THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

# Risk-based ship security analysis – a decision-support approach

Hans Liwång


Department of Shipping and Marine Technology
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
2015

**Risk-based ship security analysis – a decision-support approach**

HANS LIWÅNG
ISBN 978-91-7597-127-8



Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 3808
ISSN 0346-718X

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



Printed by Chalmers Reproservice
Gothenburg, Sweden 2015

**Risk-based ship security analysis – a decision-support approach**

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

## Abstract

The protection of shipping does not come without hazards and threats for military forces, individual civilian ship operators and crews. With particular focus on security threats, this thesis is about how to prepare for such operations without introducing unnecessary risks, i.e., supporting conscious risk-taking related to ship security. It examines both civilian and military aspects of maritime security and therefore draws from the experience of both fields.

Maritime safety regulations, guidelines and methods have a history and culture of systematic research, development and implementation. In contrast, international security is highly politicised and therefore less transparent. Unfortunately, comprehensive studies of ship security risk are rare. Moreover, applying risk-based approaches to security areas requires special considerations, and the limited research in this field has led to a knowledge gap.

To reduce the identified challenges with respect to security risk analysis, the goal of this thesis is to improve security decision support by defining an approach to ship security analysis. To increase overall safety, this approach must facilitate compromises between traditional maritime safety and maritime security. Accordingly, the objective is to develop an approach that is both systematic and gives the decision maker an appropriate picture of the security risks. To examine the requirements for a security decision-support approach, the work in the appended papers studies both threats to naval vessels and the security threat posed to commercial vessels by pirates. The results of the studies can be used to further develop military doctrines and civilian guidelines.

This study shows that the description and quantification of the (concept of) operation in the risk analysis is central for implementing both security and naval ship survivability. In addition, the crew's risk perception, procedural safeguards and how the implemented risk controls are perceived have an important role not only in risk analysis but also in deciding the effectiveness of implemented controls. It is also concluded that only using expected values—not collecting and using uncertainties—in the analysis can lead to misleading results. Therefore, the uncertainty treatment offered by a quantitative approach is crucial for risk understanding, especially if the aim is to find robust control options or to support the development of a resilient culture.

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

# Preface

First and most importantly. There are two extra influential persons among many good teachers and professors during my years at school and universities:

*Maria Olovsson and Mikael Huss who in an outstanding way showed me how to approach knowledge development (holistically, solution oriented, with a focus on relativism-procedural knowledge and with curiosity). Without You as my teachers, I would not have envisioned this journey!*

Then:

This thesis is comprised of work carried out during the years 2010-2015 at the Department of Shipping and Marine Technology at Chalmers University of Technology and at the Department of Military Studies at the Swedish Defence University. The work is mostly funded by the Swedish Defence University (www.fhs.se), but also partly by the Swedish Competence Centre in Maritime Education and Research, LIGHTHOUSE (www.lighthouse.nu).

The mix of civilian and military method development and research as well as experience from many different disciplines that I have had the opportunity to tap into is important. This thesis would not have been possible without a broad approach and support from research colleagues with different scientific perspectives, naval experts from the Royal Swedish Navy and ship owners' safety, security and operation managers.

Therefore, thanks to everyone involved in my research and thesis work in some kind of order:

- supervisors Jonas Ringsberg and Martin Norsell,
- colleagues and researchers at universities across Sweden and abroad,
- practitioners such as officers at the Swedish Armed Forces and maritime security experts, and
- my family.

Without you, this would not have been possible!

Last, but not least:

Any particular clear or smart passage in this thesis is as much a result of my colleagues' insightful comments or questions as anything else. You know who you are!

# 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 (2013). *Quantitative risk analysis – ship security analysis for effective risk control options.* Safety Science (58). 98-112.

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

**Paper IV** Liwång H. *Survivability of an Ocean Patrol Vessels – Analysis approach and uncertainty treatment.* Submitted (January 2014) for publication in Marine Structures.

**Paper V** Liwång H. *Conditions for risk based ship survivability approach: a study on the analysis of fire risk.* Naval Engineers Journal (IN PRINT/2015).

# List of other published work by the author

Liwång H, Pejlert L, Miller S, Gustavsson J-E (2001). *Management of high speed machinery signatures to meet stealth requirement in the Royal Swedish Navy Visby Class Corvette (YS2000)*. In: The proceedings to ASME Turbo Expo 2001: Power for Land, Sea, and Air, Volume 1: Aircraft Engine; Marine; Turbomachinery; Microturbines and Small Turbomachinery. American Society of Mechanical Engineers.

Andersson K, Artman K, Astell M, Liwång H, Lundberg A, Norsell M, Tornérhielm L (2007). *Lärobok i Militärteknik, vol. 1: Grunder [In Swedish]*. Stockholm: Swedish National Defence College.

Bruzelius N, Bull P, Bäck L, Eklund J, Heilert K, Liwång H, Stensson P, Svantesson C-G (2010). *Lärobok i Militärteknik, vol. 5: Farkostteknik [In Swedish]*. Stockholm: Swedish National Defence College.

Liwång H (2012). *Probabilistic risk assessment as a tool to support survivability decisions for naval ships: A case study on maritime piracy*. Paper presented at The 6th European Survivability Workshop 2012: in Halmstad, June 12-14 2012. Swedish Defence Research Agency.

Liwång H, Ringsberg J W (2013). *Ship security analysis: the effect of ship speed and effective lookout.* In: The proceedings to ASME 32nd International Conference on Ocean, Offshore and Arctic Engineering, Volume 2A: Structures, Safety and Reliability. American Society of Mechanical Engineers.

Axberg S, Andersson K, Bang M, Bruzelius N, Bull P, Eliasson P, Ericson M, Hagenbo M, Hult G, Jensen E, Liwång H, Löfgren L, Norsell M, Sivertun Å, Svantesson C-G, Vretblad B (2013). *Lärobok i Militärteknik, vol. 9: Teori och metod [In Swedish]*. Stockholm: Swedish National Defence College.

Liwång H, Bang M, Ericson M (2014). *An examination of the implementation of risk based approaches in military operations.* Journal of Military Studies (5:2). 1-27.

Liwång H, Sörenson K, Österman C (2015). *Ship security challenges in high-risk areas: Manageable or insurmountable?* WMU Journal of Maritime Affairs.

Liwång H, Jonsson H (2015). *Comparison between different survivability measures on a generic frigate*. International Journal of Maritime Engineering (IN PRINT).

**Sitting duck**
Sedens Anatis s.l.

Belongs to the *family of things* and is characterized by its helplessness and low level of protection. Can be found at sea, on land and in the air.

Evolution/history: the Sitting duck (Sedens Anatis) was first found in, and is still common in, the Anatidae (duck) family of birds. Therefore, the traditional Sitting duck is characterized by it being an easy target floating on the water, not suspecting that it is the object of a hunter or predator. During the last centuries there have been many reports of Sitting ducks in other forms, including artefacts, humans and other types of animals. Sitting duck at large is therefore today considered as *a family of things* and formally named Sedens Anatis Sensu Lato (s.l.).

-

*No one want to be onboard a sitting duck, and no one want to create one with poor design or poor operational decisions. To help in avoiding such decisions this thesis is about decision support methods for ship security.*

# Central concepts, organizations and abbreviations

Below concepts, organizations and abbreviations are describes as they are defined and used in this thesis.

***ALARP-region:*** As Low as Reasonable Practicable region. Here discussed in relation to IMO codes. In the ALARP-region the risk, according to IMO, should be weighed against cost for implementation of control options.

***Aleatory uncertainty:*** a stochastic uncertainty that describes randomness and that can be captured with frequencies.

***Antagonistic threat:*** A threat with the specific intent to harm or disturb in order to achieve own goals.

***Asymmetric conflict:*** A conflict where the two sides has different approaches, methods and/ or resources to achieve their goal.

***Bayesian network:*** An influence diagram without decision and utility nodes.

***Bayesian probability:*** A quantity that is assign for the purpose of representing a state of knowledge, or a state of belief.

***BMP4:*** The 2011 version of Best Management Practices for protection against Somalia based piracy, an influential industry guideline.

***Bureaucratic safety culture:*** An evolution level of the safety culture defined by a quantitative perspective and that 'the system' solves the safety problems.

***Case:*** Here used as a description of incident, past or future.

***Causality:*** A cause and effect description of events. Here used within cases or scenarios, but not to define how the future will enfold.

***Concept of operation:*** A description of how the ship is intended to be used to solve tasks.

***Consequence:*** A negative outcome of an incident. Can be measured with easily quantifiable aspects such as cost (in dollars) or number of deaths, but also by more qualitative operational aspects such as reaching a critical state (e.g. ship taken over by pirates).

***Control option:*** A measure that reduces or controls risk.

***COPD:*** Comprehensive Operations Planning Directive, NATO's framework for collaborative operations planning.

***Cope:*** Coping is a part of the stress process (within a resilient approach) and usually involves both task and emotion focused coping strategies.

***Deterministic:*** Describing that a process, or chain of events, is fully described by its prior state.

***Decision maker:*** The person that in the risk evaluation (based on the risk analysis) makes the necessary risk decisions. Decision makers come in many forms and roles.

***Design decision:*** Here used to describe all decisions taken about the design of the ship.

***Epistemic uncertainty:*** Knowledge-based uncertainty that represents a lack of knowledge regarding how a phenomenon affects the output of a process.

***F-N diagram:*** Frequency – Number of fatalities diagram. A cumulative diagram often used within IMO to present risk estimates.

***Force protection:*** Preventive measures taken to mitigate hostile actions against military personnel, resources, facilities and critical information.

***FSA:*** Formal Safety Assessment, IMO's risk-based approach to rule-making.

***Generative safety culture:*** The highest evolution level of the safety culture defined by that safety is integrated in all tasks and understood by individuals and the organization.

***Global commons:*** The areas beyond national jurisdiction that connects the international system.

***Hazard:*** An aspect (without intent) that potentially can threaten operational values such as human life, health, property or freedom of action.

***IACS:*** International Association of Class Societies, influential on how safety should be achieved with the use of class standards.

***IED:*** Improvised Explosive Device.

***IMO:*** International Maritime Organization, formally and informally defining the limits for maritime safety and how is achieved.

***Incident:*** A set of events that potentially can lead to negative consequences, past or future.

***Influence diagram:*** A graphical and mathematical representation of the network of influences derived from decision analysis.

***Inherently safe design:*** A safety principle which means that potential hazards or threats are excluded from the intended operation.

***ISPS:*** International Ship and Port Security code introduced 2002 by IMO as a part of SOLAS. The first international code on maritime security.

***Killability:*** The inability of a ship to survive an attack, the opposite of survivability.

***Littoral:*** The part of a sea or ocean that is close to the shore.

***Military operation:*** Coordinated military actions. Operations may be of a combat or non-combat nature and are performed both in peace and in war.

***MNE 7:*** A multinational concept development and experimentation project focusing on access to the global commons. Initiated by the U.S. Joint Forces Command with seventeen countries, from America, Europe and Asia, plus NATO.

***NATO:*** The North Atlantic Treaty Organization, here important as a developer of military standards and guidelines.

***Naval ship:*** A ship operated for military purpose by a naval organisation. Here used as synonym to *war ship* and *military ship*.

***NSC:*** The Naval Ship Code, a naval safety code developed by NATO and harmonized to SOLAS.

***OPV:*** Offshore Patrol Vessel, a type of military ship with offshore capability designed for flexibility and engaged in roles such as border protection and rescue operations.

***Prescriptive:*** Typically used to describe codes and rules that prescribe aspects of design or construction with engineering specifications.

***Probabilistic:*** A description based on events likeliness (probability).

***Procedural safeguards:*** A safety principle which is introduced via procedures and training.

***Recoverability:*** The ability of the system and its personnel to sustain operational capability after hit.

***Resilience:*** An organization's capacity to anticipate disruptions and adapt to events.

***Risk:*** The potential loss of something of value, defined by its probability and consequence.

***Risk analysis:*** An analysis of risk including scenario definition, hazard identification and risk estimation.

***Risk assessment:*** A risk evaluation includeing a risk analysis, risk tolerability decisions and analysis of options.

***Risk-based (ship) design:*** A concept for risk-based approaches that can be used throughout a ship design. Discussed and described within SAFEDOR, a project under the 6$^{th}$ framework programme of the European Commission

***Risk management:*** A management process including risk assessment, reduction and control, implementation and monitoring.

***Robustness:*** The ability to withstand surprises, changes and disturbances.

***RPG:*** Originally a Russian abbreviation for Ruchnaya Protivotankovaya Granata, meaning hand-held anti-tank grenade. RPG is a common weapon used in many situations.

***Safe fail:*** A safety principle which is implemented such that if systems fails, it does so safely.

***Safety:*** The quality achieved when the direct and indirect participants of an activity as well the goals of the activity are sufficient protected against hazards and threats.

***Safety culture:*** A culture that understands and effectively deals with hazards (safety challenges) and threats (security challenges). The culture can be described by its levels of maturity or evolution: (i) pathological, (ii) reactive, (iii) bureaucratic, (iv) proactive, and (v) generative.

***Safety reserves:*** A safety principle introduced with safety factors or safety margins.

***Scenario:*** A description of a future.

***Security:*** A sub-set of safety, which deals with protection against threats (with an intent).

***Ship design:*** The term ship design here includes the process of defining all the physical aspects such as structural aspects of the hull, human factors, the specifications of installed equipment and the infrared aspects of the paint.

***Skiff:*** Here used to describe a small boat used by pirates to attack ships.

***Socio-technical systems:*** The family of systems studied here which include technology, but also interaction between people and technology.

***SOLAS:*** The Safety of Life at Sea regulation developed by IMO. “War ships” are excluded.

***Survivability:*** In this thesis only discussed in relation to naval ships and is then the ability to survive an attack, described by susceptibility, vulnerability and recoverability.

***Susceptibility:*** The inability (including tactical measures) to avoid hit, governs the probability of a hit.

***Threat:*** A person or organisation (with intent) that potentially can threaten operational values such as human life, health, property or freedom of action.

***Tactical Task:*** A tasks performed by a military unit (such as a ship) that enables a mission or function to be accomplished.

***Traditional maritime safety:*** Here used to describe safety work only in relation to hazards, i.e. relative complement of security in safety (safety \ security).

***Vulnerability:*** The inability to resist damage, governs the probability of kill (or damage) given a hit.

*"On November 25, 2005, an attack in Afghanistan occurred which led to the death of two Swedish soldiers. This tragic event led to a review of the Afghanistan initiative from many perspectives. Among other things came to light that there were different assessments of threats, vulnerabilities and risks at various levels in the Armed Forces. The concept flora and responsibilities was unclear and there was a lack of consensus in several fields. Despite that, the knowledge of the threats in theatre and vulnerabilities in many respects was good; there were difficulties in translating this knowledge into concrete measures. There was a lack of a holistic approach to risk. There was no conscious risk-taking."*

The Swedish Supreme Commander in the introduction to The Swedish Armed Forces shared risk management model (Swedish Armed Forces 2009a).

# 1 Introduction

Both state and non-state actors pose a potential threat to the global commons through criminal intent, opposition to existing norms and other anti-access approaches (Secretary of Defense 2012). The protection of shipping does not come without hazards and threats to military forces, individual ship operators and crews (Council of the European Union 2014). With particular focus on security threats, this thesis is about how to prepare for such operations without introducing unnecessary risks, i.e., supporting conscious risk-taking related to ship security.

To enable economic stability and commerce, it is necessary to protect the free flow of goods shipped by sea(Council of the European Union 2014). The sea largely includes the areas beyond national waters, i.e., the global commons (Secretary of Defense 2012; MNE 7 2012). The shipping system is composed of many autonomous actors ranging from small local ship owners to large international ship operators that do not own their own ships. Additionally, from Sweden's national perspective compared to that of other European countries, the geographic situation makes the country especially dependent on sea transport (Swedish Maritime Administration 2013). Therefore, in general maritime security has both military and civilian implications and all ships must consider their specific security situations.

In this work, safety is defined as a quality that is achieved when an activity's direct and indirect participants, together with its goals, are sufficiently protected against hazards and threats. Security is a subset of safety and addresses protection against antagonistic threats.

In the field of transport, according to this definition, safety is achieved when categories such as the following are sufficiently protected against accidents and attacks:

- the personnel performing the transport, such as the seafarer,
- other persons along the transport route, such as the workers at the warehouse, other seafarers and communities along the route, and

– the transport itself, i.e., both the cargo and the timeliness of the delivery.

How to define *sufficiently protected* is decided by society and is usually based on both statistics and perception. Security is achieved when all three of the abovementioned categories are protected against attacks. However, it is not necessary that the same definitions for *sufficiently protected* can be used.

Therefore safety in general here refers to the total situation including all dangers (hazards and threats). This because many ship safety measures are applicable to both traditional maritime safety and maritime security. For example the damage stability depends on the extent of the damage, not who or why it happened and a life raft is useful no matter why you have to abandon the ship. To describe safety work only in relation to hazards this thesis uses the term *traditional maritime safety*. It is also important to note that even though security analysis examines incidents triggered by a threat a security analysis cannot ignore the hazards. This because the particular combination of threats and hazards is what make the situation challenging (for example security incidents in shallow waters or in bad weather).

Security and maritime security are addressed by both military and civilian organisations and often, a security decision made by one will affect the other (Council of the European Union 2014). Therefore, this thesis cannot limit itself to either military or civilian ship security and the purpose of this project has been to combine civilian and military knowledge and research. This purpose is also supported by the European Union maritime strategy that calls for a cross-sectoral approach (and including both civilian and military actors) as the first guiding principle of the strategy (Council of the European Union 2014). Experience and research from both areas are discussed and used; however, in this thesis the focus is on military ship security.

## 1.1 Background

In military operations, casualties—whether deliberate or accidental—are a reality and the desire to avoid them may drastically affect the possibilities of achieving military goals. However, in the asymmetric conflicts of today there is a drive for high efficiency and low losses. This leads to a focus on survivability in military organisations. With respect to survivability, a balance of risk is required and a comprehensive risk assessment process is essential to guide risk management decision-making and prioritisation (NATO 2007, 2010a). However, this is not easily achieved, as exemplified in the Swedish Supreme Commander's statement set forth above.

Risk is an important aspect of understanding the operational situation (NATO 2010a). However, in guidelines such as The Naval Ship Code (NSC) (NATO 2010b) and Survivability of Small Warships and Auxiliary Naval Vessels (NATO 2012), ship safety and ship survivability goals are discussed without introducing methods and tools for supporting design decisions. Therefore, the design process needs an integrated approach to security decisions for assessing the survivability and safety for naval ships. The approach should be probabilistic to connect to military survivability theory and to the risk-based framework of military planning and force protection.

For civilian ships, today's threats are managed through maritime security efforts regulated in the International Ship and Port Facility Security (ISPS) code (IMO 2002). The ISPS code was developed in the aftermath of the September 11, 2001, terrorist

attacks in the United States. The development began two months after the attacks and the final code was presented 13 months later (Wengelin 2012). The speed of this process implies that its development was characterised by the preferability of having something imperfect to having nothing at all (Mitropoulos 2004). However, according to ship operators and security experts, the guideline is inadequate to guarantee secure shipping. Moreover, when ship operators' ship security analysis is challenged, they have been shown to have problems defending its quality.

The ship operator "*is responsible for identifying the risks associated with its particular ships, operations and trade*". It is inadequately merely to comply with codes and regulations; these can only be seen as a starting point (IACS 2012). Therefore, both military and civilian ship operators must work to structure ship security, an area that needs further development (Liwång et al. 2015; Yang et al. 2013; Bichou 2008).

## 1.2 Motivation and objective

Control, efficiency and cost demands on maritime operations are high. In addition, 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 military maritime operations (Department of Defense 2007; Council of the European Union 2014).

The risk control options to achieve both security and survivability for naval ships are aspects that often are connected to central aspects of the ship design, such as damage stability and system redundancy. When the basic design is set, the possibility of changing the ship's security measures is limited. There is, therefore, a need to assess the level of security to which different concepts lead at early stages of the ship design to provide input into the decision process with respect to risk control options. Such an assessment is especially challenging when new threats are envisioned and older ships' survivability design is not a relevant benchmark.

Risk is not constant and is subject to considerable degrees of uncertainty. The rarer the event, if predictable at all, the less reliable the historical data and the estimates based on them (IACS 2012). To enable the results of an analysis to reflect both uncertainty and the possibility of surprise, there is a need for a risk-informed approach that goes beyond calculated probabilities and expected values (Aven 2009). Uncertainties and possible surprises must be considered a relevant part of the risk picture, which provides for rational input into the decision-making process (Aven 2009) and increases a study's credibility (Kunreuther 2002).

Regulations, guidelines and methods in the field of maritime safety have a history and culture of systematic research, development and implementation (Kuo 2007). In contrast, international security is highly politicised and therefore not as transparent (Wengelin 2012). The result is that the tradition of ship security is not well established (McNaught 2005). One example is the ISPS code, which "as it stands, may not be the final solution to this problem" (Mitropoulos 2004).

Unfortunately, comprehensive studies on ship security risk are rare (Yang 2011; Bichou 2008; Paper III), and systematic handling of uncertainties, which is necessary to create rational input into the decision-making process, is even rarer. Applying risk-based approaches to security areas requires special considerations, and the limited

research to date has led to a knowledge gap (Yang 2011). Therefore, there is a need for both further research and the applied development of methods and tools. This development must be able to manage the new, more complex demands for both civilian and naval ship security (Department of Defense 2007; McNaught 2005).

Examples of ship security challenges include reports of fast (~25 knots) and well-operated ships choosing to stop because of shots from pirates (IMB 2011), even though both best practises and a rudimentary risk analysis show that maintaining or increasing speed is *always* the safest alternative, especially at high speeds. Another example is the improvised explosive device (IED) attack on a Swedish military vehicle in Afghanistan on November 25, 2005. Before the incident, different levels of the organisation made different assessments of its threats, vulnerabilities and risks. This was in part a result of difficulties in communicating different security focuses—i.e., personal security versus operational security. A third example of challenges in security analysis is the US President's receipt of a range of probability estimates—from 30 to 95 percent—of the probability that Osama bin Laden was hiding in Abbottabad, Pakistan (Friedman and Zeckhauser 2014). This range of probability cannot be ignored, but the President was openly frustrated by its existence (Friedman and Zeckhauser 2014). These three examples show that security decisions—and especially, transforming knowledge about the threat to suitable decisions and communicating those decisions—are a challenge, even in otherwise well-functioning organisations.

To reduce the above-identified challenges, the goal of this thesis is to improve support for the security decision by defining an approach to ship security analysis to enhance the risk management. To increase overall safety, the approach must facilitate compromises between traditional maritime safety and maritime security. The objective is thus to develop an approach that is systematic and ensures that the ship operator's decision support gives the decision maker an appropriate picture of the risks. This approach may not only be used for an unpredictable future but also describe and model the relationships from threat to risk.

The overarching research question for this thesis is therefore as follows:

> What characterises a decision-support approach that increases ship security by translating knowledge into a suitable description of the risks and promotes a conscious risk-taking?

To examine the requirements from a security decision-support approach for ship operators' knowledge development, the work in Papers I to V combines civilian and military knowledge and research and studies ship operations with threats additional to the typical safety hazards. Such threats include but are not limited to a military threat to naval vessels (Papers I, II, IV and V) and the security threat posed by pirates to commercial vessels (Paper III). Before and during such operations, the ship designer, commander and crew must consider the security threat when reaching compromises in design or operation.

*"Think of your entire operation and the range of all potential problems as a mountain range.*

*Looking at the entire scope of your operation, you may only be able to focus on the highest of peaks within your available time frame.*

*However, if you choose a specific aspect of your operation (e.g., cargo loading) you can examine it in greater depth and detail. This approach is more effective for targeting specific problems."*

Marine Operations Risk Guide (U.S. Coast Guard n.d.).

# 2 Methodology

This thesis is composed of five different studies, all of which combined civilian and military research; required different methods; and examined the research question from different scientific perspectives. The order of the studies was chosen to gradually increase the complexity of the research object, from the conditions for implementing security and military survivability as defined by safety guidelines (Paper I) to the conditions for a fully risk-based approach to ship military survivability (Paper V). To support this progression, as illustrated in Figure 1, the result of each paper is used as a knowledge and method base for the next.

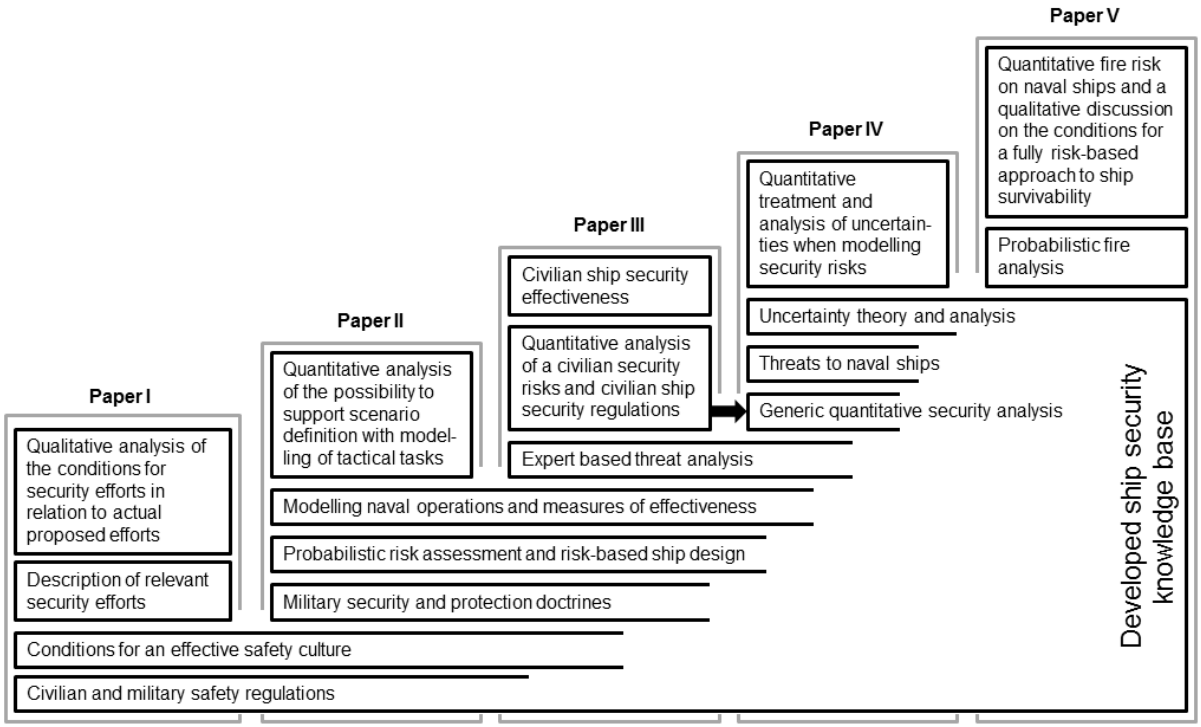


**Figure 1.** Work performed and the development of a knowledge base for ship security research.

This thesis is about the conditions for a top-level assessment approach; such an approach requires the input of methods, tools, data and models on lower levels. To include the depth and detail needed, the work is divided into studies that each have a different focus on specific aspects of the examined top-level approach. Therefore, the five appended papers cover different aspects, all chosen so that together, they examine the top-level assessment. In Papers I through V, the methodical choices, approaches and considerations for each study are discussed in more detail.

Common to all six application areas studied—supplementary ballistic protection in Paper I; bridge design for small arms protection in Paper I; a naval operation under a mine threat in Paper II; piracy attacks on merchant shipping in Paper III; an asymmetric threat to a generic Ocean Patrol Vessel in Paper IV; and fire survivability analysis in Paper V—is that each represents a maritime security area:

- where the threat is defined as important for both contemporary and future maritime operations (Department of Defense 2007; King 2013; IMB 1993-2014; McGeorge and Høyning 2002),
- where today's analyses are, whether by practise or by guidelines, described as risk-based (IACS 2012; NATO 2010a; Swedish Armed Forces 2009a), and
- for which there exists only limited research on the conditions for risk-based approaches (for further detail, see Table 1 and Paper III, along with Bichou (2008)).

The focus in Papers I and II is to examine the problem. The application areas are deliberately limited and simplified:

**Paper I, Minimising risk from armed attacks: the effects of the NATO Naval Ship Code,** examines a NATO framework for traditional maritime safety efforts on naval ships and analyses what is needed to create relevant conditions for survivability analysis in the design phase. The framework is analysed in relation to how it affects supplementary ballistic protection and bridge design for small arms protection.

**Paper II, Probabilistic risk assessment for integrating survivability and safety measures on naval ships,** discusses, based on the result of Paper I, the possibility of using a probabilistic approach and risk as the measure for introducing a quantitative rationale to use when comparing ship design choices (such as sensor characteristics and watch scheme). The suggested approach is discussed in relation to a simplified example of a naval operation under a mine threat.

Papers III through V each not only cover a specific field but also examine relevant methods and methodical aspects based on the findings in Papers I and II. In Papers III to V, the chosen application areas require a more complex background description:

**Paper III, Quantitative risk analysis—ship security analysis for effective risk control options,** deepens the examination of risk as measure with the particular focus on collection of expert data and on quantitative modelling. The analysis is performed on a civilian scenario: piracy attacks on merchant shipping (one of the models developed is examined more closely in Liwång and Ringsberg (2013)). The civilian scenario was chosen so that specific threat and scenario data

collection and analysis could be performed without disclosing confidential information. It was also important to study a scenario for which there exist official incident statistics and experts with first-hand knowledge in the area.

**Paper IV, Analysis of control options for the survivability of Ocean Patrol Vessels,** deepens the examination of risk as a measure with a particular focus on the analysis and treatment of uncertainties. Uncertainties in input and output are studied and discussed with respect to an asymmetric threat to a generic Ocean Patrol Vessel (OPV). The application area is chosen to represent an area in which there is an acute need for decisions and the uncertainties are substantial, i.e., in which decisions are generally made despite uncertainties. The focus is on typical values and typical uncertainties, not the specific probabilities for a specific ship.

**Paper V, Conditions for risk based ship survivability approach: a study on the analysis of fire risk,** examines the conditions for risk-based survivability design from design concept to operational risk. The study is limited to fire survivability analysis and discusses risk with the help of a quantified littoral scenario. Fire on naval ships is discussed in relation to several threat types. The application area is chosen because fire is one of the consequences of almost all types of attacks and because it is a well-researched area for civilian ships in general and in relation to risk-based ship design. There are also some statistics on fire on naval ships, along with scientific documentation with respect to incidents and fire protection. Paper V examines the risk-analysis process and discusses its approach with respect to risk level, not the specific risk for a specific ship.

Risk-based approaches are therefore examined from several different perspectives. Papers I and V examine specific ship protection areas and Papers II, III and IV examine specific tactical situations/scenarios.

## 2.1 General approach and assumptions

This work is primarily about creating decision support. A quantitative approach to security requires a suitable measure. The concept of risk is the candidate that is well established in both military operations and maritime safety analysis (see Paper II and Liwång et al. (2014) for further discussion of how the concept of risk is used in military operations). Therefore, in this work risk is the central measure of security—a tool to use—not the research object. The research objects are methods for decision support that aim to support a high level of security in military operations.

Security cannot be grasped within a single academic discipline. Therefore, the work in this thesis is interdisciplinary. The research must cross traditional boundaries between academic disciplines and schools of thought. This is, as stated in Section 1, also a specific purpose of this project. Compared to traditional engineering research there is, as a result of the interdisciplinary nature of the research, a greater need to define the scientific assumptions on which the research is based, especially with respect to the type of systems studied, the concept of risk and uncertainties in the analysis.

### 2.1.1 Characteristics of the examined system and the role of safety culture

The physical and non-physical attributes studied in this work are seen as a system with several interdependencies. Figure 2 presents a basic scheme for different types of systems: a general level and a sub-level of system families. This thesis focuses on systems within the socio-technological system family, i.e., systems that include not only technology but also people and aspects such as organisations, policies and social structures.

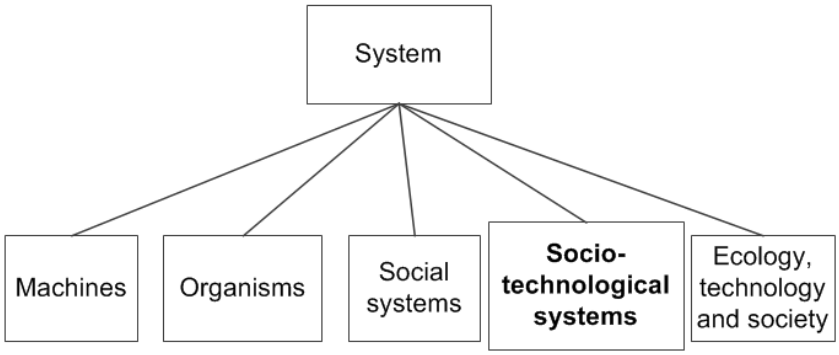


**Figure 2.** System levels and system families, redrawn from Ingelstam (2012). The focus system family for this thesis is highlighted in bold text.

The systems are studied in a probabilistic setting, which means that the studied incidents are not specific events but instead, are types of events in a possible future. Probabilistic causality is used within studied scenarios, systems and cases (to model how actions relate to each other), but causality is not used to define the future.

This thesis applies the system perspective, which shares its perspective with system science and approaches such as systems engineering, operational analysis and human-machine interaction. Thus, the focus is on the system's behaviour, not on the system itself.

Both the socio-technological systems studied and the focus on system behaviour lead to the conclusion that culture is an important aspect of a system. Therefore, in this work, an effective analysis (and usefulness) is defined by an approach that supports the development of a safety culture as defined by Section 3. It is also this usefulness of the approach that defines the validity of the approach (Pedersen et al. 2000). There is also a strong connection between the type of system studied, the acknowledgement of the importance of culture and the fact that security is often implemented based on *safe fail* and *procedural safeguards* as discussed in Section 5.1.1.

### 2.1.2 Risk and risk analysis

This work is further based on the notion that development in the area of ship security would benefit if it was consistent with the approaches utilised in maritime safety. Such consistency would then allow safety risks to be compared with security risks to find the best compromise. For further details, see Papers I and II. In this work, these assumptions lead to the use of *risk* as the central measure of ship security.

Here, risk management is defined as the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk. Risk management is often defined by the following activities (Bakx and

Richardson 2013; DCDC 2010; Kuo 2007; NATO 2010a; Department of the Army 2006):

A. A risk analysis including scope or scenario definition, hazard and threat identification and risk estimation.
B. A risk evaluation including risk tolerability decisions and analysis of options.
C. Risk reduction and control including decision-making, implementation and monitoring.

Risk assessment is defined as consisting of steps A and B from the list above. See Figure 3 for an illustration of typical military risk management and its components and sub-components. Here, risk or risk level is defined as a function of the probability and the consequence of an unexpected/unwanted event.

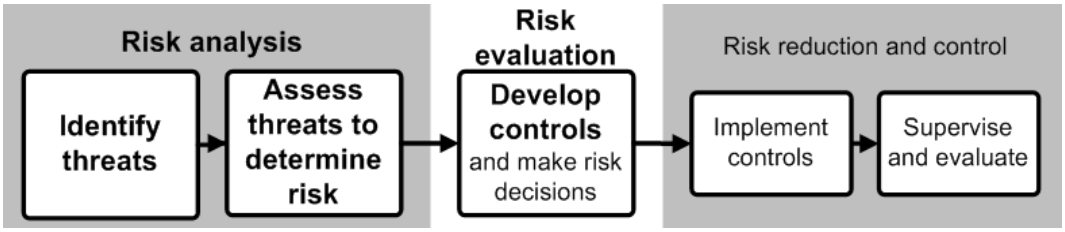


**Figure 3.** The security risk management process and its components. This thesis's areas of focus, as described in Section 2.2, are highlighted in bold text. Developed from Department of the Army (2006) and Marine Corps Institute (2002).

The traditional engineering approach to the measure *risk* and the process *risk analysis*, as described in Section 4, is based on objectivistic expected utility, which combines frequentistic (objective) probabilities with objectivistic utilities. This means that probability is interpreted as an objective representation of frequency and that there is a linear relationship between the consequences studied and their perceived negative effects, i.e., the utility assignments (Hansson, 1993). According to Hansson's research on the philosophy of risk, this can only be the case if the following five criteria are satisfied:

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

Real systems and options are never finite. Papers I through V stress that the system and scenarios must be defined and documented and that their definitions 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 and the operations scenarios definition in Paper V.

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

Difficulties in defining consequences must be documented, especially with respect to the perception of security, and these difficulties must be thoroughly weighed in risk tolerability decisions, analyses of options and risk reduction. For further discussion of risk perception see Paper III, Kunreuther (2002), and Liwång et al. (2014). Moreover, Paper V and Liwång et al. (2015) discuss the assessment of different types of consequences.

**3. The analysis must enable an objective description of the consequences of the hazard**

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

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

It is necessary to document and highlight in the process how the probabilities have been obtained, the reported actual frequencies or the expert assessment, together with uncertainties. Those uncertainties must then be considered in the decision process; see, e.g., the discussion of safety factors in Paper II, the discussion of robust solutions in Paper III and the analysis of uncertainties in Paper IV.

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

For comparison between 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 or threats with low probability or with very different probabilities. Therefore the criteria has limited validity to security analysis; see for example the discussion on measures of effectiveness in Papers I and II (weighing risk against gain), the discussion on robust solutions in Paper III and the discussion of possible conflicts among different consequences in Paper V.

**Summarising the discussion on the five criteria** above, it can be found that the risk perspective in this thesis is based on the following assumptions:

- objectivistic expected utility can serve as a base for describing security risks for ships, and
- the result of the analysis can give a reasonable representation of the risk.

The first assumption set forth above means that probabilities and consequences obtained by the analysis are assumed to objectively describe the negative outcomes of the threat.

According to the second assumption above, therefore, the result can only be seen as a simplified description of the risk. However, based on the discussion above, the result of a risk analysis is assumed to give a reasonable representation of the risk. This is particularly true if the analysis maintains a focus on communicating and continuously updating throughout the organisation the principles for system definition, methodological understanding, relevant system understanding and well-defined risk acceptance criteria. Risk reduction and control must focus on all levels of the organisation in risk reduction implementation, they must focus on a continuous and broad awareness when monitoring the different activities, and they must focus on adapting countermeasures accordingly during voyages (Liwång et al. 2014; Liwång et al. 2015).

### 2.1.3 The decision maker

As described in Figure 3, risk analysis supports the risk evaluation in which the decision maker makes the necessary risk decisions. Such decision makers come in many forms and play many roles.

The decision makers involved in the selection of ballistic protection and bridge design (Paper I) and fire survivability design (Paper V) are typically found within naval ship design projects—for example, in naval administrations—and play roles in ship design. However, risk in an operation under either a mine threat (Paper II) or an asymmetric threat (Paper IV) affects not only design decisions within naval administrations but also operational decision makers onboard. Civilian ship security decisions, such as how to decrease piracy risks (Paper III), are made within a ship operator's onshore organisation with respect to, for example, cargo, routes and general protective measures, and onboard with respect to implementing specific protective measures and executing protective actions. This thesis addresses the types of analysis needed for the above-mentioned types of decision but does not explicitly study the decision makers and their decisions.

### 2.1.4 Uncertainties in security analysis

In the early stages (project initiation, planning, analysis and alternative generation) of a ship development project, the need to understand the intended system and its limitations is crucial (Giachetti 2010). However, there are substantial uncertainties, and understanding those uncertainties is a part of understanding the system. Therefore, to manage risk as more than merely expected values, this thesis discusses both aleatory and epistemic uncertainties where:

- *aleatory uncertainty* is defined as a stochastic uncertainty that describes randomness and that can, given a perfect controllable and probabilistic world, be captured with frequencies; typical variables that often are probabilistically modeled include the wave height on an ocean or the fail frequency for a pump, and
- *epistemic uncertainty* is defined as a knowledge-based uncertainty that represents a lack of knowledge regarding how a phenomenon affects the output of a process, such as how an antagonistic threat will act in a specific situation. In this work, epistemic uncertainty is conceptualised as the difference in estimates and beliefs among different experts.

Aleatory uncertainty can be treated with frequentistic classical risk-analysis methods and is automatically included in a probabilistic risk-based approach. However, epistemic uncertainty can be approached only through Bayesian probability and expert opinions (Paté-Cornell 1996). In this thesis, epistemic uncertainty is defined as expert disagreement (see Paper III for examples of how epistemic parameter uncertainty can be quantified as the result of expert disagreement).

Epistemic uncertainty is particularly substantial for security analysis: "*an event occurring on the other side of the earth could quickly change the risk assessment*" (Aven and Krohn 2014). One example of such uncertainty is the disagreement among security experts' about Osama bin Laden's hiding place described in Section 1.2. However, despite the relatively substantial uncertainty, the US President had to take a decision

about the next step of the operation. This example provides a good description of this thesis's assumptions:

- There are substantial epistemic uncertainties in a security analysis, but
- despite those uncertainties, decisions must be made.

To work structurally with uncertainties and to provide decision support the class of the uncertainty must defined. Here, uncertainty is grouped into three classes (Abrahamsson 2002):

- parameter uncertainty as a result of the value parameters being unknown or varying,
- model uncertainty that arises from the fact that any model is a simplification of reality, and
- completeness uncertainty because not all contributions to risk are addressed.

## 2.2 Delimitations

The work in this thesis is limited to decision support; it does not have the objective of investigating the decision process. With respect to the risk management process described in Figure 2, the work therefore is limited to risk analysis and the development of risk controls. The limitation to decision support also, in relation to the concept of risk-based design described in Figure 3, leads to a research focus on how to develop risk-knowledge models.

The studies performed for this thesis are limited to a general perspective on military ship survivability and specific studies of a mine threat (Paper II), an asymmetric (low capability, high intent) antagonistic organisation (Paper IV) and fire survivability for naval ships (Paper V) and a piracy threat to civilian ships (Paper III). In this work, these threats are seen as a suitable combination of relevant threat types and analysis perspectives, but does not cover them completely.

Government bodies claim that a considerable amount of not only data but also methods and tools within the area of military ship security comprise sensitive information that requires protection. Therefore, to avoid using classified information, aspects of the studies performed for Papers II, IV and V, are limited to generic descriptions of ships, solutions and threats.

None of the studies covers conditions that represent a symmetric blue water naval combat. The reasons are that the context is thoroughly altered and that fortunately, during modern history such conditions have been uncommon even in symmetric conflicts. However, the conditions during such combat are an important special case in which traditional views are challenged, especially for concepts such as risk, culture and risk perception. Therefore, it is likely that some of the aspects and results of this study are invalid for such conditions.

## 2.3 Utilised methods and tools

The studies in this thesis use several existing methods and tools, as described below. These methods and tools are primarily chosen because they have been proven to be useful in maritime safety in general and because they meet the needs of a risk

management support approach. However, few of the methods and tools used are specifically tested for security cases. In this work, therefore, testing and discussing the suitability of these methods and tools is a goal of its own. Below is a brief introduction to the most central methods and tools used.

**Probabilistic risk assessment**

As described in Section 4, development in the area of ship safety is risk-based. Probabilistic risk assessment is seen as an approach that aims to quantify security with the measure of risk as a function of probabilities and consequences. The result is then compared with limits set by both society and the operator to decide the extent to which the process can be defined as safe or how the risk can be limited (Andrews and Moss 2002).

Therefore, the work in the appended papers utilises, where possible, the experience and requirements defined in the risk-based ship design (Vassalos 2009) and the Formal Safety Assessment (FSA) (IMO 2013).

Risk management is also promoted in military planning in general (NATO 2010a; Swedish Armed Forces 2009a) and in different application areas (DCDC 2010; Department of the Army 2006; Swedish Armed Forces 2009b). However, in most of the military approaches, the probabilistic perspective is undeveloped.

**System or scenario definition**

A risk analysis must be performed on well-defined scenarios and systems (Hansson 1993; IMO 2013; Vassalos 2009). Scenario definition and selection is central to the risk analysis process (Liwång et al. 2014) and should reflect the ship's operational concept. Generally, a scenario should be developed that considers not only predictable but also challenging and visionary possibilities (Amer et al. 2013; Kirkwood and Pollock 1982).

The work in Papers II, III and IV uses influence diagrams (Shachter 1988) to define the scenario and system and in Papers III and V, event trees are used. Influence diagrams are described by IMO in the Guidelines for formal safety assessment (IMO 2013) but are more thoroughly documented in the area of decision analysis (Shachter 1988). Papers II and III use influence diagrams to model influences and define the studied system. In Paper IV, the influence diagrams are also used to calculate probabilities for different consequences under uncertainty.

An influence diagram (and Bayesian network) is a graphical, mathematical representation of the network of influences on an event. Influence diagram methodology is derived from decision analysis and is—according to IMO—particularly useful in situations for which there may be little or no empirical data available, and the approach is capable of identifying all of the influences and therefore underlying causal information (IMO 2013).

In the area of maritime safety, Bayesian networks have been tested in different areas such as tools for cost-optimal inspection planning, a reliability model of buckling pipelines (Friis-Hansen 2000) and bridge work in a collision scenario (Pedersen 2010).

See Papers III and IV for more details on influence diagrams and strengths and weaknesses.

Other often-suitable methods for system definitions are inductive and deductive trees, which also have a graphical and a mathematical dimension. Deductive fault trees are used in Papers III and V.

**Expert assessment**

Risk analysis is often supported by data from expert assessments due to a lack of empirical data on the studied systems (Yang et al. 2013; Bichou 2008; IMO 2013), which is the case in this thesis. However, expert assessment of probabilities often lack calibration and can therefore have systematic errors (Hansson 1993); moreover, for security, they often include substantial uncertainty (Aven and Krohn 2014). Therefore, the aim herein is to have experts assess threat capabilities rather than probabilities as often as possible. 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 (and Liwång and Ringsberg (2013)) tests the concept on piracy using the threat analysis presented in the Allied joint doctrine for force protection (NATO 2007).

In this work, expert assessment is collected using a combination of questionnaires and interviews to capture both qualitative and quantitative aspects of a threat and its interaction with a ship's vulnerability. For further details, see Paper III. How the introduced uncertainty in the analysis can be treated and displayed is discussed in Paper IV.

**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, not only the variables that affect the problem but also the constraints and limitations must be defined. The simulation must contain a particular focus on the measures of effectiveness because they will provide guidance as to how the simulated system will be used and how different alternatives are prioritised (Jaiswal 1997).

The simulations must be validated and if the results of the system operation are available, statistical analysis plays an important role in model validation. Military system studies and security studies, however, suffer from a lack of historical data, and realistic experiments can be impossible to perform (Jaiswal 1997). Accordingly, model validation is often limited to sub-model validation based on statistical data and model validation by expert opinion, sensitivity analysis and hypothesis validity. An example of a quantitative simulation of operations are displayed in Papers II and III and how such data can be used is discussed in Papers IV and V.

**Quantitative uncertainty treatment**

As earlier discussed, uncertainties in security analysis can be substantial and classic risk analysis approaches does not provide for working with and displaying how epistemic uncertainties affect the result. Paper IV applies the highest level of uncertainty treatment where the uncertainty is displayed in the output as a family of risk estimates. This level requires propagating the uncertainties throughout the analysis (Paté-Cornell 1996).

Knowing the class of uncertainty is important because the class defines not only the treatment but also how and whether the uncertainty can be reduced (Abrahamsson 2002). In the model in Paper IV, the aleatory parameter uncertainty is described as a probability for the discrete states of the parameters, and the epistemic parameter uncertainty is described as a distribution around the aleatory probabilities. This description is a simplification of the general case, in which the parameters can be continuous; the aleatory uncertainties are then described according to a probability density function and the epistemic parameter uncertainty is described as a family of probability density functions (Paté-Cornell 1996).

There are several methods available to analyse parameter uncertainty and uncertainty propagation (Abrahamsson 2002). In Paper IV, Monte Carlo analysis and numerical derivative analysis are used to examine the uncertainties because these two approaches are both well-documented and feasible to implement in a real ship security analysis; additionally, they are based on different principles and therefore answer to different needs. Monte Carlo and two-phase Monte Carlo analysis make it possible to distinguish between different uncertainties, but require a probability distributions of the uncertainties (Abrahamsson 2002). Numerical derivative analysis investigates the sensitivity for each input but if the problem is nonlinear, that approach only works for relative uncertainties.

Paper IV uses parallel models that represent different beliefs about how the studied phenomenon can lead to risk. In that paper, competing models are used to illustrate how model uncertainties can be described and analysed. In Paper V, completeness uncertainty is qualitatively discussed and exemplified with different future conflict levels and susceptibility levels in the scenario description.

*"Over a long period of years, numerous new designs of marine vehicles have been developed and have been in service. While these do not fully comply with the provisions of the international conventions relating to conventional ships built of steel, they have demonstrated an ability to operate at an equivalent level of safety when engaged on restricted voyages under restricted operational weather conditions and with approved maintenance and supervision schedules."*

International code of safety for high-speed craft (IMO 2000b).

# 3 The operational perspective

For naval ships total safety can never be achieved (Hughes 2000): safety efforts focus on reducing risk. How to assess risk is therefore crucial, especially because measures to reduce risk often are interconnected with each other. Therefore, how to systematically enhance security and military survivability is an important question for both defence executives involved in technology development and field commanders in tactical deployment. When appropriate security is achieved, freedom to act is increased by reducing vulnerability to the enemy's actions (NATO 2007; University of Cincinnati 2004).

Fighting power is the ability to fight and achieve success in military operations. It is composed of three inter-related components: the conceptual, the moral and the physical. Success is therefore a combination of the thought process that provides an intellectual basis and theoretical justification for the provision and employment of armed forces; the ability to get people to fight both individually and collectively; and the means to fight (DCDC 2011). Therefore, a successful operation not only depends on the culture of the forces but also requires the culture to reflect reasonable expectations of the technology upon which an operation depends.

Reason (2000) notes that effective safety work needs informed participants that can navigate close to unacceptable danger without crossing the line. Particularly in areas with few but severe incidents, it is difficult to develop safe work and safety measures from negative outcomes (historic incidents). Unfortunately, the traditional approach to safety in maritime design and operation is to implement prescriptive regulations, which generally are formulated as the result of an accident. Such regulations are suitable for routine activities but devolve responsibility and innovation and are unsuitable for new developments (Kuo 2007). The human ability to adjust to changing events is what preserves system safety in a dynamic world. Therefore, to constrain an operator's variability undermines one of the most important safeguards. A successful culture knows that hazards and threats will not go away, *"they anticipate the worst and equip themselves to cope with it"* (Reason 2000).

According to Parker et al. (2006), a desirable safety culture does not simply emerge; instead, it results from many aspects. As a part of their work, Parker et al. describe 18 organisational, key aspects (both concrete and abstract) of safety culture. These 18 aspects of safety culture are here summarised to define three basic areas of safety culture, two concrete and one abstract:

- Formal regulations and processes.
- Competence and training, including work quality and safety observations.
- Shared risk awareness throughout the organisation.

Therefore, generally the conceptual and moral component of the fighting power is dependent on a suitable safety culture (compare with how the organizational culture affect and interacts with the safety culture (Grech et al. 2008)). It is a suitable safety culture that gives the personnel a shared and suitable understanding of the hazards and threats, but also an understanding of how actions taken and technology choices affects the risk. Therefore, this shared understanding guide individual decision makers on how to achieve set goals.

From the three basic areas of safety culture it also follows that an effective safety design process must have a strong and obvious connection to the concept of operation. This is to ensure that not only regulations, competence and training but also risk awareness during design also are relevant during operation. The cornerstone of naval thinking and acting is doctrine and it is from doctrine that a concept of operation should be extracted. Therefore, how the (concept of) operation should be described and quantified is central to implementing survivability. This is especially challenging because neither military guidelines nor rules for classification provide a theoretical base for how survivability analysis results are to be weighed against other important aspects. This makes it difficult to provide the participants in the process, for example engineers and crew, with an understanding of how total safety (including both safety and survivability) is achieved and maintained in different situations.

From the discussion on safety culture above it follows that the unbalance between how traditional maritime safety and how security is achieved (as described by Paper I) complicates the forming of a suitable safety culture. This is because the risk contribution from different areas are not reflected in the formal regulations.

It has been shown that the greatest uncertainties (possible variation in risk) are the operator's choices, such ship susceptibility implementation and operation types. For example, the analysis of risk controls must be done with respect to susceptibility, vulnerability and recoverability and an understanding of the total effect over all of these aspects is necessary to evaluate survivability. Risk cannot be analysed without a general analysis of the susceptibility and vulnerability of the ship with respect to relevant threats; this means that the analysis depends on relevant operational scenarios. For further detail, see Paper V.

Another example of the importance of the operational perspective is firefighting on naval ships. Firefighting is the most important aspect for reducing the probability of catastrophic consequences from complicated ignitions. In such cases, built-in protection is insufficient to stop a fire from escalating. Reaction times and effectiveness with respect to firefighting on board naval vessels generally is difficult to

match in other firefighting situations. This is the result of extensive training, a high level of readiness, and a high number of crew in relation to ship size and the availability of firefighting equipment. Such aspects of the operation must be considered in the design and safety analysis if actual operational conditions should be captured.

Therefore, shared risk awareness is created by an understanding of the operational effect of specific aspects, such as susceptibility or firefighting, and general aspects, such as threats, of the intended ship operation.

As a result, the purpose of a security analysis is to describe the intended operation. The description must be formulated so that it supports a development and evolution of a generative safety culture, including an understanding of relevant hazards and threats. Therefore, the purpose of a risk analysis is greater than merely answering a question or putting a number on the risk.

The purpose to understand risk as described above is for security analysis underlined by the fact that there most often are not any external explicit security criteria (no external drive for a *bureaucratic* safety culture). The importance of the statement above is also underlined by that ship operators to a large extent display a *generative* approach towards the security work (Papers III and V), i.e. the security work is a part of the organizational and individual understanding (Grech et al. 2008). But also that the studies in Papers III to V show that a generative approach is needed because many of the important risk controls are procedural and depend on crew actions.

The focus on risk management support (rather than on risk quantification) has to a large extent defined the approach discussed (as well as the methods and tools utilized) in the thesis. This is further discussed in Section 4.4.

> *"Accept no unnecessary risk. Accept no level of risk unless the potential gain or benefit outweighs the potential loss. [Risk management] CRM is a decisionmaking tool to assist the commander, leader, or individual in identifying, assessing, and controlling risks in order to make informed decisions that balance risk costs (losses) against mission benefits (potential gains)."*
>
> The US Army's approach to risk management, Composite Risk Management, Field Manual No. 5-19 (100-14), (Department of the Army 2006).

# 4 Risk-based approaches

For a risk analysis to be meaningful, the decision maker must trust that analysis and the analysis must be valid. To achieve this there is knowledge and a set of rules that must be shared between the analyst and the decision maker and a deeper methodological knowledge must be utilised in the analysis process itself.

## 4.1 Risk management

Risk management is both a decision support process and a vital tool for military planning and decision-making (NATO 2010a). According to Johnson (2007) "*Risk management provides the most important single framework for strategic, tactical and operational decision-making across the US military*". Risk management and its components, such as risk assessment and risk analysis, have been employed since the 1950s for the control of hazards in areas such as industrial plants and space travel (Andrews and Moss 2002). Sometimes risk management in military or civilian organisations, is discussed under terms such as Operational Risk Management (ORM) or Composite Risk Management (CRM)—see, e.g., the Marine Corps Institute (2002); the Department of the Army (2006) and the U.S. Coast Guard (n.d.). However, there is no substantial difference between these methods and risk management in general.

As described in Section 2.1.2, risk management is defined as the systematic application of management policies, procedures and practices to controlling risk. Risk management is often defined by (A) a risk analysis; (B) a risk evaluation; and (C) risk reduction and control. See Figure 3 for an illustration of typical military risk management and its components and sub-components.

The results of a 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 potential operational gain is high (NATO 2007, 2010a; Marine Corps Institute 2002; Department of the Army 2006; IACS 2012).

In general, probabilistic risk assessments offer a sound and systematic basis for evaluating potentially hazardous activity. However, their methods are specialised and often complex, and auditing the assessment is vital to ensure both a logical and consistent approach and that relevant data have been adopted (Andrews and Moss 2002; Liwång et al. 2015; Liwång et al. 2014; IACS 2012).

Risk evaluation must be performed against a set of risk acceptance and evaluation criteria (IMO 2013). For civilian shipping, such criteria exist for safety, but not for security. For a naval ship, such criteria must be defined by the naval administration (NATO 2010b). Such criteria could be composed of high-level implicit criteria that would imply a subjective evaluation. However, there is a drive in IMO for explicit evaluation criteria, such as quantifying maximum tolerable risk for individuals on board and on shore (Skjong 2002). The risk relative to the maximum tolerable risk is often presented in a Frequency—Number of fatalities (F-N) diagram (Andrews and Moss 2002). The F-N diagram is a cumulative diagram (exemplified in Figure 12) in which the risk is presented together with the F-N curve given by (Pawling et al. 2012; Andrews and Moss 2002):

$$F_N = \sum_{j=1}^{N_{max}} f_N(N_j), \qquad \textbf{Equation 1.}$$

where $f_N(N_j)$ is the number of exactly $N$ fatalities per ship year. However, both explicit criteria and an F-N diagram demand a full quantitative risk analysis.

Risk control options are means of controlling risk and are applied in high-risk areas. Security risk control options range from technical measures included in the design of a ship to specific changes to the on-board watch system/schedule. The implementation of control options will affect a ship's vulnerability and therefore, the threat analysis. Consequently, when analysing options, there is a need to revisit the entire risk analysis.

In civilian ship risk management, the effectiveness of risk control options are typically weighed against the cost of implementation (Skjong 2009; IMO 2013). In military risk management, the operational effects of risk controls are in focus and the cost can therefore often be described as a having negative effect on ship systems such as weapon systems or propulsion (Paper V; Liwång et al. 2001).

## 4.2 Risk-based civilian maritime development

Prescriptive codes are unsuitable for both new developments and specialised ships (Kuo 2007; IMO 1994). Since the 1960s, therefore, risk-based approaches have been developed by the IMO. The probabilistic damage stability regulation in the Safety of Life at Sea from 1974 (SOLAS74) was the first maritime risk-based regulation and in 1997, IMO adopted the FSA as a risk-based approach to rule-making (Skjong 2009). Quantitative risk-based approaches are now well established in the area of traditional maritime safety.

Risk-based approaches to ship design have been developed under the term risk-based ship design. As illustrated in Figure 4, in risk-based ship design, risk analysis serves as a knowledge model together with other knowledge models (Vassalos 2009). The purpose of introducing a risk-based approach is to identify risks in the operation of a ship and to use this information to guide concept development and ship design according to a risk-based ship design approach. The knowledge model is used to reduce uncertainty in

the design decision making, which generally is high when developing novel concepts (Brown and Mierzwicki 2004).

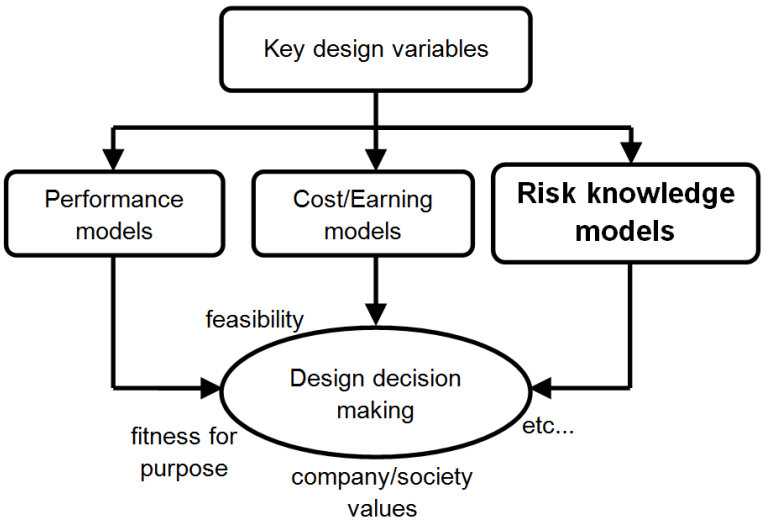


**Figure 4.** Design decision making in risk-based ship design. This thesis's areas of focus in respect to risk-based design, as described in Section 2.2, is highlighted with bold text. Redrawn from Vassalos (2009).

Risk-based ship design analysis can be performed with different tools and methods to fulfil the requirements for the relevant design project (Vassalos 2009). The risk-knowledge model is then used together with other knowledge models in the ship design, according to Figure 4.

Changes in safety risks are often a result of changes by the ship operator or in the onboard environment. However, in the context of security risks, the situation can change dramatically even though there are no changes in ship operations. Therefore, to underline the complexity of security risk management, Figure 4 presents a cyclical version of risk management. As illustrated in Figure 4, the ship security management process can be seen as both highly iterative and depending on situations both on board and beyond the ship operator's control. The illustration also shows the interdependencies between the processes, the situation on board and the political, economic and social situation in the areas transited and visited. An analysis of the risk-management process shows that the work must include these iterative aspects and interdependencies to support decision-making.

Figure 5 presents no effect on the external factors by the ship operators' risk management, only on ship-security management from external factors. However, if analysis and implementation is systematic and consistently used by a majority of ship operators in a specific region, in the long run security management can also affect the security situation. This can be seen off the coast of Somalia, where implementation the Best Management Practices for Protection against Somalia Based Piracy (BMP4) is a contributing factor to changes in pirates' modus operandi and reduced piracy (IMB 2013).

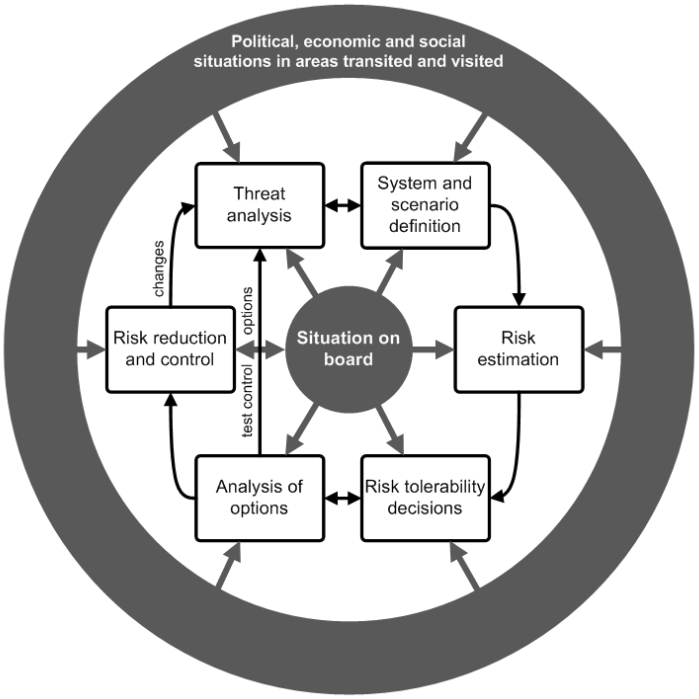


**Figure 5.** Cyclical version of ship security risk management presented in Figure 4. Of additional importance are the dependencies between internal and external conditions and the effect of risk controls (Liwång et al. 2014).

The development of ship security analysis has drawn from the experience of ship safety analysis but must acknowledge the differences between security and safety (Yang et al. 2013). System definition and threat identification and analysis are co-dependent, cannot be performed separately and are considered more challenging for security than for safety (Bichou 2008; Liwång et al. 2014; Liwång et al. 2015). These two activities must be conducted with the particular ship and operation in mind (IMO 2013) and must include a threat analysis. The understanding of safety (hazard-based) risks may come from objective incident statistics, whereas security (threat-based) risks often must be described and presented using expert judgments (Yang et al. 2013). Therefore, when analysing security risks, there is a need for a thorough threat analysis to explain causes and predict risks (Bichou 2008; Liwång et al. 2014). The security analysis also leads to a greater need to include uncertainties (Aven and Krohn 2014). The aspect of uncertainty is further discussed in Paper IV.

When analysing the conditions for risk analysis for maritime security, it is found that codes and guidelines prescribe a risk-based approach to ship security. However, there are limited descriptions of both *how* analysis should be performed (BIMCO 2013) and *how* adequate quality can be achieved (Bichou 2008). In particular, the scenario definition (Liwång et al. 2014; Liwång et al. 2015) and effects of risk perception (Frosdick 1997) are areas in which there is limited knowledge. Therefore, the challenges with respect to the security risk management process itself are as follows (Liwång et al. 2015):

– the process is applied to an area (security) for which risk management is not as tested and relatively few tools have been developed to assist the ship operator in the analysis,

- in comparison to safety risk management, the statistics on relevant phenomena are limited,
- there are no specific risk acceptance criteria for maritime security risks, and
- there is no discussion about how to define and achieve sufficient quality in the analysis.

Not only limited experience and research, but also the application area (security) itself leads to uncertainties that must be both decreased and presented.

Outside the scope of this thesis but also crucial for the success of risk-based approaches are how to communicate, approve, inspect and control both risk-based approaches and control options (Liwång et al. 2015).

## 4.3 Risk-based approaches to military activity

Casualties—whether deliberate or accidental—are a reality of military operations, and the desire to avoid them completely may have an adverse effect on achieving the mission. A balance of risk is therefore required and a comprehensive risk assessment process is essential to guiding decision making and prioritisation related to risk management (NATO 2007). Therefore, military risk management is both about comparing risk between different possible alternatives (in design and planning) and about comparing expected risk with expected gain (in planning).

Today, several nations utilise risk-based approaches to analyse the level of security in operations. Examples of military risk management approaches include the following: (1) the NATO Comprehensive Operations Planning Directive's (COPD) description of the role of risk analysis in military planning (NATO 2010a); (2) risk-management methods for military operations by the US Department of the Army (2006), the US Marine Corps Institute (2002) and the Swedish Armed Forces (2009a); and (3) specific methods for IT security (NATO 2008), force protection (DCDC 2010; NATO 2007), and antagonistic threats (Swedish Armed Forces 2009b).

From Table 1 it can be concluded that risks related to naval ships can be discussed and researched from several different perspectives; this thesis discusses the assessment of operational risk to support decisions during design and operation. According to Table 1, approximately five percent of the research focuses on naval operational risk.

**Table 1.** Articles in Web of Science with the following search conditions: title RISK and (MILITARY or NAVAL) and years 2000-2013. In total, 43 unique posts were identified.

| Topic | Total | Naval specific |
|---|---|---|
| Health and risk | 12 | 8 |
| Environmental risk | 11 | 2 |
| Operational risk | 10 | 2 |
| Risk in system engineering processes | 7 | 3 |
| Political and national security risk | 3 | 0 |
| Σ | 43 | 15 |

According to NATO, COPD analysis of operational risk is based on the probability and consequences of an operational failure. The risk analysis aims to identify risky situations and their possible consequences for mission accomplishment (NATO 2010a). According to COPD, the risk plays an integral role in creating situation awareness. In the general case, the risk should be studied over the near, mid and long term and

should include consequences to one's own troops and systems, third parties and the environment (NATO 2010a).

The system definition is a central task and will affect every aspect of risk estimation; the scenario definition will also affect which consequences can be studied (Liwång et al. 2014). A specific study often is, and must be, limited to specific consequences. However, it is not always obvious which the relevant consequences for mission accomplishment are, they could include:

- own causalities,
- own wounded,
- collateral damage,
- physical strain,
- event classified as critical,
- short term effects on the operation,
- long term effects on the operation, and
- damage to equipment.

The choice of consequences to study will affect the output and the decisions made. Without an agreement between the decision maker and the analyst on the consequences to study, the analysis can be misleading.

Military applications of risk management are substantially similar to their civilian predecessors, even though the civilian approach is primarily developed for hazards, whereas military applications often are about threats. If the focus is security rather than safety, particular attention must be given to the following issues:

- the lack of objective data because each intent has its own set of probabilities,
- the antagonistic threat, i.e., the probability of an attack is dependent on intent and implemented protection methods.

This is because hazards (without intent) and threats (with intent) evolve in different ways into risk; therefore, they must be analysed differently to capture the causal relationship (Bichou 2008; Yang et al. 2013).

Specifically for military maritime operations and in relation to ship risks the life of the ship is described by a set of tasks (Paper II). Some of these tasks are only performed in peacetime and others in wartime only. However, many tasks are assumed to be performed during both peace and war. For tasks performed in peacetime, the risk management is very similar to that of civilian risk management, i.e. to examine if the risk level is acceptable. In some situations, for example routine activity, acceptable risk could be defined by civilian regulations. In other situations, an increased risk is accepted because of a higher expected gain, but the civilian levels of acceptable risk (in relation to for example occupational risk or maritime risk as defined by IMO) are still relevant as a reference. However, civilian levels of acceptable risk loses their meaning in war. The risk management is, in a war, about weighing possible gain against risk.

When defining the requirements for a new ship or designing naval ships available resources has to be weighed against the military effect that should be achieved. That means that navies also choose to build ships that primarily are not intended for

warfighting roles, but rather for set of tasks that are assumed to be performed only in a low threat environment (NATO 2012). From a risk management perspective it could therefore be claimed that the roles and tasks such ships perform (or values they represent) are not important enough to protect in war.

## 4.4 Central aspects of the approach examined in this thesis

As a result of Sections 3, 4.2 and 4.3 (as well as Papers I and II) three central aspects of the approach examined in this thesis are identified:

- The approach must focus on expected incidents with high potential risk (that are initiated by a security threat).
- The focus of the analysis is primarily to understand the incidents.
- In order to understand future incidents available incident data has to be complemented by expert opinion.

These three aspects are discussed below.

### 4.4.1 Analyse expected incidents

In the risk management, the tasks of the ship are broken down to a set of defining incidents and it is the description of those incident types that are defined in the risk analysis as scenarios. It is within these incidents the design and operational aspects of the ship is connected to the level of the risk. Even if a conflict is defined as symmetric (between equal similar forces and tactics), the tasks defined for ships are typically asymmetrical. Therefore, generally probabilistic approaches focusing on modelling tasks has proven applicable for analysing military operations (McCue 1990; Morse and Kimball 1998; Ewell and Hunt 1995).

The focus on incidents and understanding security measures and operational alternatives also lead to that game theory based models, that could be applicable on the conflict and total effect of multiple decision makers (Washburn and Kress 2009), is not suitable as it focus on the battle (a sequence of dependent incidents) and not on the incidents. However, it must also be noted that there is no clear mathematical and methodical distinction between the probabilistic models used in the appended Papers II-V and basic game theory models used in decision theory described for military applications by Morse and Kimball (1998) and Washburn and Kress (2009).

### 4.4.2 Focus of the analysis is primarily to understand the incident

It is clear from how military doctrines define risk management that risk management is an approach primarily for internal knowledge collection and development. This is also true for the civilian risk management prescribed by the ISPS code where the analysis is a tool for guiding the ship operators in their decisions. This is particularly clear for those cases when the assessed risk is to be compared to expected gain. Therefore, in ship security generally the risk analysis is tool for understanding a ship's future and breaking down the assumed tasks into incidents and relating those incidents to the life cycle risk.

A focus on knowledge development and knowledge exchange (such as between expert and analysts; between analysts and decision makers; and between designers and operators) lead to that the methods tool used preferably also should be able to use in

the knowledge exchange. In Papers II-V this has led to the use of tools, particularly influence diagrams and event trees, with well-defined graphical and mathematical properties where these properties also has proven effective in knowledge exchange. The benefits of influence diagrams in this particular aspects has been shown by for example Friis-Hansen (2000) within maritime security and by Shachter (1986) within operational analysis. The event tree is particularly useful for describing scenarios with a clear time line (Andrews and Moss 2002).

### 4.4.3 Incident data has to be complemented by expert opinion

The availability of historic incident data varies within the studied areas. Generally, the quality of civilian security statistics is better than the military counterpart. For some areas, such as piracy against civilian ships off Somalia, the incident statistics are particularly good and is in Paper III estimated to include more than 90 percent of all incidents in the areas. In military analysis the relevant historic incidents are often few as a result of low incident frequencies and fast changing conditions (Bang 2014), see for example the description of attacks on naval vessels in Paper IV.

Even if there where incident data applicable on the future such data often lack vital information needed to understand the causality of the incident (Bang 2014), see for example Ellis (2010) and Psarros et al. (2011) and how incident data can be used to quantify the risk, but not always explain how specific ship measures affect the risk. To understand how different measures affect the operation a model describing the operation and measures are needed (McCue 1990). For creating such a model, statistics have to be complemented with expert knowledge as exemplified in Papers II-V and in a IMO FSA on dangerous goods (IMO 2009).

In this thesis, the reason for examining approaches with knowledge collection from experts is three fold:

- to be able to capture aspects (such as causality) not captured by the data, but important to the ship operators risk understanding,
- to be able to capture expected or challenging futures (as a result of future changes) in the security situation (the analysis must try to understand how the changes affect the risks), and
- because correlation in data between aspects and risk do not imply causation, i.e. without an understanding of the incidents the data can give misleading answers.

Experts however introduce uncertainties and where possible data and statistics should be used in the risk model to verify and validate input from experts. This also means that new data should be used to update existing models.

*"It should never be forgotten that, although certification is undoubtedly important, what really counts is the work that has been done on the ground: security officers appointed on ships, in companies and port facilities; training undertaken; security plans drawn up; awareness raised; and vigilance heightened."*

Secretary-General, International Maritime Organization, IMO: Rising to New Challenges (Mitropoulos 2004).

# 5 Maritime security

As stated in the Maritime Strategy of the United States of America (Department of Defense 2007) the world economy is tightly interconnected and 90% of world trade involves transported by sea. Sea lanes and the supporting shore infrastructure are therefore important to the global economy. Today's military conflicts are increasingly characterised by a blend of traditional and irregular tactics, decentralised planning and execution, and non-state actors that use both simple and sophisticated technologies in innovative ways against both military and civilian ships. Therefore, today's naval operations are more focused on the littoral and number of mission types along with increasing threats (NATO 2010b). These conditions combine to create an uncertain future and impose new demands not only on maritme security but also on naval ships to counter these threats.

The need to further develop maritime security is also recognised by non-military authorities such as the IMO and the European Union (Mitropoulos 2004; Council of the European Union 2014).

As defined by the ISPS code, maritime security includes both port and ship security (IMO 2002). This thesis discusses ship security with a focus on how to assess security for military ships. Security for civilian and military ships is both directly and indirectly connected.

## 5.1 Ship security

The IMO ISPS Code (IMO 2002) results from today's security situation and addresses the civilian aspects of maritime security. The code is based on the assumption that security of ships and ports is a risk management activity and that to determine what measures are appropriate, an assessment of the risks must be made in each scenario. The purpose of the code is to provide a standardised, consistent framework for evaluating this risk. The code defines roles, plans and procedures for ship owners and port facilities as a basis for secure interaction between ships and ports. However, as a result of the extensive piracy off Somalia, the ship security practise has been driven by

concerned ship operators rather than the ISPS code (Liwång et al. 2015). That the development is coming from genuine needs has many positive aspects. However, the development today lacks a systematic collection of identified and learnt lessons.

Security control-options range from technical measures included in a ship's design to specific changes to the watch scheme on board. For example, typical and recommended risk control options are described in the ISPS code and the BMP4 (IMO 2002; BIMCO 2013). However, each ship and threat combination has specific risk causality and therefore a specific list of suitable risk control options. These control options can be identified only with the help of a ship-specific, risk-based ship security assessment (IMO 2013).

In the field of ship security, part A of the ISPS code stipulates that a risk-based Ship Security Assessment shall be performed for all passenger ships, all cargo ships above 500 gross tons and mobile offshore units in transit. Guidelines such as the Norwegian Shipowners' Association's Guideline for performing ship security assessment (Norwegian Shipowners' Association 2008) divide the ship security assessment into four general parts: initial screening, threat assessment, onboard audit and identification of needs. The threat assessment is defined by the following two steps (Norwegian Shipowners' Association 2008):

- Identify threat scenarios, or security incident scenarios, that reflect motives and prioritised operations, areas, systems and personnel.
- Assess the likelihood and potential consequences of the scenarios in relation to the ship's vulnerability.

Ship security is of importance for both military and civilian organisations and often during operation, a security decision made by one will affect the other (Council of the European Union 2014). Therefore, approaches and research from both areas are discussed below; however, the focus is on military ship security.

### 5.1.1 Principles for ship security

In "Principles of engineering safety: Risk and uncertainty reduction", Möller and Hansson (2008) discuss the principles of engineering safety and suggest the following four principles (Möller and Hansson 2008):

- *Inherently safe design*, which means that potential hazards or threats are excluded.
- *Safety reserves* with safety factors or safety margins.
- *Fail-safe* systems so that if it fails, it does so safely.
- *Procedural safeguards* in which procedures and training is used to enhance safety.

Often, systems are designed with a combination of the principles above, and some applied approaches can be said to belong to more than one principle (Möller and Hansson 2008).

The list can also be seen as arranging the principles from straightforward to complex or from low uncertainty to high uncertainty. Therefore, demands on the decision process are increased if the later safety principles from the above list are used.

By analysing suggested ship security measures (or risk control options) in the "Best management practice for protection against Somalia based piracy" (UKMTO 2011); the appendix to the ISPS code (IMO 2002); the "Survivability of small warship and auxiliary naval vessels" (NATO 2012) and Det Norske Veritas (DNV) "Rules for Classification of High Speed, Light Craft and Naval Surface Craft" (DNV 2013), it is found that the focus is on *safe fail* and *procedural safeguards*. With respect to safe fail the ship must be built to be operational, with constraints, even if there is an attack. Measures such as physical or immaterial barriers, redundancy, segregation and diversity are typical for maritime security and Möller and Hansson (2008) classify them as fail operational.

Procedural safeguards with respect to ship security can be exemplified by, but are not limited to, prepared procedures for the crew if the ship is under attack and special emergency organisations onboard to handle the effects of an attack such as fire and flooding.

The fact that ship security relies to a large extent on safe fail and procedural safety does not necessarily increase the risk, but increases the epistemic uncertainty about the function or effectiveness of the security system. This increased uncertainty leads to an increased need to address and understand uncertainties throughout the decision process (as discussed in Sections 3 and 4.3). This because procedural safeguards in particular depend on the actions of the crew, which are partially a function of the safety culture. There is therefore a strong connection between the situation on board and the effectiveness of the security measures as shown in Figure 5 and underline the need for using a socio-technological system perspective.

## 5.2 Naval ship survivability

In this thesis, naval ship survivability is seen as a sub-component of ship security relevant to protection against physical attack. For military ships survivability is often discussed in terms of susceptibility, vulnerability, and recoverability of the ship (Ball and Calvano 1994; Boulougouris and Papanikolaou 2013; NATO 2010b; Said 1995; Kim and Lee 2012; Hughes 1995), here defined according to:

- **Susceptibility** is the inherent inability of the ship (including tactical measures) to avoid a hit and governs the probability of a hit ($P_H$).
- **Vulnerability** is the inherent inability of the ship to resist damage and governs the probability of kill (or damage) given a hit ($P_{K|H}$).
- **Recoverability** is the ability of and the crew the ship systems to return the ship to operational capability and governs the probability of damage repaired ($P_R$).

In a military operation, a ship's survivability is also determined by force protection measures. Force protection is an enabling activity by which threats and hazards to the force are countered and mitigated to maintain an operating environment that enables freedom of action (DCDC 2010). Subsequently, it is neither possible nor necessary to distinguish fully between survivability and force protection: survivability represents a design perspective, and force protection represents an action perspective.

It is clear that Cold War tactics to eliminate an opponent or its engagement system before they could hit ships is an overly simplistic description of modern naval warfare (Ball and Calvano 1994). It is no longer possible to treat vulnerability and

recoverability as constants and to assume that a hit equals a ship kill (Boulougouris and Papanikolaou 2013; Ball and Calvano 1994; Hughes 1995; Kim and Lee 2012; Harney 2010). In coastal areas, threats are more difficult to detect and avoid because of short reaction times. Accordingly, there is an increased focus on vulnerability and recoverability (Harney 2010), which is especially challenging for small warships (NATO 2012). To meet the new challenges posed by today's warfare, including asymmetric and littoral warfare, survivability must be examined more closely and must present timely contributions to the systems engineering process (Said 1995; Harney 2010).

The, instant killability of a ship is the product of the probability of a hit ($P_H$) and the probability of damage given a hit ($P_{K|H}$). Survivability ($P_S$) is the opposite of killability and if only primary and secondary effects are studied without recoverability, survivability is given by

$$P_S = 1-(P_H \cdot P_{K|H}). \qquad \textbf{Equation 2.}$$

If recoverability ($P_R$) is included, survivability is given by

$$P_S = 1-(P_H \cdot P_{K|H} \cdot (1-P_R)). \qquad \textbf{Equation 3.}$$

The concept of survivability is thus most often described in probabilistic terms (Ball and Calvano 1994; Hughes 1995; Kim and Lee 2012).

A ship kill need not be total and therefore can be defined in relation to different severity levels, such as the following (Ball and Calvano 1994; Boulougouris and Papanikolaou 2013):

- System kill in which one or more components are damaged and system failure results.
- Mission kill in which the ability to solve a particular mission is killed.
- Mobility kill in which the ship has lost its ability to manoeuvre.
- Total kill in which the ship either is lost or must be abandoned.

Important technical measures include redundancy and separation (see Kim and Lee (2012) for a probabilistic description of these concepts), but the discussion can also include top-level aspects such as fleet composition and ship numbers (Harney 2010; Hughes 1995).

It is the ship operator's responsibility to structurally (with the help from organisational knowledge) identify threats, hazards and control options. This ensures that control options are documented and inspecting and approving bodies can test the analysis.

As illustrated in Figure 6, hazards and threats to military ships largely lead to catastrophe scenarios similar to those of civilian ships. However, survivability after hostile attack—divided into susceptibility, vulnerability and recoverability—has military-specific aspects that must be analysed. In addition, the needs of the analysis differ between the three survivability aspects as discussed in the following Sections.

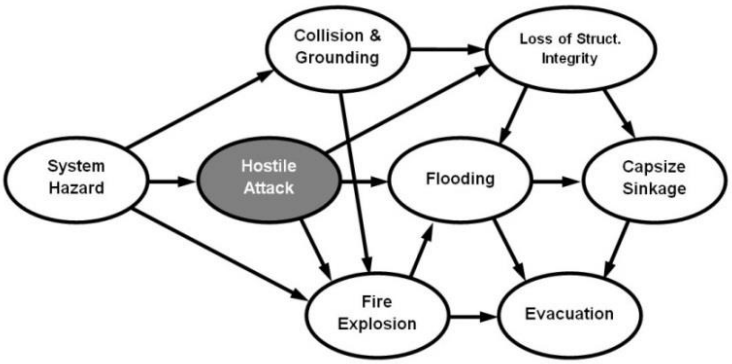


**Figure 6.** Typical catastrophe scenarios developed from (Vassalos 2009). White aspects indicate catastrophe scenarios common to civilians and the military. Grey aspects indicate a uniquely security-oriented security perspective.

### 5.2.1 Assessing susceptibility

To estimate the probabilities directly and indirectly connected to susceptibility, the modus operandi of a threat and ship actions must be either known or assumed. The design concept directly affects tactics, ship susceptibility and ship vulnerability and indirectly affects those threat characteristics that depend on ship characteristics. Therefore, the reliability and consistency of assessed susceptibility depend on well-specified tasks, type of operation and type of threat. Without these specifications, assumptions are required, which can reduce reliability. The reliability also depends on a structured and documented analysis of how different aspects interact. The validity and relevance of the analysis depend on specified tasks and threats, which respond to the actual ship use, and the scenarios and analyses, which must sufficiently consider the complexity of ship operations. The effect of susceptibility on risk and its role in a risk analysis is further discussed in Paper V.

### 5.2.2 Assessing vulnerability

To estimate the probabilities connected to vulnerability, a hit or attack is normally assumed. Accordingly, the vulnerability assessment is not as dependent on threat modus operandi or ship actions; instead, it is more dependent on physical attributes of the attack, including weapon and ammunition specifications with respect to the ship's technical specification.

Survivability analyses are well-established (civilian and military examples are discussed in Paper V). However, these models require a correct and validated model to describe post-attack damage. Moreover, the input must describe and include how the probability of impact/hit position is a result of weapon characteristics, such as is the use of a technically governed weapon (anti-ship missiles) or shooter predisposition governed weapons (hand-held, anti-tank grenade launchers) interact with aspects such as signature management and ship tactics.

### 5.2.3 Assessing recoverability

Recoverability depends on a physical description of the damage, its effect on ship functions and how it can be temporarily or permanently "fixed" by the crew.

An analysis of the failure of recoverability must include crew performance, which for complicated damages can make a substantial contribution to survivability. Several

approaches can be used to estimate crew performance and model crew effectiveness in a recoverability scenario. The literature also includes research into how incident statistics can be analysed to support the selection of risk-control measures, including crew performance (Akhtar and Utne 2014). In such an analysis, expert opinions are central, but it is important for the experts to have relevant experience and if possible, to use empirical data and calibrate techniques (Deacon et al. 2013). To validate model output, historical events must be analysed, full-scale experiments must be performed, and the effects of current training must be analysed. One example of a relevant, full-scale experiment is the Operational Sea Training performed by the Flag Officer Sea Training for the UK Royal Navy (Royal Navy 2014). A structural use of the experience and data from such experiments could be used to develop naval-specific human error and causation factor models. (See Paper V for further details about analysing the crew's role with respect to recoverability.)

## 5.3 The appropriate focus of ship security analysis

According to Section 2.1.2 and Figure 3 the risk management process contains several steps. The three sections below discuss that has to be considered. These aspects require special consideration in a ship security analysis.

### 5.3.1 Threat and scenario definition and selection

Before the effect of design decisions can be analysed, the operational environment must be defined. Pursuant to the doctrine, the relevant state must extract a concept of operation valid for design, construction and operation. The manner in which the concept of operation is described and quantified is central to the implementability of military survivability, and scenario definition and selection is central in the risk-analysis process (Liwång et al. 2014), see also Papers I and V further detail. The threat and scenario definition is particularly critical in ship security because the suitable scope, system and consequences to study vary substantially from analysis to analysis. Design scenarios must be created based on the relevant identified threats. When generic design scenarios are available, they must be adapted and customised to the specific features and expected performance of the vessel in question (IMO 2013; Vassalos 2009).

The definition of future scenarios is an effective way to support analysis of the future (Meissner and Wulf 2013), but cannot be limited to a prolongation of the present, they must include surprises (Derbyshire and Wright 2014). The scenarios need not to accurately predict the future, but they should capture possible futures (Meissner and Wulf 2013) without misleading decision makers as to their reliability (Gershuny 1976). Quality aspects to consider when choosing scenarios include that there should be multiple scenarios to account for uncertainty and each scenario must be plausible; internally consistent; relevant; and contribute to the analysis (Amer et al. 2013). The definition process include both qualitative and quantitative aspects (Amer et al. 2013).

The probability of each of these future conditions should be estimated (Kirkwood and Pollock 1982) and today, there is an increasing focus on also including uncertainties in the analysis (Aven and Krohn 2014; Derbyshire and Wright 2014; Brown and Mierzwicki 2004). Relevant historical information is often limited and expert judgment is needed to define scenarios (Kirkwood and Pollock 1982; IMO 2013). In addition to defining ship tasks, the threat description is the most important input to the scenario

definition and must both be quantitative and support a scenario definition that captures the life cycle risk (Law 2011). The description must therefore be developed specifically for the ship and tactical tasks at hand (IMO 2013; Vassalos 2009). The intelligence community is responsible for developing the threat description (Said 1995).

The scenarios must also consider the effectiveness (or gain) of the operation, especially if the scenario should be used to compare ship concepts that solve the intended operation differently. There exist theoretical frameworks for quantitatively connecting measures of operational outcome and for measuring effectiveness and component system performance (Perry 2007). However, the purpose of a risk-based survivability design process is to compare different risk-control measures in the form of concepts, systems and components. The focus is therefore on relative risk, and it is unnecessary to describe the risk in absolute terms. It is therefore possible to introduce some simplifications, such as a set of scenarios that keep the potential gain constant and examines the risk for different ship concepts.

The analysis documented in the NATO Force Protection Directive (NATO 2007) can be used to perform a stringent threat analysis (an example is presented in Paper III and is further investigated in Liwång and Ringsberg (2013)). The analysis determines the capabilities and intentions of an identified group or organisation and how likely it is to carry out its defined threat and actions. The threat analysis focuses not on the threat in isolation but also on the threat in relation to the vulnerability of the ship in question (NATO 2007).

When analysing the threat and defining the scenario, there must be a focus on the threat's modus operandi, identifying how these modus operandi can lead to ship damage and whether the intended ship tasks limits the number of relevant modus operandi. In addition, it is important to determine how the likelihood of different attack modus operandi is affected by ship tasks and ship susceptibility. The scenario must be developed for specific ship concepts, and a change in ship concept can change the probability of threat encounter and/or the probability of the success of the threat (NATO 2007).

### 5.3.2 Ship design considerations and their effect on the intended operation

Early in the design definition the design approach to critical systems, such as redundancy and separation; fire protection; ballistic protection; damage stability; and man-machine interfaces, must be set. These aspects are important not only to ship military survivability but also to the design in general. The design of such systems have their own design rationality and methods; today, however, they must also be performed with respect to survivability goals and in relation to other design areas.

The studies on ship transit through an area with mine threats, ship security attacks, an asymmetric threat to an Ocean Patrol Vessel (OPV) and fire onboard naval vessels all show that risk always depends not only on technology choices but also on crew and ship actions. Many technology choices are made early in the design process and must be tailored for the operation.

Damage stability is an example of a ship design area not only with its own research but also with important survivability implications. Probabilistic damage stability was the

first probability ship design area to be systematically investigated. Substantial research and tools exist today, including real time simulation of ships' survivability in waves validated with model tests (Schreuder et al. 2011). These simplified approaches have some limitations, specifically with respect to hull shape and speed. However, these limitations will not affect the possibility of investigating a damaged naval ship. The models require a physical description of the hull damage. One example of how these tools can be used for naval ships is in Boulougouris and Papanikolaou (2013) and their optimisation of water-tight subdivision related to weapon hits.

Another central area for military survivability is a crew's possible contribution before, during and after attacks. These activities are performed within a context that includes a broad range of human, technical, organisational and environmental factors that can influence, but not necessarily determine, an operator's performance in a system (Liwång et al. 2015; Musharraf et al. 2013). There are gaps in the literature related to the effects of security threats on crew performance. However, typical reactions to stressors include cognitive, emotional and social effects. The stress effects will lead to poor decisions. Therefore, in a situation with a perceived security threat, there are fewer resources to perform the task at hand, and the likelihood of errors increases (Liwång et al. 2015).

It is important for the analysis of crew effectiveness to acknowledge that well-learned skills and well-rehearsed tasks require less attentional control and thus, performing these tasks is less affected by stress (Beilock et al. 2002; Fisk and Schneider 1984; Smith and Chamberlin 1992). Moreover, well-designed systems enhance the performance of a given task. Therefore, it is important to ensure the inclusion of education, training and human factor design aspects in any assessment of crew effectiveness (Liwång et al. 2015). Musharraf et al. (2013) and Deacon et al. (2013) present quantitative approaches to human reliability assessment applied to offshore emergency conditions. There are also studies on causation—i.e., the probability that a crew member will not act as he or she is supposed to (Ravn 2012).

Subsequently, survivability design includes a plethora of aspects and design areas (of which only two are presented in this section). Such decision areas all have their own knowledge base and experts and no design will be successful without using appropriate approaches and experts.

### 5.3.3 A successful analysis

A successful analysis that correctly compares military survivability among alternative designs must include the following aspects (generalised from Paper V, a study on fire survivability):

– The relationship between design choices and the probability of incidents, such as a hit. There is a relationship between general design choices (and their operational implications) and the probability of incidents. Characterising this relationship depends on the threat. These relationships must be described and analysed for multiple scenarios to account for uncertainty, and each scenario must be plausible, internally consistent, relevant, and contribute to the analysis. *Specifically for fire survivability, this refers to the relationship between design choices and ignition probability that has to be included in the analysis.*

- The state of the ship at the incident. This description depends on the specifics of the ship and will vary for the same scenario among concepts due to differences in ship tactics, susceptibility and vulnerability. Different concepts will require different passive and active protection, depending on the differences in how the concepts are designed and manned. *Specifically for fire survivability, this means that analysis of the fire escalation required to estimate the consequences depends on a physical and system description of the ship upon ignition.*
- Complicated incidents with potentially severe consequences (i.e., those that likely will contribute substantially to the total risk). *Specifically for fire survivability, this refers to complicated fire ignition cases. These cases differ from typical civilian ignition cases due to additional complexity caused by added fuel (from weapons), potentially multiple dependent ignitions and severe damage to the structure and systems.*
- Qualitative human factor aspects of the design, which managed effectively, can reduce the consequences of potentially catastrophic incidents. Therefore, the analysis also depends on discerning qualitative human factor design aspects in addition to technical aspects. *Specifically for fire survivability, this means that the firefighting is crucial under conditions with a high-risk contribution, and the effectiveness of firefighting may be high.*
- Naval specific models and data. Specific models and data, along with further validation, are necessary both generally and specifically for signature management effects, military-unique vulnerability data (such as ignition models), crew performance and fire characteristics of military-specific equipment onboard.

In general, the reliability and validity of identifying incidents is relatively dependent on a qualitative and outward-focused analysis of the ship's future. The reliability and validity of the analysis of incident consequences depends on specific data and descriptions of the ship used. This analysis must be based on an understanding of operational conditions. Therefore, the civilian risk-based approaches are not applicable to naval ships because they do not guarantee that relevant aspects of ship design and the intended operation are included in the analysis. Furthermore, vulnerability tools lack this ability. However, when the incidents are defined, civilian methods and tools can be used to assess the consequences if the ship specifications are suitable for naval ships.

*"The community of risk analysts would easily interpret … a high-level evaluation criteria. It is, however, unlikely that the interpretation by different analysts would be identical."*

Det Norske Veritas chief scientist on IMO risk criteria (Skjong 2002).

# 6 The merits of a quantitative approach

Humans are notoriously unskilled at estimating probabilities and comparing probabilities, especially in regard to incidents for which we have strong feelings. Such feelings will influence the performance of risk analysis and can skew the results, exaggerate high-profile risks and under-predict common risks (Kahneman 2011). However, history also shows that conveying an idea of a probability in qualitative terms is easily misunderstood. This is exemplified in the 1961 assessment of the strategic prospects for a US invasion of the Bay of Pigs. In their report, the Joint Chiefs of Staff reported pessimism about the success of the plan, using the term "*a fair chance of success*". However, the US President understood the report as optimistic about the probability of success (Friedman 2014). Therefore, actually assigning a number to an estimated likelihood is—at least—less unambiguous.

As described in Section 4.2, the risk-based maritime safety approaches are most often quantitative; see, e.g., the IMO top-level rule-making approach (FSA) (IMO 2013) and the IMO damage stability criteria (Vassalos 2009). The suitable extent of quantitative tools and criteria in approaches to maritime security is, however, ungoverned. Here, a quantitative approach is defined as an approach that uses numbers to express likelihood and consequences in absolute terms.

Sections 6.1 to 6.3 present three examples of how quantitative data can be used in a security analysis.

## 6.1 Application example 1: skiff approach probability

In offshore piracy attacks on transiting ships, the speed of the ship has been proven to be one of the most important aspects of ship security. An increased ship speed substantially reduces the risk of a successful piracy attack. During the high-piracy activity years in the waters off Somalia (2008-2011), there were no reported attacks in which pirates had boarded a ship that was proceeding at more than 18 knots (IMB 1993-2014). Figure 7 present incidents in 2010 and 2011 plotted against ship maximum speed.

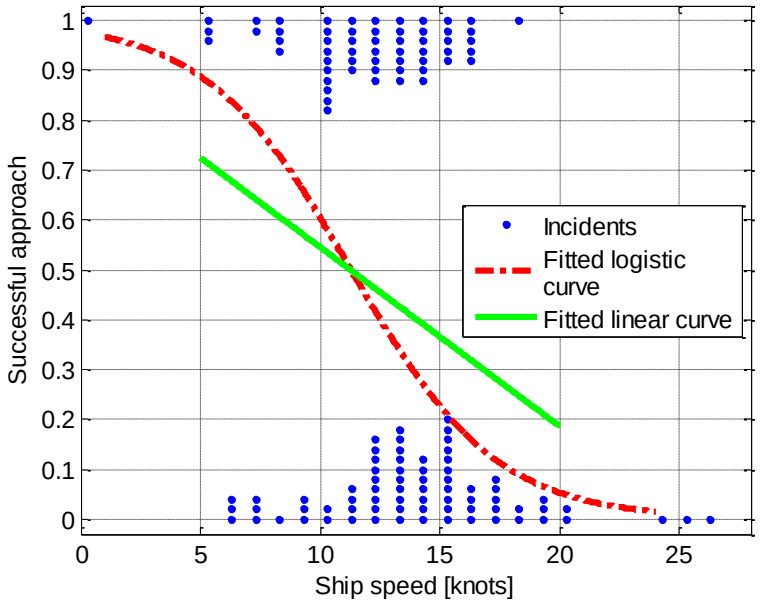


**Figure 7.** Incident statistics (binary data) for non-monsoon months in 2010 and 2011 plotted against ship maximum speed (dots) (Liwång and Ringsberg 2013). The dots at the bottom of the graph represents fail attacks and the dots at the top successful attacks.

At the same time, it is clear that many piracy skiffs can travel much faster than 18 knots and statistical reports have described skiffs that have matched speeds as high as 25 knots (IMB 2012). It is therefore possible that pirate tactics and techniques may develop to enable them to board ships at faster speeds. Therefore, it is reasonable to argue that ship operators need more information about how ship speed affects the attack probability. This is so that increased ship speed can be weighed against aspects such as routing alternatives, extra fuel costs and the use of armed guards. Figure 8 presents an analysis of approach success probability (Liwång and Ringsberg 2013) (Liwång and Ringsberg (2013) develops the models and results in Paper III). The analysis is fully based on expert input on the scenario according to Figure 9.

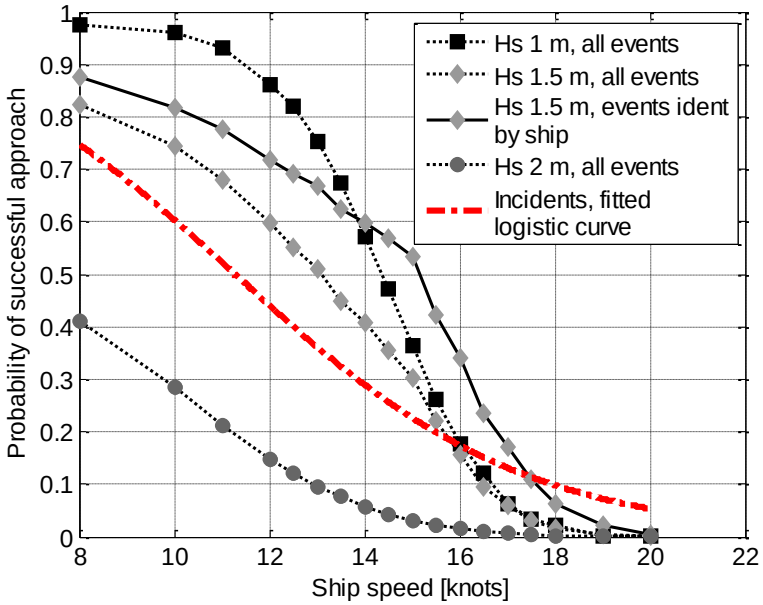


**Figure 8.** Calculated probability based on expert knowledge of a successful approach as a function of ship speed calculated for wave heights of 1, 1.5 and 2 metres (Liwång and Ringsberg 2013) compared to statistics. The dotted lines display the probability of a successful approach for all events. The solid line display the probability only for incidents not aborted before the ship sees the skiff.

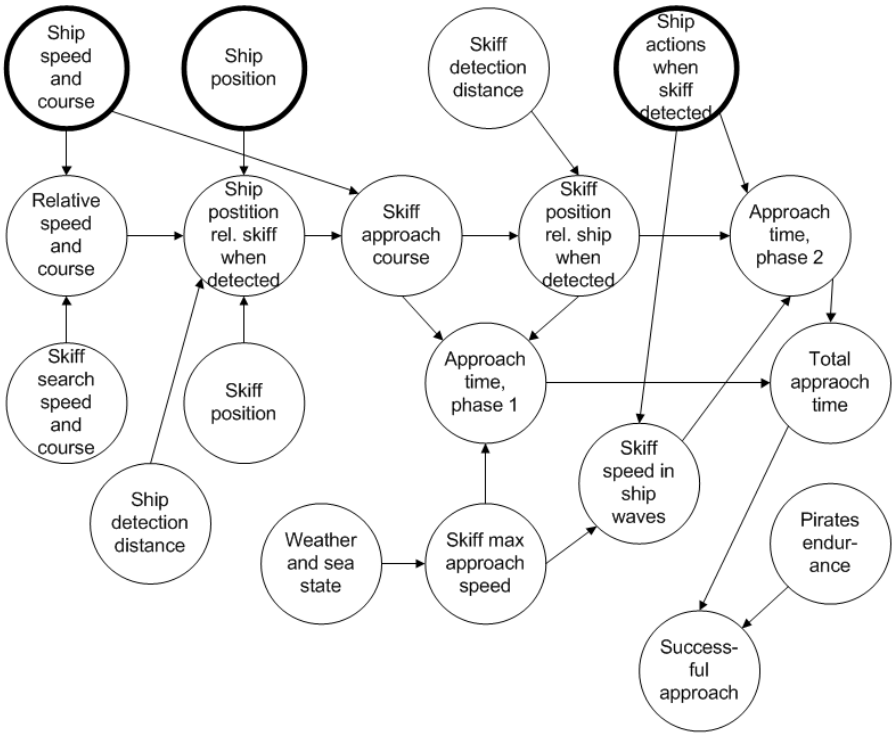


**Figure 9.** Influence diagram of approach scenario, assuming that the ship is within detection distance of a skiff (Liwång and Ringsberg 2013). See Paper III for expert data and Liwång and Ringsberg (2013) for simulation details.

There is a clear correlation between the probability of successful approach and ship speed in both the statistics (Figure 7) and the expert-based simulation results (Figure 8). 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 8 into a total probability that can be compared to the reported frequency in Figure 7. 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 logistic fit showing the calculated probability, is both 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.

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 difficult to get close to the ship even if the sea otherwise is calm.

Defining the probability of successful approach as a function of speed and detection distance, as performed in Figure 8, 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. Worthy of note, as seen in Figure 9, is that the analysis is largely based on input such as skiff speeds, detection distance, wave height and other parameters that are easy to measure and quantify. This reduces the need for subjective probability estimates.

## 6.2 Application example 2: uncertainty in risk estimates

The influence diagram in Figure 10 models how design and operational aspects affect the probability of three examined consequences (crew injuries, the ship buoyancy and the ship ability to manoeuvre) as a result of an attack.

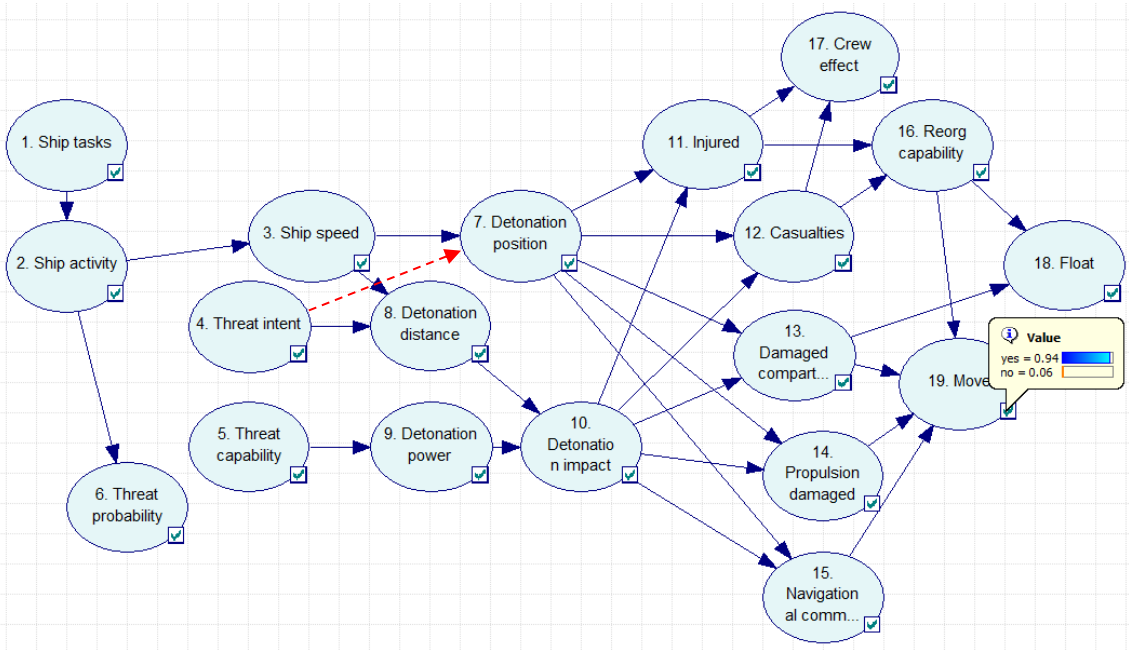


**Figure 10.** Influence diagram based on expert knowledge for assessing the probability of the consequences studied (Paper III). Values are calculated without epistemic uncertainties. The influences and solid arcs represent the base alternative (Alt. 0), and the dashed arch from $s_4$ to $s_7$ represents an alternative model (Alt. 1). The influence diagram was created using GeNIe, by the Decision Systems Laboratory of the University of Pittsburgh (Decision Systems Laboratory 2014).

As discussed in Sections 1.2 and 2.1.3, uncertainties in expert based security assessments are often substantial. In the model, aleatory parameter uncertainty is included in the probabilistic characteristics of the influence diagram. Epistemic parameter uncertainty is included as a probability density function for the conditional probabilities for each influence as described in Table 2. The highest uncertainty is for the probability that describes whether or not the threat has a high intent (ranging from 0.0 to 0.7, which is about the same uncertainty as reported in discussion on bin Laden's hiding place described in Section 1.2). Epistemic model uncertainty is included in different relations between influences and within the definition of the conditional probabilities for some influences (the model and uncertainties are described in detail in Paper IV).

**Table 2**. Modelled systems, influences, probabilities and uncertainties. Influence 4 (s4) has the highest uncertainty, here estimated as an even distribution between 0 and 0.7. See Paper IV for values of the probabilities and epistemic uncertainties.

| Influence | States [state 1; state 2, …] |
|---|---|
| s1 Ship tasks | patrol |
| s2 Ship activity | sea; coast |
| s3 Ship speed [knots] | 0;5;15 |
| s4 Threat intent | high; low |
| s5 Threat capability | high; low |
| s6 Threat probability | high; low |
| s7 Detonation position along ship | fore; mid; aft; miss |
| s8 Detonation distance from ship | at; close; far |
| s9 Detonation power | high; low |
| s10 Detonation impact | high; med; low |
| s11 Injured | high; low |
| s12 Casualties | high; low |
| s13 Damaged compartments [number of] | 0;1;2;3 |
| s14 Propulsion damaged | yes; no |
| s15 Navigational command and control damaged | yes; no |
| s16 Reorganisation capability [number of tasks] | 0;1;≥2 |
| s17 Crew effect | high; low |
| s18 Float | yes; no |
| s19 Move | yes; no |

The primary design decisions in the model studied here are as follows:

- The probabilities are calculated given the occurrence of an attack.
- The model analyses the effects on the ship 30 minutes after the attack.
- Here, several influences are defined by qualitative states. For a specific ship, these influences would be defined by quantitative (continuous) states; see for example s7, s8, s9, s10 and s12.
- Here, reorganisation is defined as restructuring the crew to concentrate on core survival activities.
- In the model (all model alternatives), restoring watertight integrity is prioritised before restoring propulsion and navigational command and control.
- Weather and degree of closed watertight doors are included in s19.
- Some influences are known with high accuracy (low epistemic uncertainty), see, e.g., s13.
- Some parts of the influence diagram function as logic operators and do not introduce parameter uncertainty. These influences can, however, introduce model uncertainty.

In this study, each of the different conditional probabilities that describe each influence ($s_1$-$s_{19}$) is itself described with a variable ($x_1$-$x_{61}$).

In Figure 11, the uncertainty of the three target influences is displayed together with the expected value calculated with the mode and median values. The biggest interquartile distance is for influence 17 and is 0.04.

Ignoring the epistemic uncertainties and using the most probable values for the input will not give the most probable output according to the Monte Carlo analysis. See especially the difference between the *expected value* and the box-plot median for influences 17 and 19 in Figure 11. Note that both calculations are based on the same expert input (however, when calculating the *expected value,* the expert uncertainty is ignored).

The output uncertainty is small relative to the input uncertainty. The maximum input uncertainty is 0.7 and 0.1 to 0.2 for many input variables. The inter-quartile distances for the output are 0.04, 0.004 and 0.02 for influence 17 state 2, influence 18 state 1 and influence 19 state 1, respectively.

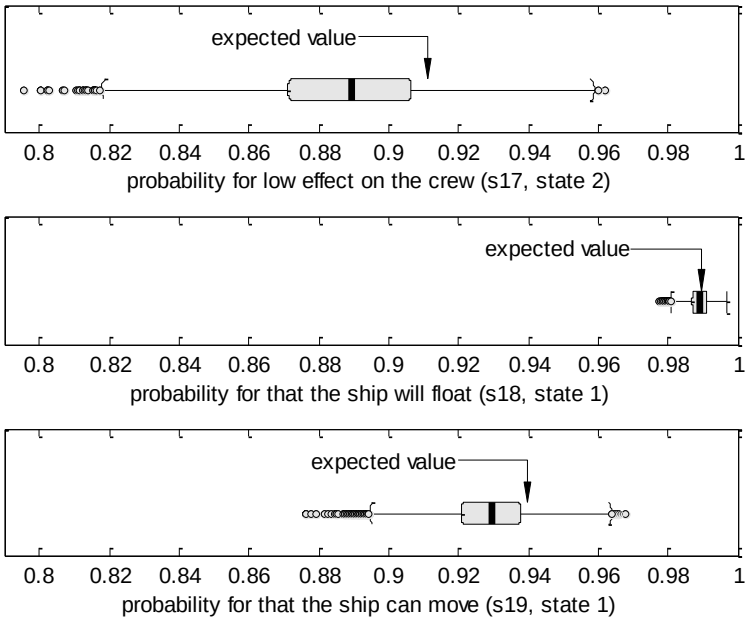


**Figure 11.** The output uncertainty for influences 17, 18 and 19 based on the Monte Carlo analysis. The *expected value* is the value calculated without epistemic uncertainties, i..e. only calculated based on the respective variables' expected value (if an even distribution) or mode values (if a triangular distribution).

The box plots for the three output parameters in Figure 11 give a good understanding of how uncertainties affect output, including not only the most probable values but also the tails. Such results give the analyst and the decision maker the information needed to take the total uncertainty into account, not only the expected probability and consequences.

High uncertainty can give rise to two different needs: one is to decrease the uncertainty in the analysis and the other is to find a protection solution with a lower uncertainty, a robust solution. When the aim is to decrease uncertainty, the parameter uncertainty must be revisited. To revisit parameter uncertainty requires structural knowledge of

how the different input parameters contribute to output uncertainty. This contribution can be estimated by the numerical derivative analysis, which investigates the sensitivity for each input. In that analysis, the term $\partial y/(\partial x_i)$ is used as a measure of how an uncertainty in $x_i$ (one of the conditional probabilities describing a influence) will affect the output. In this study, the term $\partial y/(\partial x_i)$ is numerically calculated for each variable with uncertainty and is shown in Table 4. See Section 7.4 and Paper IV for details of the data, output, analysis and methods.

The numerical derivative analysis clearly indicate which input must be revisited. Deriving similar results from the Monte Carlo analysis is calculation intensive. From the results, it is clear that the proposed approach can assess the risk, examine the uncertainties and be described to the decision maker. However, the results also show that this type of approach is needed for understanding which variables affect output uncertainty. Noteworthy is also that, according to Table 4, the only variable uncertainty with high effect on all three examined consequences is the variable describing the ship activity (operation concept).

## 6.3 Application example 3: fire as the result of weapon attack

When the fire risk for a naval ship is analysed, both accidental ignitions (such as the ignitions in civilian operations) and ignitions by weapon hits must be examined. For standard military operations, weapon hits yield a lower ignition frequency compared to accidental fires. However, as shown in Table 3, because of the severer consequences the risk contribution from weapon hits is several orders of magnitude greater than from accidental fires. Therefore, considering aspects such as general susceptibility can be an effective way of reducing fire risk, and ignoring the effects of different design choices will risk penalising design choices that can have a positive effect on combat effectiveness.

**Table 3.** Magnitude of the fire risk contribution from different types of ignition and operation developed based on Tables 2 and 4. The data and analysis approaches are presented in Paper V.

| Case type | Risk contribution | | | | |
|---|---|---|---|---|---|
| | Civ op | Std mil op | | High risk mil op | |
| | | Std ship | Low susc ship | Std ship | Low susc ship |
| Local ignition intact compartment | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ |
| Local ignition added complexity | 0 | $10^{-4}$ | $10^{-5}$ | $10^{-2}$ | $10^{-4}$ |
| Multiple ignitions added complexity | 0 | $10^{-1}$ | $10^{-2}$ | $10^{0}$ | $10^{-1}$ |
| Total fire risk per ship year | $10^{-4}$ | $10^{-1}$ | $10^{-2}$ | $10^{0}$ | $10^{-1}$ |

Figure 12 presents the fire risk for the examined operations types in an F-N diagram in relation to IMO risk safety criteria for civilian ships. As expected, the risk contribution from fire onboard naval ships is high compared to civilian operations, especially for high-risk operations. Figure 12 shows that the level of risk is greater for incidents with potentially serious consequences compared to high-frequency incidents.

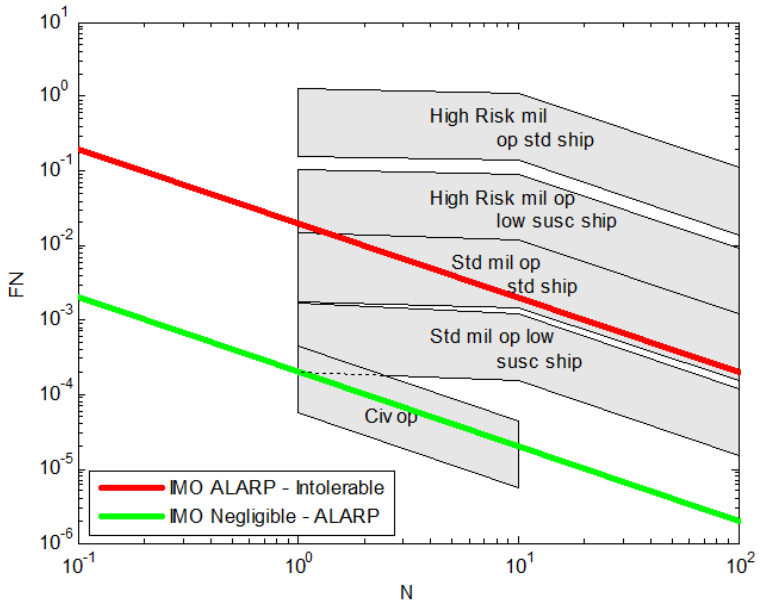


**Figure 12.** F-N diagram for the magnitude of fire risk given different types of operations. The data are calculated according to equation 1 and the data in Paper V. The IMO civilian as Low As Reasonable Practicable (ALARP) region developed from IMO (2000a) included as reference.

Based on Figure 12, when standard military operations using low-susceptibility ships are compared with high-risk operations using a standard ship, the greatest uncertainties (possible variations in risk) are associated with the operator's choices in terms of ship susceptibility and types of operation. Therefore, even if a ship fulfils its fire requirements, the fire risk can be unnecessarily high if the relationship among operation, design and risk is not understood.

Based on Equation 3, risk controls must be analysed with respect to susceptibility, vulnerability and recoverability; the total effect of these aspects must be understood to evaluate military survivability. Fire risk cannot be analysed without a general analysis of a ship's susceptibility and vulnerability with respect to relevant threats, which indicates that the analysis depends on relevant operational scenarios. Physical descriptions of fire depend on ship specifications and in the same operational scenario, the fire probability will vary between ship concepts due to differences in ship tactics, susceptibility and vulnerability. Different design concepts will also require different passive and active fire protection depending on the differences in the design and how it is manned.

Firefighting is the most important aspect for reducing the probability of catastrophic consequences from complicated ignition cases because built-in protection is insufficient to stop the escalation of a fire. This exemplifies the need for procedural safeguards, as discussed in Section 5.1.1. Therefore, application example 3 shows that without calculating the risk it is not possible to compare operational alternatives or to understand the importance of firefighting.

## 6.4 A quantitative approach supports a qualitative discussion

Risk analysis can be qualitative, but quantitative assessment is needed if the result should be able to update, validate or compare to risk acceptance criteria (Papers III-V, Liwång et al. (2014) and Liwång et al. (2015)). Quantitative analysis is also a

prerequisite for stringent estimates of probabilities and consequences, a basis for *shared* risk awareness (a topic further discussed in Paper III).

It is not possible to perform the three exemplified analyses presented in Sections 6.1 to 6.3 without a quantitative approach. However, the examples also show that an extensive amount of qualitative knowledge is needed to create the system/scenario, as exemplified in Figures 9 and 10.

Stringent scenario definition and unambiguous documented inputs and uncertainties are possible with a quantitative approach. The approach that facilitates the following:

- Structured use of easily measurable aspects (data) in the analysis, which reduces the aspects that need to be analysed and removes unrealistic consequences.
- Definition and analysis of uncertainties. For most realistic scenarios, without such an analysis it is impossible to judge which uncertainties are problematic and which may be ignored.
- Critical and objective examination of the analysis.
- Knowledge transfer to fleet management, on-board tactics and crew training.
- An update of the analysis if more data are acquired or more knowledge about the system is obtained (i.e., it is easy to identify what must be changed, and the effect of the change is automatic).

Quantitative aspects that can be clearly defined (as exemplified in Figures 8 and 9) reduce scenario alternatives and therefore decrease the work needed (see, e.g., the discussion of skiff speed in waves in Paper III). A quantitative approach also quantifies important aspects, such as available time for counter measures, which can be used, e.g., in training to create relevant readiness (Paper II). Therefore, by using a quantitative approach, naval administrators can qualitatively and quantitatively explain the rationality behind the chosen scenarios.

The result of the three examples above and highlighted in the interviews performed as a part of Application example 1 above show that the following:

A combination of graphical illustration and quantitative output 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 in the decision-making process.

Therefore, risk analysis is a part of an operations knowledge system, and its quantitative aspects guarantee unambiguous transfer of knowledge.

However, the interviews within this study also make it clear that the proposed method requires more work than what is put into the current analysis methods.

*"This thesis would not have been possible without a broad approach and support from research colleagues with different scientific perspectives, naval experts from the Royal Swedish Navy and ship owners' safety, security and operation managers."*

The author of this thesis about 40 pages earlier (Preface, page iii).

# 7 Summary of the work in the appended papers

## 7.1 Paper I

The aim of Paper I was to investigate and describe the effects of the NSC (NATO 2010b) 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 minimise the effects of attacks, two aspects of design alternatives affecting technology, tactics and manning, according to Figure 13. The two cases were chosen so that they would 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.

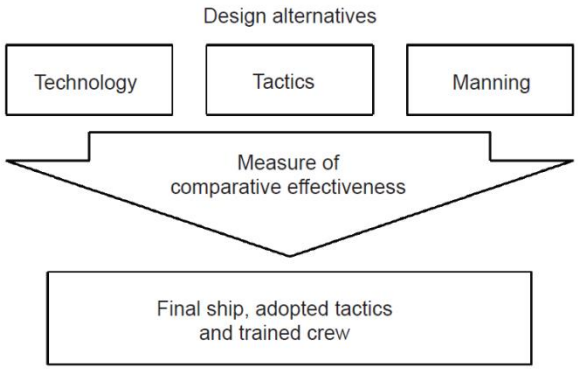


**Figure 13.** Measure of comparative effectiveness to support decisions related to design, construction and operation.

The NSC was compared with the types of measures called for in the two cases to determine how the code directly and indirectly 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 results in Paper I. The first area,

formal regulations, was analysed for each case separately and the two other areas were analysed for the two cases together.

Paper I, therefore, unveils the imbalance between traditional maritime safety and security and examines demands on the security risk management process in relation to a ship's survivability. Paper I concludes that to be able to incorporate survivability and ship security into the understanding of the overall performance of a ship, a risk-knowledge model, as one of several important measures of comparative effectiveness according to Figure 13, is needed.

## 7.2 Paper II

In Paper II, a probabilistic approach is used to investigate and describe how, based on a probabilistic risk assessment procedure, the concept of a ship's operation can be transformed into relevant safety scenarios. The scenarios should be possible to use in evaluating 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 to enhance design decision making. Military operational research, specifically related to modelling military systems, is described to ensure that safety scenarios effectively model military operations.

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. The objective of the model is to use the concept of operation to identify scenarios that relate to accident categories with major risk potential and to assess the probability of such scenarios. The model is a formalised procedure of incident quantification to support the definition of probability-based safety scenarios. The resulting scenarios can 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 are not new, but the results must be aggregated and handled so that they are consistent with probabilistic risk assessment.

The study shows that simulating tactical tasks makes it possible to quantify and analyse 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 14, which calculates the cumulative frequency of available time for counter measures for different situations. This will guide experts to more ship-specific probability functions than would have been the case if the experts had based safety

scenarios on experience alone. Therefore, the simulation can assist in a process that otherwise relied completely on expert judgment.

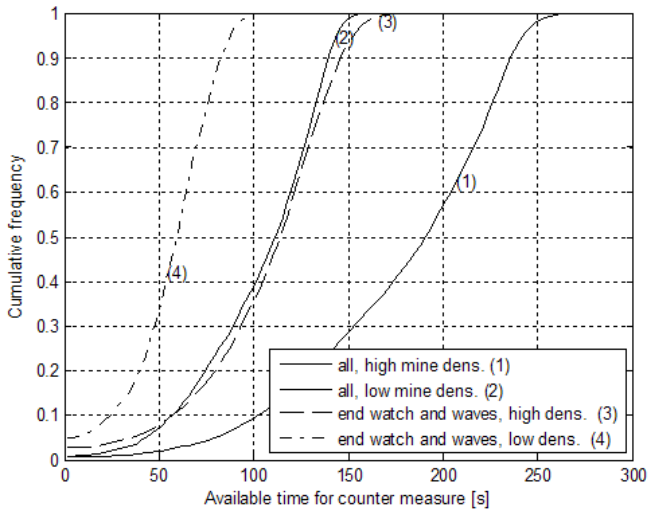


**Figure 14.** Cumulative frequency of available time for counter measure. 1,000,000 simulated events. From the figure, it is clear that the combination of end of watch and waves combine to reduce the available time, and by how much.

## 7.3 Paper III

In Paper III, the ship security assessment of the ISPS code was reviewed from a broader perspective, making use of security research and experience from military force protection and methodological lessons learned from maritime probabilistic risk assessment. The study had two primary objectives: to explore the possibilities and conduct quantified and more thorough ship security risk analysis than that described in the ISPS code and its guidelines and to examine and evaluate the extent to which this more detailed analysis increases ship security.

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

Event tree methodology was used to model and analyse both the possible consequences and the probabilities of an attack. The inductive event tree was used because a pirate attack has well-defined chronological steps illustrated by the sequences of the event tree.

Collected data were used to develop models and calculate probabilities for the event tree. The calculations are simulations representing subsets of the scenario with influences according to influence diagrams. Throughout the analysis, the results of the

important role played by analysis in describing the interaction between pirates' characteristics and ships' vulnerability. Figures 15, 16 and 17 illustrate the three different areas and types of analysis performed: Monte Carlo simulations (Figure 15), analytic probability calculations (Figure 16), and calculating probability using influence diagrams (Figure 17).

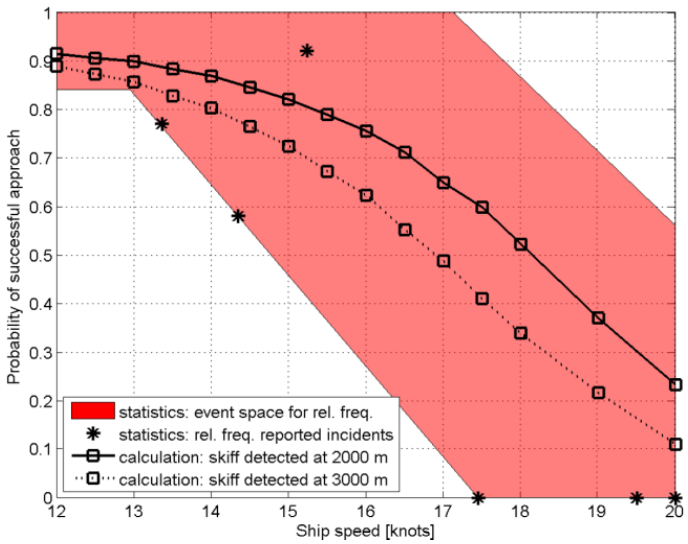


**Figure 15.** Quantitative output from the analysis in Paper III in the form of calculated probability of successful approach as a function of ship speed and skiff detection distance.

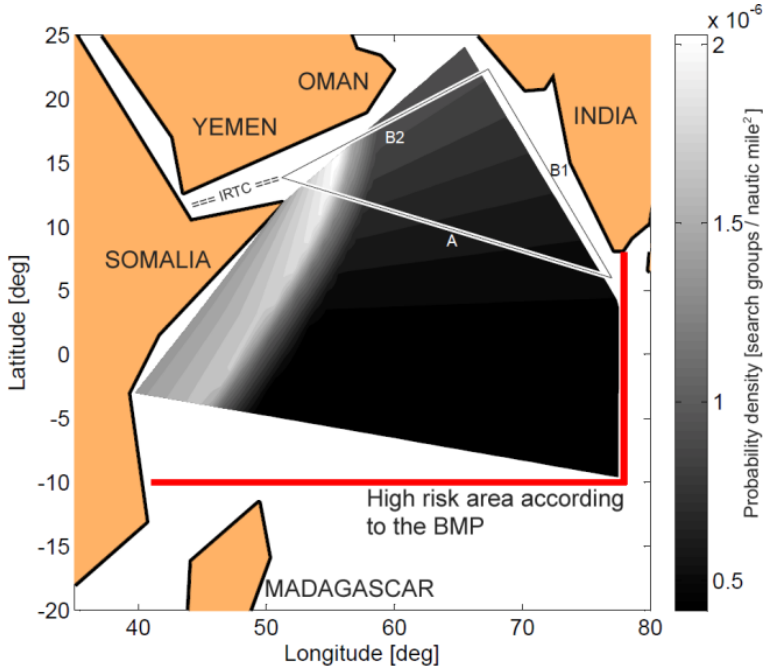


**Figure 16.** Quantitative output from the analysis in Paper III in the form of calculated probability density functions for pirate-search groups on the Indian Ocean.

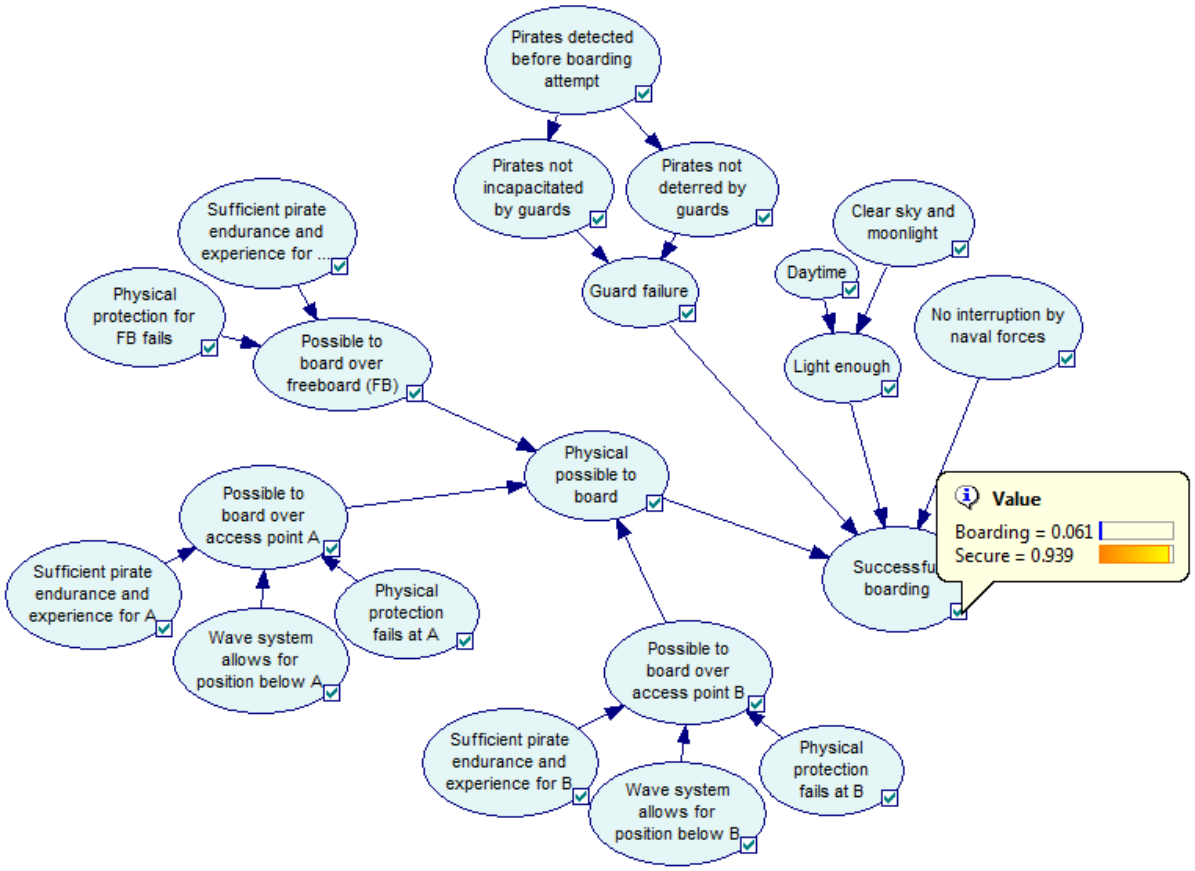


**Figure 17.** Influence diagram for assessing and comparing probability of successful boarding.

According to the interviews conducted, the combination of graphical illustration and quantitative output not only calculates probabilities and consequences but also enables a qualitative discussion on causes and measures not possible solely on a qualitative analysis. In areas in which it is possible to compare the calculation results of the performed analysis with incident 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 15 (and also Figure 8).

## 7.4 Paper IV

The aim of Paper IV was to examine how risk control options related to survivability, redundancy and technical endurance can be linked to the operational risk in a patrol and surveillance scenario. The assessment is intended to support the ship-design decision-making process and to facilitate a balanced ship design that is well suited for the intended task.

The study examined a generic OPV and used descriptions of ship design solutions such as damage stability and hull strength for survivability and redundancy. According to Figure 10 the ship operation, including the actions of the threat, was modelled using a influence diagram describing the scenario and dependency among different influences. The threat and ship were described with expert data collected from subject matter experts and include both aleatory and epistemic uncertainties. The approach included an analysis of parameter uncertainty and uncertainty propagation using both Monte Carlo analysis and numerical derivative analysis.

The results show that it is possible to link the performance of specific ship design features to operational risk. The analysis also shows that dependency among different design features and influences is high such that it is important to implement a method that accommodates these dependencies. The ability to propagate epistemic uncertainties through the model is important to understand how uncertainty in the input affects the output. As seen in Figure 10, the output uncertainty for the studied scenario is small relative to the input uncertainty. The numerical derivative analysis effectively estimates the sensitivity of the output for each uncertain input parameter. Therefore, the study shows that linking different ship design features to aspects such as survivability, redundancy and technical endurance to the operational risk gives important information to the ship design decision-making process.

Table 4 lists the ten highest $\partial y/\partial x_i$ for each examined output (target). As seen in Table 4, there each target is associated with a few variables that are of extra-high importance. In particular, for influence 18, the first three variables are all more than five times higher than the derivative for the fourth variable. However, the high effect variables (with high value for the derivative) are not the same for the three targets and are spread across the influence diagram. Only one variable, $x_1$ defining the ship activity, is in the top ten for all three influences.

**Table 4.** The ten variables with the highest effect on the output for each target, not considering the level of uncertainty for the variables.

| Rank | Effect on crew (s17, state 1) | | Can float (s18, state 1) | | Can move (s19, state 1) | |
|---|---|---|---|---|---|---|
| (importance) | Variable | $\partial y/\partial x_i$ | Variable | $\partial y/\partial x_i$ | Variable | $\partial y/\partial x_i$ |
| 1 | x5.1 | 0.129 | x55.1 | 0.272 | x61.1 | 0.125 |
| 2 | x1.1 | 0.122 | x57.1 | 0.136 | x40.1 | 0.065 |
| 3 | x18.1 | 0.115 | x59.1 | 0.108 | x50.1 | 0.062 |
| 4 | x2.3 | 0.102 | x35.4 | 0.020 | x53.1 | 0.061 |
| 5 | x2.1 | 0.097 | x35.1 | 0.012 | x5.1 | 0.059 |
| 6 | x12.1 | 0.080 | x56.1 | 0.010 | x1.1 | 0.053 |
| 7 | x16.1 | 0.079 | x35.2 | 0.009 | x18.1 | 0.053 |
| 8 | x22.1 | 0.072 | x10.4 | 0.007 | x43.1 | 0.051 |
| 9 | x3.3 | 0.068 | x34.4 | 0.007 | x2.3 | 0.049 |
| 10 | x3.1 | 0.065 | x1.2 | 0.006 | x8.3 | 0.045 |

It is also noteworthy that the variable with the second-highest uncertainty (variable $x_5$, which describes the threat capability) is the variable with the highest effect on influence 17 and the fifth most important variable for influence 19.

Given the high effect of $x_5$ on influences 17 and 19 and the high uncertainty for $x_5$, it is important to attempt to reduce the uncertainty of $x_5$ because doing so will have a substantial effect on the uncertainty for influences 17 and 19.

## 7.5 Paper V

The purpose of Paper V was to describe and investigate the conditions for a risk-based approach to ship fire survivability that can serve as a link between probabilistic survivability theory and the selection of survivability measures. The aim was to suggest key aspects for a risk-based methodology.

To aid in the analysis, the study proposes cause-and-effect models, as shown in Figure 18, for the fire risk analysis and discusses the fire risk contribution from different ignition types. The analysis shows that the reliability and validity of identifying fire

scenarios depends on a qualitative and outward-focused analysis of the ship's future and the reliability and validity of the analysis of fire-case consequences depends on the specific data and descriptions used. For example, the magnitude of the fire risk can drastically change as a result of operational choices (or unclear operational conditions).

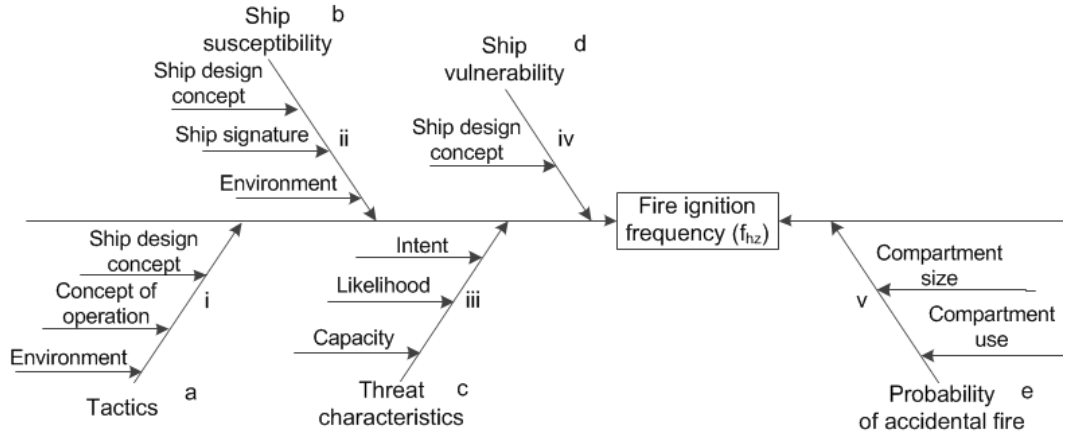


**Figure 18.** The proposed cause-and-effect model describes contributing factors to fire ignition, i.e. describes for example which design aspects affect the probability of a fire ignition. The model is used in Paper V to guide the analysis.

The study concludes that the analysis must be based on an understanding of the operational conditions. Subsequently, civilian risk-based approaches for fire risk are too limited because the approaches do not capture either aspects or the intended operation of ship design. Moreover, normally military vulnerability tools lack this ability. However, based on a stringent fire-ignition analysis, including a definition of the intended operation, ship design concept and threat civilian methods and tools can be used to assess the consequences.

Predictably, the risk contribution from fire onboard naval ships is high compared to allowable levels for civilian operations, especially for high-risk operations (Figure 12). This means that there are also societal reasons for working with fire risk on naval vessels, and Figure 12 shows that the focus should be on incidents with potentially high consequences. From Figure 12, it can also be seen that the greatest uncertainties (possible variation in risk) relate to the operator's choices in terms of ship susceptibility and operation types. Therefore, even if a ship fulfils fire requirements, fire risk can be unnecessary high if the relationships among operation, design and risk are not understood.

*"Risk is not a constant, measurable, concrete entity."*

The International Association of Classification Societies' words of caution in their A Guide to Risk Assessment in Ship Operations (IACS 2012).

# 8 Discussion

The aim of this thesis is to improve security decision support by defining an approach to ship security analysis. The approach should be systematic and should give the decision maker an appropriate picture of the risks. Thus, the overarching research question for this thesis is (from page 4) as follows:

> What characterises a decision-support approach that increases ship security by translating knowledge into a suitable description of the risks and promotes a conscious risk-taking?

Papers I through V study ship operations with threats beyond the typical safety hazards. Such threats include a military threat to naval vessels (Papers I, II, IV and V) and the security threat posed by pirates to commercial vessels (Paper III). In such operations, the security threat must be considered when making decisions.

In the previous sections, the performed work and the research questions are discussed from different perspectives. The aim of this section to join these to one more holistic perspective, i.e. the characteristics of the focused approach.

When validating approach development focus must be on the usefulness of the approach in relation to purpose of the approach and if the usefulness can be linked to applying the method beyond the studied areas (Pedersen et al. 2000). Therefore, the performed studies examine six different application areas with the aim of investigating suitable characteristics of a risk-based approach in different ship security areas. Different aspects of ship security must be studied to make general statements on the usefulness of the approaches. If a more narrow research focus had been chosen in which only one area, such as piracy attacks on civilian ships or firing on naval vessels, had been studied, then it is likely that the results with respect to risk-analysis methods and tools could have been more concrete. However, it would not be possible, based on such research, to make general conclusions on an approach for risk-based ship security. To complement the primary discussion on the usefulness of the approach the appended

papers has also, where possible, validated the output against statistics. However, this is typically only possible for civilian scenarios or military operations under civilian conditions.

In relation to quantitative validation, the results of Paper III and Paper V have been compared to available statistics and the level of risk accepted under civilian conditions respectively. The quantitative outputs have showed agreement with civilian statistics and the studied approach and models have been concluded to be able to explain central aspects of how the incidents lead to risk. However, the primary focus of Papers II-V has been to test and discuss the usefulness of the knowledge gained from the studies. Therefore, the conclusions made, in the appended papers and the thesis, focus on the usefulness (in risk management) of the qualitative aspects of the model output rather than on the quantitative output.

Based on the results of Paper I and II, the thesis only discussed risk-based approaches. There is no obvious alternative security measure. In civilian shipping and military planning, *risk* is the dominating measure discussed. However, in military operational research and applied operational analysis, there are approaches that directly assess system reliability or operational effectiveness. i.e., which analyse the total effect (gain and risk) of the solution or system without explicitly assessing the risk. Such an analysis has not been explicitly studied in this thesis. To some extent, analysing reliability is based on the same probabilistic approaches as risk analysis and therefore, some results of this thesis could apply not only to reliability analysis but also to probabilistic analysis of operational effectiveness.

The method and tool selection for this work has primarily been based on the central aspects of the approach and especially to choose tools that are well established in traditional maritime safety work and proven to support risk communication. Therefore, the transparency of the tools has been prioritized over mathematical effectiveness. Subsequently, the thesis includes no extensive literature study on potential methods and tools. Each of the appended papers however discuss the specific tool selection based the respective needs for that study. Many suitable methods and tools are therefore left untested and uncommented.

It is found that neither safety nor security can be reduced only to the question of whether the ship fulfils safety and military survivability requirements. It is about securing core values such as lives and freedom of action. Therefore, the focus must be on whether the operational risk is acceptable. Consequently, operational risk must be assessed and communicated to decision makers and others involved within the design process and operation. The studies in this thesis have shown that a risk analysis that unambiguously can treat *quantitative* data has the following qualities:

- It is an important tool for integrating safety and security and explicit risk acceptance levels.
- It is possible to support with both quantitative data and system knowledge collected from experts,
- It is crucial for understanding the causality of incidents,
- It is fully compatible with the ambition to open and structurally work with both uncertainties and present uncertainties as part of the decision support, and

– It is possible to connect to military survivability theory and use in a military risk assessment to assist in survivability design.

However, the study also shows that the reliability and validity of identifying security scenarios depends on a *qualitative* and outward-focused analysis of the ship's future. The reliability and validity of the analysis of incident consequences depends on the specific data and descriptions of the ship used. Therefore, the analysis must be based on an understanding of the operational conditions. Subsequently, the civilian risk-based approaches to risk analysis are not always applicable to naval ships because they does not include effects on the incident likelihood of the ship design or its intended operation. Furthermore, military vulnerability tools lack this ability. However, when incidents have been defined, civilian methods and tools can be used to assess the consequences if the ship specifications are suitable for naval ships.

Moreover, the studies show that the security risk management is not straightforward and that existing guidelines are inadequate to guarantee a relevant outcome of the risk analysis. Successful application requires not only an understanding beyond today's guidelines but also greater effort into the analysis than is typically done today. The quantitative perspective of the analysis is crucial, but without qualitative support, it is ineffective. The greatest challenges in the analysis are qualitative, e.g., how to capture qualitative aspects of the operation in the scenario and system definition.

Summarising the results with respect to a security decision-support approach, it is therefore found that an approach should be characterised by the following requirement levels:

**Level 0, combining quantitative and qualitative aspects:** Adhering to research, knowledge, methods and tools related to maritime safety are necessary but not sufficient to guarantee a suitable maritime security analysis. A security risk analysis requires a more rigorous scenario definition and knowledge collection. Identifying and defining scenarios must have a qualitative and outward-focused approach to the ship's operational environment, whereas the analysis of risk levels requires a combination of a qualitative and quantitative approach focused on the ship itself as a socio-technological system.

**Level 1, specific and in line with the ship's concept of operation:** Generally, the approach, methods and tools for security risk analysis must be applied more specifically than for maritime safety. This is a result of the limited availability of statistics, dependence on operational specifications, epistemic uncertainty and the intent of the threat. Consequently, the analysis must be performed using methods that are more rigorous and on a more specific level. This also leads to the conclusion that the analysis must be performed by organisations that usually do not address other safety aspects (because traditionally, those aspects are managed on a more generic level).

**Level 2, recognising the effects of risk perception:** The manner in which risk controls are chosen, implemented, explained and perceived (by one's own organisation and threats) will affect the effectiveness of controls. The understanding of these effects is crucial but also poses a genuine uncertainty.

The challenges presented by Levels 0 and 1 are possible to mitigate with a well-defined implementation of a ship security approach in an organisation. This is because a ship security risk analysis has been shown to explain how different protective measures lead to reduced risk. Therefore, the analysis supports conscious risk taking. However, the genuine uncertainty as a result of risk perception can never be resolved but instead, must be recognised and should never be hidden by the approach chosen. Level 2 also imposes requirements in terms of openness (within the organisation) about activities within Levels 0 and 1, an openness that contradicts the traditional, secretive approach to security.

It is important to note that the approach proposed here strives to explain and compare future risks. This knowledge can be used in many different ways both before and after design decisions are made. For example, using risk as a measure of security does not contradict a resilient perspective. Resilience is a question of how security is achieved, not how it is measured. Another similar example is robustness, in which the risk in different possible futures, or surprises, must be assessed and compared. However, both resilience and robustness require a risk description that includes uncertainties. Uncertainties are needed because parts of the decisions must be based on different risk uncertainty ranges of the alternatives, not only on the respective expected risk levels. Based on such information, it is then up to the decision-maker to decide how to use the risk knowledge. Therefore, risk is not a fully measurable and concrete entity, but it can be a useful measure for presenting and communicating important and possibly dangerous aspects of operations.

Specifically for the three examples in Section 1.2 the proposed approach and findings lead to that, an increased shared risk understanding is needed, specifically regarding the scope and applicability of the organization's risk management. Such understanding can then reduce frustrating disagreement and sometimes avoid severe consequences. The crew choosing to stop because of shots from pirates could probably have been avoided if the crew had been more involved in the risk management. The result from a study as the one exemplified in Paper III shows how effective speed is as a piracy protection. In the example with the IED attack on a Swedish military vehicle in Afghanistan especially an understanding of the importance of communicating and agreeing on the relevant consequences and scenarios to study would have reduced the difference in understanding in relation to threats, vulnerabilities and risks (Section 5.3.1). This would probably have made the organisation more effective, but would not necessarily have changed the outcome of the incident. Paper IV show that the organization around President Obama should have a common approach for discussing uncertainties as an aspect of the threat understanding, as such uncertainties cannot be avoided.

How to define and use risk criteria is not included in this study. However, it is clear from the work that implicit security risk criteria are important for risk management. Sometimes, general safety criteria can be used, but especially for military risk management, they are not sufficient. In many military situations, the operational risks are central, and risk-management decisions cannot be based on, e.g., an FN diagram. The criteria must also include a view of allowable uncertainties. Another challenge related to risk criteria is that different risk criteria generate different decisions. One design alternative may give the lowest short-term expected fatalities, another gives the lowest operational risk and a third gives the lowest long-term expected fatalities.

Finally, it is also important to acknowledge that using security risk-knowledge models in ship design and military planning also imposes new challenges and demands on decision makers, but also on how to perform approval and control.

# 9 Conclusions

The aim of this thesis is to improve security decision support by defining what characterises a decision-support approach that translates knowledge into a suitable description of the risks.

The approach, as well as methods and tools, are selected as a result of the focus on risk understanding. This thesis finds that a well-designed risk-based approach brings the procedure and results of ship security analysis into the open and therefore enables criticism, improvements and shared risk knowledge, which are not possible with less-structured methods. Risk is not a fully measurable and concrete entity, but it can be a useful tool for presenting and communicating important and possibly dangerous aspects of operations. The risk-based approach, therefore, enables a discussion about probabilities and facilitates feedback to experts on their assessments, which will lead to better assessments in the future. The characteristics of a risk-based ship security approach described below are relevant both as a scientific contribution and in relation to security risk management in military and civilian organisations.

In conclusion, the methods and tools developed for safety risk analysis also are generally valid for security risk analysis, but not without specific considerations. A security risk analysis requires a more rigorous scenario definition and knowledge collection. The process for identifying and defining scenarios must have a qualitative and outward-focused approach of the ship's operational environment, whereas an analysis of risk levels requires a combination of a qualitative and quantitative approach focused on the ship itself as a socio-technological system.

Relevant historical information is often limited and expert judgment is needed to define scenarios. Expert judgement can collect a qualitative understanding of important aspects of the studied socio-technological system, but also introduces uncertainties.

When analysing the threat and defining the scenario there must be a focus on the threat's modus operandi, how it can lead to damage to the ship and whether the intended ship tasks limit the number of relevant modus operandi. In addition, it is important to question how the likelihood of different attack modus operandi is affected by ship tasks and ship susceptibility. The scenario must be developed for specific ship concepts and concept of operation and a change in a ship or operation concept can change the probability of threat encounters and/or the effects of an attack.

A successful analysis that correctly compares military survivability between alternative designs must at least include and focus on the relationship between design choices and the probability of incidents, such as the following: a hit; the state of the ship at the time of incident (which varies for the same scenario among concepts due to differences in ship tactics, ship susceptibility and ship vulnerability); complicated incidents with potentially severe consequences; qualitative safety culture and human factor aspects; and models and data suitable for the ship in question.

It is also concluded that that the approach should be quantitative to facilitate the structured use of measurable aspects (data) in the analysis, which reduces the aspects that must be analysed: the definition and analysis of uncertainties; critical and objective examination of the analysis; knowledge transfer to fleet management, on-board tactics and crew training; and an update of the analysis if more data is acquired or more knowledge about the system is gained. In particular, as the security of a system relies on system robustness, the uncertainty treatment and uncertainty communication offered by the quantitative approach is central. Without this understanding of how input and model uncertainty affects risk estimates, the robustness of different alternatives cannot be discussed. This study also shows that ignoring known uncertainties, by, e.g., basing a risk analysis on expected values, can result in erroneous risk values. Therefore, the risk analysis should be seen as part of an operations knowledge system and the quantitative aspects guarantee unambiguous transfer of knowledge.

Challenges concerning selection of method and tools and knowledge collection (defined as Levels 0 and 1 in Section 8) can be dealt with, at least in theory, by a well-defined implementation of a ship-security approach in an organisation. This because a ship security risk-analysis has been shown to be able to explain how different protective measures lead to risk reduction. Therefore, the analysis supports conscious risk taking. However, the result of the genuine uncertainty caused by risk perception can never be resolved, but must be recognised and should never be hidden by the approach chosen. The need for a shared risk picture also imposes requirements in terms of openness (within the organisation) on risk-management activities, an openness that contradicts the traditionally secretive approach to security.

*"It is hoped that cross-disciplinary analysis of the perception and impact of the security-risk will stimulate thinking on appropriate tools and analytical frameworks for enhancing port and maritime security. In so doing, it may be possible to develop new approaches to security assessment and management."*

K. Bichou at the Centre for Transport studies, Imperial College London, in the Conclusions to *Security and risk-based models in shipping and ports. Review and critical analysis* (Bichou 2008).

# 10 Future work

Many institutions worldwide have spent several years on maritime safety research; the area of maritime security is much less mature. Subsequently, the understanding of how threats lead to security risks is still limited and there is an urgent need for future work.

Based on the current results, the aim in coming years is to deepen the analysis completed, to be able to verify the results and to validate the proposed approach more thoroughly.

Despite a lack of historical data and difficulties in performing realistic experiments, 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 the limited availability of data, future work must include theoretical method development. 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 for which data is either 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,
- theoretical and methodical studies on the concept of robustness, including how robustness can be described, analysed and implemented in relation to security and military survivability,

- development of ship-security simulations and verification methods, and
- how and to what extent the proposed methods and tools can be utilised in analysing reliability (rather than risk).

Such studies would be able to give specific recommendations on how ship risk analysis should be planned, performed and used on ships.

**Applied method development on naval ships**

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

Studies of naval ships could give unique insight into the following issues:

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

The studies can be performed on specific survivability aspects, such as fire risk, and connect those results to the ships' operational performance. However, to correctly capture the operational performance, the research most likely should include war games and on-board experiments.

**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 scenarios, it is possible to perform a detailed security analysis and also to verify and validate the result. Studies could be performed on the following subjects:

- projects and incidents (such as case studies), in which the traditional safety perspective is challenged by novel or specific security considerations,
- the decision process itself in relation to risk-based analysis and risk perception, human factors and uncertainties,
- piracy in different regions, and testing how accurately the model can describe how the risk is affected by the threats intent and modus operandi,
- the ship and port interaction, and
- terrorist attacks and examining how conceptually different intent (terror) changes the conditions for analysis.

Research on civilian ships also would allow the study of which results should be presented and how they should be presented for risk evaluation and risk reduction to create effective risk management.

## References

Abrahamsson M (2002) Uncertainty in quantitative risk analysis - characterisation and methods of treatment. Lund University, Lund.

Akhtar MJ, Utne IB (2014) Human fatigue's effect on the risk of maritime groundings - A Bayesian Network modeling approach. Safety Science 62:427-440.

Amer M, Daim TU, Jetter A (2013) A review of scenario planning. Futures 46 (0):23-40.

Andrews JD, Moss TR (2002) Risk assessment. In: Reliability and risk assessment. Second edn. Professional Engineering Publishing Limited, London, pp 411-448.

Aven T (2009) Identification of safety and security critical systems and activities. Reliability Engineering & System Safety 94 (2):404-411.

Aven T, Krohn BS (2014) A new perspective on how to understand, assess and manage risk and the unforeseen. Reliability Engineering & System Safety 121 (0):1-10.

Bakx GCH, Richardson RAL (2013) Risk assessments at the Royal Netherlands Air Force: An explorative study. Journal of Risk Research 16 (5):595-611.

Ball RE, Calvano CN (1994) Establishing the fundamentals of a surface ship survivability design discipline. Naval Engineers Journal 106 (1):71-74.

Bang M (2014) Pitfalls in Military Quantitative Intelligence Analysis: Incident Reporting in a Low Intensity Conflict. Intelligence and National Security:1-25.

Beilock SL, Carr TH, MacMahon C, Starkes JL (2002) When paying attention becomes counterproductive: impact of divided versus skill-focused attention on novice and experienced performance of sensorimotor skills. Journal of Experimental Psychology: Applied 8 (1):6-16.

Bichou K (2008) Security and risk-based models in shipping and ports: review and critical analysis. Imperial College, London.

BIMCO (2013) Guidelines on Ship and Voyage Specific Risk Assessment (SVSRA). BIMCO, Bagsværd.

Boulougouris E, Papanikolaou A (2013) Risk-based design of naval combatants. Ocean Engineering 65:49-61.

Brown A, Mierzwicki T (2004) Risk metric for multi-objective design of naval ships. Naval Engineers Journal 116 (2):55-71.

Council of the European Union (2014) European Union maritime security strategy (11205/14). 24 June 2014 edn. Council of the European Union, Brussels.

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

DCDC (2011) British maritime doctrine, Joint doctrine publication 0-10. The Development, Concepts and Doctrine Centre, Ministry of Defence, United Kingdom, Shrivenham.

Deacon T, Amyotte PR, Khan FI, MacKinnon S (2013) A framework for human error analysis of offshore evacuations. Safety Science 51 (1):319-327.

Decision Systems Laboratory (2014) GeNIe & SMILE. <http://genie.sis.pitt.edu/>. University of Pittsburgh. Accessed 2014-01-01

Department of Defense (2007) A cooperative strategy for 21st century seapower. Department of Defense, Washington DC.

Department of the Army (2006) Composite risk management, FM 5-19 (FM 100-14). Headquarters Department of the Army, Washington DC.

Derbyshire J, Wright G (2014) Preparing for the future: Development of an 'antifragile' methodology that complements scenario planning by omitting causation. Technological Forecasting and Social Change 82:215-225.

DNV (2013) DNV Rules for classification of high speed, light craft and naval surface craft. Det Norske Veritas, Høvik.

Ellis J (2010) Undeclared dangerous goods - risk implications for maritime transport. WMU Journal of Maritime Affairs 9 (1):5-27.

Ewell JJ, Hunt IAJ (1995) Sharpening the combat edge: the use of analysis to reinforce military judgment. Department of the Army, Washington DC.

Fisk AD, Schneider W (1984) Memory as a function of attention, level of processing, and automatization. Journal of Experimental Psychology: Learning, Memory, and Cognition 10 (2):181-197.

Friedman JA (2014) The use of probability in military decision making. September 3 edn. Dartmouth College, Dartmouth.

Friedman JA, Zeckhauser R (2014) Handling and Mishandling Estimative Probability: Likelihood, Confidence, and the Search for Bin Laden. Intelligence and National Security:1-23.

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

Frosdick S (1997) The techniques of risk analysis are insufficient in themselves. Disaster Prevention and Management 6 (3):165-177.

Gershuny J (1976) The choice of scenarios. Futures 8 (6):496-508.

Giachetti RE (2010) Enterprise analysis and design methodology. In: Design of enterprise systems. CRC Press, Boca Raton, pp 119-146.

Grech MR, Horberry TJ, Koester T (2008) Organization, society and culture. In: Human factors in the maritime domain. CRC Press, Boca Raton.

Hansson SO (1993) The false promise of risk analysis. Ratio-New Series 6 (1):16-26.

Harney RC (2010) Broadening the Trade Space in Designing for Warship Survivability. Naval Engineers Journal 122 (1):49-63.

Hughes WP (1995) A Salvo Model of Warships in Missile Combat used to Evaluate their Staying Power. Naval Research Logistics 42 (2):267-289.

Hughes WP (2000) Six cornerstones. In: Fleet tactics and coastal combat. 2 edn. Naval Institute Press, Annapolis, pp 17-44.

IACS (2012) A Guide to Risk Assessment in Ship Operations. International Association of Classification Societies, London.

IMB (1993-2014) Yearly reports, Piracy and armed robbery against ships for the years 1992-2013. ICC International Maritime Bureau, London.

IMB (2011) Piracy and armed robbery against ships, report for the period 1 January - 31 December 2010. ICC International Maritime Bureau, London.

IMB (2012) Piracy and armed robbery against ships, report for the period 1 January - 31 December 2011. ICC International Maritime Bureau, London.

IMB (2013) Piracy and armed robbery against ships, report for the period 1 January - 31 December 2012. ICC International Maritime Bureau, London.

IMO (1994) International code of safety for high-speed craft (HSC Code, MSC.36 (63)). International Maritime Organization, London.

IMO (2000a) Formal safety assessment, Decision parameters including risk acceptance criteria, Submitted by Norway (MSC 72/16). International Maritime Organization, London.

IMO (2000b) Safety measures for high-speed craft (Safety of Life at Sea, Chapter X). International Maritime Organization, London.

IMO (2002) The International Ship and Port Facilities Security (ISPS) code (Safety of Life at Sea, Chapter XI-2). International Maritime Organization, London.

IMO (2009) Formal safety assessment - dangerous goods transport with open-top containerships, submitted by Denmark (MSC 87/INF.2). International Maritime Organization, London.

IMO (2013) Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process (MSC-MEPC.2/Circ.12). International Maritime Organization, London.

Ingelstam L (2012) Inledning och problemställning. In: System, Att tänka över samhälle och teknik [In Swedish]. Swedish Energy Agency, Eskilstuna, pp 12-33.

Jaiswal NK (1997) Military operations research: Quantitative decision making. International series in operations research & management science. Kluwer Academic Publishers, Norwell.

Johnson CW (2007) The paradoxes of military risk assessment. Paper presented at the the 25th International Systems Safety Conference, Baltimore, USA,

Kahneman D (2011) Availability, emotion, and risk. In: Thinking, fast and slow. Penguin books, London, pp 137-145.

Kim KS, Lee JH (2012) Simplified vulnerability assessment procedure for a warship based on the vulnerable area approach. Journal of Mechanical Science and Technology 26 (7):2171-2181.

King A (2013) Maritime threat - an overview. NATO Allied Command Transformation counter improvised explosive device Integrated project team.

Kirkwood CW, Pollock SM (1982) Multiple attribute scenarios, bounded probabilities, and threats of nuclear theft. Futures 14 (6):545-553.

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. The Nautical Institute, London.

Law NG (2011) Integrated helicopter survivability. Cranfield University, Cranfield.

Liwång H, Ericson M, Bang M (2014) An examination of the implementation of risk based approaches in military operations. Journal of Military Studies 5 (2).

Liwång H, Pejlert L, Miller S, Gustavsson J-E (2001) Management of high speed machinery signatures to meet stealth requirement in the Royal Swedish Navy Visby Class Corvette (YS2000). In: ASME Turbo Expo 2001: Power for Land, Sea, and Air, New Orleans, 4-7 June 2001. ASME.

Liwång H, Ringsberg JW (2013) Ship security analysis: the effect of ship speed and effective lookout. In: ASME 32nd International Conference on Ocean, Offshore and Arctic Engineering, Vol 2A: Structures, Safety and Reliability, Nantes, 9-14 June 2013. ASME.

Liwång H, Sörenson K, Österman C (2015) Ship security challenges in high risk areas: Manageable or insurmountable? WMU Journal of Maritime Affairs.

Marine Corps Institute (2002) Operational Risk Management, ORM 1-0. Headquarters Marine Corps, Washington DC.

McCue B (1990) U-boats in the Bay of Biscay : an essay in operations analysis. National Defense University Press, Washington DC.

McGeorge D, Høyning B (2002) Fire safety of naval vessels made of composite materials: Fire safety philosophies, ongoing research and state-of-the-art passive fire protection. In: RTO AVT Specialists' Meeting on Fire Safety and Survivability, Aalborg, 2002. NATO Research and Technology Organisation, pp 22.01-22.22.

McNaught (2005) Effectiveness of the International Ship and Port Facility Security (ISPS) code in addressing the maritime security threat. Geddes papers:89-100.

Meissner P, Wulf T (2013) Cognitive benefits of scenario planning: Its impact on biases and decision quality. Technological Forecasting and Social Change 80 (4):801-814.

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

MNE 7 (2012) Maritime security regime concept. Multinational Experiment 7.

Morse PM, Kimball GE (1998) Methods of operations research. The military operations research society, Alexandria.

Musharraf M, Hassan J, Khan F, Veitch B, MacKinnon S, Imtiaz S (2013) Human reliability assessment during offshore emergency conditions. Safety Science 59 (0):19-27.

Möller N, Hansson SO (2008) Principles of engineering safety: Risk and uncertainty reduction. Reliability Engineering & System Safety 93 (6):798-805.

NATO (2007) Allied joint doctrine for force protection, AJP-3.14. NATO Standardisation Agency, Brussels.

NATO (2008) Improving common security risk analysis, RTO-TR-IST-049. The Research and Technology Organisation (RTO) of NATO, Brussels.

NATO (2010a) Comprehensive operations planning directive, V1.0. NATO Supreme Headquarters Allied Power Europe, Brussels.

NATO (2010b) Naval ship code, ANEP 77. NATO Standardization Agency, Brussels.

NATO (2012) Survivability of small warships and auxiliary naval vessels. DRAFT edn. NATO AC/141 (MCG/6) SG/7.

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

Parker D, Lawrie M, Hudson P (2006) A framework for understanding the development of organisational safety culture. Safety Science 44 (6):551-562.

Paté-Cornell ME (1996) Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering & System Safety 54 (2–3):95-111.

Pawling R, Grandison A, Lohrmann P, Mermiris G, Pereira Dias C (2012) The development of modelling methods and interface tools supporting a risk based approach to fire safety in ship design. In: Bertram V (ed) International Conference on

Computer Applications and Information Technology in the Maritime Industries, Berlin, 2012.

Pedersen K, Emblemsvåg J, Bailey R, Allen JK, Mistree F Validating design methods & research: the validation square. In: 2000 ASME Design Engineering Technical Conference, Baltimore, Maryland, 10-14 September 2000. ASME.

Pedersen PT (2010) Review and application of ship collision and grounding analysis procedures. Marine Structures 23 (3):241-262.

Perry WL (2007) Linking systems performance and operational effectivness. In: Loerch AG, Rainey LB (eds) Methods for conducting military operational analysis Military Operations Research Society, Washington DC, pp 657-684.

Psarros G, Christiansen A, Skjong R, Gravir G (2011) On the success rates of maritime piracy attacks. Journal of Transportation Security 4 (4):309-335.

Ravn E (2012) A tool that makes the link between aids to navigation, traffic volume and the associated risk. Efficient, Safe and Sustainable Traffic at Sea. The Danish Maritime Safety Administration, Valby.

Reason J (2000) Safety paradoxes and safety culture. International Journal of Injury Control and Safety Promotion 7 (1):3-14.

Royal Navy (2014) Flag officer sea training. The Royal Navy, United Kingdom. http://www.royalnavy.mod.uk/The-Fleet/Naval-Command-Headquarters/Flag-Officer-Sea-Training. Accessed Mars 25th 2014.

Said MO (1995) Theory and practice of total ship survivability for ship design. Naval Engineers Journal 107 (4):191-203.

Schreuder M, Hogstrom P, Ringsberg JW, Johnson E, Janson CE (2011) A method for assessment of the survival time of a ship damaged by collision. Journal of Ship Research 55 (2):86-99.

Secretary of Defense (2012) Sustaining U.S. global leadership: Priorities for 21st century defense. The Secretary of Defense, USA, Washington DC.

Shachter RD (1986) Evaluating influence diagrams. Operations Research 34 (6):871-882.

Shachter RD (1988) Probabilistic inference and influence diagrams. Operations Research 36 (4):589-604.

Skjong R (2002) Risk acceptance criteria: current proposals and IMO position. Paper presented at the Surface transport technologies for sustainable development, Valencia, 4-6 June, 2002.

Skjong R (2009) Regulatory framework. In: Papanikolaou AD (ed) Risk-based ship design. Springer-Verlag, Berlin, pp 97-151.

Smith MD, Chamberlin CJ (1992) Effect of adding cognitively demanding tasks on soccer skill performance. Perceptual and Motor Skills 75:955-961.

Swedish Armed Forces (2009a) Försvarsmaktens gemensamma riskhanteringsmodell [In swedish]. Swedish Armed Forces, Stockholm.

Swedish Armed Forces (2009b) Handbok bedömning antagonistiska hot [In swedish]. Swedish Armed Forces, Stockholm.

Swedish Maritime Administration (2013) Årsredovisning 2012 [In Swedish]. The Swedish Maritime Administration, Stockholm.

U.S. Coast Guard (n.d.) Marine operations risk guide. The U.S. Coast Guard, Washington, D.C.

UKMTO (2011) Best management practices for protection against somalia based piracy (BMP4). Witherby Publishing Group Ltd, Edinburg.

University of Cincinnati (2004) Introduction to the principles of war and operations. University of Cincinnati, Cincinnati.

Washburn A, Kress M (2009) Game theory and wargames. In: Combat modeling. Springer, New York.

Vassalos D (2009) Risk-based ship design. In: Papanikolaou AD (ed) Risk-based ship design. Springer-Verlag, Berlin, pp 17-96.

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.

Yang YC (2011) Risk management of Taiwan's maritime supply chain security. Safety Science 49 (3):382-393.

Yang ZL, Wang J, Li KX (2013) Maritime safety analysis in retrospect. Maritime Policy & Management 40 (3):261-277.