. Child nodes are the nodes of which the direction of the arc of parent nodes are headed. Extending the metaphor if there is a directed chain of nodes, one node is an ancestor of another if it appears earlier in the chain, whereas a node is a descendant of another node if it comes later in the chain. Any other terminology used is root node and leaf node. any node without parents is called a root node, while any node without children is called a leaf node. Any other node (non-leaf and non-root) is called an intermediate node. Given a causal understanding of the BN structure, this means that root nodes represent original causes, while leaf nodes represent final effects.

Figure 2.7 show an example of Bayesian Network (BN) structure. Cancer node has two parents, Pollution and Smoker, while Smoker is an ancestor of both X-ray and Dyspnoea. Similarly, X-ray is a child of Cancer and descendant of Smoker and Pollution. The set of parent nodes of a node X is given by Parents(X). Using the root and leaf terminology, for figure 2.7 Pollution and Smoker are root nodes, while the effects X-ray and Dyspnoea are leaf nodes

### 2.6.3 Bayesian Network Reasoning

How Bayesian Network (BN) reason with the domain after it is presented in a structure is a fundamental thing to do in creating Bayesian Network (BN) structure. When observing the value of some variable, it needs to be conditioned upon the new information. The process of conditioning also called probability propagation or inference or belief updating is performed via a flow of information through the network. Note that this information flow is not limited to the directions of the arcs. In our probabilistic system, this becomes the task of computing the posterior probability distribution for a set of query nodes, given values for some evidence or observation nodes. Bayesian networks provide full representations of probability distributions over their variables. That implies that they can be conditioned upon any subset of their variables, supporting any direction of reasoning.

There are several types of reasoning of Bayesian Networks (BN) structure. For example, one can perform diagnostic reasoning from symptoms to cause, such as when a doctor observes *Dyspnoea* and then updates his belief about *Cancer* and whether the patient is a *Smoker*. Note that this reasoning occurs in the *opposite* direction to the network arcs.

The other type is predictive reasoning. This style of reasoning works from new information about causes to new beliefs about effects, following the directions of the network arcs. For example, the patient may tell his physician that he is a smoker; even before any symptoms have been assessed, the physician knows this will increase the chances of the patient having cancer. It will also change the physician's expectations that the patient will exhibit other symptoms, such as shortness of breath or having a positive X-ray result.

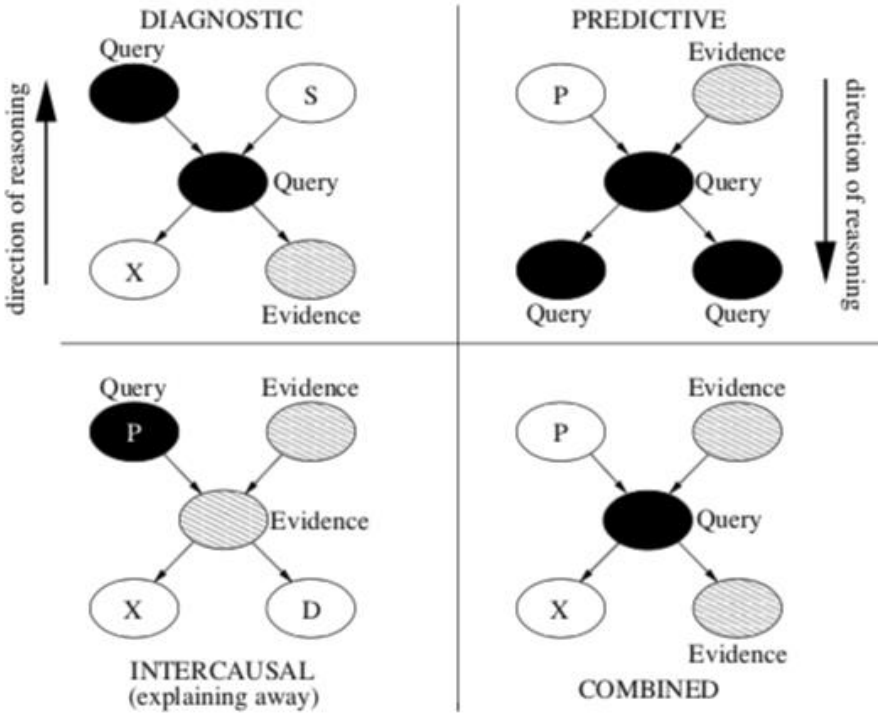



Figure 2. 13 Types of reasoning
*Source: Introduction of Bayesian Network Book*

## 2.7 Sensitivity Analysis

Sensitivity Analysis is the study of how the uncertainty in the output of a model (numerical or otherwise) can be apportioned to different sources of uncertainty in the model input (Saltelli et al., 2004). Sensitivity Analysis is essentially a measure of how responsive the output of a model is to variations in the inputs. A model tested can be divided into 2 categories diagnostic and data driven.

### 2.7.1 Entropy-based sensitivity analysis

Entropy is a well-known function in the theory of information, which indicates the loss of information within a system then, by opposition, the amount of information. The *entropy* of a discrete random variable $X$ ranging in $x_1,\ldots,x_n$ with respective probabilities $p_1,\ldots,p_n$

$$H(X) = -\sum_{k=1}^{n} p\kappa \ln(p\kappa) \qquad 2.10$$

Entropy is a term used in information technology and can be regarded as an indicator of how disordered a dataset is. Entropy is described as a value that, when increased, can be interpreted as increase in uncertainty of a dataset which would then require more information (Auder & looss, 2009). Entropy stands for a global measure of influence, whereas variance only takes into account second-order moments, we can think entropy as a complement to the variance measure: entropy-based indices will more likely be used to complete or precede an analysis using variance.

# CHAPTER III

# RESEARCH METHODOLOGY

## 3.1 General

A structured process in making this research is necessary in order to make the processed easier and more directed. In this chapter step by step of the preparation of the Novel Flexible Model for Piracy and Robbery Assessment for Port Tanjung Perak will be explained.

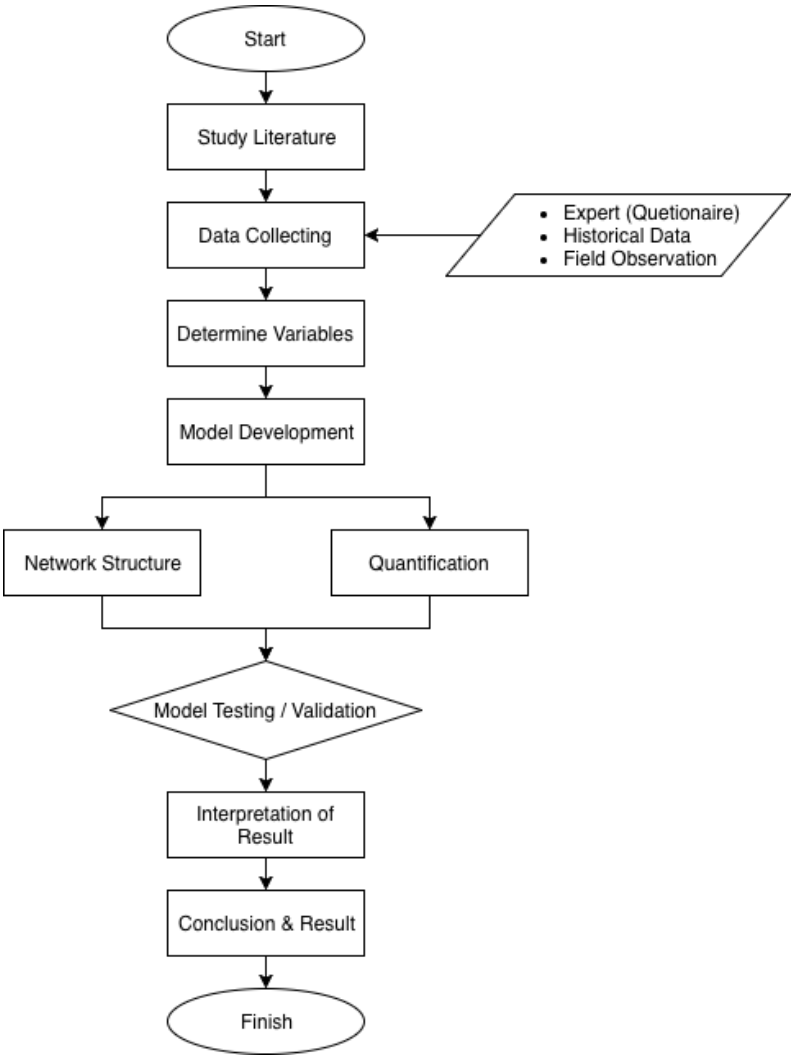



*Figure 3. 1 Research Methodology Flowchart*

## 3.2 Study Literature

Study literature in this research aims to prepare the author to understand the theory and explore all other supporting information related to this research. It will help the author to understand the problem and able to create a systematic identification of what factors can leads to successful piracy and robbery attack of which it will be set in scenarios.

## 3.3 Data Collecting

The next step is data collecting. Data will be collected from field observation in Port Tanjung Perak includes factors influencing the occurrence likelihood of successful hijacking of a ship obtained from consultation and questionnaire from experts on piracy/robbery threats (Experts in this study will be ship's captain and port manager), data statistic of ships and piracy attack in Port Tanjung Perak, piracy attack characteristics, etc.

## 3.4 Determine Variables

After data gathered, data will be analysed and processed. All the data will be analyze to determine relationships on which the initial "cause and effect" diagram could be based. Later this data (variables) will be compiled to form scenarios (network scenario) in the next step.

## 3.5 Model Development

After relationship of each data determined network structure (scenarios) will be created based on data collected. Quantification from expert opinions will be weighted to make conditional probability table.

## 3.6 Model Testing / Validation

After Bayesian network structure with each probability is determined, sensitivity analysis will be used to provide a degree of confidence that the model has been built correctly and is working as intended using NETICA Software.

## 3.7 Interpretation of Result

After model created is working, the simulation results are analysed to determine the best scenario that leads to successful attacks. From this scenario, improvements can be addressed more effectively to reduce number of piracy and robbery attacks.

## 3.8 Conclusion and Suggestion

Conclusion in this research will later answer the problem formulation and is a point to find out whether or not the objective of this final project is achieved. The advice given later is a proposal to improve the existing security protection (recommendation) and will be used as a suggestion for further research to correct errors, weaknesses, and shortcomings in the research in this final project.

"This page intentionally left blank"

# CHAPTER IV

# ANALYSIS AND DISCUSSION

## 4.1. General Description

Security Assessment in this research will be done by using Bayesian network to analyse which variable leads to the success of piracy and robbery attack in a port. The port assessed in this research is Port Tanjung Perak, Surabaya. This chapter will discuss in detail steps of creating security assessment, starting with determining data required, hypothesis of variables using fishbone diagram based on literature study, data collecting, data processing, creating Bayesian network model, model testing or validation, and recommendation for the accident based on simulation result of the model. An illustration of steps in creating Bayesian Network in this study is shown in figure

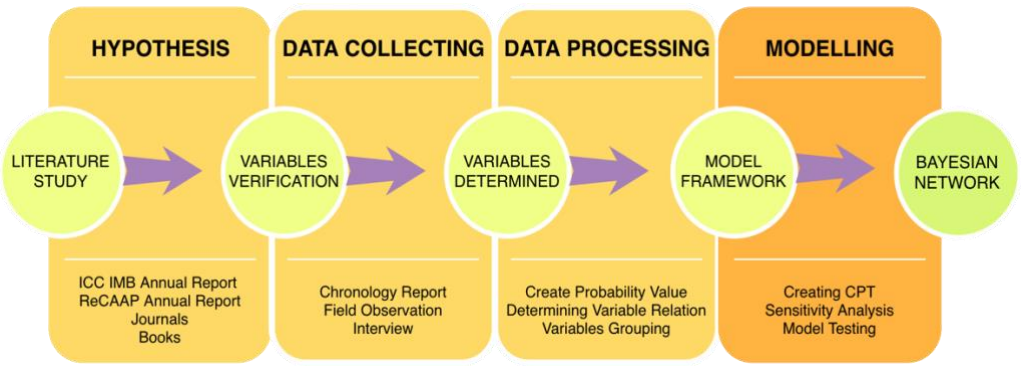



*Figure 4. 1 Steps in Creating Bayesian Network*

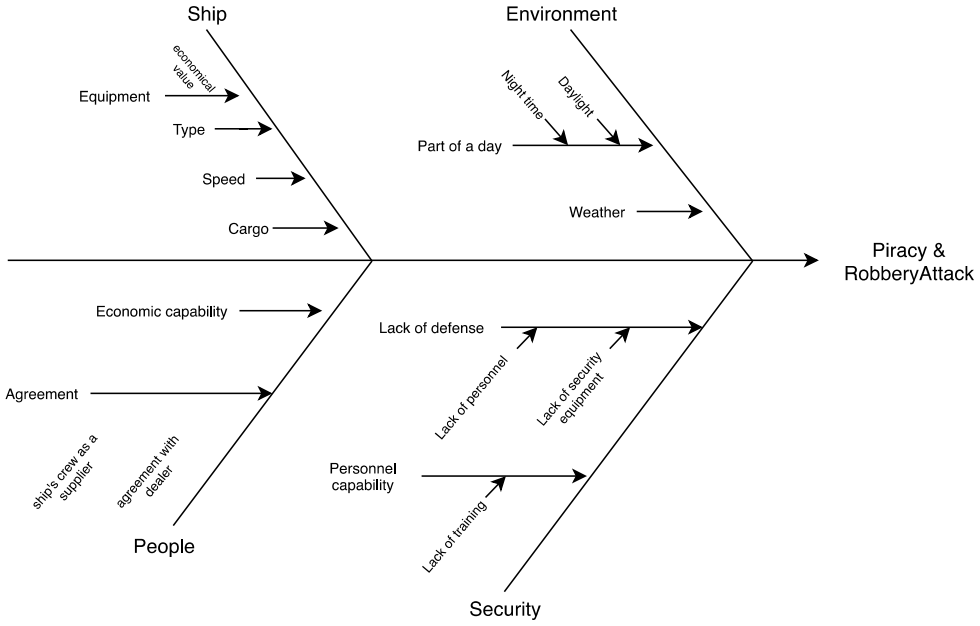
## 4.2. Hypothesis of Variables causing Piracy and Robbery

Before conducting the data collecting, study literature is done to provide knowledge and degree of confidence of the piracy and robbery characteristics. Study literature also give the writer an insight of data that must be collected to create Bayesian network. In this step, a hypothesis is made based on paper, journals, and books published discussing piracy and robbery attacks review. An assumption or a hypothesis is done to ease the data collecting process due to limited amount of time available for research. This hypothesis later will be verified in based on data collected. Hypothesis of variables contributes to the attack is made using

fishbone diagram. Fishbone diagram which also known as cause and effect diagram is one of methods to identifies potential causes according to the level of importance of a problem or an effect. The causes is categorized by groups. It enables brainstorming process to creates and covers all the potential causes in a structured diagram. A fishbone diagram consists of:

- Head of fish that represent the effect or the outcome
- 1st level of Horizontal branches that represent main causes
- Sub-branches that represent secondary causes or reasons of the 1st horizontal branches.
- 2nd level of Horizontal branches that represent the reasons or the cause for sub-branches.

Based on study literature done, a hypothesis of variables causing piracy and robbery attack in fishbone diagram is represented in Figure




4.1

*Figure 4. 2 Fishbone Diagram of Piracy and Robbery Attack*

## 4.3. Data

Data collected will be used as a verification for the hypothesis of potential causes made and as an input to create Bayesian network for security assessment of a port, in this case Tanjung Perak Port. The data needed are as follow:

1. Number of attacks

Number of attacks happen in the assessed port will be used to create probability of attack of piracy and robbery in Bayesian network. Figure 4.3 shows number of reported piracy and robbery attack in Port Tanjung Perak in the recent 5 years period based on data collected from Pelindo III, Harbour Master, and Polair Tanjung Perak.

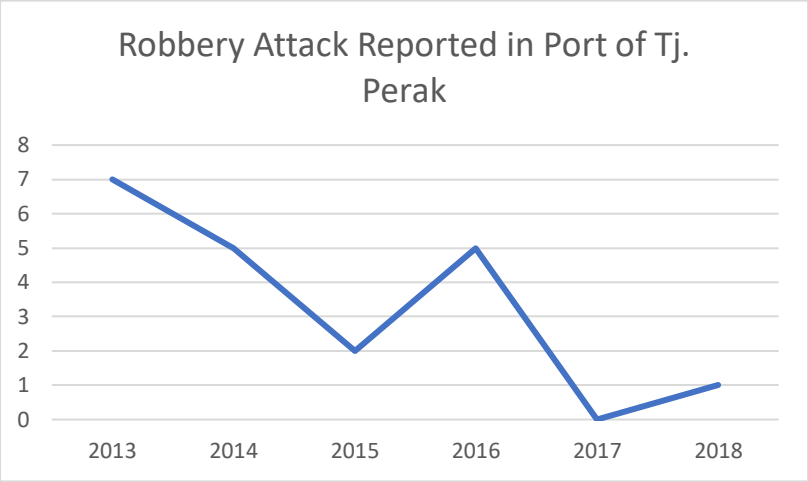



*Figure 4. 3 Number of piracy and robbery attack in Port tanjung Perak*

2. Chronology of the attack

Chronology of piracy and robbery attack report will be used as a verification of hypothesis made and also to create Bayesian Network of piracy and robbery attack. Variables or causes of the attack will be listed based on chronology reports. Chronology of the attack is collected from Polair, Harbour Master, and Pelindo III. Table 4.1 present an example of chronology of the piracy and robbery attack in the recent 5 years period. A more detail chronology report of attack will be presented in attachment

*Table 4. 1 Example of Chronology of attack obtained*

| 2013 | | | |
|---|---|---|---|
| No | Date | Evidence | Chronology |
| 1 | Wednesday, October 3 2013 | crane accessories, hammer, motor | 11 The perpetrators of theft at the Port of Tanjung Perak, Surabaya, East Java were arrested. In each action, these perpetrators use trucks to transport stolen goods that are |

| | | | |
|---|---|---|---|
| | | | carried on the boat. the crime mode carried out by the perpetrators, during the day the suspects conducted a survey first in the target location. After getting the target, the perpetrator took the sack to transport the stolen goods.<br>"In the evening, the perpetrators took the items they were targeting, then transported them in L 8090 WJ trucks, and then sold them on Jalan Tambak Mayor. |

4.4. Data Analysis

4.4.1. Factor Analysis

After all of the data gathered, an analysis will be done to verified hypothesis that has been done. Based on a thorough analysis of the report of attack chronology, factors influencing the occurrence likelihood of successful attack of piracy and robbery in the area of Port of Tanjung Perak are identified. Codes will be used to ease identification of factors influencing the attack on the gathered report. This code is provided based on the hypothesis made from fishbone diagram.

*Table 4. 2 Factors Influencing Attack*

| | | |
|---|---|---|
| E. Value | E1 | Equipment |
| | E2 | Cargo |
| Position | S1 | Anchoring |
| | S2 | Sailing |
| Part of Day | D1 | Daylight |
| | D2 | Nightime |
| Weather | W1 | Poor |
| | W2 | Moderate |
| | W3 | Good |
| Defence | N1 | Personnel |
| | N2 | Equipment |
| Capability | C1 | Trained |
| | C2 | Untrained |
| Situation | G1 | Guarded |

| | | |
|---|---|---|
| | G2 | Unguarded |

Each one of this factor will be explained and categorized into 3 major categories based on its influence and relation with one another. This categorization will ease the process and enable a structured process to create Bayesian Network.

4.4.1.1. Economical Value

Most of the robbery attack in Port of Tanjung Perak in terms of economic value occurs either due to the economic value of cargo carried by the ship or the economic value of ship equipment. This two things are the most targeted by robbers based on the chronology report. According to the results of interviews with several parties who have handled theft cases, the stolen goods will be resold. Therefore, the target of theft is usually goods that have a high selling value and are easy to resell.

4.4.1.2. Position

Position referred to in this research is the position of the ship when the attack occurs. Based on the report gathered and used in this research, most of the attack happen is classified into 2 categories. The first one is when the ship is berthing or anchoring at the port. During this position, the robbers do not need an extra transportation such as boat to accommodate the robbers to the crime location. They usually pass the guard by camouflage themselves as TKBM. The number of piracy and robbery attack happen during berthing or anchoring is higher than the second category. The second categories is when the ship is in sailing condition. The robbers usually used a fast boat to accommodate them to the targeted ship. And then they will climb the hull of the ship and sneaked themselves to the targeted object.

4.4.1.3. Part of a Day

The time of piracy and robbery attacks in Port of Tanjung Perak follow a pattern according to the obtained reports. Generally speaking, there were more incidents during the day time than the ones in the night time. This reason could be due to the visibility in this hour is better than night time. Also, the humidity level during this hour is low which will impact the on-duty guard to lower their vigilance due to inconveniences of the environmental condition. The day time in the studied is from 6 am to 6 pm.

4.4.1.4. Weather

The weather condition in this studied region varies from Clear to Thunderstorm. Weather data condition is gathered from Accuweather.com based on the chronology of the attack. Based on the varied weather, it then classified into 3 major categories. The first categories are poor. This category of weather condition consists of thunderstorm, light rain overcast. The second category is moderate. This category of weather condition consists of passing cloud and overcast. And the last category is good. This category of weather condition consists of partly sunny, scattered cloud and clear. Most of the attack in this region is happen during good weather condition. The humidity level of most attack ranges from 58 to 87 and the velocity of the wind obtained from barometer report range from 1008 to 1013.

4.4.1.5. Defence

Defence in this research refer to the lack of defence in the studied region. Lack of defence divided into 2 categories namely lack defence of personnel and lack defence of security equipment. This category is provided refers to the International Ship and Port Facility Security (ISPS) Code requirements. Based on analysis it was found that lack defence of security equipment influence the likelihood of attack the most. Based on interview, it is because most of the robber sneaked their way in the location where it is not possible for personnel stand guard. Also, from the robber perspectives they consider that if there is no security equipment then it will leave the action to be well execute because there will be no records of their crime. They consider the security equipment as an alarm for the guard.

4.4.1.6. Capability

Capability of the guard is also one of the main requirements of International Ship and Port Facility Security (ISPS) Code. Therefore, an analysis of the condition of this factor and its relation to the attack is an important factor. An analysis of this factors is based on the report provided from Harbour Master of Port of Tanjung Perak. Based on analysis the capability is divided into 2 categories namely trained and untrained. And most of the attack happened if the capability of the guard is untrained. The parameter of this variable is affected by the number of exercises, drill, training, inspection, and number of findings.

4.4.1.7. Situation

The situation in this study refer to weather the environment is guarded or unguarded. This category is based on the compliance of the port facility from the assessment done by Harbour Master of Port of Tanjung Perak. Guarded is the condition when the port facility situation is compliance to the International Ship and Port Facility Security (ISPS) Code standards. Due to the compliance of the port facility to the International Ship and Port Facility Security (ISPS), the port is categorized as guarded because there are numbers of security requirements needs to be fulfilled to get a good grade of International Ship and Port Facility Security (ISPS) Code. And for the unguarded situation corelates with the non-compliance found by Harbour Master during assessment in regards to International Ship and Port Facility Security (ISPS) Code. Based on analysis from Harbour Master report, we found that majority of the facility in the Port of Tanjung Perak has already comply to International Ship and Port Facility Security (ISPS) Code. But there is still numbers of non-compliance found regarding International Ship and Port Facility Security (ISPS) Code.

4.4.1.8. Compliance

The compliance in this research refers to the compliance of the ship entering the port facility. In this research, the correlations of the ship compliance to the robbery attack is analysed based on the report gathered from Harbour Master Tanjung Perak. Based on the report, 90% of the ship entering Port of Tanjung Perak is incompliance with the International Ship and Port Facility Security (ISPS) Code. An example case of analysis using this code is shown on table 4.3.

*Table 4. 3 An Example of Chronology Report Analysis using code developed*

| 2013 | | | | |
|---|---|---|---|---|
| No | Day, Date | Evidence | Report | Keywords |
| 1 | Wednesday, 3rd October | crane accessories, hammer, motor | 11 The perpetrators of theft at the Port of Tanjung Perak, Surabaya, East Java were arrested. In each action, these perpetrators use trucks to transport stolen goods that are carried on the boat. the | E1 |
| | | | | S2 |
| | | | | D2 |
| | | | | W3 |
| | | | | P2 |
| | | | | N2 |
| | | | | C1 |

| | | | | |
|---|---|---|---|---|
| | | | crime mode carried out by the perpetrators, during the day the suspects conducted a survey first in the target location. After getting the target, the perpetrator took the sack to transport the stolen goods.<br>"In the evening, the perpetrators took the items they were targeting, then transported them in L 8090 WJ trucks, and then sold them on Jalan Tambak Mayor. | G1 |

Table 4.3 present an example of chronology report analysis using the code developed in this study. The characteristics of each case is analysed thoroughly using the code. From this coding system, the probability value of each code obtained. Later, this value will be processed to create Bayesian Network Model. The full table of chronology report analysis using code is attached.

4.4.2. The Making of Probability Value

Probability in general can be interpreted as a mathematical measure of the tendency for an event to occur. Mathematically the opportunity has a range of values from 0 to 1. The opportunity value 0 means that the occurrence of the event is very unlikely, and the opportunity value 1 means that the event must have appeared. The opportunity value can also be between the two absolute values above, or in other words the opportunity value will appear between the expected results and unexpected results (Artana, 2013). In the context of this research study these two absolute conditions are attack and no attack.

To create the probability value for states in each node mentioned above, code is created to analyse the report of the attack. The attached code on table 4.2 is used for each case. Then, the code is processed into a table. If each state in the same node are added up the total probability value is 1. An example of making probability value for each node will be explained briefly in this section. In creating the probability value for nodes economic value, position, part of a day, and defence the report and

statistics used are obtained from Pelindo and Polair. For capability and situation nodes the report and statistics used are obtained from Harbour Master. And for weather node the verification and analysis of the weather condition during the day of the attack is based on Accuweather's website. Detailed table of probability value for each state is attached on attachment.

4.4.2.1. Economical Value

Economical value consists of 2 states which are cargo and ship's equipment. The probability value of both of this category is obtained from an analysis report analysis. Based on the analysis, it was found that there are 9 accident out of 13 accident happens of the stolen goods is equipment of the ships. And there are 4 accident out of 13 accident happen of which the stolen goods is the cargo of the ship. The probability value of cargo and equipment respectively are 0.30769231 and 0.69230769.

4.4.2.2. Position

Using the same method as economical value, the probability value in this category for the anchoring and sailing condition of the ship based on the analysis respectively are 0.53846154 and 0.46153846.

4.4.2.3. Part of a Day

This category is divided into 2 states which are daylight and night time. Based on the analysis, number of attacks happening from 2013-2018 during daylight period is 7. In total, there are 12 accidents of stated time period of the attack in the report. Therefore, the probability value of daylight is 0.58333333. For the night time, there are total bu5 accident out of 12 accident based on detail statement of the time of the attack during this hour. The probability value of night time is 0.41666667. To be noted that the total probability value of daylight and night time if we add up is 1.

4.4.2.4. Weather

Weather condition category consist of 3 states which are poor, moderate, and good. Based on the analysis most of the attack is happening during moderate weather condition, then it should be the probability value of this state is higher than the other two states. In total there are 6 accident happens during this weather condition. For the states

good there are 4 accident happens during this weather condition, and for the last state there are 2 accident happens during this weather condition. Probability value of each states good, moderate, and poor respectively are 0.38461538; 0.46153846; and 0.15384615. With the total sum of this three states are 1.

4.4.2.5. Defence

Using the same method as the other category, the probability value of states in this category are 0.28571429 for the personnel and 0.71428571 for the equipment.

4.4.2.6. Capability

For this category the making probability value is quite different from the other categories due to the report used to make this probability is obtained from Harbour Master. Based on the report, a statistical number is obtained and then analyse to fit with the aim of this study. In this category, the probability value of the states is the opposite of the statistic obtained. It is caused by the characteristic of the states. The more trained the security officer and the environment, the less probability value that the attack will happen. Probability value of the states trained and untrained are 0.32090909 and 0.67909091.

4.4.2.7. Situation

In this category the same method used in capability category is used to create probability value for the states. This category consists of guarded and unguarded states. Probability value for each state guarded and unguarded are 0.10209899 and 0.89790101 respectively.

4.4.2.8. Compliance

As stated earlier in this chapter, this category refers to the compliance of the ship entering port facility. Based on statistic report gathered from Harbour Master. Number of ship incompliance with International Ship and Port Facility Security (ISPS) Code regulation for ship with international voyage is a lot more than the ship which are not incompliance with the regulation. For the probability value of state in this category is using the same characteristics with the capability and situation category. Therefore, the value for states comply and non-comply are 0.05172414 and 0.94827586 respectively.

## 4.5. Arrangement of Category

After all of the probability value of each states in every category is defined, the next step is grouping the categories into Bayesian Network node. For this study, all of the 8 categories mentioned in the previous chapter is defined as a parent node or the first level of Bayesian Network. All of the 8 parent nodes will be grouped into 3 categories for the next level of node for Bayesian Network in this study. In this second level the categories are Ship, Environment, and Security. Based on analysis the second level of node for Ship category consist of Economical Value, Compliance and Position. For category Weather and Part of a Day is grouped into Environment category. And for Security category consist of Defence, Capability and Situation.

*Table 4. 4 Variables Grouping*

| | |
|---|---|
| Ship | Economical Value |
| | Compliance |
| | Position |
| Environment | Weather |
| | Part of a Day |
| Security | Defense |
| | Capability |
| | Situation |

## 4.6. Conditional Probability Table

After all the nodes are being grouped, the next step is creating conditional probability table for this node. There are several ways in creating Bayesian Network (BN) Conditional Probability Table (CPT). In this research study the equation used is The Weighted Sum Algorithm. This method of calculation is an equation derived from paper called Generating Conditional Probabilities for Bayesian Network: Easing the Knowledge Acquisition Problem (Das, 2004). This method is used due to the required Conditional Probability Table (CPT) required by software used in this research study (NETICA Software) are a simplified CPT.

To start the calculation for Conditional Probability Table for the $2^{nd}$ Level Nodes namely Ship, Environment, and Security each parent nodes were weighted equally. Example of the calculation for $2^{nd}$ level node will

be presented. In this chapter, the calculation of Conditional Probability Table for node Ship is used as an example.

As stated in the previous paragraph, each parent nodes for Environmental nodes will weighted equally. Environmental node consists of 2 parent nodes Part of a Day, and Weather with the relative weights 1/2 for each nodes. Based on the software used, it specifies the Conditional Probability Table is 5x2 configurations due to combination for states of each nodes shown in Table 4.5

*Table 4. 5 Environment CPT required by NETICA Software*

| Environment | | Yes | No |
|---|---|---|---|
| Daylight | Poor | | |
| Daylight | Moderate | | |
| Daylight | Good | | |
| Nightime | Poor | | |
| Nightime | Moderate | | |
| Nightime | Good | | |

After that continue the next step to added up the weighted nodes to get the probability result. The example of the calculation is presented in equation

$$P(Yes|Daylight, Poor) = \frac{Daylight}{2} + \frac{Poor}{2} \quad 4.1$$

$$P(Yes|Daylight, Poor) = \frac{0.5833}{2} + \frac{0.1538}{2} \quad 4.2$$

$$P(Yes|Daylight, Poor) = 0.3685 \quad 4.3$$

Based on that process done for each combination, the conditional probability table for Environment node obtained. Table 4.6 present the calculation result.

*Table 4. 6 Calculation result for CPT of Environment node*

| Environment | | Yes | No |
|---|---|---|---|
| Daylight | Poor | 0.36858974 | 0.63141026 |
| Daylight | Moderate | 0.5224359 | 0.4775641 |
| Daylight | Good | 0.48397436 | 0.51602564 |
| Night time | Poor | 0.28525641 | 0.71474359 |

| | | | |
|---|---|---|---|
| Night time | Moderate | 0.43910256 | 0.56089744 |
| Night time | Good | 0.40064103 | 0.59935897 |

Using the same methods, Conditional Probability Table (CPT) for Security and Ship Node were obtained. The result of Conditional Probability Table (CPT) calculation of Security and Ship node presented in Table 4.7 and Table 4.8 respectively.

*Table 4. 7 Calculation Result for CPT of Security node*

| Security | | | Yes | No |
|---|---|---|---|---|
| Personnel | Trained | Guarded | 0.76375921 | 0.23624079 |
| Personnel | Trained | Unguarded | 0.49849187 | 0.50150813 |
| Personnel | Untrained | Guarded | 0.64436527 | 0.35563473 |
| Personnel | Untrained | Unguarded | 0.37909793 | 0.62090207 |
| Equipment | Trained | Guarded | 0.62090207 | 0.37909793 |
| Equipment | Trained | Unguarded | 0.35563473 | 0.64436527 |
| Equipment | Untrained | Guarded | 0.50150813 | 0.49849187 |
| Equipment | Untrained | Unguarded | 0.23624079 | 0.76375921 |

*Table 4. 8 Calculation Result for CPT of Ship node*

| Ship | | | Yes | No |
|---|---|---|---|---|
| Equipment | Anchoring | Comply | 0.42749779 | 0.57250221 |
| Equipment | Anchoring | Non Comply | 0.72634836 | 0.27365164 |
| Equipment | Sailing | Comply | 0.40185676 | 0.59814324 |
| Equipment | Sailing | Non Comply | 0.70070734 | 0.29929266 |
| Cargo | Anchoring | Comply | 0.29929266 | 0.70070734 |
| Cargo | Anchoring | Non Comply | 0.59814324 | 0.40185676 |
| Cargo | Sailing | Comply | 0.27365164 | 0.72634836 |
| Cargo | Sailing | Non Comply | 0.57250221 | 0.42749779 |

After all the result for Conditional Probability Table (CPT) for nodes Environment, Security, and Ship were obtained we proceed to the next step to insert the calculation result to the NETICA software. After inserting the calculation result then the average probability for each state of the nodes Environment, Security, and Ship were presented in Table 4.9.

*Table 4. 9 Probability of States in NETICA Software*

| Attack | | |
|---|---|---|
| Security | Yes | 0.342 |
| | No | 0.658 |
| Ship | High Risk | 0.66 |
| | Low Risk | 0.34 |
| Environment | Poor | 0.449 |
| | Favorable | 0.551 |

Based on that value, using the same method the Conditional Probability Table (CPT) for Attack node can be done. And from the calculation, the result is presented in Table 4.10.

*Table 4. 10 Calculation Result for CPT of Attack nodes*

| Attack | | | Yes | No |
|---|---|---|---|---|
| Yes | High Risk | Poor | 0.48366667 | 0.51633333 |
| Yes | High Risk | Favourable | 0.51766667 | 0.48233333 |
| Yes | Low Risk | Poor | 0.377 | 0.623 |
| Yes | Low Risk | Favourable | 0.411 | 0.589 |
| No | High Risk | Poor | 0.589 | 0.411 |
| No | High Risk | Favourable | 0.623 | 0.377 |
| No | Low Risk | Poor | 0.48233333 | 0.51766667 |
| No | Low Risk | Favourable | 0.51633333 | 0.48366667 |

## 4.7. Bayesian Network

After all of the calculation for Conditional Probability Table (CPT) is done, the next step is to insert the calculation Conditional Probability Table (CPT) to the NETICA Software. And the result of Bayesian Network model is presented in Figure 4.3. After the model is finished, the next step is to do sensitivity analysis.

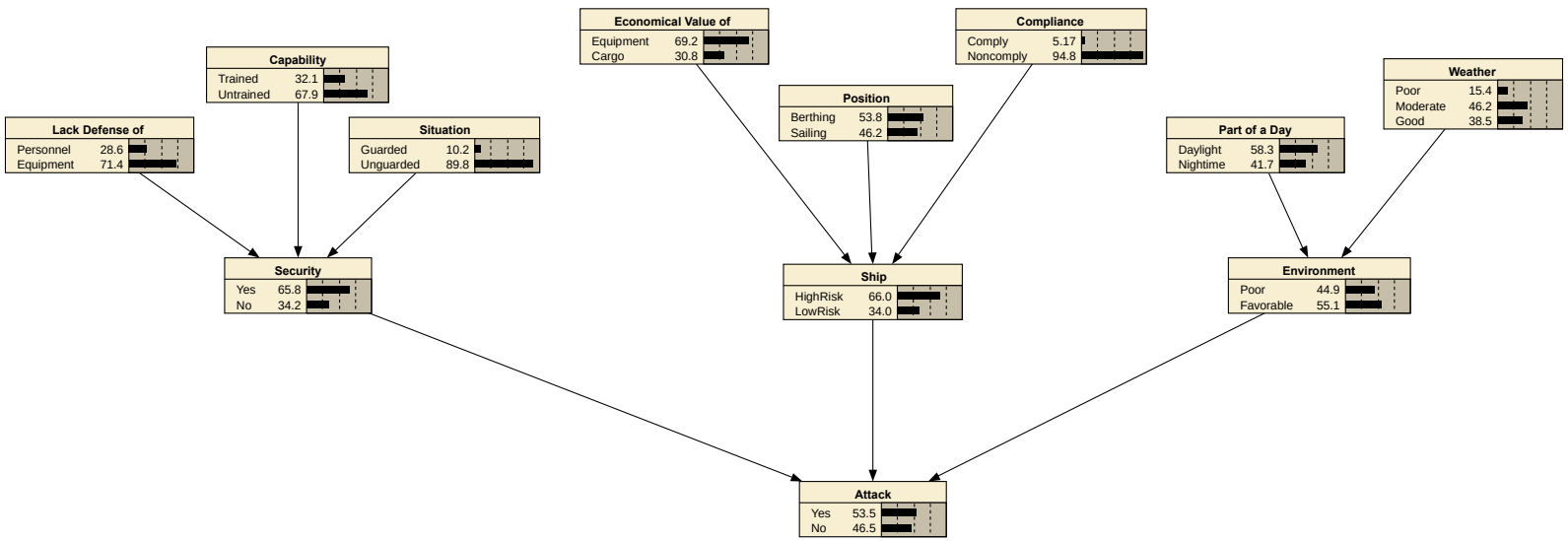



*Figure 4. 4 Bayesian Network Model Created*

## 4.8. Sensitivity Analysis

Sensitivity Analysis is done to measure how responsive the model created to variations in the inputs (parent nodes). Software used to do Sensitivity Analysis for the Bayesian Network (BN) model that has been created is NETICA Software. Due to the use of this model is to study which variable that is more likely cause an attack, therefore node attack is tested using sensitivity to findings tools in NETICA Software. The result of sensitivity of findings of node attack is presented on Figure 4.5

| Sensitivity Analysis | |
|---|---|
| Node | Entropy Reduction (%) |
| Attack | 100 |
| Ship | 74.3 |
| Security | 72.7 |
| Environment | 8.32 |
| Situation | 2.08 |
| Compliance | 1.45 |
| Lack Defence | 1.34 |
| Economical Value | 1.16 |
| Capability | 1 |
| Weather | 0.0921 |
| Part of a Day | 0.0563 |
| Position | 0.0545 |

*Figure 4. 5 Sensitivity Analysis of Node Attack*

Figure 4.5 present the result of sensitivity analysis for variable "Attack" using the term entropy reduction in percent. An increasing value of entropy indicates increasing uncertainty of dataset of which will require more direction in order to describe the data. For the result shown on Figure 4.5 the entropy reduction value of node Attack is 100% showing that the node is working properly as intended. Value of node Attack is 100% "uncertain" as it is affected by the value of its parent nodes; Ship, Security, and Environment. Comparing the result value of sensitivity analysis of each parent nodes, node Ship has the highest value. It indicates that the node Attack is affected significantly by a slight changes of node Ship. For that reason, a Sensitivity Analysis using sensitivity of findings tools in NETICA Software were done for each of nodes Security,

Ship and Environmental. The result is shown in Figure 4.6, Figure 4.7 and Figure 4.8

| Sensitivity Analysis | |
|---|---|
| Node | Entropy Reduction (%) |
| Ship | 100 |
| Compliance | 14.2 |
| Economical Value | 11.9 |
| Attack | 8 |
| Position | 0.567 |
| Security | 0 |
| Situation | 0 |
| Capability | 0 |
| Defence | 0 |
| Environment | 0 |
| Weather | 0 |
| Part of a Day | 0 |

*Figure 4. 6 Sensitivity Analysis Node Ship*

Figure 4.6 present the result of sensitivity analysis for variable "Ship" using the term entropy reduction in percent. Node Ship was first analysed due to previous finding of Sensitivity Analysis for node Attack that it causes the highest changes to the value of node Attack. For the result shown on Figure 4.6 the entropy reduction value of node Ship is 100% showing that the node is working properly as intended. Value of node Ship is 100% "uncertain" as it is affected by the value of its parent nodes; Compliance, Economical Value, and Position. Comparing the result value of sensitivity analysis of each parent nodes, node Compliance has the highest value. It indicates that the node Ship is affected significantly by a slight changes of node Compliance.

| Sensitivity Analysis | |
|---|---|
| Node | Entropy Reduction (%) |
| Security | 100 |
| Situation | 21 |
| Defence | 14.1 |
| Capability | 10.6 |

| | |
|---|---|
| Attack | 7.81 |
| Ship | 0 |
| Compliance | 0 |
| Position | 0 |
| Economical Value | 0 |
| Part of a Day | 0 |
| Weather | 0 |
| Environment | 0 |

*Figure 4. 7 Sensitivity Analysis Node Security*

Sensitivity Analysis were also done to each parent nodes of node Attack to find which root nodes affect the analysed node the most so that recommendation can be proposed. For the third Sensitivity Analysis node Security was analysed using the same method as the previous analysis. Figure 4.7 present the result of sensitivity analysis for variable "Security" using the term entropy reduction in percent. The result in Figure 4.7 shown the entropy reduction value of node Security is 100% showing that the node is working properly as intended. Value of node Security is 100% "uncertain" as it is affected by the value of its parent nodes; Situation, Defence, and Capability. Comparing the result value of sensitivity analysis of each parent nodes, node Situation has the highest value. It indicates that the node Security is affected significantly by a slight changes of node Situation.

| Sensitivity Analysis | |
|---|---|
| Node | Entropy Reduction (%) |
| Environment | 100 |
| Weather | 8.17 |
| Part of a Day | 4.97 |
| Attack | 0.836 |
| Ship | 56.7 |
| Compliance | 0 |
| Position | 0 |
| Economical Value | 0 |
| Security | 0 |
| Situation | 0 |
| Capability | 0 |

| Defence | 0 |
|---|---|

*Figure 4. 8 Sensitivity Analysis Node Environment*

To provide a second statement of Sensitivity Analysis obtained from NETICA Software and discover which states in the root nodes cause a significant change to the child nodes, the author tried to change the value of each states for each nodes Attack, Ship, Security and Environment to the maximum percentage and compare the result before and after the changes. The result is shown in form of table from Table 4.11 to Table 4.14

Note:

Indicates the states with the highest changing in the same node

Indicates the nodes with the highest sum up value of changing

*Table 4. 11 Comparation of changing for node Attack*

| Attack | | | | | |
|---|---|---|---|---|---|
| Yes | Note | | | | Difference |
| | Parent Nodes | PN States | Before | After | |
| 100 | Security | Yes | 34.2 | 29.8 | 4.4 |
| | | No | 65.8 | 70.2 | 4.4 |
| | Ship | High Risk | 66 | 70.4 | 36.5 |
| | | Low Risk | 34 | 29.5 | 9.4 |
| | Environment | Poor | 44.9 | 43.4 | 11.7 |
| | | Favourable | 55.1 | 56.6 | 1.5 |

Table 4.11 present the comparation result by changing the value of "Yes" in node attack to its maximum of 100 from a scale 0-100. By changing the value of attack from 53.5 to 100 create changes for the value of its parent nodes; Security, Ship, and Environment. The before and after value due to maximizing "Yes" of the node attack is shown. Based on the result obtained, node Security both of the states had the same difference value, meaning that both of the states equally change the value of node Ship. For node Ship and Environment shown a different result. States High Risk of node Ship has higher difference value, meaning a slight change of its value affect node Ship significantly. The same situation occurs on the node Environment. States Poor shows higher difference value than Favourable, meaning that a slight change of its value affect node Environment significantly. The table highlight node Ship with an orange

shade. This indicates that node Ship create a more significant change to the node Attack. It is found by comparing the total difference for each state in the same node to the other parent nodes. This experiment result provided a second statement that node Ship has the highest significant influence to node Attack.

*Table 4. 12 Comparation of changing for node Ship*

| Ship | | | | | |
|---|---|---|---|---|---|
| High Risk | Note | | | | Difference |
| | Parent Nodes | PN States | Before | After | |
| 100 | E. Value | Equipment | 69.2 | 73.4 | 4.2 |
| | | Cargo | 30.8 | 26.6 | 4.2 |
| | Position | Anchoring | 53.8 | 54.8 | 1 |
| | | Sailing | 46.2 | 45.2 | 1 |
| | Compliance | Comply | 5.17 | 2.95 | 2.22 |
| | | Non Comply | 94.8 | 97 | 2.2 |

Because the node Ship was found having the highest influence to node Attack, the same experiment that previously done to node Attack is also done to this node before the other parent node. Table 4.12 present the comparation result by changing the value of "High Risk" in node Ship to its maximum of 100 from a scale 0-100. By changing the value of High Risk from 66 to 100 create changes for the value of its parent nodes; Economical Value, Position, and Compliance. The before and after value due to maximizing "High Risk" of the node Ship is shown. Based on the result obtained, node Economical Value and Position each of their states in the same node has the same difference value, meaning that both of the states in each node change the value of node Ship equally. Node Compliance shown a different result. State Comply is found having a slights higher difference value, meaning if its value change it will affect node Compliance compared to Non-comply. Node Economical Value is highlighted with an orange shade that point out that node Economical Value create a more significant change to the node Ship. It is found by comparing the total difference for each state in the same node to the other parent nodes. This experiment result provided a second statement that node Economical Value has the highest significant influence to node Ship.

*Table 4. 13 Comparation of changing for node Security*

| Security | | | | | |
|---|---|---|---|---|---|
| Yes | Note | | | | Difference |
| | Parent Nodes | PN States | Before | After | |
| 100 | Situation | Guarded | 10.2 | 17.3 | 7.1 |
| | | Unguarded | 89.8 | 82.7 | 7.1 |
| | Capability | Trained | 32.1 | 39.7 | 7.6 |
| | | Untrained | 67.9 | 60.3 | 7.6 |
| | Defence | Personnel | 28.6 | 37.1 | 8.5 |
| | | Equipment | 71.4 | 62.9 | 8.5 |

Table 4.13 present the comparation result by changing the value of "Yes" in node Security to its maximum of 100 from a scale 0-100. By changing the value of "Yes" from 34.2 to 100 create changes for the value of its parent nodes; Situation, Capability, and Defence. The before and after value due to maximizing "Yes" of the node is shown. Based on the result obtained, all of the three parent nodes had the same difference value, meaning that both of the states in each node change the value of node Ship equally. Defence is highlighted with an orange shade that point out that node Defence create a more significant change to the node Ship. It is found by comparing the total difference for each state in the same node to the other parent nodes. This experiment result provided a second statement that node Defence has the highest significant influence to node Security.

*Table 4. 14 Comparation of changing for node Environment*

| Environment | | | | | |
|---|---|---|---|---|---|
| Favourable | Note | | | | Difference |
| | Parent Nodes | PN States | Before | After | |
| 100 | Part of a Day | Daylight | 58.3 | 58.7 | 0.4 |
| | | Nightime | 41.7 | 45.3 | 3.6 |
| | Weather | Poor | 15.4 | 18.6 | 3.2 |
| | | Moderate | 46.2 | 42.9 | 3.3 |
| | | Good | 38.5 | 38.5 | 0 |

Table 4.14 present the comparation result by changing the value of "Favourable" in node Environment to its maximum of 100 from a scale 0-

100. By changing the value of Favourable from 55.1 to 100 create changes for the value of its parent nodes; Part of a Day and Weather. The before and after value due to maximizing "Favourable" of the node Environment is shown. Based on the result obtained, State Night time of node Part of a Day has higher difference value, meaning a slight change of its value affect node Environment significantly. As for node Weather the same situation occurs on. It was found that state Moderate has higher difference value, meaning a slight change of its value affect node Weather significantly. Weather is highlighted with an orange shade that point out that node Weather create a more significant change to the node Environment. It is found by comparing the total difference for each state in the same node to the other parent nodes. This experiment result provided a second statement that node Weather has the highest significant influence to node Environment.

After all of the above test is done finding the range of changes of node Attack if the value of its parent nodes is varied is the next step which is important to serves a more thorough analysis. In order to analyse the effect, a state for each parent node of node Attack must be selected and the value of that states will be modified to 0, 25, 50, 75 and 100. The analysis result is presented in the form of table. The table 4.16 to 4.18 will present the result for nodes Ship, Security, and Environment respectively

*Table 4. 15 Range of Change by varying node Ship*

| Ship | | |
|---|---|---|
| High Risk | Attack | Range |
| 0 | 46.5 | 10.7 |
| 25 | 49.2 | |
| 50 | 51.8 | |
| 75 | 54.5 | |
| 100 | 57.2 | |

Table 4.15 show the result of varying the value of states "High Risk" in node Ship creates an impact of 10.7% change. The results present that changing the node ship itself leads to a likelihood attack as low as approximate 46.5% up to maximum 57.2%. Compliance node mainly responsible for this impact as it is the parent node of node Ship. This finding is based on result presented in Figure 4.6. By changing the node Compliance alone can change the probability of an attack 3.2%. The result

of this finding will be used as a recommendation to make decision as to suppressed the likelihood successful attack of piracy and robbery for Port of Tanjung Perak.

*Table 4. 16 Range of Change by varying node Security*

| Security | | |
|---|---|---|
| Yes | Attack | Range |
| 0 | 57.1 | 10.5 |
| 25 | 54.5 | |
| 50 | 51.8 | |
| 75 | 49.2 | |
| 100 | 46.6 | |

The result of varying the value of states "Yes" in node Security is shown in Table 4.16. Based on findings it was known that by varying the value of states "Yes" in node Security creates an impact of 10.5%. The results present that changing the node ship itself leads to a likelihood attack as low as approximate 46.6% up to maximum 57.1%. Situation node mainly responsible for this impact as it is the parent node of node Security. This finding is based on result presented in Figure 4.7. By changing the node Situation alone can change the probability of an attack 26.6%. The result of this finding will be used as a recommendation to make decision as to suppressed the likelihood successful attack of piracy and robbery for Port of Tanjung Perak.

*Table 4. 17 Range of Change by varying node Environment*

| Environment | | |
|---|---|---|
| Favourable | Attack | Range |
| 0 | 51.7 | 3.4 |
| 25 | 52.5 | |
| 50 | 53.4 | |
| 75 | 54.2 | |
| 100 | 55.1 | |

Table 4.17 show the result of varying the value of states "Favourable" in node Environment creates an impact of 3.4% change. The results present that changing the node Environment itself leads to a likelihood attack as low as approximate 51.7% up to maximum 55.1%. Weather node

mainly responsible for this impact as it is the parent node of node Ship. This finding is based on result presented in Figure 4.8. By changing the node Situation alone can change the probability of an attack 13.4%. The result of this finding will be used as a recommendation to make decision as to suppressed the likelihood successful attack of piracy and robbery for Port of Tanjung Perak.

## 4.9. Recommendation

A summarize of finding due to varying the value of the root nodes to the node Attack table 4.18 is presented.

*Table 4. 18 Summarize Finding of Variation of Root Nodes*

| Root Nodes | Effect to Node Attack (%) |
|---|---|
| Situation | 26.6 |
| Defence | 14.2 |
| Weather | 13.4 |
| Part of Day | 8.3 |
| Compliance | 3.2 |
| Capability | 2 |
| E. Value | 1.4 |
| Position | 0.3 |

This table present the value of changing the value of the root node as a single factor. Meaning that by only changing the value of the selected node, the value of node Attack is changing as shown on the table. The node is sorted according to its influence on changes in value of node Attack. Node Situation, Defence, and Weather is three of the nodes that has the highest influence to the likelihood of an attack. In order to suppressed the likelihood of Piracy and Robbery Attack in Port of Tanjung Perak the node Situation which has the highest effect to the likelihood of an attack of the must be prioritized and to be maintained at the assured level as possible. The Port must be kept guarded in the highest possible level to reduce the likelihood of an attack. A well-guarded situation of the port can reduce the likelihood of an attack up to 26.6%. If this scenario is applied the likelihood of an attack will be bellow 0.5 from the scale of 0-1, one as the extreme likelihood of an attack to occur. To be precise the likelihood of an attack will be suppressed to 0.315 from the current situation 0.585. The value of likelihood 0.315 is the value obtained by

changing only node Situation without considering any other node. To understand the meaning of value for other nodes can be done by the same comprehension concept. The presented result of Table 4.19 is a recommendation proposal by the author to reduce the likelihood of Piracy and Robbery Attack of Port of Tanjung Perak.

*Table 4. 19 Recommendation of actions*

| No | Action |
|---|---|
| 1 | Create a clear state of sovereignty and control for security situation in waters |
| 2 | Create a coordinated action between Port Security Committee (navy, police, army, coastguard, harbour master, etc) |
| 3 | Create an intensified information gathering process, harmonised data assessment, provision of consistent reporting, and harmonised intelligence gathering |
| 4 | Update patrolling schedule (routine checks and monitoring in all port areas, both land and sea) |
| 5 | Update security procedures tailored to actual conditions in the field and manage coordination with relevant agencies |
| 6 | Adding more security personnel |
| 7 | Optimizing SOP and supervision |
| 8 | Certification and training for all security officers in compliance to ISPS Code |
| 9 | Training, Dill and Exercise according to Schedule and ISPS Code standard |
| 10 | Installing Real time CCTV surveillance, Face Recognition & Plate Recognition |
| 11 | Identification cards for people who enter the terminal area and must be accompanied with security officer |
| 12 | Prepare security officers who accompany ticket attendants and inspection officers |
| 13 | Installing Radio Over Internet Protocol |
| 14 | Reassessment of Security Requirements |

Table 4.19 present recommendation of actions to upgrade security in the area of Port of Tanjung Perak to reduce the likelihood of attack. From the presented recommendation in order to enhance security level in Port of Tanjung Perak the recommendation proposed by this study is prioritize by 3 factors namely budget, timing, and effectiveness. To prioritize each

recommendation Risk Priority Number (RPN) Technique was used. A range of value from 1 to 5 is applied to assess each factor for each recommendation. 1 being very less and 5 being very high. The result of RPN for each recommendation is presented in Table 4.20

| No | Action | B | T | E | Total |
|---|---|---|---|---|---|
| 1 | Create a clear state of sovereignty and control for security situation in waters | 5 | 5 | 3 | 75 |
| 2 | Create a coordinated action between Port Security Committee (navy, police, army, coastguard, harbour master, etc) | 5 | 5 | 3 | 75 |
| 3 | Create an intensified information gathering process, harmonised data assessment, provision of consistent reporting, and harmonised intelligence gathering | 2 | 2 | 4 | 16 |
| 4 | Update patrolling schedule (routine checks and monitoring in all port areas, both land and sea) | 3 | 5 | 5 | 75 |
| 5 | Update security procedures tailored to actual conditions in the field and manage coordination with relevant agencies | 4 | 2 | 4 | 32 |
| 6 | Adding more security personnel | 3 | 1 | 3 | 9 |
| 7 | Optimizing SOP and supervision | 5 | 2 | 2 | 20 |
| 8 | Certification and training for all security officers in compliance to ISPS Code | 2 | 1 | 5 | 10 |
| 9 | Training, Dill and Exercise according to Schedule and ISPS Code standard | 4 | 1 | 4 | 16 |
| 10 | Installing Real time CCTV survilance, Face Recognition & Plate Recognition | 1 | 3 | 5 | 15 |
| 11 | Identification cards for people who enter the terminal area and must be accompanied with security officer | 3 | 5 | 2 | 30 |
| 12 | Prepare security officers who accompany ticket attendants and inspection officers | 3 | 1 | 4 | 12 |
| 13 | Installing Radio Over Internet Protocol | 2 | 4 | 5 | 40 |
| 14 | Re-assessment of Security Requirements | 2 | 2 | 3 | 12 |

Based on the result of RPN Calculation, it was obtained 3 recommendation that is suggested by this study due to value of RPN is the highest. This recommendation was prioritized for immediate improvements to enhance security level in Port of Tanjung Perak based on 3 criteria that has mentioned before namely budget, time, and effectiveness. A number scale from 1-5 was given for each recommendation. For budget value 5 means that the budget needed to implement the recommendation given is very less and 1 means that the budget needed is significant. As for time value 5 means that the time needed to implement the recommendation is short and 1 means that it took a while to the recommendation come into force. And for effectiveness value 5 means that the recommendation proposed is very effective to enhance security in the port, and 1 means that the recommendation is less effective than other recommendation proposed. Those recommendation were as follow:

- Create a clear state of sovereignty and control for security situation in waters
- Create a coordinated action between Port Security Committee (navy, police, army, coastguard, harbour master, etc)
- Update patrolling schedule (routine checks and monitoring in all port areas, both land and sea)

"This page intentionally left blank"

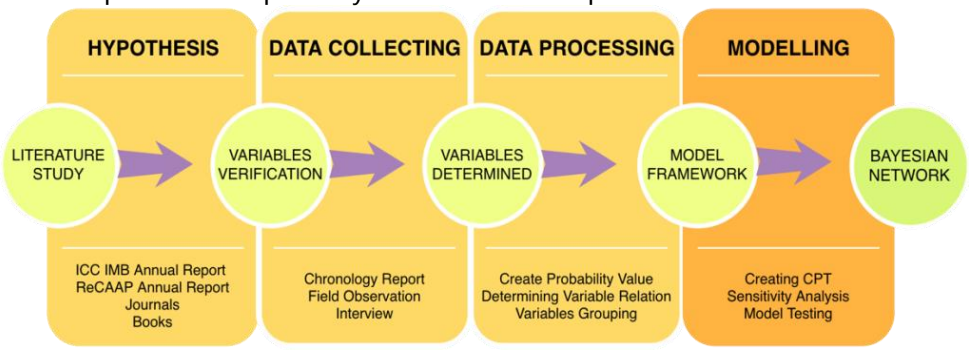
# CHAPTER V

# CONCLUSION

## 5.1. Conclusion

According to the research Bayesian Network Model for Piracy and Robbery Assessment of Tanjung Perak Port done it can be concluded that:

1. Variable that potentially leads to successful attacks of piracy and robbery in Port of Tanjung Perak is determined. Variables were obtained through literature review as a hypothesis and is confirmed by analysing the report of attack happened from 2013-2018. Variables that potentially leads to successful attacks are Economical Value, Compliance, Position, Weather, Part of a Day, Defense, Capability, Situation.
2. Bayesian Network Model is developed to estimate the likelihood of successful attack of piracy and robbery in Port of Tanjung Perak. Variables that already determined is later processed and analysed thoroughly to fit the requirement of the model. An illustration of steps to developed Bayesian Network is presented bellows.




3. Based on Bayesian Network Model created, the model points out which variable has the most significant impact to the likelihood of successful attack of Piracy and Robbery in Port of Tanjung Perak. The model created has find that Situation is the variables that highest effect to the likelihood of an attack of the must be prioritized and to be maintained at the assured level as possible. The Port must be kept guarded in the highest possible level to reduce the likelihood of an attack. A well-guarded situation of the port can reduce the likelihood of an attack up to 26.6%.

## 5.2. Suggestion

1. As found in this research that Situation hold a significant impact to the likelihood of an attack happen, the author suggest that the guarding of the port must be prioritized and to be improved to a more secured level. 3 recommended actions to enhance security situation in the port are:
   a. Create a clear state of sovereignty and control for security situation in waters
   b. Create a coordinated action between Port Security Committee (navy, police, army, coastguard, harbour master, etc)
   c. Update patrolling schedule (routine checks and monitoring in all port areas, both land and sea
2. Reporting of an incident must be improved. During this research the author find difficulties to find the report of an attack. Many of the accident that happened has gone unreported.

## REFERENCES


Artana, K. B. & Dinariyana, A. B., 2013. *Teori Keandalan Sistem dan Aplikasinya Edisi Pertama.* Surabaya: Guna Widya.

Auder, B. & Iooss, B., 2009. Global Sensitivity Analysis Based on Entropy. *Safety, Reliability and Risk Analysis: Theory, Methods and Applications,* pp. 2107-2115.

Auder, B. & Iooss, B., 2009. *Global sensitivity analysis based on entropy. Safety, Reliability and Risk Analysis: Theory, Methods and Application.* s.l.:s.n.

Bouejla, a., Chaze, X., Guarnieri, F. & Napoli, A., 2014. A Bayesian network to manage risks of maritime piracy against offshore oil fields. In: *Safety Science, Vol.68* . s.l.:s.n., pp. 222-230.

Budiyanto, D. E. H. & Gurning, R. O. S., 2015. *ISPS CODE Seri: Manajemen Pelabuhan.* s.l.:PT. Andhika Prasetya Ekawahana.

Das, B., 2004. Generating Conditional Probabilities for Bayesian Networks: Easing the Knowledge Acquisition Problem.

Frécon, E., 2018. [Online] Available at: https://theconversation.com/pirates-with-black-magic-attack-shipping-in-indonesian-waters-94106

Hellberg, P., 2009. Effects of the ISPS Code on ship and port security - a Swedish perspective. *The Maritime Commons: Digital Repository of the World Maritime University.*

Hribernik, M., 2013. Countering Maritime Piracy and Robbery in Southeast Asia: The Role of the ReCAAP Agreement. *EIAS Briefing Paper 2013/2.*

Huang, D.-z., Li, Y. & Hu, H., 2015. Application of Geographic Information System to Calculate the Probability of Piracy Occurrence. *IEEE Explore.*

I., B.-G., F., F. & R., K., 2007. *Encyclopedia of Statistics in Quality & Reliability.* United Kingdom: Wiley & Sons.

IMB, I., 2017. Piracy and Robbery Against Ship Report. *Piracy and Robbery Against Ship Report for Period 1 January – 31 December 2017.*.

IMB, I., 2018. Piracy and Robbery Against Ship Report. *Piracy and Robbery Against Ship Report for Period 1 January – 30 June 2018.* .

Morris, L. J. & Paoli, G. P., 2018. *A Preliminary Assessment of Indonesia's Maritime Security Threats and Capabilities.* Santa Monica: RAND Corporation.

Motik, C. & Djemat, Y., 2005. ISPS Code Diterapkan di Pelabuhan Perikanan Samudera Jakarta, Mungkinkah. . In: *Indonesian Journal of International Law Vol. 2 Nomor 3.* s.l.:s.n.

Pristrom, S., 2016. A novel flexible model for piracy and robbery assessment of merchant ship operations.. *Science Direct.*

RECAAP, 2018. Piracy and Armed Robbery Against Ships in Asia. *Annual Report.*

Rindarto, A. P., 2012. Implementasi International Ship and Port Facility Security (ISPS) Code dalam Mencegah Petty Theft dan Armed Robbery Against Ships di Indonesia Tahun 2009-2013. *Ejournal S1 Undip.*

Saltelli, A. et al., 2008. *Global Sensitivity Analysis: The Primer.* s.l.:John Wiley & Sons Ltd..

Triola, M. F., 2014. *Elementary Statistics Twelfth Edition.* s.l.:Pearson Education, Inc..

Weber, P. & Simon, C., 2016. *Benefits of Bayesian Network Models Volume 2.* Great Britain: ISTE Ltd.

# ATTACHMENT

"This page intentionally left blank"

*Chronology Report of Attack Happen in 2013-2018*

| 2013 | | | |
|---|---|---|---|
| No | Date | Evidence | Chronology |
| 1 | Wednesday, October 3 2013 | crane accessories, hammer, motor | 11 The perpetrators of theft at the Port of Tanjung Perak, Surabaya, East Java were arrested. In each action, these perpetrators use trucks to transport stolen goods that are carried on the boat. the crime mode carried out by the perpetrators, during the day the suspects conducted a survey first in the target location. After getting the target, the perpetrator took the sack to transport the stolen goods.<br>"In the evening, the perpetrators took the items they were targeting, then transported them in L 8090 WJ trucks, and then sold them on Jalan Tambak Mayor. |
| 2 | Wednesday, December 14 | container filled with processed wood | The gang of thieves who used to take action on a boat which was docked at the Port of Tanjung Perak, Surabaya, was successfully dismantled by the East Java Regional Police Chief of Police. This plot involved the crew in carrying out the action. In disclosing this case, there were two suspects who were successfully secured by the police. This plot was arrested in the case of a container break in (KM) Alken Pikat which was docked on port of Tanjung Perak. The suspect Andriyanto and his partner damaged the bolts in the targeted container. Arriving at Tanjung Perak, he immediately contacted Ynt after the ship anchored. Furthermore, Ynt and his accomplice came to the boat using his fishing boat. In order not to be caught, the bolts of previously damaged containers were |

| | | | |
|---|---|---|---|
| | | | replaced with new bolts. So, it was impressed that the container was never opened |
| 2014 | | | |
| No | Date | Evidence | Chronology |
| 1 | Wednesday, January 8, 2014, at 2:00 a.m. | • 1 (one) roller lasing;<br>• 1 (one) fruit closed manhole;<br>• 1 (one) head of ventilation;<br>• 1 (one) iron pipe;<br>• 3 (three) pieces of plate. | On Wednesday 08 January 2014 at 02.00 WIB. The Patrol Boat X-1008 carried out a routine patrol led by the Head of the National Operations Office, which had inspected anonymous boats carrying goods in the form of 1 (one) roller lasing, 1 (one) manhole lid, etc. Suspected of the proceeds of crime, then the boat was ad-hocked to Mako Ditpolair East Java Regional Police for further processing. |
| 2 | Friday, January 31, 2014, at 11.00 WIB | • 24 boxes Mixed Fish as many as or ± 200 Kg<br>• 1 (one) unnamed boat unit | On Friday, January 31, 2014 when the Police vessel X-1008 conducted a patrol in the 10th section of the East Surabaya Watershed at around 11.00 WIB. Has carried out an nameless boat inspection which is transporting goods in the form of fish as many as 24 (twenty four) boxes, then the boat and boat crew and fish were taken to the East Java Regional Police's Ditpolair office for further processing. |
| 3 | Wednesday, February 12, 2014, at 10:00 p.m. | • 39 Gen or ± 1.365 L of solar<br>• a boat without name | At the time of KP. PIPIT - 3003 conducts a routine patrol to detect the presence of a boat (Without Name) by Nur Ghozali with a charge of 39 generals @ 35 liters or 1,365 liters, then an inspection and alleged violation of Article 374 and Article 480 jo article 55 of the Criminal Code concerning embezzlement and fencing, then the boat (Without Name) |

| | | | |
|---|---|---|---|
| | | | escorted to the base of the East Java Regional Police Directorate of Ditpolair for further investigation. |
| 4 | Saturday, 08 February 2014, 11.00 WIB | • on 03 February 2014 BA (Minutes) check manhole<br>• Letter of CPO sounding result, February 8, 2014 | A woman named DRA. LUKI INDRIANI on Monday, February 24, 2014 at 11.00 WIB reported that there had been an alleged embezzlement of CPO Oil with proof of evidence as:<br>- Reports on February 3, 2014 about checking seals that found a broken seal at Manhole<br>- Letter on February 8, 2014 |
| 5 | Tuesday, April 1, 2014 at around 5:00 a.m. . | • 1 unnamed boat unit;<br>• 8 iron hardener needles;<br>• 12 iron shoe containers. | On Tuesday, April 1, 2014 at around 5:00 a.m. In Surabaya East Shipping Channel (APTS) at position 07 ° 11'401 "S-112 ° 42'273" E, Police Ship X-1013 was lowering iron (container lasing equipment) then 3 (three) boat crew along with evidence it was brought to Mako Ditpolair East Java Regional Police for further examination. |
| 2015 | | | |
| No | Date | Evidence | Chronology |
| 1 | Sunday, March 1, 2015 at 02:30 wib | • 1 unnamed boat unit with 13 PK Honda engine<br>• 3 container chains with a length of ± 5 meters<br>• 6 pieces of spans screw containers<br>• 4 pieces of container fittings | On Sunday, March 1, 2015 at around 05:30 WIB KP X-2001 Police Ship was carrying out a Thuggery Operation and at the time of carrying out the sweeping in the Surabaya East Shipping Channel region APTS found an unnamed boat carrying Old Iron, then 2 (two) unnamed boats and Old Iron boat were taken to Mako Ditpolair East Java Regional Police for further examination. |

| | | | |
|---|---|---|---|
| | | • 4 welding wire boxes @ 5kg<br>• 4 pieces of bendit plate<br>Rp 700,000, | |
| 2 | • Sunday, September 20 2015 at 10:00 p.m. | Welding equipment include:<br>a. 1 (one) 3 kg elpigi gas cylinder<br>b. 2 (two) oxygen tubes<br>c. Welding hose ± 5 meters<br>d. 1 (one) small hammer<br>e. 1 (one) blender<br>f. 1 (one) wrench<br>• 3 (three) pieces of iron buffer ± 30 cm wide and ± 2 mm thick<br>• 1 (one) unit of Boat Eka | On Monday, September 21, 2015 at around 21:30 WIB in the APBS Waters (Surabaya West Cruise Line) in position 070 03 '746 "LS - 1120 38' 620" E. Police Ship X 1013 Ditpolair East Java Regional Police has examined the perpetrators theft of iron ship by cutting using welding and then the case was handed over to the East Java Police Ditpolair Investigator for further examination. |
| 2016 | | | |
| No | Date | Evidence | Chronology |
| 1 | Sunday, April 24, 2016 at 9:30 a.m. | • 1 Yamaha Brand generator set<br>• 1 set of hacksaw<br>• 1 size 19 shock lock | On Sunday, April 24, 2016 at around 9:30 a.m., above TB. Niaga Mas 1 anchor / anchor in the waters Bouy Pisang Alur Pelayaran Barat Surabaya / APBS (west of ICT dock), visited by Br. Moh Gofar to ask for a drink. After being given a drink by Br. Warman (Olie Man TB. Niaga Mas |

| | | | |
|---|---|---|---|
| | | • 1 boat unit<br>• 1 cutter knife | 1) Br. Moh. Gofar borrows a hacksaw and locks the shock, after the saw and the key to shock are taken from the ship's engine room and given by Br. Warman, Bro. Moh. Gofar returns to the boat. After 1 minute, Bro. Moh. Gofar with his colleague Bro. Heri returns to TB. Niaga Mas 1, when walking Moh. Gofar followed Bro. Warman into the TB kitchen. Niaga Mas 1, when walking, Bro. Moh Gofar is closing in on you Warman was in the kitchen door and pointed the saw towards the stomach and the knife towards the right side of the neck and threatened that Br. Warman doesn't move. After 1 minute, Bro. Warman heard that someone was lifting the generator engine from the engine room, then Bro. Warman heard the sound of the boat engine and Bro. Moh. Gofar ran and jumped on the boat and went straight to the Teluk Lamong harbor dock. After that Bro. Muskardi reported to the company office to ask for help. |
| 2 | Sunday, July 9 2016 | • 1 Dynasty brand 2000 volt Transformer unit<br>• 1 long blue red gas evaporation pipe ± 1 meter<br>• 1 red boat unit<br>• 1 sickle | At the time of KP X-2001, Ditpolair of East Java Regional Police headed by Aiptu Partika Guntur carried out a Patrol, getting information from the public that above one ship there is a theft. Then the officers came to the scene where the ship is meant to be lego anchor. After going to the scene, the officer gets information from the Ship Mechanic that there were several people boarded the ship by taking several items and the people in question were in Tug Boat. Then the officers came to Tug Boat. The visa met Faisal Imron and Mulyono's relatives carrying goods from the ship, |

| | | | |
|---|---|---|---|
| | | | after a brief examination of the two perpetrators and found evidence of evidence according to what was conveyed by Br. Rafles, with initial proof. Then the perpetrators of a.n. Bro Faisol Imron was taken to Mako Ditpolair of East Java Regional Police to conduct further investigations, 1 (one) person who committed Mulyono fled when he wanted to show other evidence in Bangkalan. |
| 3 | Friday, August 26 2016 at 11.00 wib | • 1 (one) Unnamed Boat unit<br>• 3 (three) sheets of photos when the theft occurs | On Friday August 26, 2016 at around 11.00 a man arrived at the East Java Regional Police's Ditpolair office and reported that on Friday 24 June 2016 at around 05:30 hours in the Madura Strait Tg. Perak Surabaya has stolen 1 (one) Man Over Boat unit and 1 (one) ship radar antenna done by 3 (three) perpetrators by using a nameless boat. And from one of the perpetrators threatened the crew by pointing the knife towards the crew. |
| 2018 | | | |
| No | Date | Evidence | Chronology |
| 1 | Monday, September 17, 2018 at around 08:40 a.m | • CCTV Record;<br>• 1 nozzle missing | a. On Monday, September 17, 2018 at around 08:40 a.m., members of the North Security Jamrud Port received a report that the MV Indigo Silva had lost 1 (one) Nozzle unit;<br>b. Receiving the report, members of Port Security (PS) North Jamrud (JU) immediately coordinated with members of the Patrol PS post to coordinate with the ship, and PS Patrol immediately drove to the location and coordinated with the ship / ABK vessel MV officers. Indigo Silva and checking / investing; |

| | | | |
|---|---|---|---|
| | | | c. From checking correctly there is 1 (one) nozzle in one missing and the position is on the sea side. based on the information from ABK, the nozzle disappeared around 24.00 WIB;<br>d. To ensure that members of Port Security monitor from CCTV footage but for the sea side CCTV can not reach;<br>e. And also conveyed to CCTV monitors that are on standby 1 (Patrol post) the network is often error because the network uses the Wireless System, so it cannot be maximized to monitor the occurrence of the loss;<br>f. As a result of the shortage of the above mentioned bookstore, we cannot continue to invest and only receive reports and will carry out repairs on the security of both the port operator and the MV. Indigo Silva. |

Analysis of Chronology Report using Coding System

| 2013 | | | | |
|---|---|---|---|---|
| No | Day, Date | Evidence | Report | Keywords |
| 1 | Wednesday, 3rd October | crane accessories, hammer, motor | 11 The perpetrators of theft at the Port of Tanjung Perak, Surabaya, East Java were arrested. In each action, these perpetrators use trucks to transport stolen goods that are carried on the boat. the crime mode carried out by the perpetrators, during the day the suspects conducted a survey first in the target location. After getting the target, the perpetrator took the sack to transport the stolen goods. "In the evening, the perpetrators took the items they were targeting, then transported them in L 8090 WJ trucks, and then sold them on Jalan Tambak Mayor. | E1<br>S2<br>D2<br>W3<br>P2<br>N2<br>C1<br>G1 |
| 2 | Wednesday, 14th December | container filled with processed wood | The gang of thieves who used to take action on a boat which was docked at the Port of Tanjung Perak, Surabaya, was successfully dismantled by the East Java Regional Police Chief of Police. This plot involved the crew in carrying out the action. In disclosing this case, there were two suspects who were successfully secured by the police. This plot was arrested in the case of a container break in (KM) Alken Pikat which was docked on port of Tanjung Perak. The suspect Andriyanto and his partner damaged the bolts in the targeted container. Arriving at Tanjung Perak, he immediately contacted Ynt after the ship anchored. Furthermore, Ynt and his accomplice came to the boat using his fishing boat. In order not to be caught, the bolts of previously damaged containers were replaced with new bolts. So, it was impressed that the container was never opened | E2<br>S1<br>D0<br>W2<br>P2<br>N1, N2<br>C1<br>G2 |

| 2014 | | | | |
|---|---|---|---|---|
| No | Day, Date | Evidence | Report | Keywords |
| 1 | Wednesday , January 8, 2014, at 2:00 a.m. | 1 (one) roller lasing; 1 (one) fruit closed manhole; 1 (one) head of ventilation; 1 (one) iron pipe; 3 (three) pieces of plate. | On Wednesday 08 January 2014 at 02.00 WIB. The Patrol Boat X-1008 carried out a routine patrol led by the Head of the National Operations Office, which had inspected anonymous boats at 07 11′ 14″ LS - 1120 43′ 21″ BT carrying goods in the form of 1 (one) roller lasing, 1 (one) manhole lid, etc. Suspected of the proceeds of crime, then the boat was ad-hocked to Mako Ditpolair East Java Regional Police for further processing. | E1<br>S2<br>D2<br>W2<br>P0<br>N1<br>C<br>G |
| 2 | Friday, January 31, 2014, at 11.00 WIB | 24 boxes Mixed Fish as many as or ± 200 Kg, 1 (one) unnamed boat unit | On Friday, January 31, 2014 when the Police vessel X-1008 conducted a patrol in the 10th section of the East Surabaya Watershed (07 10′ 48″ S - 1120 43′ 24″ T) at around 11.00 WIB. Has carried out an nameless boat inspection which is transporting goods in the form of fish as many as 24 (twenty four) boxes, then the boat and boat crew and fish were taken to the East Java Regional Police's Ditpolair office for further processing. | E2<br>S2<br>D1<br>W3<br>P3<br>N2<br>C<br>G |
| 3 | Wednesday , February 12, 2014, at 10:00 p.m. | 39 Gen or ± 1.365 L of solar, a boat without name | At the time of KP. PIPIT - 3003 conducts a routine patrol to detect the presence of a boat (Without Name) by Nur Ghozali with a charge of 39 generals @ 35 liters or 1,365 liters, then an inspection and alleged violation of Article 374 and Article 480 jo article 55 of the Criminal Code | E2<br>S1<br>D2<br>W2 |

| | | | | |
|---|---|---|---|---|
| | | | concerning embezzlement and fencing, then the boat (Without Name) escorted to the base of the East Java Regional Police Directorate of Ditpolair for further investigation. | P3<br>N1<br>C<br>G |
| 4 | Saturday, 08 February 2014, 11.00 WIB | on 03 February 2014 BA (Minutes) check manhole, Letter of CPO sounding result, February 8, 2014 | A woman named DRA. LUKI INDRIANI on Monday, February 24, 2014 at 11.00 WIB reported that there had been an alleged embezzlement of CPO Oil with proof of evidence as: - Reports on February 3, 2014 about checking seals that found a broken seal at Manhole - Letter on February 8, 2014 | E2<br>S1<br>D1<br>W1<br>P<br>N2<br>C<br>G |
| 5 | Tuesday, April 1, 2014 at around 5:00 a.m. | 1 unnamed boat unit, 8 iron hardener needles, 12 iron shoe containers. | On Tuesday, April 1, 2014 at around 5:00 a.m. In Surabaya East Shipping Channel (APTS) at position 07 ° 11'401 "S-112 ° 42'273" E, Police Ship X-1013 was lowering iron (container lasing equipment) then 3 (three) boat crew along with evidence it was brought to Mako Ditpolair East Java Regional Police for further examination. | E1<br>S2<br>D1<br>W3<br>P3<br>N2<br>C<br>G |

| |
|---|
| 2015 |

| No | Day, Date | Evidence | Report | Keywords |
|---|---|---|---|---|
| 1 | Sunday, March 1, 2015 at 02:30 wib | 1 unnamed boat unit with 13 PK Honda engine, 3 container chains with a length of ± 5 meters, 6 pieces of spans screw containers, 4 pieces of container fittings, 4 welding wire boxes @ 5kg, 4 pieces of bendit plate, Rp 700,000, - | On Sunday, March 1, 2015 at around 05:30 WIB KP X-2001 Police Ship was carrying out a Thuggery Operation and at the time of carrying out the sweeping in the Surabaya East Shipping Channel region APTS found an unnamed boat carrying Old Iron, then 2 (two) unnamed boats and Old Iron boat were taken to Mako Ditpolair East Java Regional Police for further examination. | E1<br>S2<br>D2<br>W2<br>P<br>N2<br>C<br>G |
| 2 | Sunday, September 20 2015 at 10:00 p.m. | Welding equipment include: 1 (one) 3 kg elpigi gas | On Monday, September 21, 2015 at around 21:30 WIB in the APBS Waters (Surabaya West Cruise Line) in position 070 03 '746 "LS - 1120 38' 620" E. Police Ship X 1013 Ditpolair East Java Regional Police has examined the perpetrators theft of iron ship by cutting using welding | E1<br>S2<br>D2<br>W2 |

| | | | | |
|---|---|---|---|---|
| | | cylinder, 2 (two) oxygen tubes, Welding hose ± 5 meters, 1 (one) small hammer, 1 (one) blender, 3 (three) pieces of iron buffer ± 30 cm wide and ± 2 mm thick, 1 (one) unit of Boat Eka | and then the case was handed over to the East Java Police Ditpolair Investigator for further examination. | P<br>N2<br>C<br><br><br><br><br><br><br>G |

| 2016 | | | | |
|---|---|---|---|---|
| No | Day, Date | Evidence | Report | Keywords |
| 1 | Sunday, April 24, 2016 at 9:30 a.m. | 1 Yamaha Brand generator set, 1 set of hacksaw, 1 size 19 shock lock, 1 boat | On Sunday, April 24, 2016 at around 9:30 a.m., above TB. Niaga Mas 1 anchor / anchor in the waters Bouy Pisang Alur Pelayaran Barat Surabaya / APBS (west of ICT dock), visited by Br. Moh Gofar to ask for a drink. After being given a drink by Br. Warman (Olie Man TB. Niaga Mas 1) Br. Moh. Gofar borrows a hacksaw and locks the shock, after the saw and the key to shock are taken from the ship's engine room and given by Br. Warman, Bro. Moh. Gofar returns to the boat. After 1 | E1<br>S1<br>D1<br>W3<br>P<br>N1<br>C |

| | | | | |
|---|---|---|---|---|
| | | unit, 1 cutter knife | minute, Bro. Moh. Gofar with his colleague Bro. Heri returns to TB. Niaga Mas 1, when walking Moh. Gofar followed Bro. Warman into the TB kitchen. Niaga Mas 1, when walking, Bro. Moh Gofar is closing in on you Warman was in the kitchen door and pointed the saw towards the stomach and the knife towards the right side of the neck and threatened that Br. Warman doesn't move. After 1 minute, Bro. Warman heard that someone was lifting the generator engine from the engine room, then Bro. Warman heard the sound of the boat engine and Bro. Moh. Gofar ran and jumped on the boat and went straight to the Teluk Lamong harbor dock. After that Bro. Muskardi reported to the company office to ask for help. | G |
| 2 | Sunday, July 9 2016 | 1 Dynasty brand 2000 volt Transformer unit, 1 long blue red gas evaporation pipe ± 1 meter, 1 red boat unit, 1 sickle | At the time of KP X-2001, Ditpolair of East Java Regional Police headed by Aiptu Partika Guntur carried out a Patrol, getting information from the public that above one ship there is a theft. Then the officers came to the scene where the ship is meant to be lego anchor. After going to the scene, the officer gets information from the Ship Mechanic that there were several people boarded the ship by taking several items and the people in question were in Tug Boat. Then the officers came to Tug Boat. The visa met Faisal Imron and Mulyono's relatives carrying goods from the ship, after a brief examination of the two perpetrators and found evidence of evidence according to what was conveyed by Br. Rafles, with initial proof. Then the perpetrators of a.n. Bro Faisol Imron was taken to Mako Ditpolair of East Java Regional Police to conduct further investigations, 1 (one) person who committed Mulyono fled when he wanted to show other evidence in Bangkalan. | E1<br>S1<br>D1<br>W1<br>P<br>N2<br>C<br>G |

| | | | | |
|---|---|---|---|---|
| 3 | Friday, August 26 2016 at 11.00 wib | 1 (one) Unnamed Boat unit, 3 (three) sheets of photos when the theft occurs | On Friday August 26, 2016 at around 11.00 a man arrived at the East Java Regional Police's Ditpolair office and reported that on Friday 24 June 2016 at around 05:30 hours in the Madura Strait Tg. Perak Surabaya has stolen 1 (one) Man Over Boat unit and 1 (one) ship radar antenna done by 3 (three) perpetrators by using a nameless boat. And from one of the perpetrators threatened the crew by pointing the knife towards the crew. | E1<br>S2<br>D1<br>W3<br>P<br>N2<br>C<br>G |

| 2018 | | | | |
|---|---|---|---|---|
| No | Day, Date | Evidence | Report | Keywords |
| 1 | Monday, September 17, 2018 at around 08:40 a.m | CCTV Record, 1 nozzle missing | a. On Monday, September 17, 2018 at around 08:40 a.m., members of the North Security Jamrud Port received a report that the MV Indigo Silva had lost 1 (one) Nozzle unit; b. Receiving the report, members of Port Security (PS) North Jamrud (JU) immediately coordinated with members of the Patrol PS post to coordinate with the ship, and PS Patrol immediately drove to the location and coordinated with the ship / ABK vessel MV officers. Indigo Silva and checking / investing; c. From checking correctly there is 1 (one) nozzle in one missing and the position is on the sea side. based on the information from ABK, the nozzle disappeared around 24.00 WIB; d. To ensure that members of Port Security monitor from CCTV footage but for the sea side CCTV can not reach; e. And also conveyed to CCTV monitors that are on standby | E1<br>S1<br>D1<br>W3<br>P<br>N1<br>C<br>G |

| | | | | |
|---|---|---|---|---|
| | | | 1 (Patrol post) the network is often error because the network uses the Wireless System, so it cannot be maximized to monitor the occurrence of the loss; f. As a result of the shortage of the above mentioned bookstore, we cannot continue to invest and only receive reports and will carry out repairs on the security of both the port operator and the MV. Indigo Silva | |

This page intentionally left blank

Probability Table for Each State

| | Code | Causes | 2013 | 2014 | 2015 | 2016 | 2018 | Probability |
|---|---|---|---|---|---|---|---|---|
| E. Value | E1 | Equipment | 1 | 2 | 2 | 3 | 1 | 0.69230769 |
| | E2 | Cargo | 1 | 3 | | | | 0.30769231 |
| Position | S1 | Anchoring | 2 | 2 | | 2 | 1 | 0.53846154 |
| | S2 | Sailing | | 3 | 2 | 1 | | 0.46153846 |
| Part of Day | D1 | Daylight | | 3 | | 3 | 1 | 0.58333333 |
| | D2 | Night time | 1 | 2 | 2 | | | 0.41666667 |
| Weather | W1 | Poor | | 1 | | 1 | | 0.15384615 |
| | W2 | Moderate | 1 | 2 | 2 | 1 | | 0.46153846 |
| | W3 | Good | 1 | 2 | | 1 | 1 | 0.38461538 |
| Defence | N1 | Personnel | 1 | 1 | | 1 | 1 | 0.28571429 |
| | N2 | Equipment | 2 | 4 | 2 | 2 | | 0.71428571 |
| Capability | C1 | Trained | | | | | | 0.32090909 |
| | C2 | Untrained | | | | | | 0.67909091 |
| Situation | G1 | Guarded | | | | | | 0.10209899 |
| | G2 | Unguarded | | | | | | 0.89790101 |
| Compliance | P1 | Comply | | | | | | 0.05172414 |
| | P2 | Non-comply | | | | | | 0.94827586 |

”

This page intentionally left blank

Existing Mitigation Plan

| No | LOCATION | | MITIGATION STRATEGY |
|---|---|---|---|
| 1 | Access, entrance, entrance to the port, and lego anchor area, ship and dock movement area | | |
| | A | Entrance from the sea | - Making PROTAP and Communication Nets<br>- Entry Flow Monitoring<br>- Determination of Patrol Schedule<br>- Monitoring of the Pier Area |
| | | Lego Anchor Area | |
| | | Flow into the port | |
| | | Ship movement area | |
| | | Dock area | |
| | B | Access from land | - Adding Security Personnel |
| | | Door | |
| | | Fence | |
| 2 | Cargo facilities, terminals, goods stacking areas and loading and unloading equipment | | |
| | A | Pier Facilities | - Add lighting<br>- Marking<br>- Monitoring stacking areas<br>- Add immigration checks for international passengers<br>- Prepare security officers who accompany ticket attendants and inspection officers<br>- The porter in charge must wear a numbered uniform according to the employee's number |
| | B | Terminal / Offices | |
| | C | Stacking Area | |
| 3 | Electric power generation, transfer of goods through pipes and water supply | | |
| | A | Power plant | - Marking<br>- Lock the electrical panel and secure it<br>- Perform routine checks in the generator area<br>- Optimizing SOP and supervision |
| | B | Water supply | |
| 4 | Ships that provide services at the port, including guided ships, tugs and barges etc. | | |
| | A | Guide ship | - Optimizing SOP and supervision |
| | B | tugboat | |
| | C | Barge | |
| 5 | Security and equipment and security systems | | |
| | A | Security Personnel | - Training / Training Dill and Exercise according to Schedule |
| | B | Security equipment | |

| | | | |
|---|---|---|---|
| | C | Security system / procedure | - All security officers must have a port security certificate<br>- Update security procedures tailored to actual conditions in the field and manage coordination with relevant agencies<br>- ISPS Code training for all certified security officers |
| 6 | Waters around port facilities | | - Optimizing SOP and supervision<br>- Conduct monitoring in all port areas, both land and sea |
| 7 | Systems, such as electric power systems, radio systems and telecommunications as well as computer systems and networks | | |
| | A | Electric Power System | - Making PROTAP and Communication Nets<br>- Addition of Central Communication Room<br>- Prepare a central communications room and install CCTV monitors in the PFSA room |
| | B | Radio and communication systems | |
| | C | Computer network system | |
| 8 | Ship traffic management in ports and navigational aids | | |
| | A | Management of ship traffic | - Making PROTAP and Communication Nets |
| | B | Navigation aids | |

## AUTHOR'S BIOGRAPHY

I Putu Gede Bagus Parta Saputra is a student of Marine Engineering Department (Joint Degree Hochschule Wismar, Germany) Faculty of Marine Technology, Institut Teknologi Sepuluh Nopember specialized in Marine Reliability, Availability, Management and Safety. He was born in Denpasar, Bali on March 4th 1997. He completed his Senior High School at SMAN 4 Denpasar in 2015, Junior High School at SMPN 7 Denpasar in 2012 and Elementary School at SD Saraswati 4 Denpasar in 2009. During his study in University he was active in several organizations and projects. He took the position as Student Ambassador of CICIL Surabaya, Committee of Maritime Safety International Conference (MASTIC) 2018, Job Manager of ITS Student Choir in 2016-2017, Staff of Creative Media and Information of TPKH ITS 2016-2017, Staff of Fundraising of Marine Icon 2016 & 2017. He participated in National Student Art Competition as an ambassador of ITS. He also holds certification of IMarEST and training of PT Pelabuhan Indonesia 3 Benoa in 2018 and PT. Daya Radar Utama Jakarta in 2017. For further discussion and suggestion regarding this bachelor thesis, the author can be reached through his email: partabagus@gmail.com

"This page intentionally left blank"