Accepted Author Manuscript: Liwång, H., Ringsberg, J. W., & Norsell, M. (2013). Quantitative risk analysis – Ship security analysis for effective risk control options. *Safety Science*, 58(0), 98-112. 10.1016/j.ssci.2013.04.003

Quantitative risk analysis – Ship security analysis for effective risk control options

Hans Liwång [Chalmers and SNDC], Jonas W. Ringsberg [Chalmers], Martin Norsell [SNDC]

[Chalmers] Chalmers University of Technology
Shipping and Marine Technology, 412 96 Gothenburg, Sweden
hans.liwang@chalmers.se
jonas.ringsberg@chalmers.se

[SNDC] Swedish National Defence College
Department of Military Studies, Box 278 05, 115 93 Stockholm, Sweden
hans.liwang@fhs.se
martin.norsell@fhs.se

Abstract

This study reviews ship security assessment. The objectives are to explore the possibilities for quantifying and performing a more thorough ship security risk analysis than that described in the International Ship and Port Facility Security code and to evaluate to what extent this more detailed analysis increases ship security and facilitate the effective selection of risk control options.

The study focuses on Somali-based maritime piracy, using piracy on the Indian Ocean as a case study. Data are collected using questionnaires and interviews with civilian and military security experts who possess firsthand experience of piracy off the coast of Somalia. The data are collected specifically for this study and describe and quantify the threat's capability, intent and likelihood of exploiting a ship's vulnerability. Based on the collected description of the threat, the study analyzes and describes: probability of detection by pirates, probability of successful approach, and probability of successful boarding.

The performed work shows good agreement between calculated probabilities and frequencies in the cited incident reports. Also, the developed scenarios describe the most important influences on the analyzed areas. The research therefore shows that the proposed risk-based approach, which uses structurally collected and documented information on the threat, can increase ship security by assisting in selecting risk control options. The approach also allows for a better understanding of the causal relationship between threat and risk than that provided in today's security analysis by ship owners, for example. This understanding is crucial to choosing effective and robust risk control options.

Keywords: control option, influence diagram, piracy, quantified risk management, ship security analysis

Corresponding author: Hans Liwång
Chalmers University of Technology
Shipping and Marine Technology, 412 96 Gothenburg, Sweden
hans.liwang@chalmers.se
Phone: +46 73 622 1974
Fax: +46 8 55 34 25 98

1 Introduction

The 2008 hijacking of the 333-meter tanker Sirius Star when it was 400 miles out to sea was unprecedented because pirate attacks had previously been performed closer to the Somali shore (Kraska & Wilson, 2008). According to the Best Management Practice for Protection against Somalia-based Piracy (BMP), the attacks have since occurred throughout the Gulf of Aden, the Arabian Sea and the Northern Indian Ocean, affecting all shipping in the region (BIMCO et al., 2011). The United Nations Security Council has turned its attention towards combating piracy as a result, placing demands on flag, port, and coastal states for both the victims and perpetrators of piracy to cooperate in counter-piracy actions off the Somali coast (Kraska & Wilson, 2008). The Security Council has also passed several resolutions regarding maritime piracy, the most important being UNSCR 1816, 1846, and 1851, which are unprecedented in the level of authority they grant the international community to counter threats in the maritime realm (Chalk, 2010).

Ships' security measures are often the first and only measures preventing criminal acts at sea, and commercial vessels must assume that they are on their own if attacked (Kraska & Wilson, 2008). The conditions for shipping through the high-risk waters off the coast of Somalia are therefore largely dictated by piracy and the security efforts onboard the ships.

The International Ship and Port Facility Security (ISPS) code regulates the ship security analysis that must be performed by ship owners and operators (IMO, 2002a). The code was developed in the aftermath of the terrorist attacks on the United States on September 11th, 2001. The development processes for the code commenced two months after the attacks, and the final code was presented only thirteen months later (Wengelin, 2012). Due to this rapid turnaround time, the development was characterized by the need to create an imperfect product rather than having nothing at all (Mitropoulos, 2004). The depth of ship security assessment suggested by this code is therefore very limited in comparison to, for example, the depth demanded by probabilistic risk assessments for ship safety. Areas of ship design with more stringent methods and tools for risk assessment include the SOLAS Chapter II-2 on fire safety, including Regulation 17 on alternative design and arrangements (Juhl, 2009), the Formal Safety Assessment (IMO, 2002b) and Risk-Based Ship Design (Vassalos, 2009), as well as military threat analysis (NATO Standardization Agency, 2007). The limited and imperfect nature of the code in question indicates a need for further research and development in maritime security. In a review of recent literature concerning maritime security Yang (2011) identifies that there is limited research on quantitative risk management in regards to maritime security. Twenty-three research articles in the area of maritime or ship security risks are registered in the Web of Science (Thomson Reuters, 2013) during the years 2006 to 2012. As summarized in Table 1, only four out of 23 articles discuss risk in regard to ships and only 2, out of these 4, discuss risk in a quantitative manner.

Table 1. Results of a literature study on research articles in the Web of Science (Thomson Reuters, 2013) with the search words *Security* AND *Risk* AND (*Ship* OR *Maritime*) during the years 2006 to 2012. A risk management article is defined as an article that both describes the risk and discusses how it could be reduced. Numbers given in parenthesis are the number of articles that specifically discuss ship security.

	Risk management	Risk descriptive	Σ
Quantitative	9(1)	1(1)	10(2)
Qualitative	7(1)	6(1)	13(2)
Σ	16(2)	7(2)	23(4)

Based on the summary in Table 1, it is clear that research on how ship security can be analyzed and risks effectively reduced is very limited, especially with quantitative methods that can be compared to the methods proposed by IMO for risk management in other areas. The process of ship security risk analysis is therefore mostly described in regulations and guidelines from organizations such as IMO, International Association of Classification Societies (IACS) and to some extent NATO (IMO, 2002a, IACS 2004 and NATO Standardization Agency, 2007). These documents are here assumed to describe a best practice but lack of traditional scientific background. The documents therefore risk to be subjective. This subjectivity could lead to that key aspects are omitted, or, that the perspective on the problem is too one sided. Therefore, the focus here is to research the process described in regulations and guidelines and to examine and document to what extent the best practice can increase ship security.

This investigation reviews the ISPS code's ship security assessment procedure, making use of security research, experiences from military force protection, and methodical lessons from maritime probabilistic risk assessment. The study has two main objectives:

- to explore possibilities and perform quantified and more thorough ship security risk analysis than what is described in the ISPS code and its guidelines, and
- to examine and evaluate the extent to which this more detailed analysis increases a ship's security.

The study focuses on Somali-based maritime piracy, using piracy in the Indian Ocean as a case study. Data are collected through questionnaires and interviews with civilian and military security experts who possess firsthand experience of piracy off the coast of Somalia. The data are collected specifically for this study and describe the threat's capability, intent and likelihood of exploiting a ship's vulnerability.

Sections 2 and 3 describe theoretical risk management and ship security assessment, respectively, the goal of which is to lay a foundation for the current study. The methods used for data collection and evaluation in the study are presented in section 4, and section 5 evaluates the probability of detection by pirates, their successful approach and successful boarding of a ship. The analysis performed for these three steps is then used to discuss the feasibility and value of in-depth quantitative security analysis. Section 6 discusses the analysis and section 7 presents the conclusions.

2 Ship security management

Risk-based approaches have been developed by the IMO since the 1960s. The first risk-based regulation was the 1974 Safety of Life at Sea (SOLAS74) that assessed probabilistic damage stability. In 1997, the IMO adopted the Formal Safety Assessment as a risk-based approach to rule-making (Skjong, 2009). Quantitative risk-based approaches are therefore well established in the area of maritime safety, even though the approaches have not yet been developed for all areas of safety. Ship security methods are not as well developed as ship safety methods. The first security measures and regulations were developed and approved by IMO in 1986 after the terrorist attack on the cruise ship Achille Lauro. However, these measures were mandated only by the US, Canada and the UK (Wengelin, 2012). The ISPS code is therefore the first regulation with the possibility to affect the ship security efforts and it has been classified as a first step in this area by the IMO (Mitropoulos, 2004).

According to the IACS, the class requirements and general industry guidance should be viewed only as a starting point for ensuring the safe and secure operation of a ship. The ship operator is responsible for identifying the risks associated with his or her particular ship, operation and trade. The applied methods must be systematic if assessment and response are to be complete and effective, and the process must be documented to provide evidence of the decision-making process (IACS, 2004).

Figure 1 presents the tools used in the current study that are taken from risk-based ship design, probability risk analysis, military force protection and military operational research (MOR) to perform the analysis and make use of available methods to structurally illustrate, analyze and assess risk.

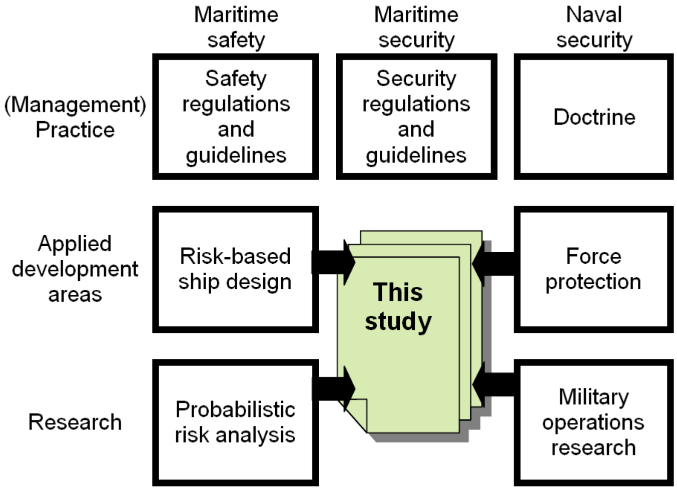
Maritime safety
Maritime security
Naval security
(Management) Practice
Safety regulations and guidelines
Security regulations and guidelines
Doctrine
Applied development areas
Risk-based ship design
This study
Force protection
Research
Probabilistic risk analysis
Military operations research

Figure 1. Schematic of the methodology of the study. As a result of the limited research in the studied area, the methodology uses research and development from relevant areas in maritime safety and naval security to define the proposed tools in order to limit the effects of any subjectivity in the management practice of maritime security.

In this study, risk is considered to be a function of the probability and consequences of a threat. For simplified examples, this function can be described as

$$\text{risk} = \text{consequence} \times \text{probability}. \qquad \textbf{Equation 1}$$

However, the analysis must generally be able to assess more than one type of consequence, and the definition must then be defined specifically for that combination of consequences.

2.1 Risk criteria

Ship owners are responsible for weighing the risks against the costs of implementing control options, but relevant organizations and society also set limitations on allowed risks called risk criteria. Risk criteria have been discussed within the IMO in relation to risk-based approaches (Skjong, 2009).

According to Pedersen (Pedersen, 2010), different principles must be used to formulate risk criteria depending on the nature of the consequence in question. For example, there must be a special focus on incidents with several fatalities because society considers these incidents more severe than multiple incidents with few fatalities. It is therefore reasonable to assume that the risks associated with ship security, that is, piracy and other types of crime at sea, require specific risk criteria as the consequences (possible great human suffering and multiple fatalities) that are incomparable with the traditional operational risks encountered in shipping.

According to NATO, security measures are used not only to minimize the vulnerability of personnel and material but also to preserve freedom of action and operational effectiveness (NATO

Standardization Agency, 2007). Based on this definition, the following types of security risk criteria are suggested for ship security in this study:

- Fatalities.
- Loss of technical systems and materiel.
- Impact on operational effectiveness and freedom of action.

It is important to minimize fatalities and the loss of technical systems, but an incident’s impact on operational effectiveness and freedom of action must also be considered.

Relevant and well-defined risk criteria are a condition for risk analysis because the analysis must assess the types of consequences relevant to the risk criteria.

2.2 Risk control options

A risk analysis must identify different outcomes of a hazard or threat with quantified consequences and their respective probabilities. The level of risk is a function of the consequence and its probability. In other words, the risk is considered high if both the consequence and probability exceed limits set by general or local criteria.

Risk control options, which are a means of controlling of risk, are applied in areas of high risk. Security risk control options range from technical measures included in the design of a ship to specific changes to the watch scheme on board. Typical and recommended risk control options are described in, for example, the ISPS code and the BMP (IMO, 2002a and BIMCO et al., 2011). However, each security threat and ship has a specific risk causality and therefore a specific list of suitable risk control options. These control options can be identified only with the help of a ship-specific risk-based ship security assessment (IMO, 2002a).

3 Ship security assessment

Quantitative risk assessment offers a sound and systematic basis for evaluating potential hazardous activity. However, the methods used for this assessment are specialized and often complex, and an audit of each assessment is vital to ensure that a logical and consistent approach and relevant data have been adopted (Andrews & Moss, 2002).

In the field of ship security, part A of the ISPS code stipulates that a risk-based Ship Security Assessment (SSA) shall be performed for all passenger ships, all cargo ships above 500 gross tons and mobile offshore units in transit. Guidelines exist for performing a SSA according to the ISPS code, and the Norwegian Shipowners’ Association’s Guideline for performing ship security assessment (Norwegian Shipowners’ Association, 2008) is used in this study to define the SSA more precisely in four general parts: initial screening, threat assessment, onboard audit and identification of needs. This study focuses on threat assessment defined by the following two steps:

- Identify threat scenarios, or security incident scenarios, that reflect motives and prioritized operations, areas, systems and personnel.
- Assess likelihood and potential consequences of the scenarios in relation to the ship’s vulnerability (Norwegian Shipowners’ Association, 2008).

3.1 Threat scenario identification and analysis

According to the guideline for performing ship security assessment (Norwegian Shipowners' Association, 2008), the objective for the step *Identify threat scenarios* is to identify the incidents most relevant to the ship's critical operations and trade.

This study applies the analysis documented in the NATO Force Protection Directive (NATO Standardization Agency, 2007) to perform a stringent threat analysis. Threat analysis is described as a tool to support risk management decisions, and it must describe the causality and process of an attack, boarding and hostage-taking. The analysis determines the capabilities and intentions of an identified group or organization and how likely they are to carry out the defined threat and actions (NATO Standardization Agency, 2007):

1. ***Threat capability***. The ability of potential threats to cause harm to assets. Analysis of threat capability considers threat structure, leadership, professionalism, tactics, weaponry, targeting and logistics.
2. ***Threat intent***. The willingness of potential threats to target assets. Analysis of intent considers threat ideology, objectives, strategy, likely intentions and previous history.
3. ***Threat likelihood of exploiting vulnerability***. Analysis of likelihood includes threat history under similar circumstances, the threat's overall campaign plan, currently implemented security controls and measures and the most probable threat course(s) of action.

This description shows that the threat analysis focuses on not only the threat but also the threat in relation to the vulnerability of the assets in question. The importance of analyzing threat and asset interaction has also been stressed by Kunreuther when describing security risk analysis (Kunreuther, 2002).

A threat analysis should address the full range of threats and attack possibilities. This analysis is used as a basis for risk assessment and a tool for countermeasure planning (NATO Standardization Agency, 2007). The NATO threat analysis does not contradict the threat analysis described in the guidelines for performing an SSA (Norwegian Shipowners' Association, 2008), but the force protection directive (NATO Standardization Agency, 2007) is more detailed in its description of the analysis. The analysis described above therefore serves as a baseline for the identification of scenarios, with the goal of defining scenarios with calculable probabilities as demanded by safety risk analysis (Vassalos, 2009).

3.2 Assessing likelihood and potential consequences in relation to vulnerability

According to the Guideline for performing an SSA (Norwegian Shipowners' Association, 2008), the application of the step *Assess likelihood and potential consequences in relation to vulnerability* involves identifying whether and which additional security measures are required. The vulnerability assessment describes a ship's vulnerabilities in terms of a pirate attack. According to the NATO Force Protection Directive (NATO Standardization Agency, 2007), the vulnerability analysis should include deficiencies in planning, preparedness, training, awareness, warning, physical security, hardening, redundancy/back up and response capability. A vulnerability assessment is used to determine the susceptibility of assets to attack from threats identified in the threat analysis, so the analysis must focus on describing the interaction between a pirate's intent, capability, and likelihood to perform an attack and a ship's vulnerabilities.

Risk analysis is used to perform this assessment, and the threat scenarios are structurally compared with the ship's vulnerability to assess possible consequences and their likelihoods (Norwegian Shipowners' Association, 2008).

4 Methodology and data collection

4.1 Statistics on maritime piracy

Piracy incidents involving civilian ships should be reported (Sörenson, 2011) and are collected and documented by the International Chamber of Commerce (ICC) Commercial Crime Services' (CCS) International Maritime Bureau (IMB) (ICC IMB, 2011 and ICC IMB, 2012). The ICC IMB reports on Somali piracy have been criticized; one view states that there is a certain amount of over-reporting of piracy incidents due to the Best Manage Practice (BMP) developed by the shipping industry (BIMCO et al., 2011), which recommends that seafarers who pass the waters off the coast of Somalia and in the Gulf of Aden report any suspicious approaches in the vicinity. There have also been claims of underreporting in the ICC IMB statistics because some ship operators fear that their illegal activity will be disclosed if they report piracy activity (Sörenson, 2011).

According to ship security experts consulted in this study to more accurately describe the piracy occurring off the coast of Somalia, between 85 and 97 % (Figure A.1 in the appendix) of the piracy incidents in the waters off Somalia are reported and documented in official piracy statistics and the ICC IMB reports.

In this investigation, data from incidents from January to May, 2011, are used . They have been extracted from NATO Shipping Centre's overview of the incidents 2009 to 2012 (NATO Shipping Centre, 2012**)** and judged not to be affected by the Northeast or Southwest monsoon. The incidents from January and February are analyzed in depth together with data on maximum ship speed from AIS data (Marine Traffic, 2012).

Table 2. Overview of studied attacks January to May, 2011. The study is based on reports documented in ICC IMB statistics for 2011 (ICC IMB, 2012) and maximum ship speed from AIS data (Marine Traffic, 2012).

Period/ Speed interval	Reported attempts	Aborted approaches	Successful approaches	Average approach success
Jan - May	122	62	60	49 %
Analyzed in regards to ship speed (Jan and Feb)				
No speed info	6	1	5	83 %
< 10 knots	10	6	4	40 %
≥ 10 and < 12 knots	10	5	5	50 %
≥ 12 and < 18 knots	30	20	10	33 %
≥ 18 knots	3	3	0	0 %
Σ Jan and Feb	59	35	24	41 %

Reliable and well-documented statistics on the total shipping activity in the waters off the coast of Somalia are difficult to verify. It is often said that at least 20,000 ships pass through the Gulf of Aden every year (Chalk, 2010 and Kraska, 2010). This investigation therefore assumes annual traffic of 20,000 to 30,000 ships in the part of the Indian Ocean under study based on the fact that not all ships on the Indian Ocean pass through the Bay of Aden.

4.2 Data collection - questionnaires and interviews

Data was collected for use as inputs to the threat description. The data collection was performed in three different steps. In the first step, a questionnaire was sent to experts to collect data on the piracy operating out of Somalia during 2010 and 2011. The second step consisted of interviews with experts to build a wider knowledge base on piracy and the risk management performed by ship owners and operators. In the third step, selected areas of the piracy were revisited with a second questionnaire to decrease the uncertainty of the answers.

4.2.1 Experts

The selection of experts is made to cover different aspects of piracy, security measures and the risk management process. In total, 18 experts from northern Europe are used in the study. All have personal international experience in security work related to the piracy operating out of Somalia. All of the experts:

- are currently, or have been, a part of an organization in which the piracy off the coast of Somalia has had a substantial operational impact,
- possess detailed knowledge on the general conditions for navigation and shipping off the coast of Somalia, and
- have insight into ship security efforts against piracy in their own organizations and internationally.

The experts' profiles are summarized in Table 3.

Table 3. Expert profiles. The expert type *Ship owner and security consultant repr.* contains one expert from a security consultant company.

		Military experience		Senior	Commanding or	Taking part in	
Type of expert	Total	Generic	Off Somalia	position	executive pos	questionnaires	interviews
Navy officers	10	10	10	9	3	10	0
Ship owner and security consultant repr.	8	3	0	8	2	2	8
Σ	18	13	10	17	5	12	8

4.2.2 Questionnaires

The first questionnaire was sent to twelve experts, see Table 3, to collect data on piracy threats' capability, intent, and likelihood. Eleven out of the twelve experts answered the questionnaire, for a response rate of 92 %.

The data treatment and results from the questionnaire used in this study are presented in appendix A and Figures A.1 through A.12, A.14, A.16 and A.18.

Based on the replies of the other panel members, the ten navy experts were encouraged to revise their earlier answers in four areas (number of search groups, percentage using mother ships, number of days at sea, and skiff attack speed) in a second questionnaire according to the Delphi method. This second questionnaire was administered to decrease the range of uncertainty in the answers and approach a consensus assessment (Dalkey, 1969). Eight out of the ten experts answered the second questionnaire, the results of which are presented in Figures A.13, A.15, A.17 and A.19.

4.2.3 Interviews

Semi-structured interviews followed the first questionnaire and were performed with ship security experts and operation managers for ship owners and ship security consultants at four companies. The focus of the interviews was to collect information on relevant risk control options, their purpose, and their effect on the risk of piracy and how the SSA is performed today in the industry. All of the experts have extensive experience with the analysis of operations off the coast of Somalia.

An additional objective of the two interviews was to specifically test the feasibility of the methods discussed for the assessment of the probability of boarding.

4.3 Influence diagrams

As shown in Figure 2 and 3, an event tree methodology is used to model and analyze the possible consequences and probabilities of an attack. The inductive event tree is used because the pirate attack has well-defined chronological steps that are appropriately illustrated by the event tree's sequences. The interviews have also shown that the structure of the event tree is intuitively understood and therefore facilitate effective discussions regarding scenarios with the experts.

The collected data are used to develop models and calculate probabilities in the event tree. The calculations are simulations representing subsets of the scenario, with influences determined according to influence diagrams. The results of the influence analysis play an important role in describing the interaction between pirate characteristics and ship vulnerability throughout the analysis.

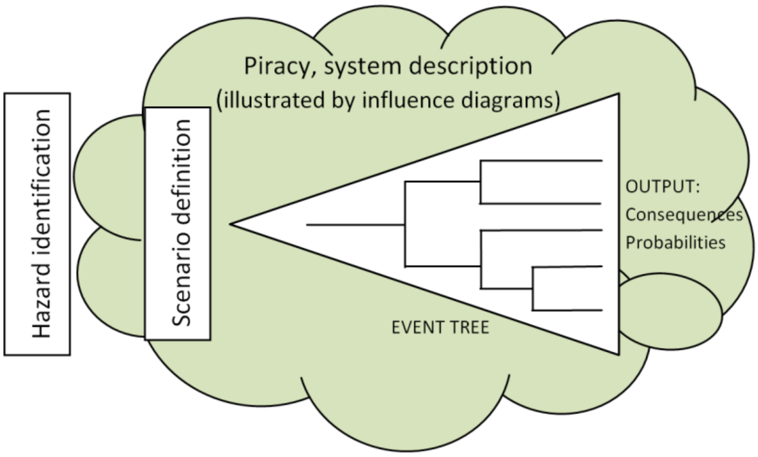

Figure 2. Schematic of the study methodology. The piracy system description serves as a background for hazard identification and risk analysis, and the risk analysis consists of scenario definition and event tree analysis.

The data collected using the methods in section 3.2 are used to perform the analysis according to Figure 2, and the statistics described in section 3.1 are used to discuss the validity of the results.

An influence diagram is a graphical and mathematical representation of a network of influences on an event. The methodology of influence diagrams is derived from decision analysis, and according to IMO, it is particularly useful in situations for which there may be little or no empirical data available and the approach is capable of identifying all the influences (and therefore the underlying causal information). An influence diagram is composed of nodes and arcs depicting known and uncertain elements and indicating which elements influence the outcome of the event. The influence diagram approach described by IMO uses expert judgment to model the network of influences, and these influences link factors at the operational level with their causes and the underlying influences (IMO, 2002 and Shachter, 1988). The difference between the influence diagram approach proposed by IMO and the decision analysis application of influence diagrams described by Shachter is that IMO proposes to use influence diagrams only to illustrate influences, as performed in sections 5.1.1 and 5.2.1. However, the diagrams are most often both an illustration of influences and a mathematical analysis tool in decision analysis, as performed in section 5.3.1.

This study uses influence diagrams to illustrate how low-level aspects affect a scenario, and the diagrams serve as a system definition and system description. The diagrams also describe the limitations and demarcations of modeled parameters, and the links between the different influences and threat components define the system in this study.

Based on the influence analysis, hazards and scenarios are defined and used as inputs to the risk analysis. The system's underlying causal information is described by the influence analysis, and it provides inputs to the event tree development.

5 Analysis

The threat scenario is in this study is divided into six chronological steps, as illustrated by steps A through F in the event tree in Figure 3. The structure of the tree, A through F, is constructed from the results of the interviews and questionnaires. The probabilities in the tree (P_A through $P_{F,2}$) denote the conditional probabilities for each step given the outcome of the previous step in the figure.

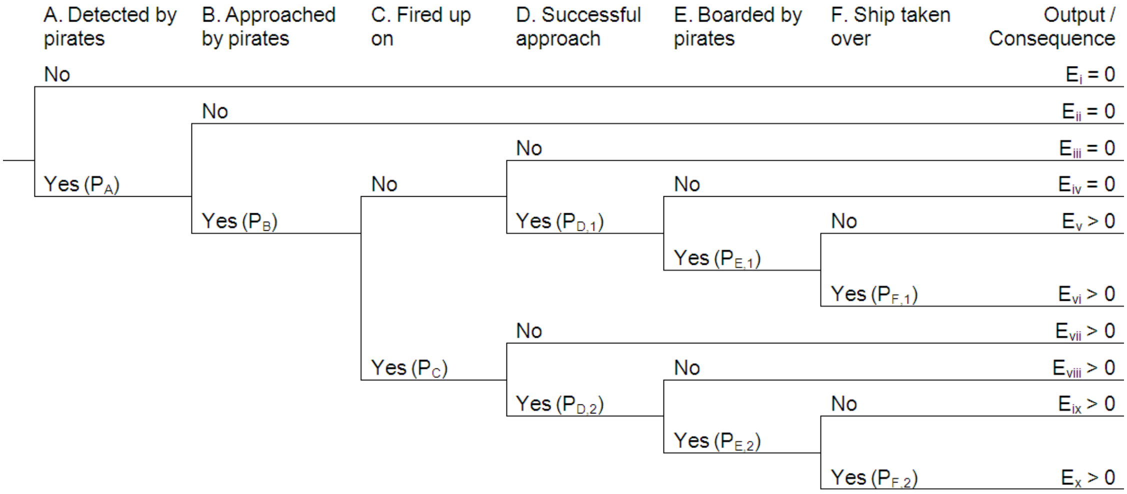

Figure 3. Event tree for the definition of a general scenario in this study.

If the probabilities P_A through $P_{F,2}$ in Figure 3 are known the probability for each output E_i to E_x can be calculated by multiplying the probabilities for each branch, for example is the probability for E_x given by

$$P(E_x) = P_A\, P_B\, P_C\, P_{D,2}\, P_{E,2}\, P_{F,2}$$ **Equation 2**

and the probability for E_{iii} given by

$$P(E_{iii}) = P_A\, P_B\, (1\text{-}P_C)\, (1\text{-}P_{D,1}).$$ **Equation 3**

The steps *A. Detected by pirates*, *D. Successful approach*, and *E. Boarded by pirates* are evaluated in sections 5.1, 5.2 and 5.3, respectively, and the analysis performed for these tree steps is used to discuss the feasibility and value of the proposed quantitative security analysis.

The study is limited to piracy operating out of Somalia on the Indian Ocean during 2010 and 2011, and the numerical results are calculated assuming that $P_{D,1} = P_{D,2}$ and $P_{E,1} = P_{E,2}$. This investigation studies only the consequences of a pirate attack and/or approach. Piracy in the Indian Ocean is selected as the focus of study because this area is relatively well documented in incident statistics and allows for expert assessments.

5.1 Probability of detection by pirates on a route across the Indian Ocean (P_A)

5.1.1 Identification of threat scenarios

The high risk area on the Indian Ocean has changed in recent years with the changing modus operandi of the pirates, as described in section 1. The probability of detection in different areas is therefore important when choosing a route over the Indian Ocean.

The threat capability is defined as follows.

- The average number of groups at sea on the Indian Ocean is 12, with a quartile distance of 7, during periods of high piracy activity, as seen in Figure A.13.
- The experts assess that approximately half (48 %) of the searching attack groups on the Indian Ocean operate from a mother ship. However, the value is assessed with great uncertainty, as seen in Figures A.15 and A.14.
- The number of days an attack group can be at sea without support from a mother ship or land is 7.5, with a quartile distance of 4 (Figures A.17 and A.16).
- According to the experts (Figures A.2 to A.7), the search groups have very limited ability to collect information about ship movements and specific ships. The skiffs, however, sometimes possess GPS as a navigational aid. Search groups therefore lack specific information about ship movements but often have a rough idea about their own positions. There is very little information exchange and cooperation between different search groups.
- Shore bases are spread out along the Somali shoreline.
- Fuel is a limiting resource (Figure A.8), and according to the interviews, speed is therefore low during searches.
- During periods of good visibility, a skiff with a good lookout can detect a ship at a great distance, and this study bases the detection distance on the ship height, skiff height and Earth’s curvature.

The threat intent is defined as follows.

- A search group departing from land wants to search as far from shore as possible to reduce the probability of detection by military forces and increase the possibility of finding ships to attack.
- Mother ships attempt to cover relevant areas of the Indian Ocean but avoid the waters close to the Somali shore.
- The search groups attempt to spread out from other groups and change position frequently to reduce the risk of interception.
- The search groups have no specific knowledge about other search groups (Figure A.4).

The likelihood of exploiting a ship’s vulnerability is defined by the following factors.

- Height.
- Ability to choose a route with low probability of detection.

These factors are illustrated by an influence diagram in Figure 4.

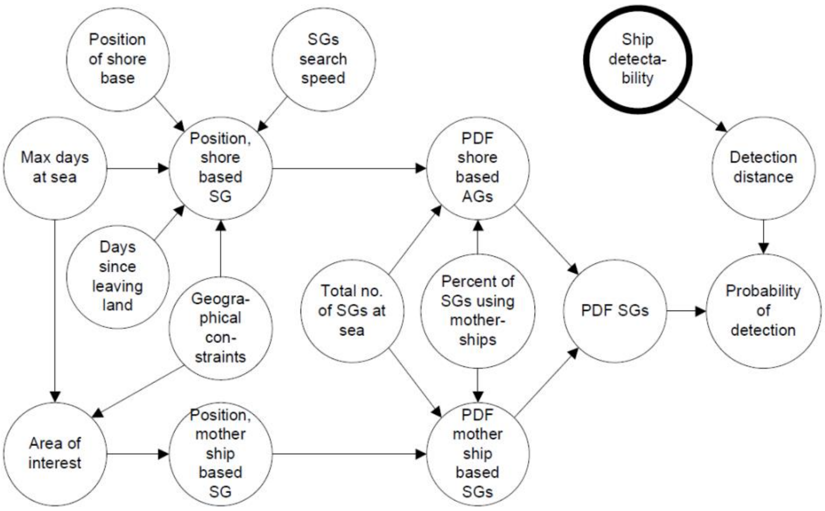

Figure 4. Influence diagram of the influences on search groups' (SG) probability density function (PDF) and the probability of detection by pirates in a high risk area (P_A). A thick line indicates that the node's states are deterministically decided. In other words, the ship's height is given, and it is the only aspect in this study that governs the ship's detectability.

5.1.2 Assessment of likelihood and potential consequences in relation to the ship's vulnerability

By developing the influences on the probability density functions of search groups in Figure 4, the density distribution over a simplified representation of the Indian Ocean is calculated and visualized in Figure 5.

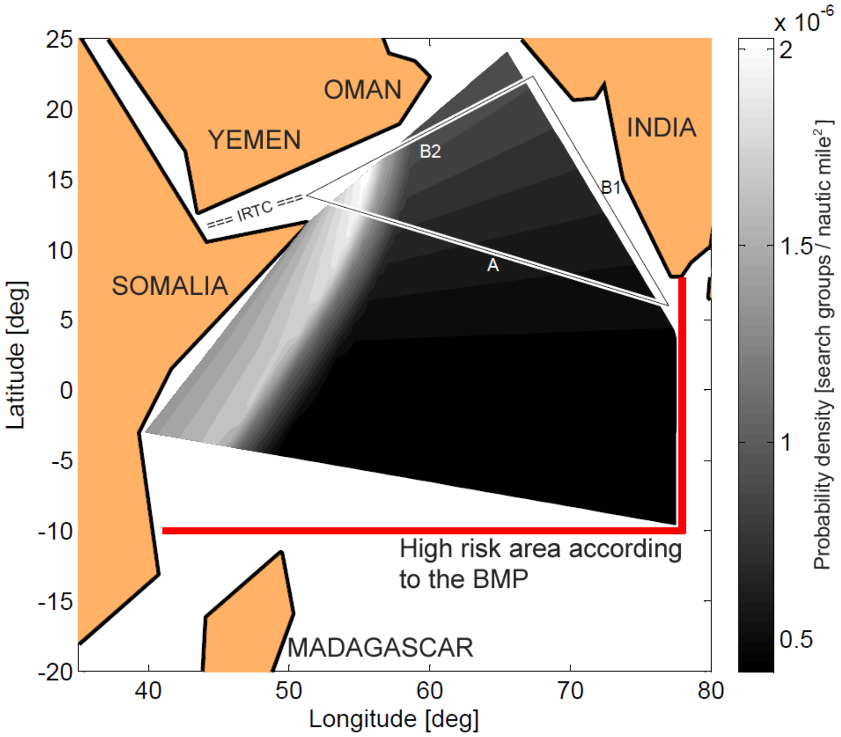

Figure 5. Probability density for search groups in a representation of the high risk area (BIMCO et al., 2011) on the Indian Ocean. The calculations are given for 58 % mother ships during high skiff activity and good weather conditions. A and B=B1+B1 represent the routes analyzed with respect to the detection probability in Table 4.

To calculate the probability of detection by pirates, this investigation studies two different alternatives for ships traveling from East Asia on a route to the east entrance of the International Recommended Transit Corridor (IRTC). Alternative A is the shortest route from the south tip of India to the entrance of IRTC and alternative B (B1+B2) follows India’s coastline through safe waters to the closest point to the IRTC. Alternative A minimizes the total distance, and alternative B minimizes the distance traveled through a high risk area; both routes are currently in use by ships, as shown in Table 4.

Table 4. Evaluation of detection probability on different routes through the high risk area during high skiff activity and good weather conditions. This is a conservative assumption because a reduction in ship detection distance will reduce the probability of detection. The probability of detection is calculated from the probability density of the attack groups, as shown in Figure 5, and based on the assumption that the pirates can detect a ship at 20,200 meters (given a ship height of 20 meters, a pirate skiff height of 2 meters and ship vulnerability according to section 5.1.1).

		Probability of a pirate encounter (P_A)		
Route	Total distance [NM]	40 % mother ships	48 % mother ships	58 % mother ships
A	1,600	0.014	0.014	0.014
B	2,200	0.015	0.014	0.014

5.1.3 Results and their validity

The ICC statistics for 2011 described in Table 2 document 32 actual attacks and 90 attempted attacks, for a total of 122 incidents over 5 months. Assuming that only 90 % of incidents are reported (see Figure A.1), the total number of incidents is approximately 136. The total traffic per year through the area is 20,000 to 30,000 ships, assuming that the traffic is evenly distributed over the year, which means that approximately 8,300 to 12,500 ships pass through the area every five months. This assumption means that approximately one to two percent of the ships traveling through the area are sighted by pirates. The results of 1.4 % to 1.5 % in Table 4 are therefore a reasonable assumption based on the available statistics on piracy incidents.

The total value of the probability density is proportional to the number of attack groups at sea, but more importantly, the density distribution is sensitive to the assessed percentage of attack groups operating from mother ships. Because the tested routes in table 1 move through the area from east to west and only the total probability of an encounter is calculated and compared to the statistics, the calculation is not sensitive to specific variations in the PDF along the route. A route from north to south is much more sensitive to the percentage of mother ships.

5.2 Probability of successful approach (P_D)

5.2.1 Identification of threat scenarios

To date, there have been no reported attacks in which pirates board a ship that is proceeding at more than 18 knots (BIMCO et al., 2011), but the results from the questionnaire show that many skiffs can travel much faster than 18 knots. It is therefore possible that pirate tactics and techniques may develop to enable them to board ships moving at faster speeds.

The threat capability is defined as follows.

- When attacking a ship, the average attack speed for skiffs is between 20 and 30 knots (Figures A.19 and A.18).
- The maximum skiff speed is reduced when the skiff enters the wave system of a ship, especially for ships moving at fast speeds.
- A skiff with a good lookout can detect a ship at a great distance during good visibility, and this study bases the detection distance on the ship height, skiff height and Earth's curvature.
- According to Figure A.8, the second most limiting factor for pirates is fuel, which limits their maximum approach time. Attacks typically last between 30 and 45 minutes on average (Chalk, 2010).

The threat intent is defined as follows.

- The pirates plan to test the feasibility of approach and boarding and try to intimidate a ship to reduce its speed or stop to allow for easy boarding.
- The pirates are reasonably conservative with fuel, as shown in Figure A.8.

The likelihood of exploiting a ship's vulnerability is defined by the following factors.

- A ship with a good lookout can detect a skiff during the day at distance of 2,000 meters, with a quartile distance of 1,600 meters. The detection distance decreases to 200 meters during the night. The experts' assessment of radar detection distance in calm seas is 3,000 meters, but this figure has high uncertainty (a quartile distance of 4,500 meters). In rough seas, the radar detection is drastically decreased to 100 meters (Figure A.9).
- According to the interviews, a ship's vigilance is important and dictates at what distance the ship detects an approaching skiff. The ship can alter its course to increase the approach time by as much as possible when pirates are detected.

This analysis is used to develop the influence diagram for the probability of a successful approach shown in Figure 6.

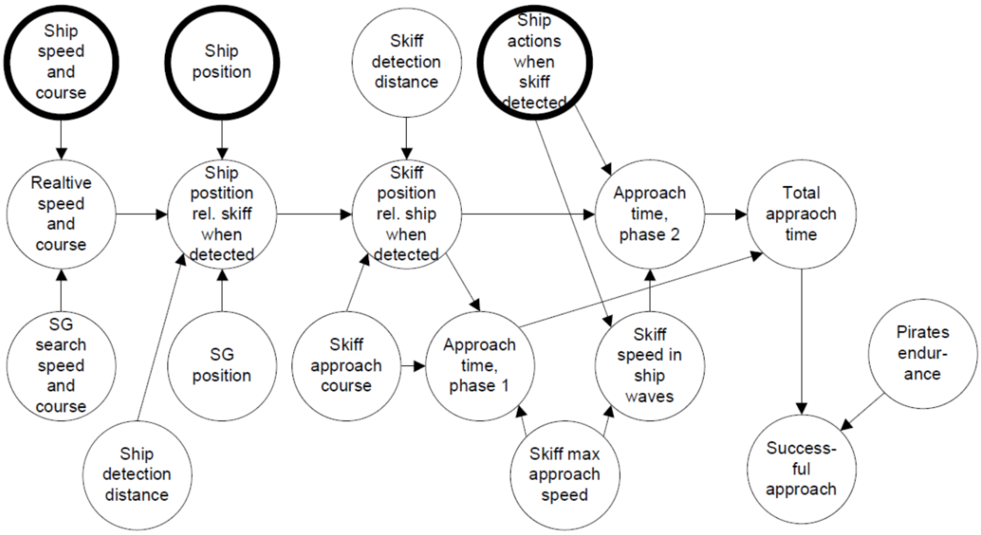

Figure 6. Influence diagram of approach scenario, assuming that the ship is within detection distance of a skiff. A thick line indicates that the node's states are deterministically decided.

5.2.2 Assessment of likelihood and potential consequences in relation to the ship's vulnerability

A successful approach is defined as an approach that can bring the skiff to the ship in less than t_{abort} minutes. The probability is calculated assuming that the ship is detected by the skiff. The influence diagram in Figure 6 is developed in a Monte Carlo simulation (Parnell, 2007) where the specific values for the low level influences, such as skiff maximum speed, are generated according to the experts' assessments and the scenario described above. The approach time is then deterministically calculated, where the skiff approach is defined by a dog curve with an aiming point 1,000 meters ahead of the ship and that the ship alters its course away from the skiff when the skiff is detected. The calculation is therefore a simulation of repeated attacks on calm seas during daytime and good visibility. The calculated results of the simulation are presented in Figure 7.

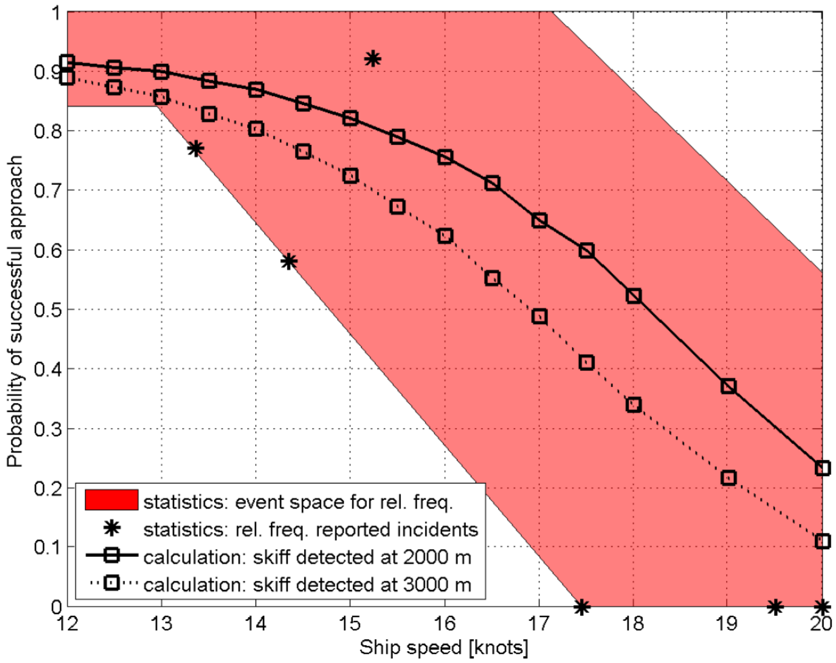

Figure 7. Calculated probability of a successful approach (P_D) and event space based on the frequency of successful approaches in reported incidents and the relative average frequency of successful approaches for ships with speeds below 12 knots. The calculations are performed for t_{abort} = 30 minutes, based on the capability and intent described in section 5.2.1 and with the assumption of good weather conditions. See Figure A.20 for the frequency of successful approaches in reported incidents and the reference value used to calculate the relative frequency.

5.2.3 Results and their validity

A statistical hypothesis test of the reported attacks and attempted attacks on the Indian Ocean described in Table 2 shows that there is no statistically significant difference between the frequency of successful approaches for ships traveling below 10 knots and those traveling between 10 and 12 knots. In other words, it is reasonable to assume that circumstances other than speed lead to unsuccessful approaches when considering ships that travel at speeds below 12 knots. The statistics are more scattered when considering ship speeds above 12 knots, and the 33 incidents studied in this region are too unreliable for extensive quantitative analysis, especially because it is impossible to eliminate the effects of circumstances other than speed. However, by using the frequency of successful approaches for ships traveling at speeds below 12 knots as a reference measure for the approaches aborted for reasons other than speed, the relative frequency of successful approaches is plotted in Figure 7 for speeds between 12 and 18 knots. The maximum and minimum values for the plotted frequency are then used to define an event space for the probability of approach as a function of ship speed. See Figure A.20 for more details on the successful approaches in reported incidents.

The results of the calculations fall within the event space of the reported incidents under study and the speed dependency of the event space agrees with the calculated dependency. Therefore, it is reasonable to assume that the performed analysis captures several important aspects of the approach sequence.

As described in section 5.2, the BMP states that no ships with speeds above 18 knots have been successfully boarded, but there are also reports in the statistics describing skiffs that have matched speeds as high as 25 knots (ICC IMB, 2012). Defining the probability of successful approach as a function of speed and detection distance, as performed in Figure 7, rather than defining a secure speed, is therefore a much more reasonable description of the threat.

According to the calculations using the proposed methods, the probability of successful approach for ships traveling at 18 knots is between 0.4 and 0.5 during good conditions. In many situations, the weather conditions reduce the skiff maximum speed, which decreases the probability further and means that boarding fast ships is unfeasible. According to Figure 7, the breaking point, where the speed's effect on the probability of successful approach increases, lies somewhere between 15 and 18 knots, which is in agreement with the BMP's statement.

5.3 Probability of successful boarding (P_E)

5.3.1 Identification of threat scenarios

The interviews with ship owners show that the philosophies on protection measures against boarding differ from owner to owner and are dependent on the type of ship in question. Some ship owners focus on keeping pirates far from the ship, while others assume that the ship can be made almost impossible to board with high speed and high freeboard.

The threat capability is defined as follows.

- The pirate's endurance and experience to perform a successful boarding (Figure A.10).

The threat intent is defined as follows.

- The pirates intend to board at the position with the lowest protection.
- The pirates are willing to risk injury but not life during the attempt.

The likelihood of exploiting a ship's vulnerability is defined by the following factors.

- The interviews make it clear that different boarding points have specific characteristics and protective measures. Boarding at low access points (i.e., mooring stations) is possible only if they are situated at positions where the ship's wave system at speed allows for a suitable skiff position, and these points are often the easiest to protect. The freeboard, on the other hand, is harder to protect, and there are always positions suitable for skiffs along the ship (Figure A.18).
- The probability of military intervention (Figure A.10).
- Light conditions (Figure A.11), which can be supplied either by daylight or moonlight.
- Prepared armed guards (Figure A.10).

Using the threat analysis above and the description of a ship owner's protection against boarding, a network of influences on the probability of successful boarding is defined in the influence diagram in Figure 8. Each node in this diagram is described by a discrete number of states, such as *yes* or *no*.

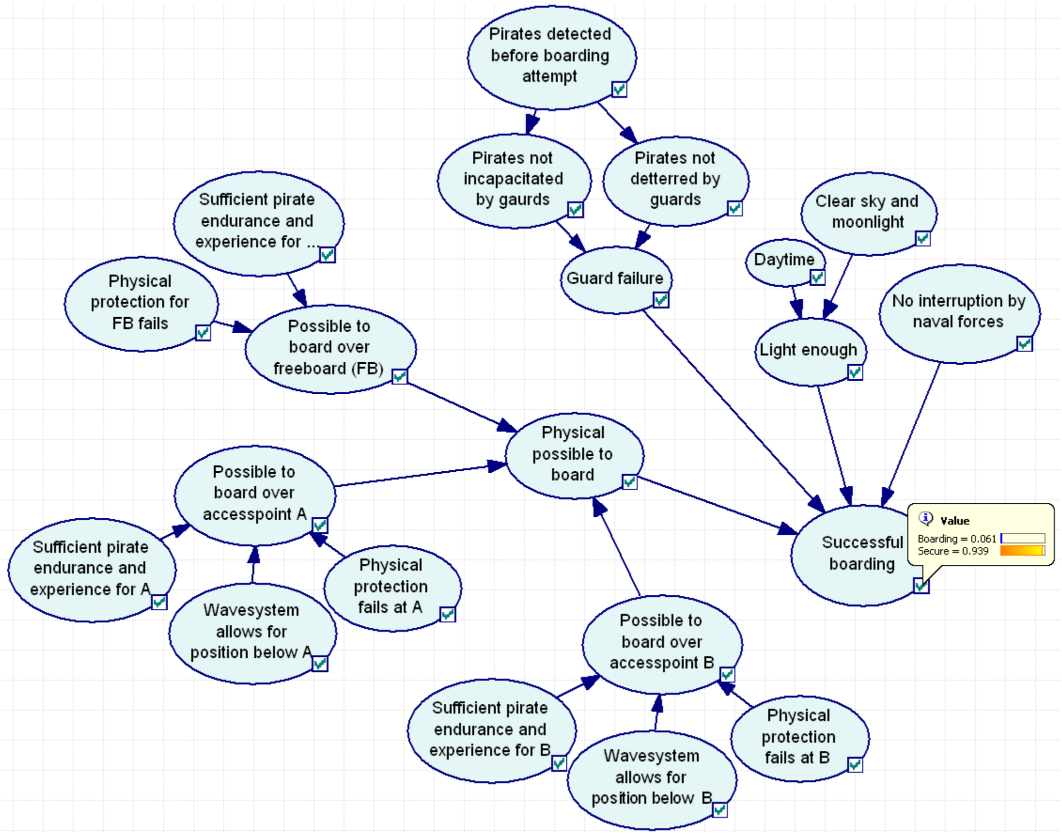
Pirates detected before boarding attempt
Pirates not incapacitated by gaurds
Pirates not deterred by guards
Sufficient pirate endurance and experience for ...
Clear sky and moonlight
Physical protection for FB fails
Guard failure
Daytime
Possible to board over freeboard (FB)
No interruption by naval forces
Light enough
Physical possible to board
Possible to board over accesspoint A
Successful boarding
Value
Boarding = 0.061
Secure = 0.939
Sufficient pirate endurance and experience for A
Physical protection fails at A
Wavesystem allows for position below A
Possible to board over accesspoint B
Sufficient pirate endurance and experience for B
Physical protection fails at B
Wavesystem allows for position below B

Figure 8. Influence diagram describing the probability of a successful boarding, P_E. The probability of a successful approach can be calculated given defined states and probabilities or conditional probabilities for each node. The values given in the figure are a result of a sample calculation. This influence diagram is created using GeNIe by the Decision Systems Laboratory of the University of Pittsburgh (Decision Systems Laboratory, 2012).

5.3.2 Assessment of likelihood and potential consequences in relation to the ship's vulnerability

A specific influence diagram must be developed for each ship under study based on the influence diagram in Figure 8. This process must also be supported by clear and precise definitions of the terms and states being used and how the quantified probabilities should be understood.

The probability of successful boarding can be calculated using the influence diagram itself for a specific ship if the probabilities and conditional probabilities can be assessed for the states of each node.

5.3.3 Results and their validity

There are no available statistics with which to estimate the frequency of successful boarding. It is therefore impossible to test quantified outputs obtained from an influence diagram such as that illustrated in Figure 8.

The feasibility of using the influence diagram in Figure 8 as a tool to assess the effectiveness of boarding protection measures is discussed in two interviews, which reveal that calculating absolute probabilities from the model is difficult without experience and benchmarking. However, calculating the relative probabilities for different ships in a fleet to examine the need for further measures is feasible and can give insight on the causality between various measures and the protection they offer. One suggestion given in the interviews involves using the influence diagram approach when changes in piracy risk control options are being discussed. The influence diagrams and probabilities can be used to document the options under consideration and facilitate a rational discussion process.

The interviews also focus on the fact that the influence diagram can function as a communication tool between parties on board and at shore. The structure of the diagram and probability assessment can also be easily updated during this information exchange, which will allow the organization to gain and document knowledge on risk control options and the vulnerability of specific ships over time.

The current results are supported by the results from Friis-Hansen's research on influence diagrams in maritime safety (Friis-Hansen, 2000). Friis-Hansen uses influence diagrams to analyze several different cases in maritime safety, and it is found that the real advantage of influence diagrams is the focus on causal relationships and that they are "intuitive, conceptual, and easily understood by all involved parties" (Friis-Hansen, 2000). Consequently, it is possible to agree on and validate the topology of the system with the help of engineers, operators and others.

6 Discussion

The study has two main objectives: to explore possibilities and carry out quantified and more thorough ship security risk analysis than that described in the ISPS code and its guidelines and to examine and evaluate to what extent this more detailed analysis increases a ship's security. The study collects data on piracy from subject matter experts to support the quantified analysis because the available statistics do not fully describe the causality of the incidents.

To meet the demands placed on systematic methods, the study follows recommendations from other areas of risk and security analysis and uses tools from maritime safety, military force protection and decision analysis.

The results of the calculations for the probability of detection (P_A) and probability of successful approach (P_D) are compared to available incident reports. The uncertainties of the frequencies obtained from the reports are high due to limitations, but the results of the calculations are inside the event space of the statistics and cannot be rejected by the statistical analysis. Based on the results of the statistical analysis, it is therefore reasonable to assume that the performed calculations capture several of the important causalities involved. Apart from that the calculated probabilities are reasonable; there are also important qualitative aspects of the approach under study.

Based on the conducted interviews, it can be concluded that the ship security efforts performed by many European ship owners are sound and well thought out, but if the security experts' preferred risk control options are challenged, they will have problems with presenting proof of that their choices were appropriate. A greater focus on methods that quantify probabilities and consequences, along with quantified data, would allow the specific analysis to be continually tested against, and updated with, data collected over time. Such a process is almost impossible to accomplish with the qualitative analysis performed today. Continuous testing and updating would provide a more detailed and validated analysis and a better understanding of the problem itself and why and how different ship security measures work. This understanding would then also allow for experts to receive feedback that would be crucial to reducing the errors in expert assessment (Hansson, 1993).

The proposed method therefore provides the possibility of illustrating and understanding the causality and influences on a risk more extensively than what is possible with the current methods discussed in the interviews. The analysis methods allow for the testing of different risk control options and explain how and to what extent the chosen options reduce the risk to stakeholders such as masters, security officers, owner representatives and flag state officials.

Risk analysis is used to minimize risk in many engineering applications, but the method can also be used to identify the most robust control options, such as the options that work for the largest range of threat parameters or the options that are least sensitive to the uncertainty in the analysis (Parnell, 2007). Because the analysis and threat are described with relatively substantial uncertainties, the option of identifying robust control options is most likely the most appropriate.

It is not necessary for all of the areas described in this study to be analyzed by ship owners. General analysis can be performed by international organizations, but final analysis must always be ship-specific and under full control of the ship owner. For example, the attack group probability density function, illustrated in Figure 5, could be calculated by international organizations based on a basic model of attack group activity as a service to the shipping industry and updated based on reports and intelligence. Making such a detailed probability density easily accessible would facilitate routing decisions and support more detailed analysis by ship owners.

This study is performed on a case study concerning maritime piracy off the coast of Somalia. Other types of crime exist at sea, such as piracy with other modus operandi and smuggling. The data and models developed in this study are specific to the piracy off the coast of Somalia and the years 2010 and 2011, but the possibilities for quantitative risk assessment could most likely be generalized to other ship security areas, especially when documenting the threat’s capability, intent and likelihood in relation to a ship’s vulnerability.

We analyze only those threats related to actual consequences in this study, even though the perception of safety is also important in security measures. The reassurance that the measures give is important because the utility of security measures is not equal to the risk reduction (Kunreuther, 2002). Therefore, it is important to minimize fatalities and the loss of technical systems, but these issues also combine to affect the impact on perceived safety. There can also exist relevant measures that do not affect actual risk, only perceived safety.

7 Conclusions

This study shows that it is possible to collect data on pirates’ capability, intent and likelihood of exploiting vulnerabilities through a combination of questionnaires and interviews. The use of the Delphi method decreases the uncertainty in the collected data.

Influence diagrams facilitate the use of a combination of quantified data and qualitative descriptions to analyze threats. In areas where it is possible to compare the results of the performed analysis (in terms of probabilities) with incidents reports (aggregated to frequencies), the results of the study fall within the statistics’ event space and can therefore be assumed to capture several of the causes contributing to the situation.

The interviews performed as part of this study show that the combination of graphical illustration and quantitative output used in this analysis method, including influence diagrams based on quantitative data and qualitative descriptions, not only calculates probabilities but also enables a qualitative discussion on causes and measures that is impossible with the qualitative analysis often performed today. Such a discussion is very valuable to the decision-making process. However, the interviews also make it clear that the proposed method requires more work than what is put into the current analysis methods.

Acknowledgements

This work would not have been possible without support from naval experts in the Royal Swedish Navy, such as Cdr Håkan Nilsson (CO of HSwMS Carlskrona during Operation Atalanta in 2010), and the safety and security managers of ships with operations off the coast of Somalia.

The study was funded by the Swedish National Defence College (www.fhs.se) and the Swedish Competence Centre in Maritime Education and Research, LIGHTHOUSE (www.lighthouse.nu).

The models described in section 5.3 of this paper were created using the GeNIe modeling environment developed by the Decision Systems Laboratory of the University of Pittsburgh (http://genie.sis.pitt.edu/).

References

Andrews, J. D., Moss, T. R., 2002. Risk Assessment. In: Reliability and Risk Assessment, (2:nd ed.), pp. 413-448. Professional Engineering Publishing Limited, Suffolk.

BIMCO, CLIA, ICS, IGP&P, IMB, IMEC, et al., 2011. Best management practices for Protection against Somalia Based Piracy. Witherby Publishing Group Ltd, Edinburgh.

Chalk, P., 2010. Piracy off the Horn of Africa: Scope, Dimensions, Causes and Responses. Brown Journal of World Affairs XVI (Issue II), 89-108.

Dalkey, N. C., 1969. The Delphi method: An experimental study on group opinion. The Rand Corporation, Santa Monica.

Decision Systems Laboratory, 2012. GeNIe & SMILE. http://genie.sis.pitt.edu/. (Oct. 2, 2012).

Friis-Hansen, A., 2000. Bayesian networks as decision support tool in marine applications. Technical University of Denmark, Kgs. Lyngby.

IACS, 2004. A guide to risk assessment in ship operations. International Association of Classification Societies, London.

ICC IMB, 2011. Piracy and armed robbery against ships, Annual report 2010. ICC International Maritime Bureau, London.

ICC IMB, 2012. Piracy and armed robbery against ships, Annual report 2011. ICC International Maritime Bureau, London, UK.

IMO, 2002a. Chapter XI-2, The international ship and port facility security code. In SOLAS. International Maritime Organization, London.

IMO, 2002b. Guidelines for formal safety assessment (FSA) for use in the IMO rule-making process. International Maritime Organization London.

Hansson, S. O., 1993. The false promise of risk analysis. Ratio-New Series 6 (1), 16-26.

Juhl, J. S., 2009. Risk-Based Approval. In: Papanikolaou, A. D. (Ed), Risk-Based Ship Design, Methods, Tools and Applications, pp. 153-194. Springer, Berlin.

Kraska, J., 2010. Freakonomics of Maritime Piracy. Brown Journal of World Affairs xvi (issue ii), 109-119.

Kraska, J., Wilson, B., 2008. Fighting Pirates: The Pen and the Sword. World Policy Journal, 41-52.

Kunreuther, H., 2002. Risk analysis and risk management in an uncertain world. Risk Analysis 22 (4), 655-664.

MarineTraffic, 2012. Search Vessels Details. December 2012. http://www.marinetraffic.com/ais/. [Available: 2013-02-20.]

Mitropoulos, E. E., 2004. IMO: Rising to new challenges. WMU Journal of maritime affairs 3 (2), 107-110.

NATO Shipping Centre, 2012. Piracy Statistics. 28th of December 2012. http://www.shipping.nato.int. [Available: 2013-02-20.]

NATO Standardization Agency, 2007. Allied joint doctrine for force protection, AJP-3.14. NATO, Brussels.

Norwegian Shipowners' Association, 2008. Guideline for performing ship security assessment. Norwegian Shipowners' Association, Oslo.

Parnell, G. S., 2007. Value-focused thinking. In: Loerch, A. G., Rainey, L. B. (Eds) Methods for conducting military operational analysis, pp. 619-655. Military Operations Research Society, Washington DC.

Pedersen, P. T., 2010. Review and application of ship collision and grounding analysis procedures. Marine Structures 23, 241–262.

Shachter, R. D., 1988. Probabilistic inference and influence diagrams. Operations Research 36 (4), 589-604.

Skjong, R., 2009. Regulatory Framework. In: Papanikolaou, A. D. (Ed), Risk-Based Ship Design – Methods, Tools and Applications, pp. 97-151. Springer, Berlin.

Sörenson, K., 2011. Wrong Hands on Deck? Combating Piracy and Building Maritime Security in Eastern Africa. Swedish Defence Research Agency, Stockholm.

Thomson Reuters, 2013. Web of Science. http://wokinfo.com/. [Available: 2013-02-20.]

Vassalos, D., 2009. Risk-Based Ship Design. In: Papanikolaou, A. D. (Ed), Risk-Based Ship Design – Methods, Tools and Applications, pp. 17-96. Springer, Berlin.

Wengelin, M., 2012. Service, regulations, and ports. An actor perspective on the social dimension of service-dominant logic. Lund University, Lund.

Yang, Y.-C., 2011. Risk management of Taiwan's maritime supply chain security. Safety Science 49, 382-393.

Appendix

Experts are asked to choose the interval that best suited their assessment in 9 questions on the first questionnaire. The intervals are decreased for high and low values to ensure that these values are captured correctly. The results from the interval questions are analyzed using a histogram in which the y-axis represents the relative frequency density of each interval.

The experts are asked to give a specific number representing their assessment in 3 questions on the first questionnaire and 4 questions on the second. These questions are analyzed using a box plot.

The experts are asked to name a specific number of factors that have the most influence on the area being discussed in 3 questions on the first questionnaire. The results of these 3 questions are displayed using a column plot in which each column displays the percentage of the times the factor is mentioned in relation to the total number of mentions of all factors.

The data are treated to increase robustness and decrease sensibility to outliers. For questions with interval answers, the lowest and highest answers are classified as outliers and removed from the data set before the results are plotted. The outliers on the box plots are defined as the observations that fall beyond the:

lower limit: $Q1-1.5(Q3-Q1)$, or **Equation 4**

upper limit: $Q3+1.5(Q3-Q1)$ **Equation 5**

where Q1 and Q3 are the first and third quartile, respectively. These observations are depicted using a circle, and the whiskers in the box plot represent the lowest and highest values not classified as outliers.

Areas assessed only in the first questionnaire presented in Figure A.1 to A.11. Areas both assessed in the first and the second questionnaire presented in Figure A.12 to A.19. Incident statistics presented in Figure A.20.

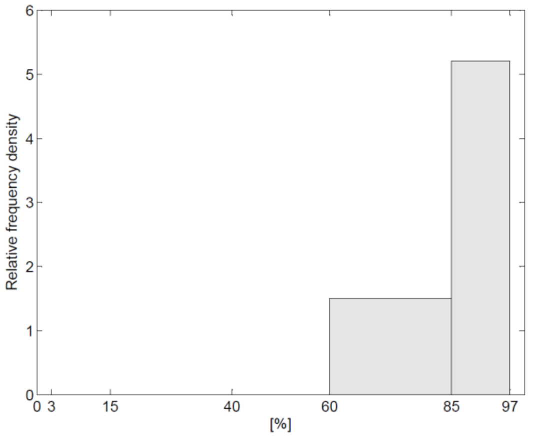

Figure A.1. Percentage of incidents reported in statistics.

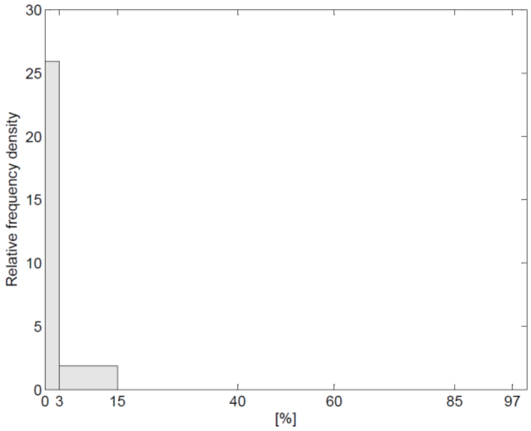

Figure A.2. Percentage of search groups with information from radar.

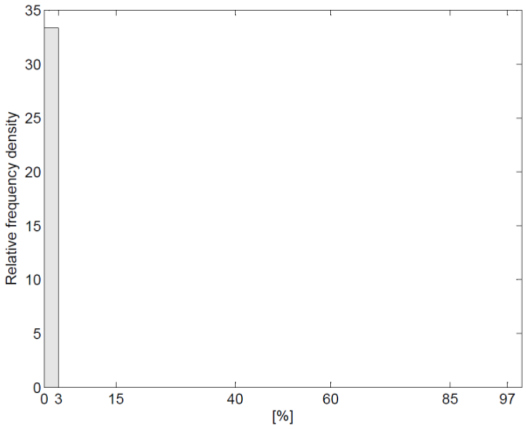

Figure A.3. Percentage of search groups with information from AIS.

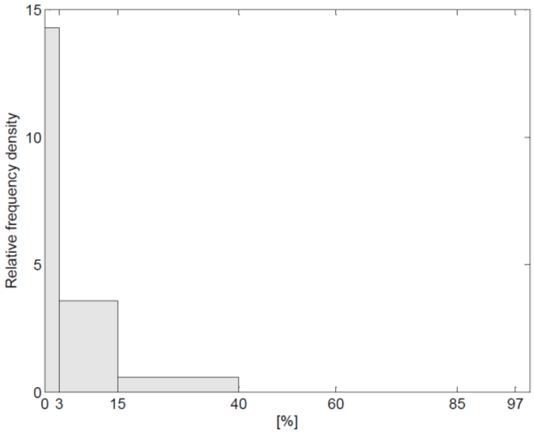

Figure A.4. Percentage of search groups with the ability to contact other search groups by radio.

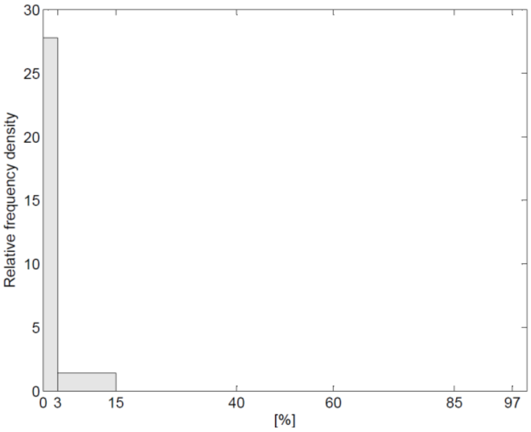

Figure A.5. Percentage of search groups with information from the Internet.

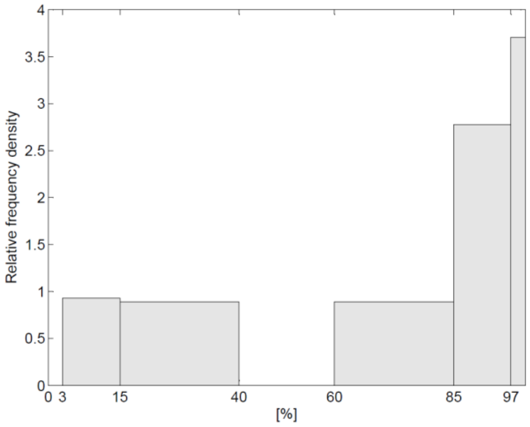

Figure A.6. Percentage of search groups with information from GPS.

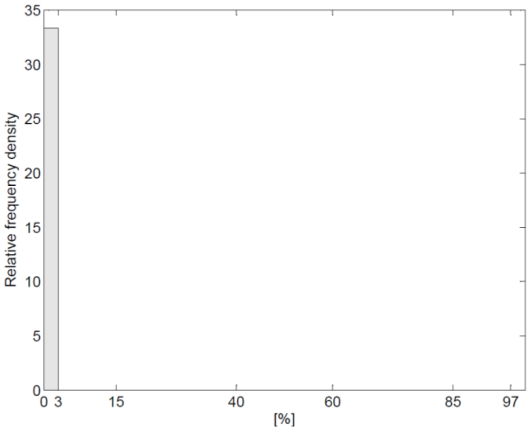

Figure A.7. Percentage of search groups with information from night vision devices.

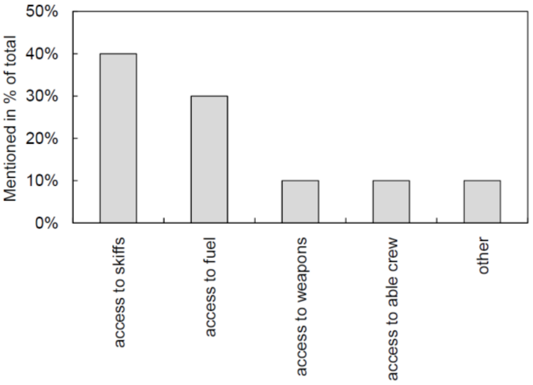

Figure A.8. Limiting factors for pirates.

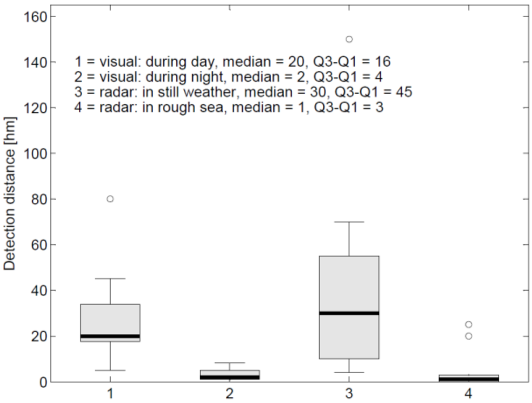

Figure A.9. Skiff detection distance.

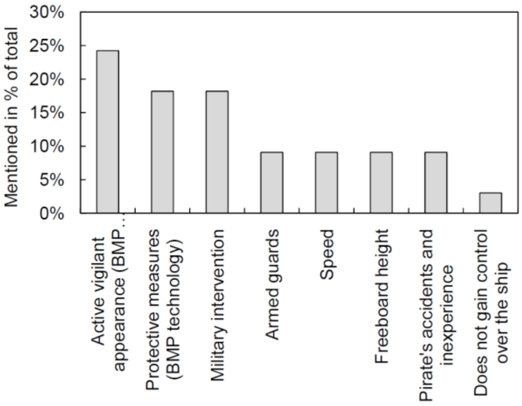

Figure A.10 Factors most influencing pirates' choice to abort an attempt.

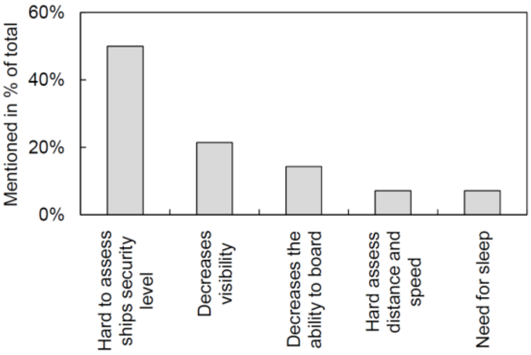

Figure A.11 Most important effects of darkness.

Areas assessed in both the first and second questionnaires

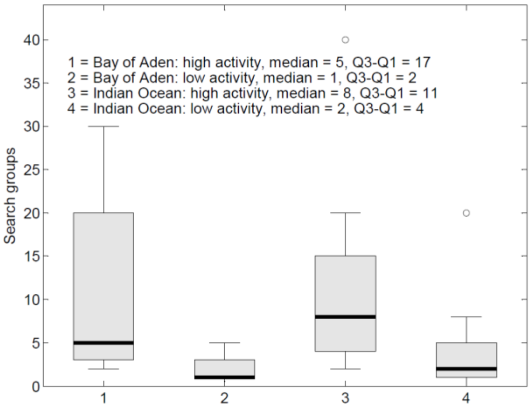

Figure A.12. Number of search groups at sea, first questionnaire.

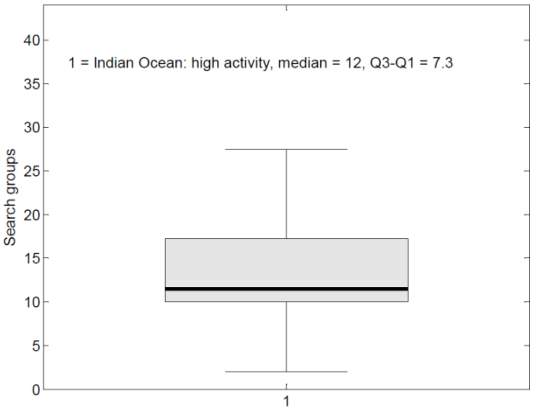

Figure A.13. Number of search groups on the Indian Ocean during high activity, second questionnaire.

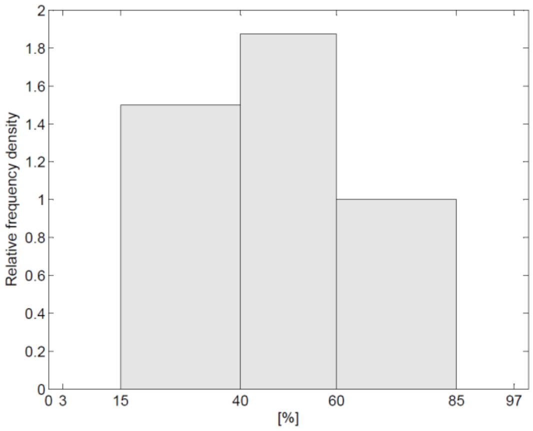

Figure A.14. Percentage of search groups operating from a mother ship, first questionnaire.

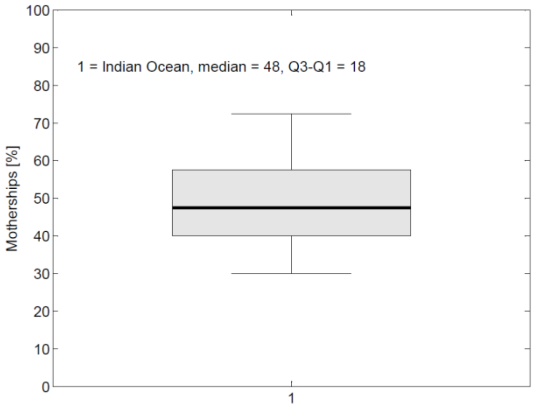

Figure A.15. Percentage of search groups operating from a mother ship, second questionnaire.

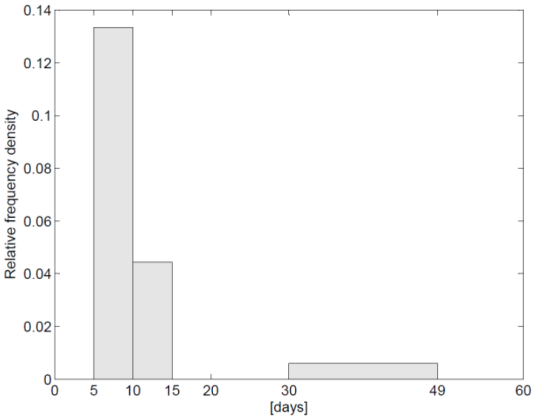

Figure A.16. Number of days a skiff can be at sea, first questionnaire.

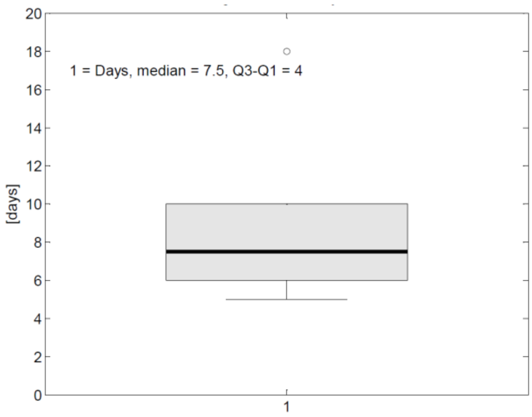

Figure A.17. Number of days a skiff can be at sea, second questionnaire.

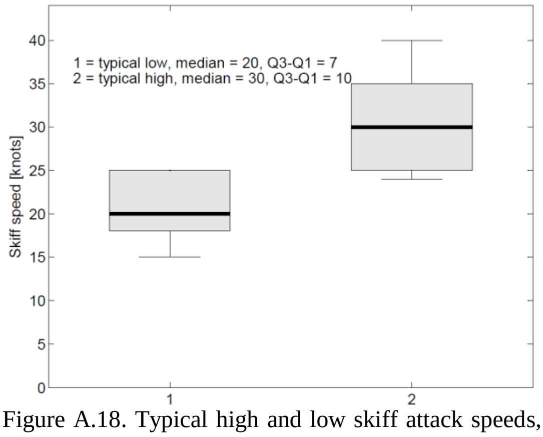

Figure A.18. Typical high and low skiff attack speeds, first questionnaire.

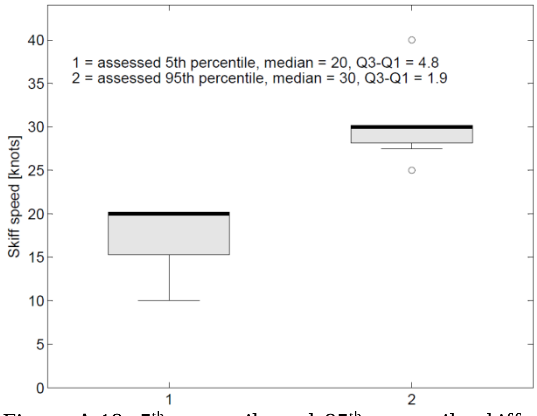

Figure A.19. 5th percentile and 95th percentile skiff attack speeds, second questionnaire.

Incident statistics

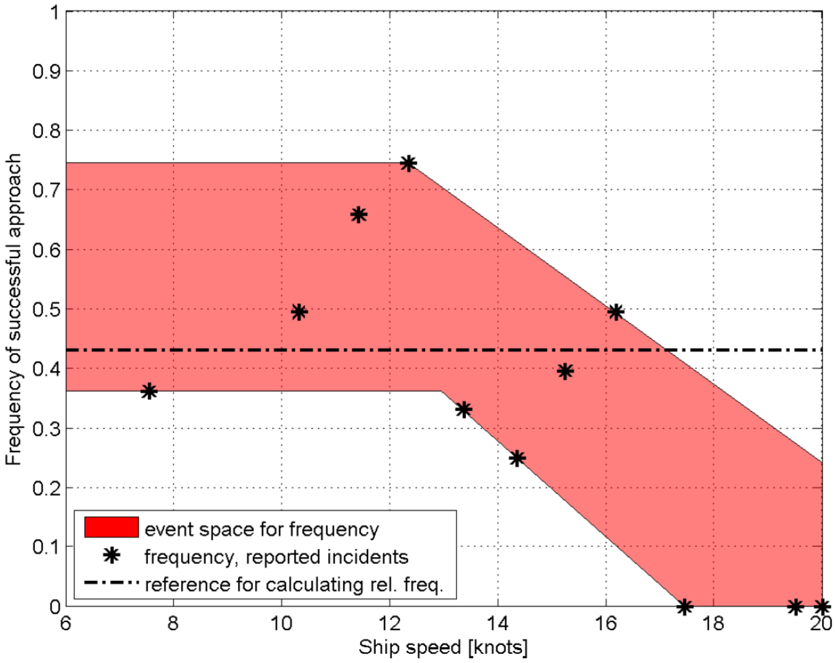

Figure A.20. Frequency of successful approaches in incident reports (divided into 11 speed intervals), January and February 2011. The event space is defined by the maximum and minimum frequencies of successful boarding at the different speeds and the fact that the frequency is independent of speeds below 12 knots and varies with speeds above 12 knots. The reference value is the average success frequency below 12 knots.