Proceedings of the ASME 2013 32nd International Conference on Ocean, Offshore and Arctic Engineering
OMAE2013
June 9-14, 2013, Nantes, France

OMAE2013-10166

SHIP SECURITY ANALYSIS - THE EFFECT OF SHIP SPEED AND EFFECTIVE LOOKOUT

Hans Liwång
Chalmers University of Technology
Department of Shipping and Marine Technology
412 96 Gothenburg, Sweden

Jonas W. Ringsberg
Chalmers University of Technology
Department of Shipping and Marine Technology
412 96 Gothenburg, Sweden

ABSTRACT

The threat of piracy to commercial shipping is a concern for the protection and safeguarding of human lives, property and environment. Therefore, ships under piracy threat should follow security measures suggested by the International Maritime Organization (IMO) and the Contact Group on Piracy off the Coast of Somali. It is, therefore, important to choose the proper security measures for the right situation.

This study presents a simulation model that can be used for probabilistic risk assessments regarding the operation of commercial ships. This investigation specifically studies the pirate approach phase and quantifies the effect of ship speed and effective lookout. The purpose of introducing probabilistic risk assessment into the analysis of pirate attacks is to meet safety goals more effectively through a well-balanced combination of proactive and reactive measures whilst keeping focus on the intended over all purpose of the particular ship.

The study presents collected and documented knowledge regarding pirate capability, intention and likelihood to perform attacks. The knowledge is collected from experts with experience from the situation off the Horn of Africa. The collected information is input to an influence analysis that identifies the network of influences that govern the skiff approach. The simulation model describes piracy characteristics and decision making on the threatened ship, the characteristics and countermeasures of the ship under attack, as well as weather.

Based on a comparison with available statistics the overall conclusion of the work is that the threat analysis and the simulation model can quantify and explain how the studied risk control options affect the probability of a successful approach. The result therefore exemplifies how a quantified ship security analysis can support the recommendations in industry guidelines and also enable recommendations that to a greater extent can facilitate an educated decision by the ship operators.

Keywords: Piracy, risk analysis, ship security analysis.

1. INTRODUCTION

Attacks from Somalia-based piracy, as exemplified in Figure 1, have the last years occurred throughout the Gulf of Aden, the Arabian Sea and the Northern Indian Ocean, affecting all shipping in the region [1]. The United Nations Security Council has turned its attention towards combating piracy and as a result, placed 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 [2]. 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 [3].

Figure 1. Suspected pirates in a typical skiff used for approaching ships. Photo taken in the Gulf of Aden prior to the suspects apprehension by USS Vella Gulf (CG 72). Photo: Copyright © Swedish Armed Forces/US Navy.

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 [2] as help most often is hours away. 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 specific ships.

 Copyright © 2013 by ASME

The International Ship and Port Facility Security (ISPS) code regulates the ship security analysis that must be performed by ship owners and operators. 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 were fast and took only thirteen months [4]. Due to this rapid turnaround time, the development was characterized by the need to create an "imperfect product" rather than having nothing at all [5]. The depth of ship security assessment suggested by this code is very limited in comparison to, for example, the depth demanded by probabilistic risk assessments for ship safety. The limited and imperfect nature of the code in question indicates a need for further research and development in maritime security.

1.1 OBJECTIVE AND METHODOLOGY

This investigation uses the quantified risk-based security analysis approach described by Liwång [6]. The investigation is a case study of a detailed part of the ship security assessment described in the ISPS code. The method in the investigation is making use of security research, experiences from military force protection, and methodological lessons from maritime probabilistic risk assessment. The current study's main objective is to examine how the ship speed and effectiveness of the lookout affects the probability of successful approach, and to validate the result against available statistics.

There is research describing piracy structures and the effects of piracy on shipping. The results show that piracy is not random. The probability of being subjected to a pirate attack is influenced by factors such as the size, speed, cargo and vulnerability of the ship. However, more research is needed to further describe the network of influences on an attack and how these affect the probability and the consequences of an attack.

The studied risk control options *increased ship speed* and *increased lookout* are chosen because they are assessed to be of high importance (see Figure 6) and also are inherent to the ship. The study focuses on Somali-based maritime piracy, using piracy performed with a typical pirate skiff, shown in Figure 1, on the Indian Ocean as a case study. Data were collected through questionnaires and interviews with civilian and military security experts who possess firsthand experience of piracy off the coast of Somalia. The data were collected specifically for this study and describe the threat's capability, intent and likelihood of exploiting a ship's vulnerability.

Section 2 describes security risk management to lay a foundation for the current study. The method used for the analysis is described in section 3. Section 4 describes the data collection for the threat analysis and the available statistics on piracy incidents. Section 5 evaluates the probability of the pirates' successful approach as a function of ship speed and detection distance. Section 6 and 7 discuss the results and present the conclusions respectively.

2. SHIP SECURITY RISK 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 [7]. 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 [4]. The ISPS code is therefore the first regulation with the possibility to substantially affect the ship security efforts and it has been classified as a first step in this area by the IMO [5].

According to the International Association of Classification Societies (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 [8].

This investigation utilizes the probabilistic approach for ship security analysis described by Liwång [6]. The approach is a method for collecting data, defining the scenario and threats, analyze the risks, and document the considerations and results. The method utilizes a wide range of tools and methods such as interviews, questionnaires, influence diagrams, event trees and Monte Carlo simulations. The method is consistent with requirements on safety risk assessment and takes use of military models to analyze and describe threats. The method is a specific way of performing the risk analysis as a part of ship security risk management. In risk management the purpose of risk analysis is to produce input to the risk evaluation according to Figure 2. Based in the output of the risk analysis the decision maker can choose the right mix of risk control options.

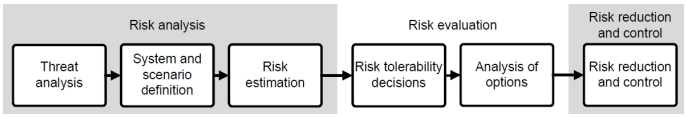

Figure 2. The security risk management process, developed from Liwång [6].

The purpose of risk management is to find the most suitable measures and risk control options to reduce the risk. A risk analysis must therefore 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.

In the risk evaluation ship owners are responsible for weighing the risks against the costs of implementing control options, but relevant organizations and society also set

Copyright © 2013 by ASME

limitations on allowed risks called risk criteria. Risk criteria have been discussed within the IMO in relation to risk-based approaches [7].

Risk control options 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 [9] and the Best Management Practice for protection against Somalia-based piracy (BMP) [1]. 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 [9].

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 a logical and consistent approach and that relevant data have been adopted [10].

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.

The ship security risk analysis presented in Liwång [6] is defined by three steps:

1. Threat analysis, documents qualitative and quantitative aspects that describe how the threat will act in relation to protection methods and the specific ship (see section 3.1).
2. Definition of the system and scenarios. The definition should be able to describe how a change in the threat or protection changes the risk (see section 3.2).
3. Risk estimation with tools from probabilistic risk assessment (see section 3.3).

3.1 THREAT ANALYSIS

This study applies the analysis documented in the NATO Force Protection Directive [11] to perform a stringent threat analysis. 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 [11]:

a. 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.
b. Threat intent. The willingness of potential threats to target assets. Analysis of intent considers threat ideology, objectives, strategy, likely intentions and previous history.
c. 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 [12].

Risk analysis is often supported with data from expert assessment due to a lack of empirical data on the studied system [13]; this is also the case in this study. This is because the causal relationships behind the incidents are not described in the statistics. Expert assessment of probabilities, however, often lack calibration and can, therefore, have systematic errors [14]. Therefore, the aim here is, as often as possible, to have experts assess capabilities of the threat rather than probabilities. The assessed capabilities are more easily understood and can, for example, be calibrated using measurements or intelligence reports. The assessed capabilities are then linked to the risk with the system description and simulations.

3.2 DEFINITION OF THE SYSTEM AND SCENARIOS

The threat description is used to define the system studied as well as the scenarios that collectively describe the harmful consequences. The definition should be such that it describes the causal relationships involved and is, therefore, also able to describe how a change in the threat or protection changes the risk. This ability is central to be able to capture the threat and asset interaction discussed in section 3.1.

Influence diagrams can be used to describe the causal relationships of the scenario and define the system [6], see Figure 10 for an example of an influence diagram. Influence diagrams are described by IMO in the Guidelines for formal safety assessment [13], but more thoroughly documented in the area of decision analysis [15].

An influence diagram is a graphical and mathematical representation of the network of influences on an event. Influence diagram methodology is derived from decision analysis and, according to IMO, 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 underlying causal information. The influence diagram approach described by IMO uses expert judgment to model the network of influences. These influences link factors at the operational level with their causes, and with the underlying influences [13, 15].

3.3 RISK ESTIMATION

The risk is calculated with tools from probabilistic risk assessment. The calculations are simulations representing subsets of the piracy scenario, with influences determined according to the influence diagram. The influence diagram therefore plays an important role in describing the interactions between pirate characteristics and ship vulnerability throughout the analysis.

Interviews on ship security analysis performed show that influence diagrams not only facilitate the calculations needed to calculate the expected outcomes of the scenarios, but also

Copyright © 2013 by ASME

enables a discussion on the results and the validity of the analysis with involved parties and decision makers.

4. INCIDENT REPORTS AND DATA COLLECTION

Piracy incidents involving civilian ships should be reported [16] and are collected and documented by the International Chamber of Commerce (ICC) Commercial Crime Services' (CCS) International Maritime Bureau (IMB) [17, 18]. Incident reports on piracy are described in section 4.1. However, the incident reports do not describe the piracy system and activity, they only describe the activity noted and chosen to be reported.

In order to gain the knowledge needed about the threat this investigation collects a piracy description presented in section 4.2. The data collected according to the description in section 4.2 are used to perform the risk analysis according to Figure 2, and the statistics described in section 4.1 are used to discuss the validity of the results.

4.1 STATISTICS ON MARITIME PIRACY

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 BMP [1], which recommends that seafarers who pass the waters off the coast of Somalia 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 [16].

According to Figure 3, ship security experts consulted in this study assess that between 85 and 97 % of the piracy incidents in the waters off Somalia are documented in official piracy statistics and the ICC IMB reports.

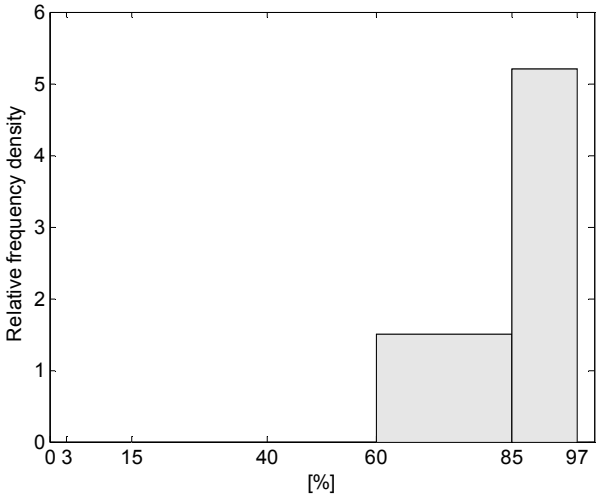

Figure 3. Assessed percentage of incidents reported in statistics.

In this investigation, data from incidents from March to May, 2010, and January to May, 2011, are used. These months are from NATO Shipping Centre's overview of the incidents 2009 to 2012 [19] judged not to be affected by the Northeast or Southwest monsoon. In Figure 4 the outcome of approaches (binary data) is presented against ship speed from 130 attacks for which the ship maximum speed could be attained from AIS data [20]. The logistic model [21] according to:

$$E(Y_i|X_i) = \pi_i = \frac{e^{(\beta_0+\beta_1 X_i)}}{1+e^{(\beta_0+\beta_1 X_i)}} \quad (1)$$

and the linear model [21] according to:

$$E(Y_i|X_i) = \pi_i = (\beta_0 + \beta_1 X_i) \quad (2)$$

is used to model the relationship between the ship speed (X) and the approach success (Y). There are, however, large uncertainties in the data about actual ship speed, weather conditions and crew alertness that will have affected the outcome of every incident.

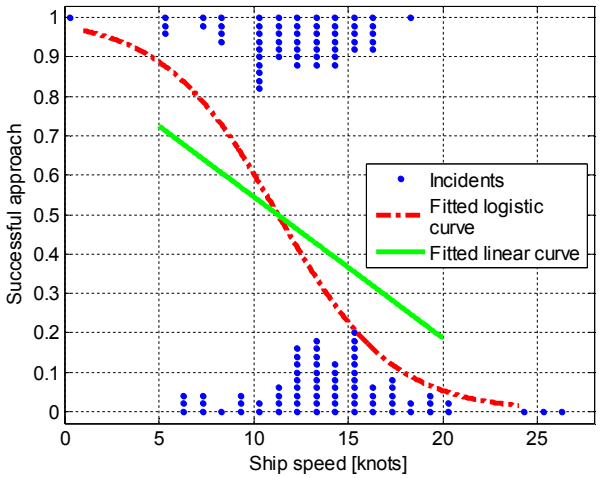

Figure 4. Incident statistics (binary data) for non monsoon months in 2010 and 2011 plotted against ship maximum speed (dots). The lines represent the fitted logistic curve according to Equation 1 and fitted linear curve according to Equation 2.

Of the studied attacks in 2010 and 2011, the distance of skiff detection is only given or can be assessed in less than 10 out of documented 172 attacks. Therefore no statistical analysis is performed on the correlation between successful approach probability and the distance at which the skiff is detected.

4.2 DATA COLLECTION - QUESTIONNAIRES AND INTERVIEWS

According to IMO [13] the approach used for gaining knowledge on hazards generally comprises a combination of both creative and analytical techniques, the aim being to ensure that the process is proactive. Central in the process is structured group reviews that include experts in the various appropriate aspects.

In this investigation data was collected for use as inputs to the threat description. To meet the IMO requirements described above the data collection was performed in three different steps. In the first step, a questionnaire was sent to experts to collect

Copyright © 2013 by ASME

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 used risk control options. 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 QUESTIONNAIRES

The first questionnaire was sent to twelve Swedish experts to collect data on piracy threats' capability, intent, and likelihood. The experts all have personal international experience in security work related to the piracy operating out of Somalia. Ten of the experts are military personnel, and two are civilian maritime security managers. All of the experts:

- are currently or have been a part of an organization on 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.

Eleven out of the twelve experts answered the questionnaire, for a response rate of 92 %. The results from the questionnaire used in this study are presented in Figures 3, 6, 8 and 9.

Following the Delphi method [22], the ten military experts were encouraged to revise their earlier answers, based on the replies of the other panel members, in a second questionnaire on skiff attack speed. This second questionnaire was administered to decrease the range of uncertainty in the answers and to approach a consensus assessment [22]. Eight out of the 10 experts answered the second questionnaire, see Figure 7 for the results.

4.2.2 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. All of the experts have extensive experience from analysis of operations off the coast of Somalia. The result of the interviews is used together with the result of the questionnaire to define the pirate attack scenario (see Figure 4) and the threat analysis (see section 5.1).

5. PROBABILITY OF SUCCESSFUL APPROACH

The threat scenario studied in this work is one part of a piracy threat analysis. The study is limited to piracy operating out of Somalia on the Indian Ocean during 2010 and 2011. Piracy in the Indian Ocean is selected as the focus of study because it is relatively well documented in incident statistics and allows for expert assessments.

This study is limited to the skiff approach phase which is a part of a piracy attack scenario. A successful approach is necessary, but not a sufficient criterion for a boarding. The probabilities are calculated given that the pirate search group has located and identified the ship as suitable for attack. The role of the probability of successful approach is illustrated by step C in the event tree of a simplified pirate attack scenario in Figure 5. The event three in Figure 5 is a result of the questionnaires and interviews performed.

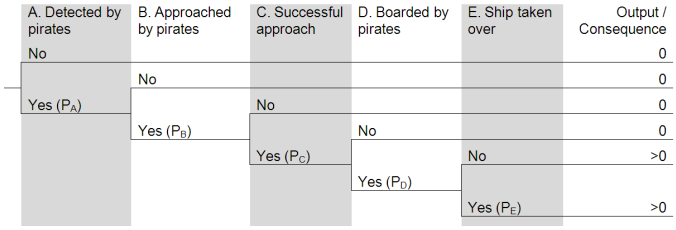

Figure 5. Simplified pirate attack scenario illustrating the importance of the probability of successful pirate approach (P_C).

Ship speed and skiff detection distance are important factors in the skiff approach phase. The ship speed influences the pirates' decision to attack and governs the approach time and early detection of approaching pirates is needed to initiate protective measures such as evasive maneuver, see Figure 6.

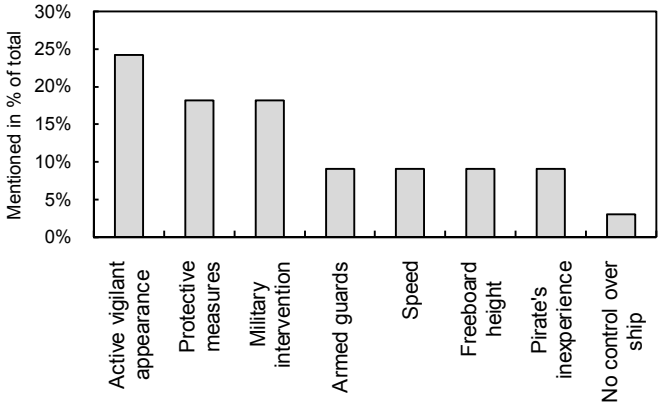

Figure 6. Expert assessment of the most influential aspects governing the pirates' decision to abort an initiated attack. The use of the highest four ranked aspects are only possible after the attack is detected and speed is a physical limitation but does also affect the pirates' decision.

5.1 THREAT ANALYSIS

Based on the threat description collected from experts the capability of the threat is defined as follows.

- When attacking a ship, the maximum attack speed for skiffs in calm seas is between 20 and 30 knots (see Figure 7).
- The maximum skiff speed is reduced by swells, waves and when the skiff enters the wave system of the ship as a function of added resistance in waves.

Copyright © 2013 by ASME

- A skiff can detect a ship at a great distance during good visibility, this study bases the detection distance on the ship height, skiff height and Earth's curvature.
- According to Figure 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 [3].

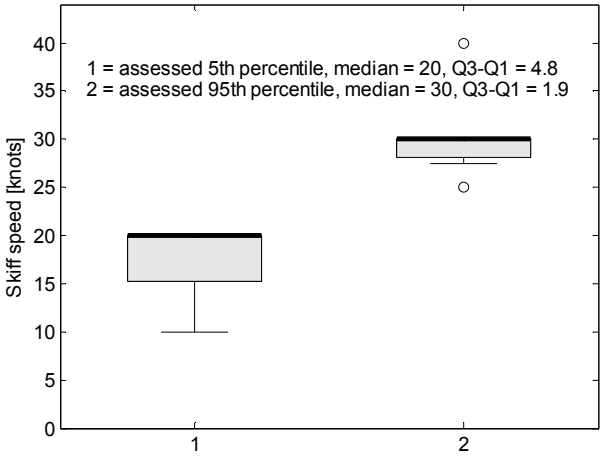

Figure 7. Expert assessment of skiff speed in calm seas.

Based on the threat description collected from experts the intent of the threat 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 8.

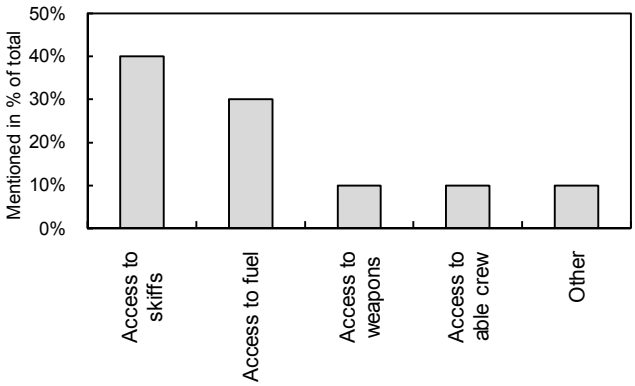

Figure 8. Expert assessment of limiting factors on the pirates' activity.

Based on the threat description collected from experts the likelihood of exploiting a ship's vulnerability is defined by the following factors.

- A ship with a good lookout can visually 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 (see Figure 9).
- According to the interviews, a ship crew's vigilance and alertness is important and dictates at what distance the ship detects an approaching skiff. The ship can alter its course to increase the approach time when pirates are detected.

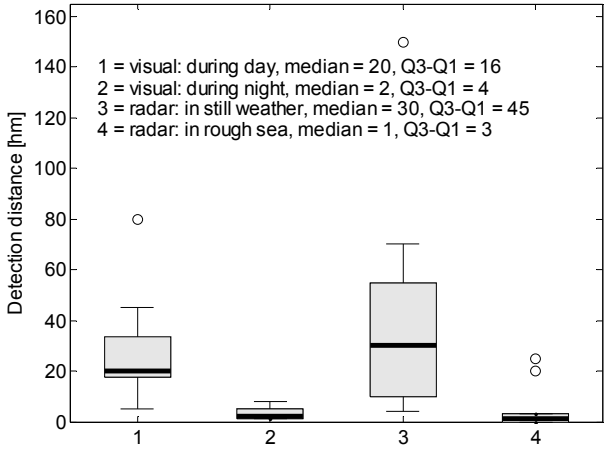

Figure 9. Expert assessment of skiff detection distance.

5.2 DEFINITION OF THE SYSTEM AND SCENARIO

The threat analysis in section 5.1 is used to develop the influence diagram for the probability of a successful approach shown in Figure 10.

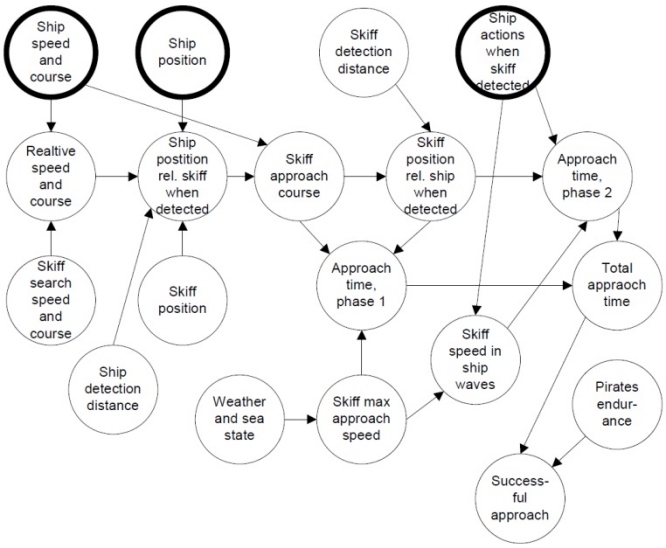

Figure 10. Influence diagram of approach scenario, assuming that the ship is within detection distance of a skiff. A thick line indicates that the node's state is deterministically decided.

Copyright © 2013 by ASME

5.3 RISK ESTIMATION

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 from a simulation of repeated attacks during daytime and good visibility assuming that the ship is detected by the skiff.

5.3.1 MONTE CARLO SIMULATION

The influence diagram in Figure 9 is developed into a Monte Carlo simulation [23] 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 in section 5.1.

In the simulation the relation between distance, speed, course and sea condition is modeled to calculate the time needed for the skiff to get close to the ship.

Analyzing statistics on significant wave heights (H_s) for the studied part of the Indian Ocean [24] it is found that the wave height during non-monsoon periods often vary from 1 to 2 meters and during monsoon periods often between 2 and 4 meters.

The effect of the waves on the skiff speed is given by added resistance in waves according to Savistky and Koelbel [25]. Speed reduction in the simulations is based on a typical skiff, 7 meter hard chined hull with moderate length to beam ratio and deadrise angle, see Figure 1. Speed reduction is calculated only in relation to added resistance without considerations to skiff motions and accelerations because it is here assumed that pirates are highly motivated. The resulting speed reduction as a function of skiff maximum speed in calm seas and significant wave height used in the simulation is presented in Figure 11.

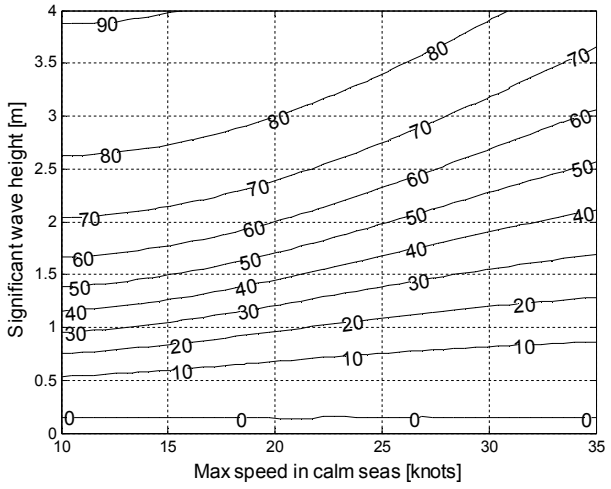

Figure 11. Speed reduction in percent as function of skiff maximum speed in calm seas and wave height.

The approach time is then deterministically calculated based on the skiff route in an orthogonal coordinate system were the ship travels along the x-axis. The skiff approach course is defined by a dog curve, were the skiff speed and course at every position is given by:

$$\bar{v}_{\text{skiff}} = v_{skiff} \frac{[x_{ship}+\xi-x_{skiff} \quad y_{skiff}]}{|[x_{ship}+\xi-x_{skiff} \quad y_{skiff}]|} \tag{3}$$

were $[x_{skiff} \quad y_{skiff}]$ is the skiff position, $[x_{ship} \quad 0]$ is the ship position and ξ is the pirates' aiming point ahead of the ship. For the simulations ξ is set to 1,000 meters. This model means that the pirates at every moment will aim their skiff at a point 1,000 meters ahead of the ship. When the skiff is detected the ship maintains the speed and alters its course away from the skiff.

5.4 RESULTS

The results of the simulation are presented in Figure 12 and 13.

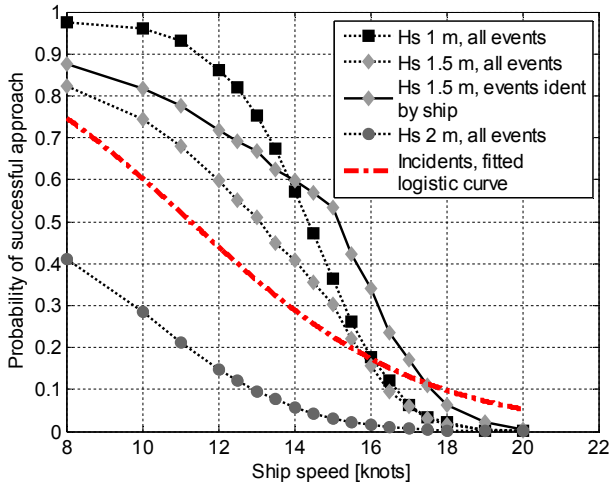

Figure 12. Calculated probability of a successful approach (P_C) as a function of ship speed calculated for the wave heights 1, 1.5 and 2 meters. The dotted lines display the probability of successful approach for all events. The solid line display the probability only for the incidents not aborted before the ship sees the skiff. The calculations are performed for t_{abort} = 45 minutes and the skiff is detected at 2,000 meters, based on the capability and intent described in section 5.1.

Copyright © 2013 by ASME

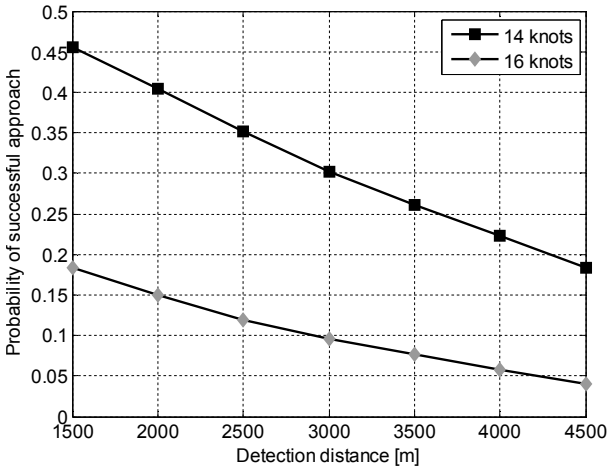

Figure 13. Calculated probability of a successful approach (P_C) for the ship speeds 14 and 16 knots and the significant wave height of 1.5 meters as a function of detection distance.

5.4.1 EFFECT OF SHIP SPEED

There is a clear correlation between the probability of successful approach and ship speed in both the statistics (see Figure 4) and simulation results (see Figure 12). To date, there have been no reported attacks in which pirates board a ship that is proceeding at more than 18 knots [1] and according to the calculations the probability of successful approach is for 18 knots never higher than 5 %. From the simulations it can be found that this is a result of the speed range of the skiffs, and also that the wave system generated by the ship under attack at this speed makes it very difficult to get close to the ship even if the sea is calm.

It is reasonable to assume that the likelihood of pirates initiating an attack decreases with higher waves. Therefore the amount of attacks at different wave heights is not constant which makes it difficult to merge the probabilities for different wave heights in Figure 12 into a total probability that can be compared to the reported frequency in Figure 4. However, a comparison between the simulation results for the significant wave height 1.5 meters, which is a common wave height and makes attacks feasible, with the linear fit show that the calculated probability is reasonable and cannot be rejected by the statistics at hand. Therefore, it can be assumed that the performed analysis captures several important aspects of the approach sequence.

From the simulation results it is also shown that attacks often can be aborted before the ship identifies the attack. This fact shows that frequencies taken from reports can be overreporting the pirates' success rate, especially for approaches in high waves.

Defining the probability of successful approach as a function of speed and detection distance, as performed in Figure 12, rather than defining a secure speed as performed in the BMP, is a much more reasonable description of the threat. This probability function can guide the ship owners to better decisions.

5.4.2 IMPACT OF EFFECTIVE LOOKOUT

There is no available statistics for comparing the interaction between increased skiff detection distance as a result of effective lookout and probability of successful approach. However, the results from the analysis of ship speed show that it is reasonable to assume that the simulation model captures the relevant aspect of the approach scenario.

The results presented in Figure 13 show that the simulated evasive maneuver to increase the approach time has a substantial effect on the total approach time and therefore also the probability of successful approach. If it is possible to increase the detection distance from 2,000 meters to 4,000 meters the approach probability is reduced with 41 and 62 % for the ship speeds 14 and 16 knots respectively.

A detection of an approaching skiff is necessary to perform protective measures such as commence evasive maneuvers, radio for assistance and set the crew in safety by gathering the entire crew in a citadel onboard [1]. The time needed for such actions is different for different ships, but in the interviews assessed to at least 5 to 10 minutes. A detection distance which gives the crew at least 10 minutes for preparations will therefore reduce the probability of successful approach, but also reduce the probability of hijacking in the event of a successful approach. Figure 13 presents the available preparation time for the speed 16 knots and for the detection distances 2,000, 3,000 and 4,000 meters.

From Figure 14 it can be noted that for the ship speed 16 knots a detection distance close to 4,000 meters in needed to guarantee a preparation time of over 10 minutes.

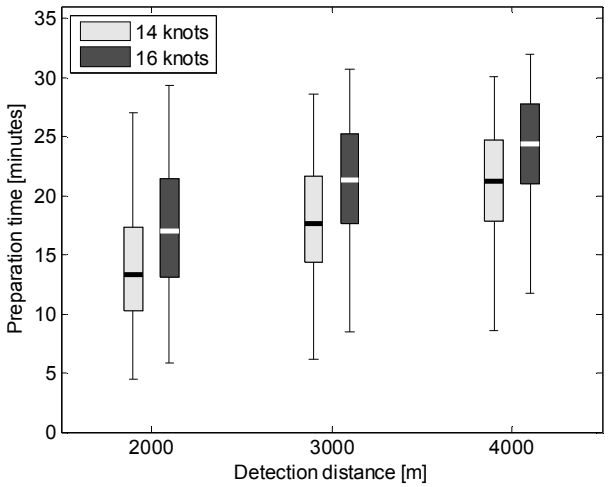

Figure 14. Time available for protective measures for the significant wave height 1.5 meters for three detection distances.

6. DISCUSSION

The study's main objective is to examine how the ship speed and effective lookout affects the probability of successful approach, and to validate the result against available statistics. 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.

Copyright © 2013 by ASME

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 successful approach 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 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.

There is a clear correlation between the probability of successful approach and ship speed in both the statistics and simulation results. The ship speed 18 knots is in the reports as well as in the simulations the speed at which very few skiffs are able to get close and board the ship. From the simulations it can be derived that this is a result of the skiff speed, but also that the ship wave system at this speed makes getting close very difficult even if the sea is calm otherwise.

An effective lookout increases the distance at which the skiff is detected and a simulated evasive maneuver to increase the approach time has a substantial effect on the total approach time and therefore also the probability of successful approach. Increasing the detection distance from 2,000 meters to 4,000 meters reduces the successful approach probability with 50 %.

A detection distance giving the crew at least 10 minutes for preparations will reduce the probability of successful approach, but also reduce the probability of hijacking in the event of a successful approach. Effective lookout giving at least a detection distance close to 4,000 meters is needed to guarantee sufficient time for security preparations.

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 used by industry today.

The results of the simulations show that the frequencies obtained from incident reports probably contains systematic error since incident reports only contain information about aspects noted by the ships. This means that a correct understanding cannot be built on statistics alone, the causality from threat to risk must also be analyzed with other tools such as threat analysis and simulations.

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 ship security analysis performed by ship owners today. Continuous testing and updating would provide for a more detailed and validated analysis and a better understanding of the problem itself and why and how different ship security measures work.

The used method therefore provides the possibility of illustrating and understanding the causality and influences on a risk more extensively and the analysis methods allow for the testing of different risk control options and explain to stakeholders how and to what extent the chosen options reduce the risk.

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. Simulations show that in areas where it is possible to compare the results of the performed analysis (in terms of probabilities) with incident reports (aggregated to frequencies), simulation can be assumed to capture several of the causes contributing to the situation.

The analyzed control options ship speed and increased skiff detection both have a great influence on the probability of a successful approach. The results of the simulations also quantify the effect of significant wave height and how the detection distance affect the available time for security measures needed.

The combination of graphical illustration and quantitative output used in this analysis method not only calculates probabilities but also enables a qualitative discussion on causes and measures. Such a discussion is very valuable to the decision-making process.

8. ACKNOWLEDGEMENTS

This work would not have been possible without support from naval experts in the Royal Swedish Navy 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).

REFERENCES

[1] UKMTO, 2011, *Best Management Practices for Protection against Somalia Based Piracy*, Witherby Publishing Group Ltd, Edinburg.

[2] Kraska, J. and Wilson, B., 2008, "Fighting Pirates: The Pen and the Sword", World Policy Journal, **25**(4), pp. 41-52.

[3] Chalk, P., 2010, "Piracy Off the Horn of Africa", Brown Journal of World Affairs, **16**(2), pp. 89-108.

[4] Wengelin, M., 2012, "Service, Regulations, and Ports: An Actor-Network Perspective on the Social Dimension of Service-Dominant Logic", Department of Service Management, Lund University, Lund.

[5] Mitropoulos, E., 2004, "Imo: Rising to New Challenges", WMU Journal of Maritime Affairs, **3**(2), pp. 107-110.

Copyright © 2013 by ASME

[6] Liwång, H., 2012, "Risk-Based Ship Security Analysis – an Approach Based on Civilian and Military Methods", Department of Shipping and Marine Technology, Chalmers Univeristy of Technology, Gothenburg.
[7] Skjong, R., 2009, "Regulatory Framework", *Risk-Based Ship Design*, Papanikolaou, A. D., eds., Springer-Verlag, Berlin, pp. 97-151, Chap. 3.
[8] IACS, 2004, *A Guide to Risk Assessment in Ship Operations*, International Association of Classification Societies, London.
[9] International Maritime Organisation 2002, *The International Ship and Port Facilities Security (Isps) Code*, International Maritime Organisation London.
[10] Andrews, J.D. and Moss, T.R., 2002, "Risk Assessment", *Reliability and Risk Assessment*, Professional Engineering Publishing Limited, London, pp. 411-448, Chap. 13.
[11] NATO Standardisation Agency, 2007, *Allied Joint Doctrine for Force Protection*, NATO Standardisation Agency, Brussels.
[12] Kunreuther, H., 2002, "Risk Analysis and Risk Management in an Uncertain World", Risk Analysis, **22**(4), pp. 655-664.
[13] International Maritime Organization, 2002, *Guidelines for Formal Safety Assessment (Fsa) for Use in the Imo Rule-Making Process*, International Maritime Organization, London.
[14] Hansson, S.O., 1993, "The False Promise of Risk Analysis", Ratio-New Series, **6**(1), pp. 16-26.
[15] Shachter, R.D., 1988, "Probabilistic Inference and Influence Diagrams", Operations Research, **36**(4), pp. 589-604.
[16] Sörenson, K., 2011, *Wrong Hands on Deck? : Combatting Piracy and Building Maritime Security in Eastern Africa*, Swedish Defence Research Agency, Stockholm.
[17] IMB, 2012, *Piracy and Armed Robbery against Ships, Report for the Period 1 January - 31 December 2011*, ICC International Maritime Bureau, London.
[18] IMB, 2011, *Piracy and Armed Robbery against Ships, Report for the Period 1 January - 31 December 2010*, ICC International Maritime Bureau, London.
[19] NATO Shipping Centre, 2012, *Piracy Statistics*, 28th of December 2012, http://www.shipping.nato.int.
[20] MarineTraffic.com, 2012, *Search Vessels Details*, December 2012, http://www.marinetraffic.com/ais/.
[21] Cook, D., Dixon, P., Duckworth, W.M., Kaiser, M.S., Koehler, K., Meeker, W.Q., and Stephenson, W.R., 2001, "Binary Response and Logistic Regression Analysis", *Beyond Traditional Statistical Methods*, Duckworth, W. M. and Stephenson, W. R., eds., Iowa State University, Ames, Chap. 3.
[22] Dalkey, N.C., 1969, *The Delphi Method: An Experimental Study on Group Opinion*, Rand, Santa Monica.
[23] Parnell, G.S., 2007, "Value-Focused Thinking", *Methods for Conducting Military Operational Analysis* Loerch, A. G. and Rainey, L. B., eds., Military Operations Research Society, Washington DC, pp. 619-655, Chap. 19.
[24] Vethamony, P.S., K.; Rupali, S.P.; Babu, M.T.; Jayakumar, S.; Saran, A.K.; Basu, S.K.; Kumar, R.; Sarkar, A., 2006, "Wave Modelling for the North Indian Ocean Using Msmr Analysed Winds", International Journal of Remote Sensing, **27**(18), pp. 3767-3780.
[25] Savitsky, D. and Koelbel, J.G., 1993, *Seakeeping of Hard Chine Planing Hulls*, Soceity of Naval Architects and Marine Engineers.

 Copyright © 2013 by ASME