THESIS FOR THE DEGREE OF LICENTIATE OF ENGINEERING

Risk-based ship security analysis – an approach based on civilian and military methods

Hans Liwång

Department of Shipping and Marine Technology
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
2012

Risk-based ship security analysis – an approach based on civilian and military methods

HANS LIWÅNG

© HANS LIWÅNG, 2012

ISSN 1652-9189
Report No 12:141

Department of Shipping and Marine Technology
Division of Marine Design
Chalmers University of Technology
SE-412 96, Gothenburg
Sweden
Telephone: + 46 (0)31-772 1000

Front cover illustration: © KAJSA JÄRNER, 2012

Printed by Chalmers Reproservice
Gothenburg, Sweden 2012

Risk-based ship security analysis – an approach based on civilian and military methods

HANS LIWÅNG
Department of Shipping and Marine Technology
Division of Marine Design

Abstract

The demands on maritime operations today are increasingly higher in terms of control, efficiency and cost. The margins for accidents and security incidents are therefore decreasing. In the area of ship safety the regulations, guidelines and methods have a history and culture of systematic research, development and implementation. In contrast, international security is highly politicized and therefore not as transparent. The result is that a tradition of ship security is not as well established.

The overall aim of this thesis is to propose a method for ship security analysis that increases the overall safety of the crew and the ship. The objective is to develop a method that is systematic in order to ensure that assessment and response are complete and effective, and that the process is documented to provide evidence of decision-making.

The method used is probabilistic risk assessment where quantitative analysis is central. The proposed approach is consistent with the requirements of maritime safety work. However, in the work here, the proposed methods are specifically tested for security cases. This is because hazards (without intent) and threats (with intent) evolve in different ways into risk. Therefore, they must be analysed differently in order to capture the causal relationship.

The proposed approach consists of three steps: the first step consists of a threat description that documents qualitative and quantitative aspects that together describe how the threat most likely will act in relation to the ship's vulnerability; the second step uses the threat description to define the system studied as well as the scenarios that collectively describe the harmful consequences; the third step evaluates the risk with tools from probabilistic risk assessment.

The overall conclusion is that the proposed method brings the procedure and results of ship security analysis into the open and therefore allows for criticism, improvements and shared risk knowledge, not possible with less structured methods. The results also show that the calculated probabilities agree with available statistics, which indicates that the analysis succeeds in describing the central causal relationships of the scenarios modelled.

Keywords: naval ship, piracy, risk-based, risk control options, ship security analysis.

Preface

This thesis is comprised of work carried out during the years 2010-2012 at the Division of Marine Design at the Department of Shipping and Marine Technology at Chalmers University of Technology and the Department of Military Studies at the Swedish National Defence College. The work is 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 mix of civilian and military experience, method development and research that I have had the opportunity to tap into is important. This work would not have been possible without the support of naval experts from the Royal Swedish Navy and ship owners' safety, security and operation managers and maritime security consultants.

Firstly, I would like to thank my supervisor Professor Jonas Ringsberg and co-supervisor Professor Martin Norsell for their support and believing in me. I would also like to thank all of my colleagues at the Department of Shipping and Marine Technology and the Department of Military Studies as well as the military students at the Swedish National Defence College for their support and good ideas.

Last, but by no means least, I would also like to thank my wife and children for thinking that what I do is cool!

Stockholm, October 2012.
Hans Liwång


SECURITY
DEVELOPMENT
AREA
SHIP
RISK
HAZARD
METHODS
SAFETY
PIRATES
SHIPS
RESEARCH
ALSO
EFFECTIVE CONTROL
NAVAL
WEATHER
SET
DEMANDS
EXAMPLE
FACT
INCREASINGLY
SYSTEMATIC
COST
OPERATIONS
WELL
TOOLS
THREAT
OFTEN
CIVILIANCOMPLEX
ENSURE
SEA
MEANS
TOOL
ASSESSMENT
CONSISTENT
ROUGH
DESIGN
AFFECTS
MUST
ALLOW
TYPICAL
THEREFORE
AREAS
IMPORTANT
OPTION
DESCRIBED
SUPPORTING
SUSTAINABLE
CLEAR
WORK
IRREGULAR
INTELLECTUAL
ANALYSIS
OBJECTIVE
VESSELS
ADOPTED
IMPLEMENTATION
NEW
SEPARATE
OPERATING
POSED
GUIDELINES
ESTABLISHED
RESULTS
SMALL
ANALYSED
LOW
USING
NEED
GIVEN
ASSUME
COMPARING
COMPROMISE
CAPTURE
DEVELOPED
PROBABILITIES
PIRACY
ONE
COMBINATION
DETAIL
INCIDENTS
TRADITIONAL
UNDERSTAND
TODAY
BLEND
USED
BUSY
HIGHLIGHTED
CONSISTENCY
BOATS
HISTORY
PREPARATIONS
TODAY'S
BENEFIT
DECREASING
RELEVANT
UNDEVELOPED
PROCEDURES
EFFICIENCY
POPULATED
CONSIDERATION
TAKING
TRANSPORT
ACCIDENTS
COMPROMISES
CONFLICTS
DOCUMENTED
ABLE
GREATER

Contents

List of appended papers

Paper I Liwång, H., Westin, J., Wikingsson, J., Norsell, M. (2011). *Minimising Risk from Armed Attacks: The Effects of the Nato Naval Ship Code.* In: Åke Sivertun (Ed.), Stockholm Contributions in Military-Technology 2010 (pp. 65-81). Stockholm: Swedish National Defence College.

The author of this thesis was responsible for the ideas presented and the planning of the paper and wrote most of the manuscript.

Paper II Liwång, H., Ringsberg, J. W., Norsell, M. (2012). *Probabilistic risk assessment for integrating survivability and safety measures on naval ships.* International Journal of Maritime Engineering (154), A21-A30.

The author of this thesis was responsible for the ideas presented and the planning of the paper, performed the numerical simulations and wrote most of the manuscript.

Paper III Liwång H., Ringsberg J. W., Norsell M. *Quantitative risk analysis – ship security analysis for effective risk control options.* Submitted to Safety Science, October 2012.

The author of this thesis was responsible for the ideas presented and the planning of the paper, collected the data, using questionnaires and interviews, carried out the numerical simulations and wrote most of the manuscript.

"There is an opportunity for ... bringing together vulnerability analysis, risk assessment, risk perception, and risk management in ways that will produce substantial benefits to our society"

Howard Kunreuther (2002), Professor of Operations and Information Management, University of Pennsylvania.

1 Introduction

There have always been hazards at sea, both traditional safety hazards, such as the possibility of grounding, and security threats such as piracy. As shipping and society changes, the threat also changes. In this work there is a difference between the terms *safety* and *security*. The term security is used here only in relation to external antagonistic threats and security is, therefore, achieved when the ship is protected from such threats. Safety, on the other hand is achieved when the ship is designed, manned and equipped to reduce the possibility of hazards (without intent) leading to harm. This work is about understanding the threat, and how to find the most effective measures to reduce the harmful effect of any threat, i.e. ship security analysis.

Shipping and ships represent great monetary as well as symbolic value and can therefore be the target of security threats such as robbery, piracy or terrorist attack. The purpose of naval ships is to protect (offensively and defensively) national interests against threats during war or other types of crisis. Therefore, for both civilian and naval ships there is a need to analyse the threat and reduce the possible harmful effects of an attack. This work studies security analysis for both civilian and naval ships. Ship security analysis lacks a tradition of research and development and there is therefore a need for further development (McNaught, 2005 and Mitropoulos, 2004).

1.1 Ship security

Total security of a ship can never be achieved. Hence, the efforts focus on reducing possible risks that affect security. Different measures, or risk control options, to reduce risks are often interconnected with each other and it is not possible to change these measures without affecting other aspects of the security, safety or effectiveness of the system. Security, as well as safety, is therefore a matter of compromise.

Civilian ships' security measures are often the first and only measures preventing criminal acts at sea. The International Ship and Port Facility Security (ISPS) code regulates ship security. The code was developed in the aftermath of the terrorist attacks in USA on September 11th, 2001. The development started two months after the attacks and the final code was presented only 13 months later (Wengelin, 2012). The fast process meant that the development was characterized by it being better to have something imperfect rather than nothing at all (Mitropoulos, 2004). See Paper III for further details on the ISPS code.

Security is crucial to successful military planning and actions (NATO Standardization Agency, 2007). Security is achieved when you take measures to protect your forces. Appropriate security allows for freedom of action by reducing your vulnerability to your enemy's actions (DCDC, 2010, NATO Standardization Agency, 2007 and University of Cincinnati, 2004). Security is therefore an important measure of success for naval ships. See Paper I and II for further discussions. In this work, survivability is seen as one of the most important properties for a naval ship in terms of achieving security. Both security and survivability are not only a function of technology, but also tactics and efforts carried out onboard, see more detailed discussion in Papers I and II.

In the Malmö Declaration the participants at the International Conference on Piracy at Sea (ICOPAS 2011) political, industry and research representatives called on the international community to enhance cooperation between national and international

actors in combating piracy and other violent crimes at sea (WMU, 2011). One example of such cooperation, discussed during the conference, is to use both civilian and military experience to further develop the risk-based ship security that the declaration calls on companies to perform (WMU, 2011).

1.2 Risk management

Risk management and its components, such as risk assessment and risk analysis, have been employed since the 1950s for the control of major accident hazards in areas such as space travel and industrial plants. Risk management is defined here as the systematic application of management policies, procedures and practices to the task of analysing, evaluating and controlling risk. Risk management is often defined by the following activities:

A. Risk analysis including scope or system definition, hazard identification and risk estimation.
B. Risk evaluation including risk tolerability decisions and analysis of options.
C. Risk reduction and control including decision making, implementation and monitoring. (DCDC, 2010, IACS, 2004, IEC, 1995 and Kuo, 2007).

Risk assessment is defined here as consisting of steps A and B from the list above and risk is defined as a function of the probability of the occurrence of an unexpected/unwanted event and the consequence of it happening. See also Figure 1 for an illustration of risk management and its components and sub-components.

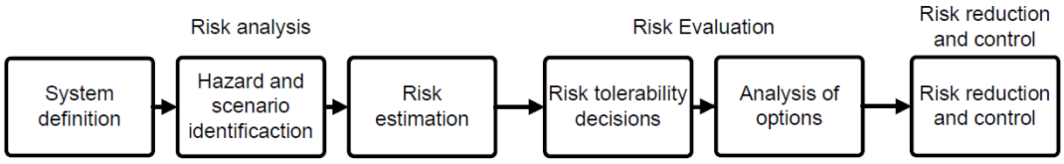

Figure 1. Risk management and its components.

The results of risk analysis must always be weighed against both risk tolerability levels and other operational parameters, such as financial considerations, requested reliability and possible operational gain. Generally, higher risks are tolerable if the possible operational gain is high (IACS, 2004 and NATO Standardization Agency, 2007).

2 Objective and motivation

The demands on maritime operations today are increasingly higher in terms of control, efficiency and cost. The margins for accidents and security incidents are therefore decreasing. At the same time there are increasing levels of conflict in highly populated coastal areas. In these areas, there are busy sea-lanes and the conflicts place new security demands on both civilian and naval ships (Department of Defence, 2007). An example of such an area is the waters off Somalia studied in Paper III.

In the area of maritime safety the regulations, guidelines and methods have a history and culture of systematic research, development and implementation (Kuo, 2007). In contrast international security is highly politicized and therefore not as transparent (Wengelin, 2012). The result is that a tradition of ship security is not as well established (McNaught, 2005). Therefore, there is a need for further research and applied development of methods and tools. This development must be able to handle the new and more complex demands on ship security for both civilian and naval ships (Department of Defence, 2007 and McNaught, 2005). Being able to understand and describe the risk of activities important to our way of life, such as sea transport, is also an important intellectual tool on its own. This tool can then be used to support an innovative and sustainable development of our society.

To capture the need for further development, the work in Papers I to III studies ship operations with additional hazards beyond the typical safety hazards. Such hazards could be the result of a military threat to naval vessels (Papers I and II) or the security threat posed by pirates to commercial vessels (Paper III). In such operations, the ship, crew and operating procedures must also take the security threat into consideration when reaching compromises in design and operation. One example of a situation where safety must be weighed against security is highlighted in Figure 2. Rough weather and pirates: two separate hazards, but also an example where the safety hazard (rough weather) is also an effective and low cost risk control option for the security hazard (pirates).

Figure 2. Rough weather at sea, a typical safety hazard, is an effective risk control option against piracy because the weather affects the pirates' small boats to a much greater extent in than it affects the ships. Illustration: Kajsa Järner.

The overall aim of this thesis is to propose a method for ship security analysis, which aims to increase the overall safety of the crew and the ship. To be able to increase the

overall safety, the analysis must facilitate compromises between traditional maritime safety and maritime security. The objective is to develop a method that is systematic and ensures that assessment and response are complete and effective. It must be possible to use the method in future scenarios and thus describe and model the causal relationships from threat to risk. The aim has been broken down into three steps, chosen to gradually increase the complexity and develop a consistent method base:

- define the requirements of the analysis process (Papers I and II),
- test the feasibility of scenario modelling (Papers II and III), and
- test the feasibility of expert based threat analysis (Papers III).

2.1 Assumptions

The traditional engineering approach to risk analysis, as described in sections 1.2 and 3, is based on *objectivist expected utility*, which combines objectivist probabilities with objectivist utilities. This means that the probability used is interpreted as an objective representation of the frequency and that there is a linear relationship between the consequences studied and their utility assignments (Hansson, 1993). The method proposed here is based on the assumptions:

- that objectivist expected utility can be used to describe security risk for ships, and
- that the result of the analysis can give a reasonable representation of the risk.

The first assumption above means that probabilities and consequences obtained by the analysis are assumed to objectively describe the negative outcomes of the threat. According to Hansson, in his research on the philosophy of risk, this can only be the case if the following criteria are satisfied:

1. The decisions options, as well as the system studied, must be finite and defined.
2. The analysis must be able to identify the negative outcomes of the studied hazard.
3. From the analysis it must be possible to objectively describe the consequences of the hazard.
4. It must be possible to obtain/assess the probabilities with reasonable accuracy.
5. It must be rational to keep the expected outcome (the risk i.e. the probability times the consequence) as low as possible. (Hansson, 1993) and further developed in (Hansson, 2012)

These criteria are seldom fully fulfilled (Hansson, 1993), which is also the case here. According to the second assumption above, the result can therefore only be seen as a simplified description of the risk. However, based on the discussion below and on Hansson's criteria in relation to the work in Papers I to III, the results are assumed to give a reasonable representation of the risk.

1. The decisions options, as well as the system studied, must be finite and defined

The real system and options are never finite. In the work in Papers I to III it is stressed that the system and scenarios must be defined and documented and that the definition must be easily understood throughout the risk management process. See, for example, the discussion on safety culture in relation to risk analysis in Papers I and II.

2. The analysis must be able to identify the negative outcomes of the studied hazard

Difficulties in defining consequences must be documented, especially in relation to the perception of security, and these difficulties must be thoroughly weighed in risk tolerability decisions, analysis of options and risk reduction. For further discussion on risk perception see Paper III and Kunreuther's article on risk analysis for an uncertain world (Kunreuther, 2002).

3. From the analysis it must be possible to objectively describe the consequences of the hazard

The decision maker has the responsibility to weigh different consequences against each other, not the analyst, and this work focuses on being able to disclose and document the causal relationships from threat to risk under the assumption that such an understanding facilitates the risk tolerability decisions and risk reduction. For further detail, see discussion on safety culture in Papers I and II.

4. It must be possible to obtain/assess the probabilities with reasonable accuracy

How the probabilities has been obtained, reported actual frequencies or expert assessment, must be documented and highlighted in the process together with uncertainties. The uncertainties must then be taken into account in the decision process, see for example the discussion on safety factors in Paper II and robust solutions in Paper III.

5. It must be rational to keep the expected outcome (i.e. the probability times the consequence) as low as possible

For frequently occurring cases, it makes sense to keep the expected outcome to a minimum; however, this is not always valid in case-by-case comparisons for hazards with low probability. See discussion on measures of effectiveness in Papers I and II and on robust solutions in Paper III.

3 Method

Today civilian and military security assessment is often risk-based and therefore has the aim of describing security challenges in terms of a risk in the form of consequences and their likelihood. However, most of the assessments lack quantitative investigation and analysis and are therefore only qualitative (DCDC, 2010, IMO, 2002a, NATO Standardization Agency, 2007 and Norwegian Shipowners' Association, 2008). The method of this work is probabilistic risk assessment where quantitative analysis is central.

3.1 General approach

The purpose of introducing probabilistic risk assessment into the ship security analysis is to meet security goals more effectively through a well-balanced combination of proactive and reactive measures. This could then be used as input to operational planning as well as a systems engineering process for concept development, new-builds and midlife upgrades. The aim is to get ships more fitted to their intended use.

In the approach proposed in the current thesis, the aim is, as often as possible, to use quantification of low-level aspects such as aspects of the threat's capability. The low-level aspects are then linked to the risk with causal relationships, see Papers II and III for further details. The proposed approach is consistent with the requirements for maritime safety work. However, the methods proposed here are specifically tested for security cases. This is because hazards (without intent) and threats (with intent) evolve in different ways into risk; therefore, they must be analysed differently in order to capture the causal relationship. There must be particular focus on:

- the lack of objective data, because each intent has its own set of probabilities,
- the antagonistic threat, i.e. changes according to intent and ship protection methods, and
- the relation between the operations measure of effectiveness and the risk taken.

The proposed approach consists of three steps, which all allow stringent documentation of the analysis and results. The first step consists of a threat description that documents qualitative and quantitative aspects that together describe how the threat will act in relation to protection methods and the specific ship. The threat analysis is based on expert assessment, but should if possible also be supported by such things as empirical measurements and intelligence data. The second step uses the threat description 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. In the third step the risk is evaluated with tools from probabilistic risk assessment. Examples of how the quantitative analysis can be documented can be found in Papers II and III.

The result of the security risk analysis described above is meant to be used as a risk knowledge model together with other knowledge models on the same system. Such knowledge models could describe safety risks or the system's effectiveness as a function of operational freedom. Based on this comprehensive understanding of the system studied, decisions regarding such things as risk control options and alternative use of the system can be taken. It must, however, be clear that there will be

uncertainties in the outcomes of the analysis, which must be taken into account when decisions are taken, see section 2.1.

In relation to other work performed today, which most often lacks a quantitative perspective, the proposed method utilises both qualitative and quantitative knowledge. The quantitative aspects allow well-defined ship performance data, such as speed, size and sensor performance, to be included into the model. This enables the analysis to examine how performance data affects the risk for example to test how ship speed affects the probability of successful pirate approach, as shown in Paper III. This relationship is not possible to obtain without a quantitative analysis.

The quantitative aspects, however, make the proposed analysis more demanding than the analysis performed today. The benefits are that it is possible to verify and validate the results, which means that the analysis can be improved over time. The improvements can be a result of lessons from the validation, but also from the fact that the input to the threat analysis, system definition or scenario definition, can be updated. Such a process enables a discussion on probabilities and facilitates feedback to experts on their assessment, which will lead to better assessments in the future.

3.2 Utilised methods and tools

Probabilistic risk assessment is, as described in section 5.2, often complex and an audit of the assessment is vital to ensure that a logical and consistent approach and relevant data has been used. In order to make sure that the risk management process is systematic, and thus facilitates a complete and effective response, the studies in Papers II and III also make use of the analysis tools presented below. These tools come mostly from the areas risk analysis, military force protection, military operations research and decision analysis, see Figure 3.

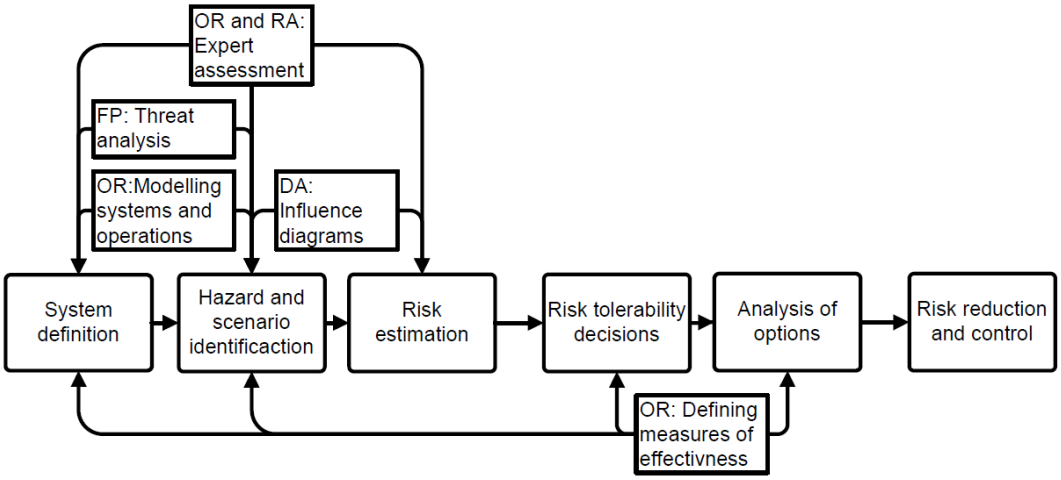

Figure 3. Illustration of generic tools and methods from the areas of Operational research (OR), Decision analysis (DA), Force protection (FP) and Risk analysis (RA) supporting the risk management process in the appended papers.

Probabilistic risk assessment

As described in sections 4 and 5 the development in the area of ship safety is risk-based. It is reasonable to assume that development in the area of ship security would benefit from being consistent with the same fundamental aspects, such as the definition

of risk and demands for quantification of, for example, scenario probabilities. Such consistency would then allow safety risks to be compared with security risk in order to find the best compromise. For further details, see Paper I.

Probabilistic risk assessment is seen here as an approach, which aims to quantify the risk in terms of probabilities and consequences. The result is then compared with limits set by society and the operator to decide to what extent the process can be defined as safe or how the risk can be limited (Andrews & Moss, 2002). See section 5 for further discussion.

Therefore, the work in the appended papers utilises, where possible, the experience and requirements defined in the risk-based ship design (Sames, 2009) and International Maritime Organisation's (IMO) formal safety analysis (IMO, 2002b), where the procedure is well documented.

System definition

A risk analysis must be performed on well-defined scenarios and systems (Hansson, 1993, IMO, 2002b and Vassalos, 2009). The work in Papers II and III makes use of influence diagrams (Shachter, 1988) to define the system.

Influence diagrams are described by IMO in the Guidelines for formal safety assessment (IMO, 2002b), but more thoroughly documented in the area of decision analysis. Papers II and III use influence diagrams to model influences and define the studied system.

An influence diagram is a graphical, 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 (IMO, 2002b and Shachter, 1988).

A Bayesian network is an influence diagram without the ability to include decision and utility nodes (Friis-Hansen, 2000). The work presented in this thesis uses the more general term: influence diagrams; however, the term Bayesian networks could have been used as well. In the area of maritime safety Bayesian networks have been tested in different areas such as tool for cost-optimal inspection planning, a reliability model of buckling of pipelines (Friis-Hansen, 2000) and bridge work in a collision scenario (Pedersen, 2010). Friis-Hansen's research on Bayesian networks show that Bayesian networks and influence diagrams have many advantages to offer the marine community, especially in the area of risk analysis.

Expert assessment

Risk analysis is often supported with data from expert assessment due to a lack of empirical data on the studied system (IMO, 2002b); this is also the case in this thesis. 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 (Hansson, 1993). 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. Paper II discusses the possibility of basing the threat analysis on expert assessment and Paper III tests the concept on piracy using the threat analysis presented in the Allied joint doctrine for force protection (NATO Standardization Agency, 2007).

In this work, expert assessment is collected through a combination of questionnaires and interviews in order to capture both qualitative and quantitative aspects of the threat and the interaction with the vulnerability of the ship. For further details, see Paper III.

Simulations of operations

To capture important aspects of maritime operations a safety scenario is seen here as a model of reality to be used when analysing risks associated with the operations studied.

When setting up the simulation the variables that affect the problem must be defined as well as the constraints and limitations. In the simulation there must be particular focus on the measures of effectiveness, as they will give guidance on how the simulated system will be used and how different alternatives are prioritized (Jaiswal, 1997).

The simulations must be validated and statistical analysis plays an important role in model validation if results of the system operation are available. Military system studies and security studies, however, suffer from a lack of historical data and realistic experiments can be impossible to perform (Jaiswal, 1997). The model validation is therefore often limited to sub-model validation based on statistical data and model validation by expert opinion, sensitivity analysis and hypothesis validity, see Paper II for further discussion and Paper III for examples of validation based on statistics.

4 Regulations for maritime risk management

There are maritime safety and security regulations and requirements with varying degrees of importance and applicability such as international regulations, regional regulations, flag state regulations, classification requirements and industry guidance. More detailed examples and descriptions are presented in Papers I to III. According to the International Association of Classification Societies (IACS), regulations and requirements should only be seen as a starting point for ensuring safe and secure operation of the ship. The ship operator must, therefore, follow the applicable regulations and requirements, but is also responsible for identifying and safeguarding against the risks associated with its particular ships, operations and trade. The methods applied must be systematic, if assessment and response are to be complete and effective, and the process documented to provide evidence of the decision making (IACS, 2004).

4.1 IMO regulations and civilian ships

Maritime safety regulations developed by the IMO are designed to make sure that passengers, cargo, crew, surrounding ships and environment are kept as safe as possible (Kuo, 2007). Traditionally the codes were prescriptive in their nature, which means that the codes prescribe aspects of design or construction with engineering specifications. Prescriptive standards are generally formulated as a result of accidents and are suitable for routine activities, but devolve responsibility and innovation and are unsuitable for new developments (Kuo, 2007). The IMO Code of safety for high-speed craft (IMO, 1994) states that for traditional ships it is possible to use a prescriptive code and ensure a suitable low risk level. However, for novel or specialised types of ship, a prescriptive safety code is too restrictive and probabilistic (or risk-based) methods, where the risk for different incidents is kept acceptably low, need to be used. Such a probabilistic method uses a series of standardized expressions to evaluate events, and events with minor effect are allowed to have a higher acceptable probability than an event with hazardous effect. See Papers I and II for more details.

Risk-based approaches have been developed by the IMO since the 1960s. The probabilistic damage stability regulation in Safety of Life at Sea from 1974 (SOLAS74) was the first risk-based regulation. In 1997, the IMO adopted the Formal Safety Assessment as a risk-based approach to rule making (Skjong, 2009). Quantitative risk-based approaches are thus well established in the area of maritime safety, even though such approaches have not yet been developed for all safety areas.

Risk-based ship design, operation and regulation have, in terms of safety risks, has also been the focus of the integrated project SAFEDOR (Sames, 2009) under the 6th framework programme of the European Commission. According to SAFEDOR the results of risk analysis and other ship performance data should be used as a risk knowledge model in design decision making (Vassalos, 2009), in accordance with Figure 4. This allows comparison of operational risk with operational gain in design decision making.

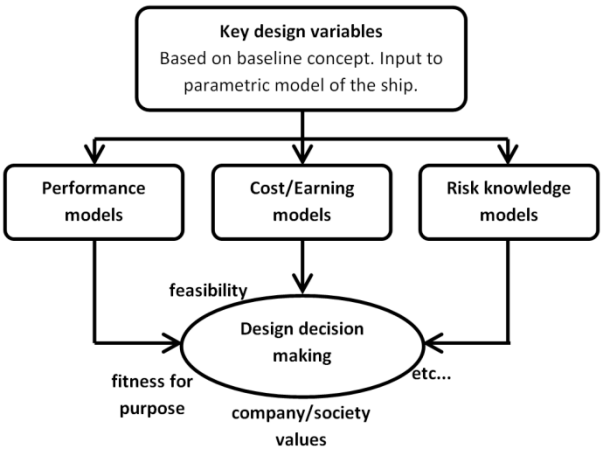

Figure 4. Design decision making in risk-based ship design. Redrawn from Vassalos (Vassalos, 2009).

The first maritime and ship security measures and regulations were developed and approved by IMO in 1986 after the terrorist attacks on the cruise ship Achille Lauro. However, these measures were only made mandatory by the US, Canada and the UK (Wengelin, 2012). Therefore, the ISPS code, introduced in 2002, which regulates ship security analysis, is the first regulation with the possibility of affecting ship security efforts. The ISPS code can be classified as risk-based, but is described by IMO as a first step (Mitropoulos, 2004).

4.2 Naval ships

The safety of a ship under attack is the responsibility of the state in question and is not governed by international regulations. SOLAS does not apply to "*ships of war and troopships*" (NATO Standardization Agency, 2010). However, a naval ship often operates under non-military conditions and civilian maritime safety regulations are often applicable for many parts of the ship (James, 2010), for example, see the man overboard case highlighted in Figure 5. Today there are a number of classification societies that have rules for the classification of naval ships (Simpson, 2010). Det Norske Veritas classification rules for naval ships (DNV, 2009) are described in Papers I and II.

Figure 5. Should the analysis procedure of risk associated with a man overboard be different depending on whether or not it is the result of a safety hazard or security threat? Dummy overboard during an exercise testing the war fighting and damage control readiness of crews in the Swedish Navy. Photo: Hans Liwång

The Naval Ship Code (NSC) is a code developed by NATO's standardisation agency (NATO Standardization Agency, 2010). The code is developed for surface naval

vessels and other vessels operated by the armed forces or agencies of a state. The NSC, which is optional, is based on, and benchmarked against, IMO conventions and resolutions. The code does not include measures specifically designed to address the effects of military attack. The NSC is goal-based and the ship should be verified against the goals during the design and construction stages as well as during operation. See Paper I for more details on the structure of the NSC.

Even though the NSC does not include measures to address hostile attacks, *Annex A, Guide to the Naval Ship Code*, describes how required survivability should be defined as a result of the specific operation profile of the ship. The annex states that potential damage caused by hostile acts, post-damage ship capability requirements and a philosophy for recovery from the damaged state must be defined for effective application of the code. This should be defined as scenarios in the ship's concept of operation and the code also states that policies and doctrines should be made available so that staff involved in design as well as operation can understand the basis for decisions.

In theory, the goal-based approach of the NSC permits alternative arrangements, but the choice of verification method often reduces that freedom substantially. It is therefore very important to choose a verification method that is suitable for the type of ship and concept of operation in question. The goals in the NSC are not risk-based. However, a risk-based verification method is not contradictory to the definition of performance-based verification. See Paper II for further details.

Paper I studies two cases, ballistic protection on smaller naval vessels and bridge configuration to minimize the effects of an attack, and shows that the NSC does not give any insight into how a quantitative analysis of the ships' survivability can, for example, be compared to a probabilistic analysis, in accordance with the classification rules. The NSC states that survivability should be analysed using defined scenarios in the ships' concept of operation. However, this is not possible without a common base for probabilities and the NSC does not specify that probabilities should be defined for the scenarios in the concept of operation. This means that defining a method for assessing probabilities of armed attack and its consequences is needed to allow integrated survivability and safety analyses for naval ships.

4.3 Current research and developments in maritime security

As described above, when it was introduced in 2002, the ISPS code was described as a first step. However, development since the code was introduced has been limited. In a review of recent literature concerning maritime security, Yang found 30 relevant research papers, of which only 10 are quantitative and none has a risk management perspective (Yang, 2011).

There are, however, a few papers on ship security relating to piracy. Two typical examples of such papers are *Is piracy random?* by Mejia et al. (2009) and *Risk modelling of non-lethal response to maritime piracy and estimating its effect* by Psarros et al. (2011). Both these papers use statistics on piracy incidents and on the world merchant fleet to analyse the risk of piracy. The use of statistics, however, limits the description of the causes, or risk drivers, resulting in the analysed risk. These papers show, therefore, that there is a need for more thorough threat analysis in order to explain causes and predict future risks.

In both the UK and NATO doctrines, the method for understanding the threat is well defined (DCDC, 2010 and NATO Standardization Agency, 2007). However, the method for the suggested risk analysis is only described on a general level. Therefore the military development is more developed in regards to threat analysis in comparison to civilian maritime security, but in regards to methods for risk analysis both the civilian and military development in maritime security lack the structured and documented perspective found in maritime safety. This supports the need for combining civilian and military experience discussed in section 1.1.

5 Maritime risk management, today's methods and tools

This chapter presents central, and generic, concepts and methods used in maritime risk management today. These concepts and methods are also utilized in the approach for ship security presented here.

5.1 Risk criteria and risk control options

Both civilian and military ship owners are responsible for weighing the risk against the cost of implementing controls and measures and the impact on operational gain. However, other organizations and society also set limitations on permitted risks and risk criteria. Risk criteria have been discussed within the IMO because of risk-based safety approaches (Skjong, 2009).

According to Pedersen different principles must be used to formulate risk criteria depending on the form of the consequence; the appropriate principles and levels are different for situations involving individual fatality compared to accidents involving multiple fatalities or environmental consequences. There must be particular focus on accidents with multiple fatalities because society is more concerned about single events with many fatalities and societal risk, than it is about several incidents with few fatalities per incident (Pedersen, 2010). Therefore, it is reasonable to assume that the risks associated with ship security, such as example piracy, other types of crime at sea and attack against military ships, need specific risk criteria, as the consequence is not comparable with traditional operational risks for shipping. For further discussion on risk criteria and ship security, see Papers II and III.

Risk criteria within IMO are often formulated in the form of a diagram where the risk criteria limits the combination of the cumulative frequency (F) and number of persons harmed (N), in a F-N diagram as shown in Figure 6. Risk in the Non-Acceptable domain, for example an activity were 10 persons is expected to be killed every 100 years, must be reduced at all costs. For risks in the As low as reasonable possible (ALARP) domain, for example an event where 100 people are expected to be killed every 10,000 years, the effectiveness of safety measures should be considered alongside other criteria, e.g. finance. IMO and IACS will only introduce or propose new risk reducing measures, if the resultant cost of a new measure is less than three million USD per potential life saved (Pedersen, 2010 and Skjong, 2009).

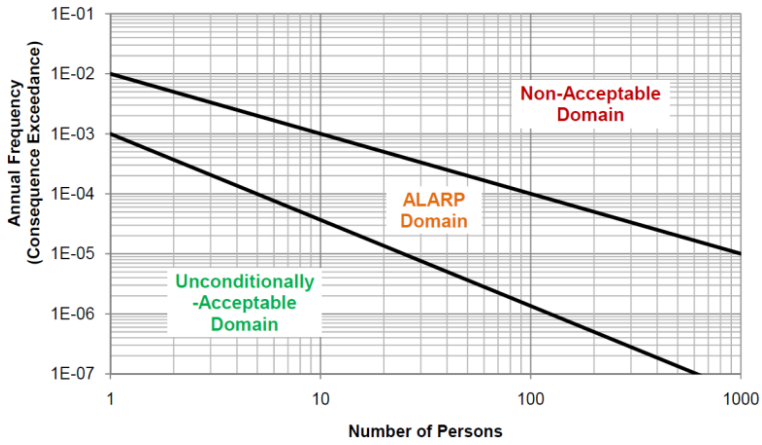

Figure 6. Typical risk acceptance criterion, F-N diagram. Redrawn from Pedersen (2010).

Relevant and well-defined risk criteria are a prerequisite for risk analysis because the analysis must assess the type of consequences relevant for the risk criteria. Risk control options (means of controlling the risk) are applied for risks in the Non-Acceptable and ALARP domains. Risk control options can range from technical measures included in the design of the ship to specific changes to such things as the watch-keeping scheme on board. Typical and recommended risk control options are described in IMO regulations and classification requirements.

Typical security control options are also described in the ISPS code (IMO, 2002a) and the Best Management Practise for Protection against Somalia Based Piracy (BMP) (BIMCO, et al., 2011). However, each security threat and ship has specific risk causality and, therefore, a specific list of suitable risk control options. These control options can only be found with the help of a ship-specific risk-based ship security assessment (IMO, 2002a).

5.2 Probabilistic risk assessment

Probabilistic risk assessment offers a sound and systematic basis for evaluating potential hazardous activity. Risk analysis is a tool for identifying and assessing possible unwanted events and finding effective measures to minimise the risk. However, the methods used are specialized and often complex and an audit of the assessment is vital to ensure a logical and consistent approach and that relevant data has been adopted (Andrews & Moss, 2002).

The first step of the risk analysis is the scope and system definition. The system definition will always affect the validity and outcome of the analysis, but a clear and sound definition is also a requirement for effective analysis. Therefore, the definition of the system must be thoroughly documented and presented with the results of the analysis (Hansson, 2012).

5.2.1 Hazard and scenario identification

In the identification of hazards step, both creative and analytical techniques are used. The "*what can go wrong*" question must be explored systematically, usually based on expert judgment; see (Kuo, 2007 and IMO, 2002b).

Risk scenarios must be based on the hazards identified. The scenarios should have calculable probability and consequences that are able to collectively quantify the life-cycle risk of a ship at sea. They relate to event categories with major hazard potential. When generic scenarios are available, they must be adapted and customised to the specific design features and expected performance of the ship in question.

5.2.2 Analysis of consequences and probabilities

After hazard identification and scenario definition, the scenarios must be analysed in detail in order to estimate the risk. The purpose of this analysis is to investigate the consequences of the identified hazards and to calculate their probabilities. This is a complex procedure and the criteria discussed in section 2.1 must be taken into account throughout the analysis.

In the analysis, low-level factors, such as engineering specifications, system schematics and measured or assessed probabilities, are linked to the probability of the identified consequences. For this analysis there are several tools documented in risk analysis

literature. However, each tool has specific limitations and benefits and the analysis process has to be chosen carefully. The analysis can, for example, be carried out using a combination of event trees, influence diagrams and Monte Carlo simulations as in Paper III.

6 Summary of the work in the appended papers

The work in the appended Papers I to III is related to the risk management process for ships, but for different kinds of systems and with different scope and methods, as outlined in Figure 9.

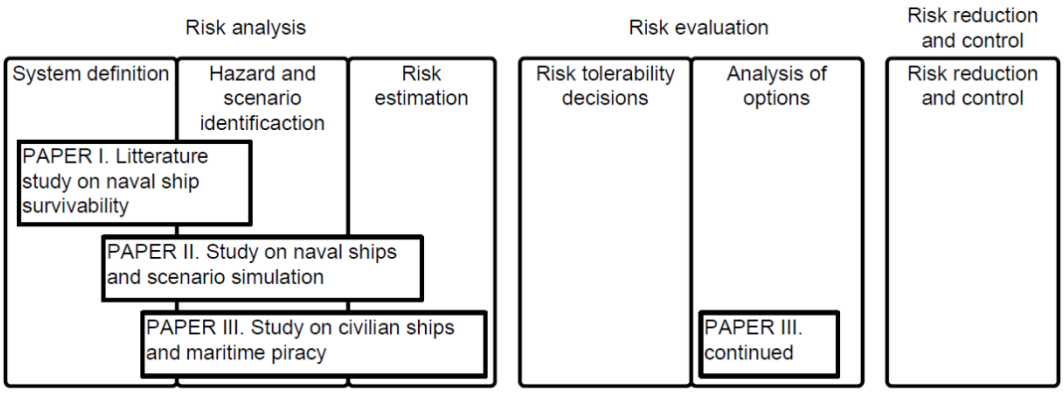

Figure 9. Illustration of the risk management process and the scope and methods for Paper I, Paper II and Paper III.

6.1 Paper I

The aim of Paper I is to investigate and describe the effects of the NSC on efforts to enhance ship survivability. The study is a qualitative case study with two cases: ballistic protection of smaller naval vessels and bridge configuration to minimize effects of attacks. The two cases are chosen so that they cover a range of requirement types. In these two areas, the NSC regulations (i.e. the aims, goals, functional areas, performance requirements and verification methods) are compared to survivability measures. The result is discussed in terms of how the NSC affects total safety efforts.

The NSC is compared with the types of measures called for in the two cases in order to see how the code interacts with measures to increase ships' survivability. The three basic areas of safety culture; (a) formal regulations and processes, (b) competence and training and (c) shared risk awareness throughout the organisation, were used to structure the analysis and the results in Paper I. The first area, formal regulations, is analysed for each case separately and the two other areas are analysed for the two cases together.

Paper I, therefore, unveils the imbalance between safety and security and examines the demands on the security risk management process in relation to a ship's survivability. Paper I concludes that in order to be able to include survivability, or ship security, in the understanding of the overall performance of a ship, a risk knowledge model that includes safety and security is needed.

6.2 Paper II

In Paper II probabilistic risk assessment is used as a method to quantify safety and security. The aim is to investigate and describe how, based on probabilistic risk assessment procedure, the concept of operation for a ship can be turned into relevant safety scenarios. It should be possible to use such scenarios in the evaluation of consequences and probabilities as a decision support tool in the design of naval ships.

Aspects of safety culture, codes, regulations and rules are analysed in terms of the requirements of safety scenarios. The analysis focuses on requirements, which ensure that the result can be used to improve the design process and enhance design decision making. Military operational research, specifically on modelling military systems, is described in order to ensure that safety scenarios model military operations effectively.

Safety scenarios for commercial ships are often based on accident statistics combined with expert judgment, but for military operations, statistical data is rare. The paper presents an example of a numerical simulation for event probability estimation. It demonstrates how probability-based scenarios can be derived, based on the requirements discussed in the previous sections of this thesis. The objective of the model is to use the concept of operation to identify scenarios that relate to accident categories with major hazard potential and to assess the scenario probability. The model is a formalised procedure of incident quantification to support definition of probability-based safety scenarios. The resulting scenarios could then be used in risk analysis.

The inputs to the simulation model are typical design parameters such as ship speed, sensor characteristics and intended fleet composition. Based on the concept of operation, the relevant types of naval operation are divided into tactical tasks defined with measures of effectiveness, environmental data and threat characteristics. These kinds of simulations are in their structure and model characteristics not new, but the results here must be aggregated and handled so that they are consistent with probabilistic risk assessment.

The study shows that simulation of tactical tasks makes it possible to quantify and analyse the operation procedures and system configurations in relation to scenario probability. Simulation, therefore, supports scenario definition based on a combination of simulation output and expert judgment. The simulation will then illustrate the causal relationships that link the characteristics of the ship to the operational risks, for example, see Figure 9, where the cumulative frequency of available time for counter measures is calculated for different situations.

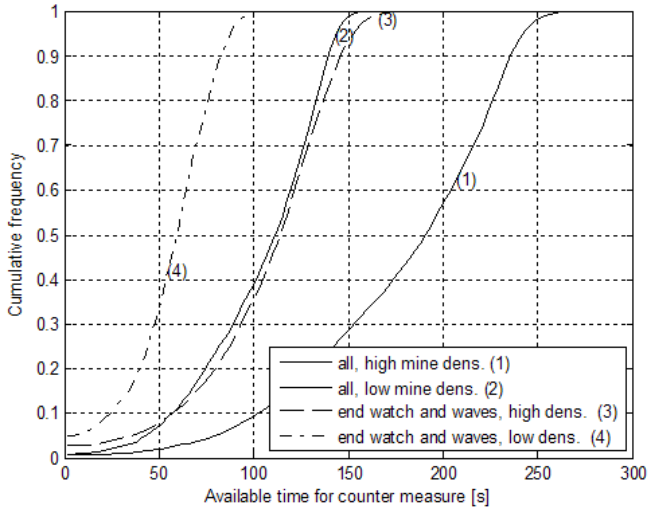

Figure 9. Cumulative frequency of available time for counter measure. 1,000,000 simulated events. From the figure, it is clear that the combination of end of watch and waves combine to reduce the available time, and by how much.

The output from scenario simulations will therefore guide experts to more ship-specific probability functions than would have been the case, if the experts had based safety scenarios on experience alone. The simulation can, therefore, assist in a process that otherwise relied completely on expert judgment.

6.3 Paper III

In Paper III the ship security assessment of the ISPS code is reviewed with a wider perspective making use of security research and experience from military force protection, and methodological lessons learned from maritime probabilistic risk assessment. The study has two main objectives: to explore the possibilities and carry out quantified and more thorough ship security risk analysis than that described in the ISPS code and the guidelines to the code, and to examine and evaluate to what extent this more detailed analysis increases ship security.

The study focuses on the Somali based maritime piracy using the piracy on the Indian Ocean as the example case. Data is collected, using questionnaires and interviews, from civilian and military security experts with firsthand experience from piracy off the coast of Somalia. The data is specifically collected for this study and describes the threat capability, threat intent and the likelihood of exploiting the ships' vulnerability. The data collection is performed in three different steps. In the first step a questionnaire was sent to experts in order to collect data on the piracy operating out of Somalia. The second step was interviews with experts to collect a wider knowledge base on piracy and the risk management performed by ship owners and operators. In the third step selected areas of piracy were revisited using a second questionnaire in order to decrease the range of the uncertainties in the answers.

Event tree methodology is used to model and analyse the possible consequences and the probabilities of an attack. The inductive event tree is used because a pirate attack has well defined chronological steps that are illustrated by the sequences of the event tree. Collected data is used to develop models and calculate probabilities for the event tree. The calculations are simulations representing sub sets of the scenario with influences according to influence diagrams. Throughout the analysis the results of the influence analysis play an important role in describing the interaction between pirates' characteristics and ships' vulnerability. See Figures 10, 11 and 12.

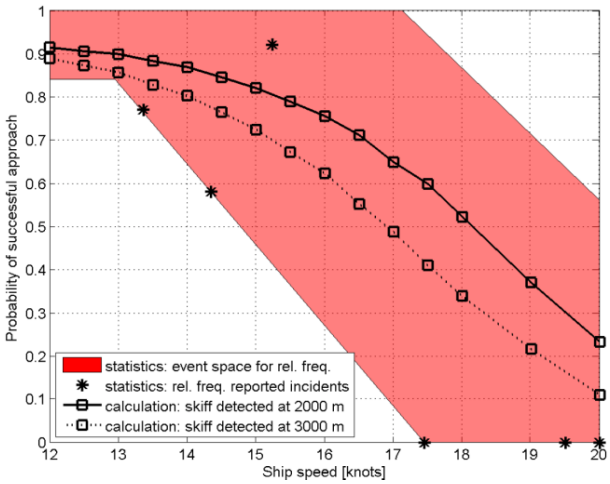

Figure 10. Quantitative output from the Monte Carlo simulations in Paper III in the form of calculated probability of successful approach as a function of ship speed and skiff detection distance.

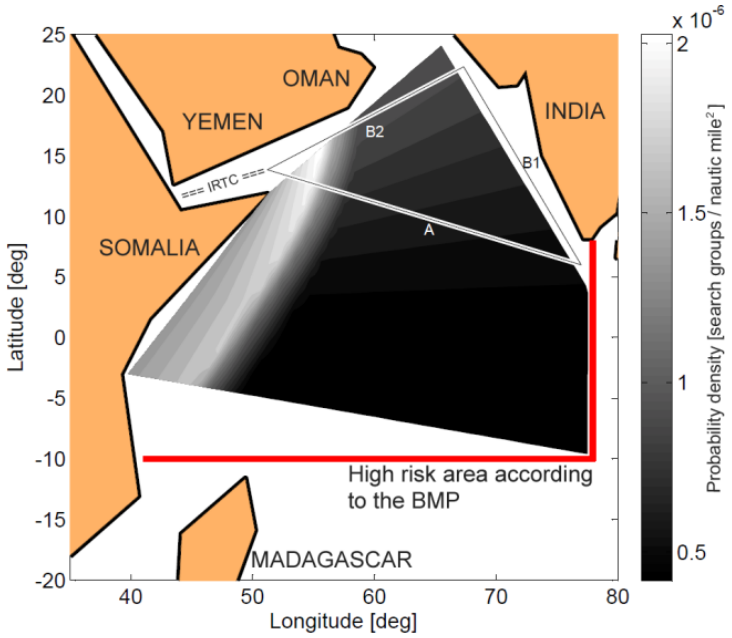

Figure 11. Quantitative output from the analytic probability calculations in Paper III in the form of calculated probability density function for pirate search groups on the Indian Ocean.

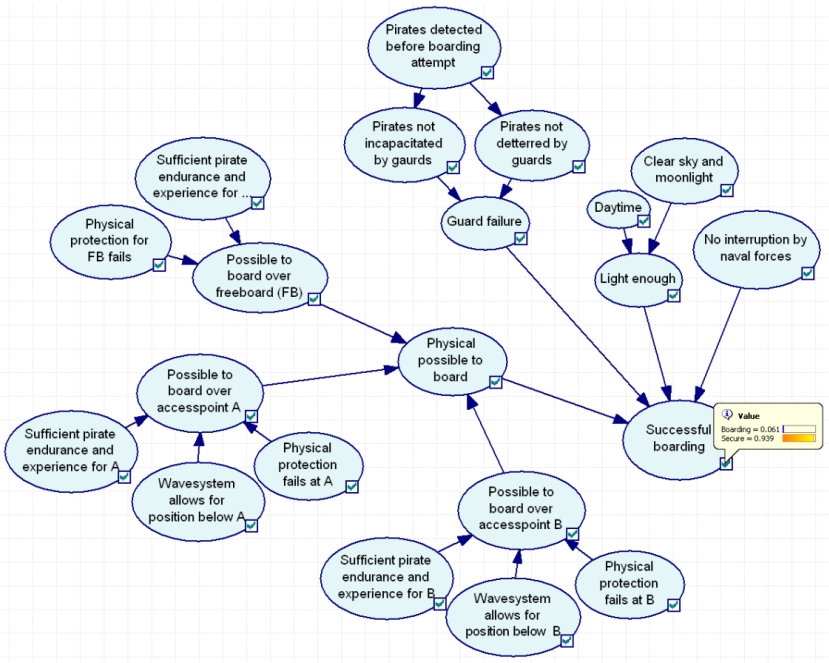

Figure 12. Influence diagram for assessing and comparing probability of successful boarding.

According to the interviews conducted, the combination of graphical illustration and quantitative output not only calculates probabilities and consequence, it also enables a qualitative discussion on causes and measures not possible with the qualitative analysis often performed today. In the areas where it is possible to compare the calculation results of the performed analysis with incidents reports the result of the study is inside the event space of the statistics and can therefore be assumed to model the relevant aspects of the threat, see for example Figure 10.

7 Conclusions

The overall conclusion is that the proposed method brings the procedure and results of ship security analysis into the open and therefore allows for criticism, improvements and shared risk knowledge, not possible with less structured methods. The proposed method, therefore, enable a discussion on probabilities and facilitate feedback to experts on their assessment which will lead to better assessments in the future (Hansson, 2012). Below the conclusions are divided into two categories: scientific contributions, and industrial relevance and findings.

Scientific contributions

It has been found that risk analysis for a naval ship should include events that follow an armed attack so that redundancy, for example, is not only based on safety measures derived from civilian shipping scenarios. It is, therefore, concluded that a method for assessing probabilities of armed attack and its consequences is needed in order to allow integrated survivability and safety analysis for naval ships.

It has been shown that the scenarios modelled in the analysis must have calculable probability, be adapted and customised to the specific design features and expected performance of the vessel in question with an emphasis on disaster escalation scenarios. Results from simulations show that modelling tactical tasks in military operations is a possible way of supporting experts in the definition of probability based security scenarios.

It is further concluded that influence diagrams facilitate the use of a combination of quantified data and qualitative descriptions to analyse the threat and that the calculated probabilities agree with the frequencies in the incident reports. The scenarios developed are found to describe the most important influences in the areas analysed, see for example Figure 10.

An understanding of the causal relationship between threat and risk, gained from the risk-based approach with structurally collected and documented information on the threat, is important in order to effectively select robust risk control options. This is because such an understanding allows examination of how the different risk control options contribute to security. This understanding and examination can then be used to design the optimal risk control option for a specific ship, which gives high security without any unnecessary negative impact on operations.

Industrial relevance and findings

It is concluded that the use of probabilistic safety scenarios supports risk analysis of both traditional maritime safety areas as well as military survivability areas and the key aspects of safety culture throughout the design, construction and operation of the ship. Such scenarios were found to give an insight into how quantitative analysis of a ship's survivability can, for example, be compared to a probabilistic analysis in accordance with the classification rules.

This study shows that it is possible with, the use of experts, to collect data on a pirate's capability, intent and likelihood of exploiting vulnerability through a combination of questionnaires and interviews.

The interviews show that the combination of graphical illustration and quantitative output in the analysis method used, influence diagrams based on qualitative descriptions and quantitative data, not only calculates probabilities, it also enables a qualitative discussion on causes and measures not possible with the qualitative analysis often performed today. Such a discussion is very valuable in the decision process. However, it is also clear from the interviews that the proposed method demands more work than that put in to ship security analysis today.

8 Future work

Existing research in the area of quantitative ship security risk analysis is very limited. Much more is needed in order to develop reliable methods that can be applied generally. Papers II and III, however, show that it is reasonable to assume that the approach is feasible and can already give important input to the risk analysis process when discussing such issues as anti- piracy measures on ships. The aim in coming years therefore, based on the current results, is to deepen the analysis completed so far, in order to be able to verify the results and validate the proposed method more thoroughly.

As mentioned in section 3, quantitative risk assessment offers a sound and systematic basis for evaluating potential hazardous activity, but is specialized and often complex and an audit of the assessment is vital to ensure a logical and consistent approach and that relevant data has been adopted (Andrews & Moss, 2002).

Despite a lack of historical data and realistic experiments, as discussed earlier, future studies must be performed to further verify the calculations of both probabilities and consequences and to further validate the results of the risk analysis. Three different principal approaches to such a verification and validation are briefly discussed below.

Theoretical method development

Due to the immaturity of the field and limited availability of data, future work should focus on theoretical method development. In order to cover all aspects of risk analysis, the work is to be divided into several small areas and, for each of these areas, the results are to be both verified and validated on simplified base cases where data is available or obtainable.

Focus areas for theoretical method development could include, but not be limited to, the following:

- tools for developing and validating probability based security scenarios,
- reliability and calibration of expert assessment for ship security analysis, and
- development of ship security simulations and verification methods.

Such studies would be able to give specific recommendations on how these activities should be planned, performed and used in ship risk management.

Applied method development on naval ships

For naval ships the connection between security risks and the concept of operation of the ship is specifically strong. This puts the focus on validity of the risk analysis in relation to the ship's measures of effectiveness. Without such validity the risk analysis is pointless. Studies of naval ships are, therefore, important for establishing an understanding of the utility of security risk analysis.

Studies of naval ships could give unique insight to:

- how a safety culture of calculated risk taking can utilize risk analysis, and
- how, and to what extent, the analysis should be performed in order to make the analysis useful.

Applied method development on civilian ships

Ship specific analyses are important because the detail of such studies will introduce problems not encountered in the more general studies performed so far. For civilian ships there are statistics and incident reports available to study and, based on the experience from Paper III, it can be assumed that for limited cases it is possible to perform a detailed security analysis and also verify and validate the result. These studies could be performed on:

- piracy in different regions, and testing how accurately the model can describe how the risk is affected by the threats intent and modus operandi, and
- terrorist attacks, and examining how the conceptually different intent (terror) changes the conditions for analysis.

Studies of civilian ships also allow study of which results should be presented, and how they should be presented, in risk evaluation and risk reduction in order to create effective risk management.

References

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

BIMCO, CLIA, ICS, IGP&P, IMB, IMEC, et al. (2011). *Best management practices for protection against Somalia based piracy*. Edinburgh: Witherby Publishing Group Ltd.

DCDC. (2010). *Joint doctrine publication 3-64, Joint force protection*. Shrivenham: The Development, Concepts and Doctrine Centre, Ministry of Defence, United Kingdom.

Department of Defence. (2007). *A cooperative strategy for 21st century seapower*. Washington DC: Department of Defence, United States of America.

DNV. (2009). *Rules for classification, high speed, light craft and naval surface craft*. Høvik: Det Norske Veritas.

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

Hansson, S. O. (2012). *Riskfilosofi, en introduktion*. Stockholm: Liber. (In Swedish).

Hansson, S. O. (1993). *The false promises of risk analysis*. Ratio **6**: 16-26.

IACS. (2004). *A guide to risk assessment in ship operations*. London: International Association of Classification Societies.

IEC. (1995). *Part 3: Application guide, Section 9: Risk analysis of technological systems*. In: Dependability management. Geneva: International Electrotechnical Commission.

IMO. (2002). *The international ship and port facility security code*. In: SOLAS. London: International Maritime Organisation.

IMO. (2002). *Guidelines for formal safety assessment (FSA) for use in the IMO rule-making process*. London: International Maritime Organisation.

IMO. (1994). *International code of safety for high-speed craft (HSC Code)*. London: International Maritime Organisation.

James, P. (2010). *Use of class and standards for assurance*. The Royal Institute of Naval Architects, Warship 2010: Advanced technologies in naval design and construction: 7-15.

Jaiswal, N. K. (1997). *Operations research in defense*. In: Military operations research, quantitative decision making (pp. 1-12). Boston: Kluwer Academic Publishers.

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

Kuo, C. (2007). *Safety management and its maritime application*. London: The Nautical Institute.

McNaught, F. (2005). *Effectiveness of the International ship and port facility security code*. Geddes Papers 2005: 89-100.

Mejia Jr, M. Q., Cariou, P., & Wolff, F.-C. (2009). *Is maritime piracy random?* Applied Economics Letters **16**: 891-895.

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

NATO Standardization Agency. (2007). *Allied joint doctrine for force protection, AJP-3.14*. Brussel: North Atlantic Treaty Organization.

NATO Standardization Agency. (2010). *Naval ship code, ANEP 77, rev 1*. Brussels: North Atlantic Treaty Organization.

Norwegian Shipowners' Association. (2008). *Guideline for performing ship security assessment*. Oslo: Norwegian Shipowners' Association.

Pedersen, P. T. (2010). *Review and application of ship collision and grounding analysis procedures*. **23**: 241–262.

Psarros, G. A., Kessel, R., Strode, C., & Skjong, R. (2011). *Risk modelling of non-lethal response to maritime piracy and estimating its effect*. The international conference on piracy at sea, ICOPAS 2011. Malmö: World Maritime University.

Sames, P. C. (2009). *Introduction to risk-based approaches in the maritime industry*. In: Papanikolaou, A. D. (Ed), Risk-Based Ship Design, Methods, Tools and Applications (pp. 1-15). Berlin: Springer.

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

Simpson, B. (2010). *Implications of the NATO Naval ship code*. The Royal Institute of Naval Architects, Warship 2010: Advanced technologies in naval design and construction: 1-6.

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

University of Cincinnati. (2004). *Principles of war*. Cincinnati: University of Cincinnati.

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

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

WMU. (2011). *The Malmö declaration*. Malmö: World Maritime University.

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