WORLD MARITIME UNIVERSITY
Malmö, Sweden

A SELECTION AND COMPARISON OF RISK ASSESSMENT METHODS AND MODELS TO BE USED FOR THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE

By

FIDEL EDUARDO REYES MELENDEZ

Perú

A dissertation submitted to the World Maritime University in partial Fulfilment of the requirements for the award of the degree of

MASTER OF SCIENCE
in
MARITIME AFFAIRS

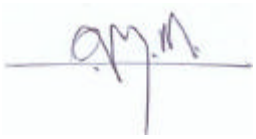
(Maritime Administration)

2004

DECLARATION

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

(Signature): 

(Date): 2004-08-27

Supervised by: Jens-Uwe Schröder
Assistant Professor
World Maritime University

Assessor: Jennifer Ketchum
Lecturer
Institution: World Maritime University

Co-assessor: R. Tallas
Institution:

ACKNOWLEDGEMENT

My special thanks to the Peruvian National Maritime Authority – Dirección General de Capitanías y Guardacostas – and the Peruvian Navy for granting me this unique opportunity to enrol at the World Maritime University.

I wish to thank to my dissertation supervisor, Dr. Ing. Jens-Uwe Schröder, for the of the research topic idea and for his excellent support, knowledge and guidance.

I wish to thank to the WMU Maritime Administration staff for their knowledge and permanent support on the achievement of the student's objectives. Thanks are due to Susan and Cecilia from the University Library for their kind assistance. Also, special thanks to Clive Cole, for his support during the ESSP.

I am thankful to my parents Fidel and Luz and my sisters Maria Elena and Marleni for being always close to me and for their unconditional support. Finally, my very deep gratitude to my wife Pilar and to my sons Carlos and Joaquin for being with me all this time and for permanently encourages my work.

Title of Dissertation: **A Selection and Comparison of risk assessment methods and models to be used for the International Ship and Port Facility Security Code**

Degree: **MSc**

ABSTRACT

The purpose of this study is the selection of risk assessment techniques commonly used for safety with the intention to evaluate whether their application on security assessments is feasible or not. For this purpose as a first step an overview of the concept of security risk is made in order to define their main characteristics and the features related to the most important maritime security issues. Additionally at this stage a general description of the new maritime security framework is done.

The current maritime security framework, mainly the ISPS Code, have been designed with a risk-based approach. In this sense an analysis of the concepts of risk and the common risk management and risk assessment methodologies used by the industry ashore are analysed in relation to security. The main factors that a security assessment should take into account are identified and placed in an initial framework.

The current approaches for security assessments developed by the United States Coast Guard and the Norwegian Shipowner's Association are analysed to identify their completeness in relation to the requirements of security assessment previously identified. Also, risk assessment techniques such as Hazard and Operability Studies, Failure Mode and Effect Analysis and Fault Tree Analysis, are analysed and their advantages and disadvantages with respect of their application to security assessment are highlighted.

Finally a new security framework based on the Formal Safety Assessment methodology is proposed and the implications of the application of the methodologies previously identified and the economical considerations of the implementation of security measures are analysed.

KEYWORDS: Risk Assessment, Ship Security Assessment, Port Facility Security Assessment, ISPS Code, Maritime Security, Risk Management.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIS	Automatic Identification System
ALARP	As low as reasonable and practicable
CSO	Company Security Officer
CSR	Continuous Synopsis Record
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
GAO	United States General Accounting Office
HAZOP	Hazard and Operability Studies
IMB	International Maritime Bureau
IMO	International Maritime Organization
ISM	International Safety Management Code
ISPS	International Ship and Port Facility Security Code
NSA	Norwegian Shiipowner's Association
PFSA	Port Facility Security Assessment
PFSP	Port Facility Security Plan
PRA	Probabilistic Risk Assessment
RCM	Risk Control Measure
RCO	Risk Control Option
RSO	Recognized Security Organization
SAS	Security Alert System
SOLAS	International Convention for the Safety of Life at Sea, 1974
SSA	Ship Security Assessment
SSP	Ship Security Plan
STCO	Security Risk Control Option.
SUA	International Convention for the Suppression of Unlawful Acts against the safety of navigation, 1988.
USCG	United States Coast Guard

CHAPTER 1 INTRODUCTION

The catastrophic events of September 11, 2001 promoted a different perception of the international community with respect to the security of transport. The fact that a mean of transportation can be used as a weapon was the spark for the maritime industry to think on the catastrophic consequences that a terrorist attack against a ship might cause to this industry in particular and to the international trade in general. It was in that sense that the International Maritime Organization (IMO) began the effort to develop a new maritime security framework with the purpose to guarantee that a standard of security is maintained on ships and port facilities at international level.

The new maritime security framework was introduced by IMO trough amendments to the International Convention for the Safety of Life at Sea 1974 which included the issue of the International Ship and Port Facility Security Code (ISPS). The objectives of this Code are, inter alia, to establish an international framework to detect security threats against ships and port facilities; to establish the respective roles and responsibilities within the international maritime community for ensuring maritime security; and, to provide a methodology for security assessments with the purpose to implement plans and procedures to react to changing security levels. The new regime incorporates a risk-based approach to manage maritime security.

In this sense one of the important tasks that ships and port facilities should carry out in compliance to the new maritime security framework is the ship or port facility security assessment. However, maritime security is a concept that is not familiar to the maritime community, save those problems concerning piracy, for which IMO has issue some recommendations and mainly addressed from the legal point of view but not from the physical or operational side.

The main problem of security assessment is the difficulty to assess security risks, especially due to the particular nature of some of them like terrorism which contrary to safety issues do not create patterns. Additionally maritime security issues like terrorism, piracy, stowaways, hijacking, etc are security threats that even though they could be predicted in some degree, the real fact is that there is not too much that a ship or port facility can do to eliminate or minimize those threats. However, what the ship or port facility can do is to improve their physical and operational security measures in order to be a more difficult target. Therefore, a clear methodology that considers all the particular aspects concerning the assessment of security is necessary and also the adequate techniques to perform the studies at an acceptable level of detail.

Two approaches were developed in the early stages of the implementation of the ISPS Code. One by the United States Coast Guard (USCG) with the NVIC 10-02 and the other by the Norwegian Ship Owners Association (NSA) with its "Guideline for Performing Ship Security Assessment". These two approaches give guidelines for the development of security assessments but more indicating what to do than how to do the study. That is why more detailed techniques, like those used in safety risk assessment, are necessary to perform security assessments in a more detailed, structured and systematic way.

The purpose of this dissertation is to select and compare risk assessment techniques like Hazard and Operability Studies, Failure Mode Effect Analysis and Fault Tree Analysis, commonly used for safety purposes, in order to identify their possible application on security assessments of ships and port facilities. For that purpose the general context of security will be explained and a security assessment framework, that takes into account the main issues a security assessment requires, are proposed as a reference for the application of the above mentioned techniques and the methodologies currently developed by the USCG and NSA.

The results of this study could be useful for those with the responsibility of performing security assessments. In this sense, this work could be a complementary tool to develop ship or port facility security assessments in a comprehensive,

structured and systematic way. Additionally, maritime administrations or designated authorities could use the framework and techniques proposed in this work as a reference for the evaluation of port facility security assessments performed by recognized organizations.

CHAPTER 2 MARITIME SECURITY

This chapter has three main objectives. Firstly it seeks to understand the concept of maritime security using for that purpose the well-known concept of maritime safety. Maritime Safety is and has been one of the most important tasks of the international maritime community through the International Maritime Organization (IMO), therefore analysing its main differences with maritime security will help us to find a more comprehensive meaning of this concept.

Secondly, the scope of maritime security and the main maritime security issues will be given through the analysis and a brief description of the security regulatory framework that deals with these issues. Maritime security issues like stowaways, theft, armed robbery against ships, hijacking, piracy or terrorism are addressed from the legal side in the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (the 1988 SUA Convention). It was not until the aftermath of 9/11 that new regulations were designed to address maritime security issues, but now with operational and technical requirements established through the International Convention for Safety of Life at Sea 1974 (SOLAS 74).

Thirdly, the main problems arising from the implementation of the new security framework are identified. In this sense the methodology for security assessments, established in the International Ship and Port facility Security Code (ISPS Code), will be analysed. In this process risk assessment techniques will also be identified taking into account those techniques that have been used mainly for safety assessments in different sectors of the industry, but not extensively for security issues.

2.1 Security and Safety

Maritime Safety is and has been by large the main preoccupation of the international maritime community through the International Maritime Organization (IMO). The main regulatory framework created by IMO is related to maritime safety. These regulations focus in what Kuo (1998) considers the main areas of maritime safety: Engineering, Operations, Management and the Human Element.[1] Therefore we can see that these regulations establish measures against the threat of accidents caused by failures in one of the above-mentioned areas, which are part of the normal operation of a ship.

Maritime Security has another dimension; the threat is not an accident or an unintentional activity during the normal performance of a task or a failure of ship structure. In this case the threat is an intentional action with the purpose to cause damage to the ship or to use the ship for illicit purposes. In that sense Maritime Security has been defined by Hawkes (1988) as "those measures employed by owners, operators, and administrators of vessels, port facilities, offshore installations, and other marine organizations or establishments to protect against seizure, sabotage, piracy, pilferage, annoyance, or surprise"[2].

The main difference, however, is not only in the concept but also in the feasibility to assess safety risks and security risks. The assessment of safety depends largely on accident probabilities and statistics, but a risk security assessment is much more difficult because it depends on our estimate of the threat of a hostile act (Wells, 2001, p. 303) [3]. The problem is that a security assessment is not always possible to rely in past activities because those which plan acts against maritime security can change their tactics and attack different points not considered by the security assessor. This feature will have an important impact on the techniques to be used for security assessments.

[1] Professor Kuo concludes from the analysis of several accidents in different sectors that the role of engineering, operation and management in balance with the human element is the key for safety.

[2] K. Hawkes is possibly the only author that has defined maritime security and has written a book on the subject.

The main concern among security issues is, of course, the possibility of terrorist attacks. These activities can take different forms and as we have seen above they can change their strategies to attack weaker points of the installation. The problem at this point is that we cannot do too much if a terrorist decides to attack a ship or port facility with, for instance, a portable missile. Therefore for the development of security assessments it will be necessary to clearly identify the features of the different maritime security issues in the context of the current maritime security framework.

2.2 Maritime Security Issues and the Maritime Security Framework

The maritime community in general, and the IMO in particular, has been looking after maritime security issues as early as in 1983 with IMO Assembly Resolution 545 (13) "Measures to prevent acts of piracy and armed robbery against ships" and IMO Assembly Resolution 584 (14) "Measures to prevent unlawful acts with threaten to safety of ships and the security of their passengers and crews". Maritime Security issues taken into account by IMO were mainly those concerning piracy, armed robbery or stowaways. However, the hijacking of the Achille Lauro in 1985 and the bombing of the City of Poros in 1988 indicated that the shipping industry was also vulnerable to terrorist attacks.

The first international reaction to these issues was a legal one with the adoption of the 1988 SUA Convention. Even when the issue of maritime security was taken up at the IMO, a fixed agenda item since 1984 (Mejía, 2003, p. 162), it was not until the 9-11 events that the maritime community realized the possibility of a terrorist attack against shipping with catastrophic consequences. IMO, in a fast reaction to the situation and with the strong support of the USA, adopted in 2002 new regulations to address the issue of maritime security throughout amendments to the SOLAS 74 Convention and particularly with the issue of the ISPS Code.
The main maritime security regulatory framework will be briefly described in the following sections, and its link with the main maritime security issues involved.

[3] Alexander T. Wells is an expert in aviation management and dedicates the whole chapter 12 of his book –Commercial Aviation- to analyse safety and security in this sector.

2.2.1 The SUA Convention 1988

The SUA Convention 1988 was the result of a process designed by IMO to expand the scope of the law to cover the acts and threats to the safety of navigation that were not covered adequately by the existing law (Mensah, 2003, p. 20). In fact this was a legal approach to address new maritime security issues like the hijacking of the Italian cruise ship Achille Lauro on October 7, 1985. In that sense the main objective of this convention is first to define clearly the scope of a maritime offence and second to establish the responsibility of the states to become such offences punishable under their national laws.

Article 3 of the SUA Convention specifies as offences certain acts against shipping, including the seizure of ships, and the endangering of safe navigation by the use of violence against persons on board or by damage to the ship, its cargo or equipment, and attempts to commit those acts (Churchill & Lowe, 1999, p.211). The common factor of this definition is the requirement that the unlawful act is likely to endanger the safety navigation of the ship, however that is not always the case as for example when the ship is at anchor (Mejia, 2003). This situation highlights the fact that the different maritime security issues have different features and scopes. Therefore, to deal with them either from the legal side or from the functional and technical side these particular characteristics should be taken into account.

Article 5 of the SUA Convention states that parties must make Convention offences punishable under their laws. Also the convention gives state parties the right to prosecute any offender who is found in their territory. However if one state is not willing or able to prosecute an offender, it is required to extradite that person to another State Party which has jurisdiction and is willing to prosecute (SUA, Art. 5).

These regulations, however, are not enough to deal with the new problems that have emerged in the aftermath of the 9/11 events. That is why the Legal Committee of IMO is now undertaking the revision of the Convention to consider measures to prevent ships from being used as the means or support for terrorist activities and to ensure that persons who have perpetrated acts of violence at sea will be brought to

justice. Crucial importance has been given to the necessity that the convention includes direct reference to “terrorist acts” and also the inclusion of a wide range of acts that are already treated as “terrorist acts” in a number of existing international treaties (Mensah, 2003, p. 23).

2.2.2 Amendments to SOLAS 74

2.2.2.1 SOLAS 74 Chapter V, Safety of Navigation

There is only one regulation in this chapter concerning maritime security; the Automatic Identification System (AIS) introduced by regulation 19. The AIS is a system by which a ship shall provide automatically to shore stations and other ships, its identity, type, position, course, speed, navigational status and other safety related information. Also according to Regulation 19, paragraph 2.4.5, the system shall receive automatically such information from similarly fitted ships, monitor and track ships and exchange data with shore-based facilities.

The problem with this system in relation to maritime security is that it can be used for unlawful purposes in case criminal or terrorist organizations could obtain information such as the position of the ship or other safety related information. Since ships fitted with AIS shall maintain AIS in operation at all times, except where international agreements, rules or standards provide for the protection of navigational information, attention should be paid to the maritime security issues possibly involved. Some maritime security issues are restricted to specific zones in the world while others can be expected around the world, therefore analysing these characteristics will be crucial to the security of a ship which in contrast to a port facility is constantly changing its environment.

2.2.2.2 SOLAS 74 Chapter XI-1, Special Measures to enhance Maritime Safety

This chapter contains two regulations concerning maritime security issues. First of all, Regulation 3 establishes that every ship shall be provided with an identification number which conforms to the IMO ship identification number scheme adopted by

this organization. Moreover, Regulation 3 establishes that this ship's identification number shall be permanently marked in a visible place on the ship's hull or superstructure and in the machinery space or on one of the hatchways. The IMO ship identification number is a unique seven-digit number that is assigned to ships by Lloyd's Register-Fairplay, which is the sole authority for identifying and assigning an IMO number. The IMO number is never reassigned to another vessel.[4]

The second regulation of concern is Regulation 5, which establishes that every ship should be issued with a Continuous Synopsis Record (CSR) with the intention of providing an on-board record of the history of the ship. The CSR shall be issued by the Administration and, inter-alia, shall contain relevant information like the name of the flag state, the ship's identification number, the name of the registered owner and their registered address, the name of the registered bareboat charterer, the name of the company for ISM purposes, the name of the classification society, etc.

These two regulations have an important effect in the facilitation of the identification of ships. According to the International Maritime Bureau (IMB) stamping the hulls of ships with a permanent identity code would reduce crimes that involve the masking of a ship's origins and would be an important crime prevention measure in particular against "phantom ships" crimes, which rely on fake documents.[5] Therefore, as the use of ships for unlawful purposes an important maritime security issue, these measures are an easy and effective way to verify the identity of a ship.

2.2.2.3 SOLAS 74 Chapter XI-2, Special Measures to Enhance Maritime Security

The new maritime security regime of IMO outlined in this chapter firstly defines the main actors which shall comply in general with the relevant requirements of this

[4] See IMO Assembly Resolution.600 (15) and more information about the assignment of IMO numbers can be found in < http://www.lrfairplay.com>

[5] For more information about Maritime Crime see: Abyankar: *Maritime Crime* (2004), Unpublished lecture handout, World Maritime University, Malmö, Sweden and in the International Chamber of Commerce-International Maritime Bureau web page: www.iccwbo.org

chapter and with the ISPS Code: The ships including mobile offshore drilling units; companies; port facilities; the Designated Authority and Recognized Security Organizations (RSO). These regulations provide particular obligations, requirements and responsibilities for these elements that can be summarized as follows.

In relation to ships, Regulation 6 establishes that they shall be provided with a ship security alert system (SAS) capable of transmitting a ship-to-shore security alert indicating that the security of the ship is under threat. This chapter also requires that ships have to be implemented with a security system, produce the documents to attest it, follow the security levels dictated by the interested port or coastal state and keep the records of the measures taken in this respect for the last ten ports.

As for companies, they shall ensure the master's discretion for ship safety and security, and that the master has available on board the necessary information to identify the person responsible for appointing the crew, for deciding the employment of the ship and, if that is the case, who are the parties of the charter party under which the ship is operating (Regulation 5).

The Designated Authority also has a number of obligations provided by Chapter XI-2. One very important it is the obligation to set security levels and provide related information to ships entitled to fly its flag, its port facilities and ships within their territory (Regulation 3). Also it shall provide a point of contact through which such ships can request advice or assistance in security aspects (Regulation 7). On the other side the administration can exercise its right of control of ships in port to verify, using duly authorized officials, that a ship is in possession of a valid International Security Certificate. These controls might be avoided if the ship, prior to entering a port, provides the necessary information to ensure compliance with chapter XI-2 (Regulation 9).

Port facilities are a new element in the IMO regulatory context and this is the first time IMO sets regulations for shore-based operations. In that sense port facilities shall comply with chapter XI-2 and the ISPS Code as well. Port Facility Security Assessments (PFSA) shall be carried out and Port Facility Security Plans (PFSP)

shall be developed to ensure the security of the installation. The Designated Authority shall approve both the PFSA and the PFSP (Regulation 10). Developing the PFSA and PFSP is where the Recognized Security Organizations play an important role, supplying the necessary expertise and workforce to perform this work.

The new regime, therefore, addresses maritime security in a holistic way, involving all the main elements of the shipping industry in a common effort to protect the shipping industry as a whole. The philosophy behind this new regime stems from the fact that in contrast to the majority of maritime security issues, terrorism has reached an international level and therefore the protection of the shipping industry should be addressed internationally. As Efthimios Mitropoulus has said "…terrorism is not a matter of concern to one country or a group of countries – it has, unfortunately, become a global issue and we should address it as such ".[6]

The conclusion is that security measures can not be taken inconsistently, simply because if the security measures in one country are more effective than in other, the terrorists motivated to harm the interests of that country are likely to seek targets of that country in those countries with weaker security measures. Therefore, the same level of implementation of the new maritime security regime will be the key for the success of the shipping industry in this matter (Wells, 2001, p. 310).

2.2.3 The International Ship and Port Facility Security Code

The ISPS Code is certainly the most significant part in the security framework (Schröder, 2004). It embodies a number of functional requirements that are the basis to achieve the objectives of the Code: to establish an international framework to detect security threats and take preventive measures; to establish the roles and responsibilities of the main stakeholders of the maritime community for ensuring maritime security; to ensure the early collection and exchange of security-related

[6] Speech to the Singapore Shipping Association, Singapore, 25 May 2004. <http://www.imo.org/home.asp> (11 June 2004)

information; to provide a methodology for security assessments that allows the development of security plans capable to deal with any change in the level of security; and, to ensure confidence that the security measures in place are reliable (Part A, Section 1.2).

Even though the ISPS Code was designed mainly against terrorism, the security system created in port facilities and ships with the involvement of Administrations, Companies and Recognized Security Organizations, is able to deal with any maritime security issue. That is possible because the functional requirements of the Code have a risk-based approach to address security issues and therefore an assessment of risk must be made for each particular ship and port facility to determine the necessary risk control options to be implemented in a security plan. These control options will be oriented in one way or another depending on the type of security issues they probably will face. For example, some operational and physical control options should be established in general to prevent unauthorized access to ships or port facilities, or to raise the alarm in reaction to security threats. However, if the ship calls at ports with armed robbery or stowaway antecedents additional measures should be implemented for these particular cases (Part A, Section 1.3).

The new security framework provided in the ISPS Code involves another important element: security related information. The whole security system requires that governments in the international security framework gather, assess and exchange security related information. But not only is security information required by governments, the Company Security Officer (CSO) also requires security information to advise the level of threats likely to be encountered by ships. This particular situation could represent a problem because in practice it could be very difficult to gather security related information from government agencies that can consider that kind of information classified, or from a port which can lose money if the information is released to the public (Cooper, 2004, pp. 3, 6). However, some effort has been made by the private sector, as for example the Lloyd's Register's See Threat, which is a web service that scans news, networks and provides specific security related information useful for the responsibilities of the CSO.

All this security system will require is, indeed, the important participation of the human element. Therefore training, drills and exercises should be carried out on a regular basis to ensure familiarity with security plans. However, the problem is not only in the execution of the plan but also in the development of all the process to assess security risks, because it requires a level of expertise in maritime affairs and security. This job has been taken by the RSO's, mainly Classification Societies, with vast experience and the necessary network to perform the task. The results are of course still to be seen as a result of the system entering into force on July 01, 2004.

2.2.4 Issues of Maritime Security

We have seen in the previous sections how the maritime community has addressed the different security issues from the legal side and with physical, operational and management tools embodied in the new maritime security framework. But the most important thing that we have seen is how the particular characteristics of each issue of maritime security affects the design of measures to control them, and more specifically, how these characteristics could affect the security assessment for both port facilities and ships.

There are six main issues of maritime security that in different degrees affect all ports and ships: theft, drug smuggling, stowaways and illegal immigrants, piracy and armed robbery against ships, sabotage and terrorism.[7] Even though sometimes their borders are not clear or overlap we can divide them between locally restricted and locally unrestricted maritime security issues (Schröder, 2004). Table 1 provides an idea of that distinction.

In maritime transport cargo theft is the most common threat to security. It has been estimated that cargo theft constitutes approximately 20% of all cargo lost. This is a locally restricted maritime security issue given that this problem varies depending on the security measures established by the port. Drug smuggling can be considered a

[7] The author has taken this information from material received in the International Course and Workshop on Maritime Security organized by IMO in Montevideo, Uruguay, 28 October to 1st November 2002.

locally restricted issue too because normally this problem is intensified in direct voyages from producer countries to consumer countries. The issue of stowaways and illegal immigrants presents the same characteristic with some specific routes in the world where this problem is truly a headache for ship owners. Moreover, piracy and armed robbery is a locally restricted maritime security issue related to specific maritime routes, as for example the Malacca Strait.

Table 2.1: Examples of locally restricted and locally unrestricted maritime security issues.

Locally restricted maritime security issues	**Locally unrestricted maritime security issues**
• Theft • Drug Smuggling • Stowaways and illegal immigrants • Piracy and armed robbery • Sabotage	• International Terrorism

Source: Adapted from J. Schröder, *Maritime Security - an overview of the new requirements*, 2004

What is interesting here is, the point of view of risk assessment approach established by the new maritime security framework where these locally restricted maritime security issues follow a certain pattern that can be gathered in statistics and used for security assessment purposes. For example, the International Maritime Bureau of the International Chamber of Commerce has a report system of piracy incidents, based on which, prepare an annual report with statistics of these incidents around the world (Figure 2.1 shows the statistics for 2003). IMO has also designed a report system for member states and publish the results monthly. These reports help ship operators to identify critical zones that require special security measures.

Terrorism in general, and International Terrorism in particular, has emerged as a locally unrestricted threat since the 9/11 events. As explained during the analysis of the new maritime security framework, this new security regime implies that the creation of an international maritime security system is the only way to respond to this international threat. However, the assessment of this threat is always difficult

because international terrorism does not follow any pattern to avoid being detected. We cannot build any statistics on these threats due to the fact that there have been only a few of them, like the incidents of the Achille Lauro in 1985, the bombing of the City of Poros in 1998 or more recently the bombing of the Limburg in 2002. The only real pattern is that terrorists will seek the weaker points of the system to attack. That is why the new regulatory framework is also focused on protecting particularly those key operations, trying to minimize the effect of any attack on the ship or port facility.

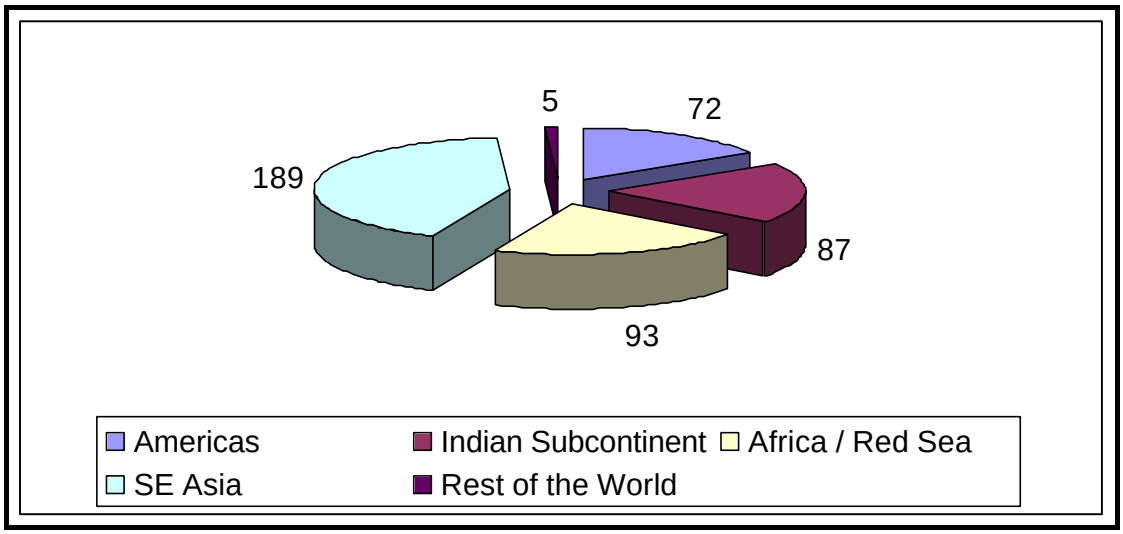


Figure 2.1: Regional breakdown of total reported incidents in 2003

Source: International Maritime Bureau

2.3 Analysis of the ISPS Security Assessment methodology

2.3.1 Ship and Port Facility Security Assessment

One of the five objectives of the ISPS Code is “to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels”. Likewise the correspondent functional requirement to achieve this objective is “requiring ship and port facility security plans based upon security assessments”. So the Security Assessment is the essential tool to obtain consistent security plans.

Figures 2.2 and 2.3 show the process established by the ISPS Code for the Ship Security Assessment (SSA) and the Port Facility Security Assessment, as a summary of the considerations taken into account in the Part A and Part B of the Code. Even though, these two processes are described separately in the Code they follow the same criteria: identify the main threats, identify vulnerabilities, assess the likelihood of occurrence, its possible consequences and the most suitable countermeasures to eliminate the threat or minimize the impact of them.

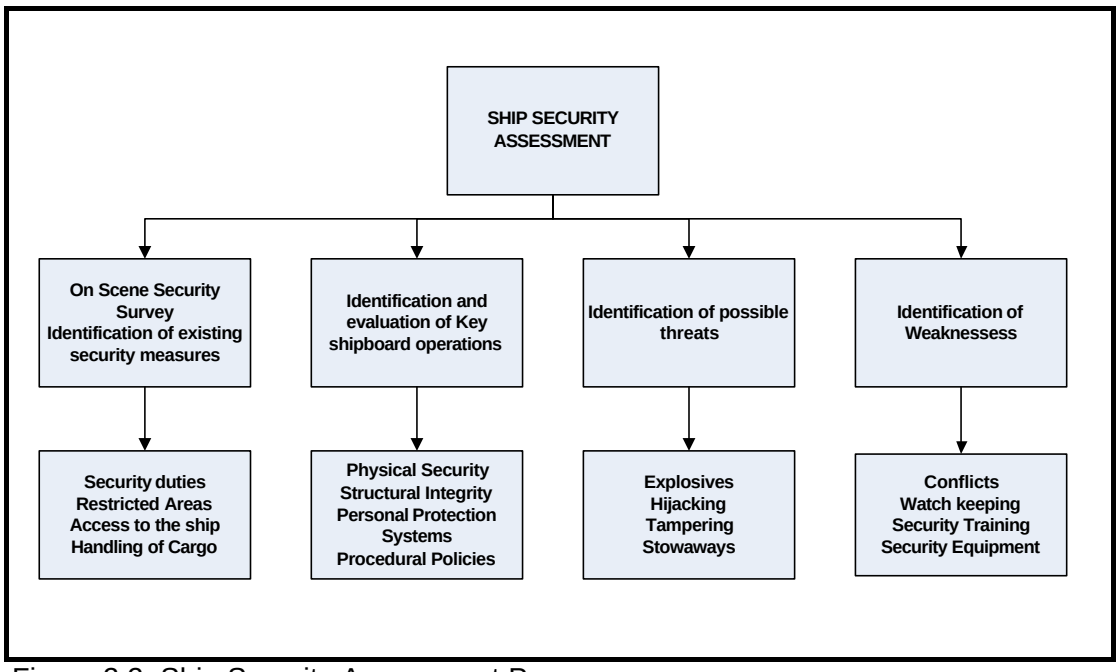


Figure 2.2: Ship Security Assessment Process

The ship, however, presents a more complex environment since it is moving continuously. In this regard the type of operation of the ship plays an important role in security assessments, because for instance liner ships with a fixed itinerary will be in a better position than tramp ships to coordinate or obtain security information of the ports where the ship usually calls (Part B, Section 8.2). This situation brings out the fact that the assessment of security must be done case by case, which means that the assessment should be specific for each ship or port facility.

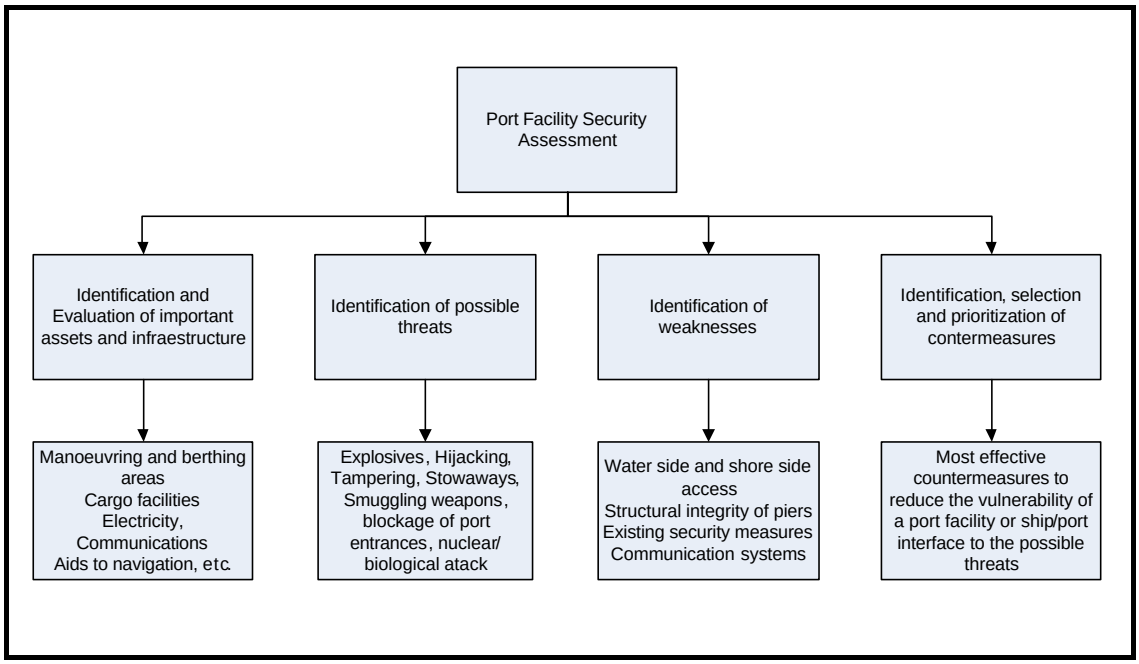


Figure 2.3: Port Facility Security Assessment Process

The methodology established by the ISPS Code is therefore based on the concept that to determine what security measures are appropriate for a ship or port facility, an assessment of the risks must be made in each particular case (Hesse, 2003). This methodology in consequence involves a risk management approach because it is a process of handling risk in a conscious manner (Frame, 2003, p. 14). The ISPS Code gives the risk management framework that Ships and Port Facilities need to plan and, as Frame also says, deal with risk proactively, identifying risk events, developing strategies to deal with them, and then handling risks when they arise.

Figure 2.4 shows how the ISPS approach to manage risk follows a typical risk management framework which involves five steps: plan for risk, identify risk, examine risk impacts, develop risk handling strategies and monitor and control risk.[8] Steps two to four constitute the risk security assessment and step five involves activities to be considered in the SSP or PFSP.

[8] This risk management framework is based on the framework promoted by the Project Management Institute (PMI) in its Guide to the Project Management Body of Knowledge, PMBOK (2000), as is commented upon by Davidson Frame, 2003.p. 15.

The problem to develop a Risk Security Assessment, as we have seen in the previous section, is the fact that some maritime security issues create statistical patterns and some of them do not. The ISPS Code assumes a position that the necessary expertise to perform the security assessment should be based mainly on persons with knowledge of maritime or port aspects as well as security, for it seems most feasible that the assessment of security issues will be more qualitative than quantitative, meaning experience based (Part B, Sections 8.4,15.4).

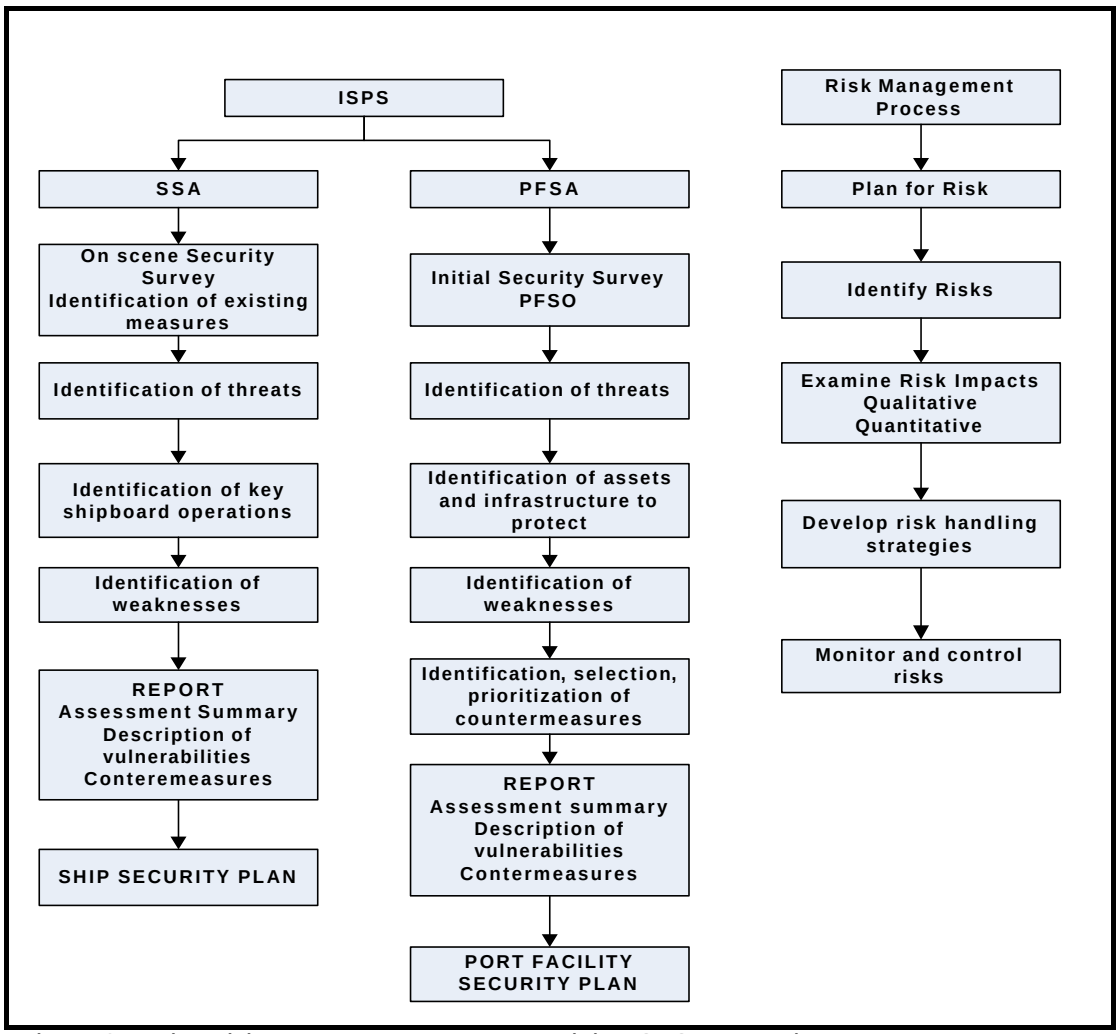


Figure 2.4: The Risk Management Process and the ISPS approach.

Source: Adapted from J. Davidson Frame, 2003 and the ISPS Code.

This approach is useful to assess threats like terrorism, which does not create statistical patterns and therefore the assessment will lead to the creation of

measures to protect key infrastructure and operations. However, some other maritime security issues like piracy, armed robbery or even stowaways create statistical patterns and therefore could be possible to apply quantitative methods to evaluate their probability of occurrence. In both cases some techniques exist, used mainly in safety assessment, that could be used now in security assessment.

Among qualitative techniques we have Hazard and Operability Studies (HAZOP), Failure Mode and Effect Analysis (FMEA), which are techniques based on individual's expertise and they are therefore more subjective. On the other side among quantitative techniques we have Probabilistic Risk Assessment (PRA) and Fault Tree Analysis, Event Tree Analysis. These are techniques that require formal training and always imply quantitative modelling. Additionally, the United States Coast Guard (USCG) and the Norwegian Ship Owners Association/ Det Norske Veritas (NSA/DNV) have developed their own approaches for security assessments.

2.4 Conclusions

This chapter has shown how the main problem of security is the difficulty to assess security risks, due to the particular nature of maritime security issues like terrorism which contrary to safety issues do not always have specific patterns. Moreover, maritime security issues being intentional and usually premeditated try to avoid being predictable, changing targets and mode of operations. The reaction of the international maritime community has been to address the problem creating an international maritime security system implemented through amendments to the SOLAS 74 Convention, the ISPS Code, an the SUA Convention 1988.

This new security framework on one side addresses maritime security issues since the legal point of view creating the legal basis to prosecute and punish those who have committed maritime offences that affect the safety of navigation. Maritime issues like piracy, armed robbery, hijacking or terrorism can be covered by this regulation. On the other side, it was necessary to implement new regulations that consider technical and operational measures to deal with those threats. Ship Security Alert Systems (SSAS) can help to alert the authorities when a ship is being

subject to a piracy attack or if terrorists threaten the ship. However, it was clear that maritime security issues should be addressed taking into account the important characteristic that some of them are locally restricted and some are locally unrestricted. This means that those that are locally restricted create statistical patterns and therefore can be used for security assessment purposes.

The new security framework addresses maritime security with a risk management approach, dealing with security risks proactively, identifying security threats, developing strategies to eliminate or minimize those threats and handling security risks in case they arise. The central part of the risk management process is the risk security assessment. The ISPS Code provides a general methodology for security risk assessments; hence some techniques normally used in safety risk assessments may be useful for security assessment purposes. Some of them being quantitative are useful only in case statistical data is available. Others being qualitative are more useful to assess those maritime security issues that do not create statistical patterns, focusing the assessment mainly on protecting key infrastructure and procedures in a way to minimize the impact in case of an attack. The next chapters will analyse these techniques in detail and determine the feasibility of being applied effectively for security assessment.

CHAPTER 3: Managing Risk: An overview of Risk and Risk Assessment

In the previous chapter it has been shown how the new maritime security framework addresses maritime security with a risk management approach. Likewise the proposed methodology for security assessments in the ISPS Code follows in general a typical framework of risk management that is used in some parts of the industry ashore. For this reason, before starting to analyse current security and safety risk assessment approaches, it is necessary to introduce the general concept of risk, risk management and the risk assessment process.

In this sense it is the purpose of this chapter to give an overview of the concept of risk in the familiar context of safety and establish how the approach to this concept should be clearly defined from the security point of view. As it has been seen in chapter 2 ship's safety has to do with unplanned failures or mistakes related to engineering, operation and management underpinned by the human element, and its assessment depends largely on the statistics of these factors. Security on the other hand has to do with external and intentional threats that in some cases create statistical patterns but in several other cases do not. Therefore, risk in the context of security will have another dimension that makes its assessment particularly complicated.

Moreover is the intention of this chapter to clearly define the Risk Assessment process in the context of security. For this purpose it will be necessary to analyse some of the methodologies that are used for risk management studies in several parts of the industry (especially for safety purposes) and establish a preliminary risk security assessment framework based on these methodologies. This framework will then be the reference for the analysis of different approaches and techniques to be analyzed in the following chapters with the objective to find if some safety risk assessment techniques can be used for security assessments.

3.1 Risk

Risk is a term used loosely in everyday life because risk in fact is part of our lives. According to Merriarn-Webster's Online Dictionary risk is a possibility of loss or injury. If we analyse this definition it can be found that the concept involves two parts: the possibility that something happens and the adverse effect of this occurrence. Therefore it is the relationship between probability and consequence that defines risk. We can summarise this concept in the following equation:

$$R = C \times P \tag{3.1}$$

Where C is the Consequence, P is the probability of occurrence and R is a coefficient called Risk.

In a safety context, probability and consequence involve a number of factors related to management, engineering and operational aspects underpinned by human factors like human behaviour, decisions and actions (Kuo, 1998, p. 64). All these elements are inside the maritime industry: shipping companies, shipbuilders, port facilities and regulators; and therefore they can be analysed and assessed based on information gathered from the ordinary performance of them.

In a security context, on the contrary, probability and consequence involve not only factors inside the maritime industry but also outside. As we have seen in chapter 2 terrorism, hijacking, drug smuggling, piracy, armed robbery, stowaways, illegal immigrants, etc., are security threats external to the maritime industry which can be assessed depending on the availability of information, like for example in the case of those locally restricted maritime security issues which generate some statistical patterns. However, other security threats such as terrorism are much more difficult to assess due to the fact that they do not create statistical patterns. Therefore, our capability to determine their probability of occurrence through equation 3.1 will be very limited.

In this sense, with the lack of information of security threats, they may then be categorized in some credible basic scenarios on a case-by-case basis, and concentrating our efforts in the assessment of weaknesses of the security systems of ships or port facilities. This means focusing in those elements that are under ship's or port facility's management and upon which it is possible to establish measures to enhance their protection against security threats.

This particular situation leads us to extend the basic equation of risk, establishing a concept of Security Risk in function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack (ISPS, Part B, Secc.1.17). This means replacing Probability (P) by Threat and Vulnerability due to the lack of statistical information to assess likelihood. The new equation then would be:

$$R = T \times V \times C \qquad (3.2)$$

Where T represents threat, V vulnerability and C consequences. The term threat represents the perceived probability of an attack based on maritime domain awareness and the existence of intelligence. Moreover, vulnerability measures the conditional probability of success given that a threat scenario occurs, and consequence is the estimation of the adverse effects of an attack (USCG, 2003, p. 39244). This last factor also brings about not only the need to identify all the effects of an attack but also identify those critical components or operations where the effect goes further than the component reaching all of the system.

We can see therefore, that Risk in terms of security implies the assessment of several factors that make the overall study more complicated. The likelihood of occurrence of a security threat will not depend only on the threat; it will also depend on vulnerability as a measure of our capacity to deter a threat. In this sense if we have information on the threat we will be in a better position to assess the whole security risk more precisely, but if we do not have information what we need is to assess our weaknesses, identify our critical points, evaluate the possible consequences and then try to harden the target as much as possible.

Risk in consequence, either for safety or security, has to be managed. As it has been said before risk is a constant in our daily lives sometimes with simple decisions that imply a degree of risk. Organizations, companies and industries have to deal with a variety of risks in order to be successful in achieving their objectives. These risks, as in the maritime industry, can be diverse and complicated to deal with, therefore it is necessary to use a systematic technique to develop strategies to reduce the level of risk.

3.2 Risk Management

According to Frame (2003), risk management is a process of handling risk in a conscious fashion. Moreover the application of risk management methodologies has proven to be and effective and consistent way to mitigate risk and to avoid the danger of purely intuitive or experimental decision-making (Fergus, 2004). The industry in general has developed several guidelines and standards defining different approaches to risk management with the intention of handling risks associated with its particular requirements. Some of them are aimed to manage risks related to safety, occupational health or security, and others for investment purposes. As, for instance, in the following risk management frameworks:

- Australian/New Zealand Standard AS/NZ4360 1999. [1]
- Project Management Institute 2000
- Institute of Risk Management 2002

These risk management models take slightly different approaches, however, all of them follow the same basic steps described below (Hillson, 2003):

- **Definition**; the objective of this phase is to define the objectives and level of detail of the risk management process. It is the planning stage and its scope is included in the Risk Management Plan.

[1] A detailed description of this standard can be found in: Broadleaf Capital International PTY LTD, *Tutorial Notes: The Australia and New Zealand Standard on Risk Management, AS/NZS 4360: 1999* < http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf > (28 June 2004)

- **Risk Identification**; using different available techniques to identify as many risks as possible.
- **Risk Assessment**; the identified risk are assessed by qualitative or quantitative methods in order to prioritize those risks that are most probable and whose dangerous effects are higher.
- **Response Planning**; in this stage risk-handling strategies are developed in a way that is appropriate, achievable and affordable.
- **Monitor and Control**; effectiveness of the risk process is assessed and adjustments can be made.
- **Review and Update**; risk is always changing therefore the process should be reviewed regularly identifying and assessing new risks, and developing new mitigation strategies.

From these basic steps it can be seen how risk is handled through a systematic and analytical process. Also the Risk Management framework can be smoothly adapted for different situations as for instance to manage security risks. In this regard, for example the United States General Accounting Office (GAO)[2] proposed in its report of October 2001 before the Subcommittee of National Security the application of risk management techniques to assess and manage the risk from terrorism in the USA. This demonstrates how flexible the general risk management framework is. The terminology and the situations can change but the basic structure and the intention is the same.

Moreover, the main objective of a risk management framework is to reduce risk to a level that is acceptable. Response measures to mitigate risk, as we have seen above, should be appropriate, achievable and affordable. Therefore, decisions should make sense in several ways, not only from the technical point of view but also from the economic side. It is important to highlight this point because, for instance, in terms of safety some level of risk is generally accepted based, for example, on the ALARP principle (As Low As Reasonable and Practicable). In terms

[2] The US General Accounting Office is an independent agency that works for the US Congress. GAO advises the US Congress and the heads of executive agencies about ways to make government more

of security the same issue arises and the question of what level of security risk is unacceptable, acceptable or negligible should be taken into account.

In this respect it could be useful to comment on a concept that Kuo (1998) calls “The ship’s operator goal”. This author says that the marine operation goals are: “to be competitive in meeting the client’s specifications with solutions that are cost-effective at an acceptable level of safety.” (p.1). In the current context we can add security as a fifth element to the ship’s operator goal, but keeping in mind that the goal is to achieve all the factors together: the safety and security level that allows competitiveness and economical benefit.

Another aspect that is important to remark upon the general risk management framework described above is that the core steps of the process are actually a risk assessment process. Sometimes the boundaries are not clear due to the diverse models in use and also because of the variety of terminology. However, regardless of the terminology, what is important is that the underlying concept is the same: organizations are required to plan and deal with risk proactively, identifying risk events, developing strategies and then handling risks when they arise (Frame, 2003, p. 14).

In the next section the risk assessment process will be analyzed and some of the diverse terminology will be defined for the purpose of this work.

3.3 Risk Assessment

Risk assessment, as we have seen in the previous section, is the central part of the Risk Management process. The objective of risk assessment is to provide information on which decisions may be made about proposed actions, the adequacy of risk controls and what improvements might be required (Waring & Glendom, 1998, p. 21). This information is the outcome of a process of identifying potential hazards or threats, estimating the likelihood that these hazards or threats can cause

---

effective and responsive and its work usually leads to laws and acts to improve government operations.

adverse effects, assessing the possible consequences and developing control measures to reduce or eliminate the risk that these hazards or threats impose.

Figure 3.1 shows a model of risk assessment methodology. There are, of course, several models available. However, for the purpose of the analysis this particular model has the virtue of dividing the process of risk assessment into two parts, making the whole process easier to understand. The first part is a Risk Analysis process that analyses risks in order to determine their consequences and the probability of occurrence. The second part is the process of managing all identified risks to develop the adequate risk reduction strategies and measures as a function of an acceptance criteria previously defined. These two processes will now be analysed in more detail.

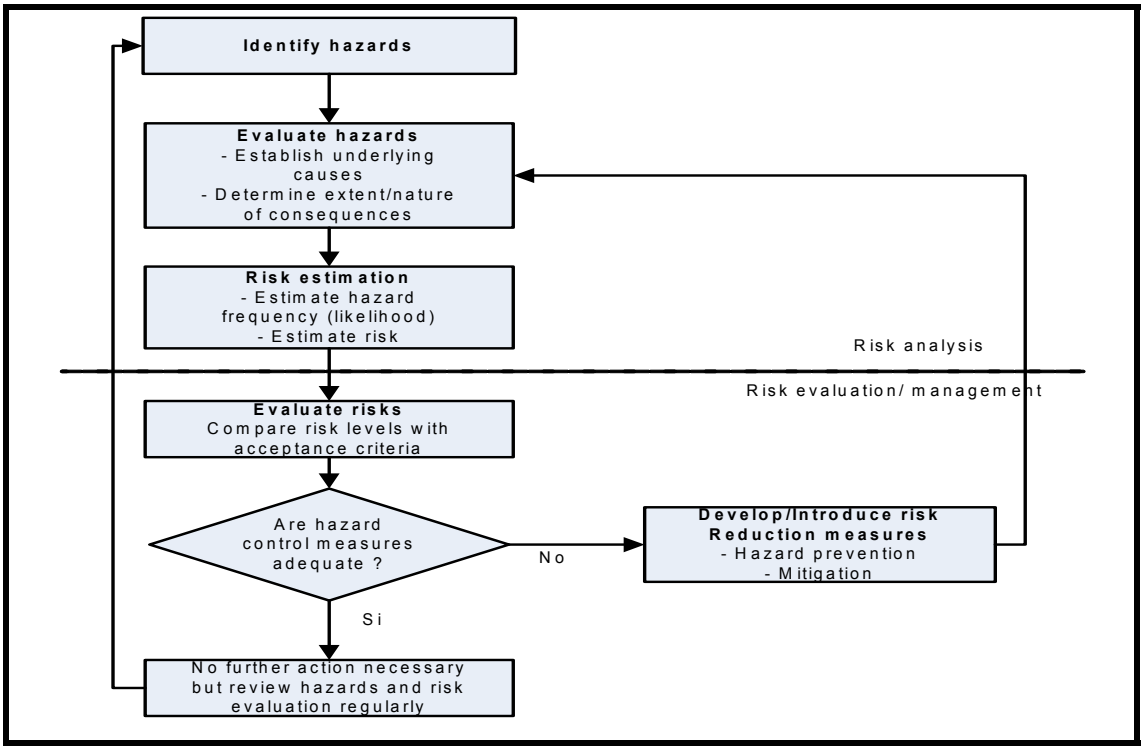


Figure 3.1. Example of Risk Assessment Methodology

Source: Waring and Glendon, 1998

3.3.1 Risk Analysis

Risk analysis is defined by Dickson (1991) as "…the entire task of identifying and measuring the potential impact of risk" (p. 27). To identify risks will imply the evaluation of their possible causes and likelihood of occurrence. Also any risk will have an effect on the organization, which has to be estimated. The outcome of these two steps of risk analysis leads us to the basic equation of risk: Probability and Consequences. Once the risk has been identified for its likelihood and consequences, it is possible to estimate risk and see what is its level. This information will then be utilized for the decision-making process to define the best risk control options.

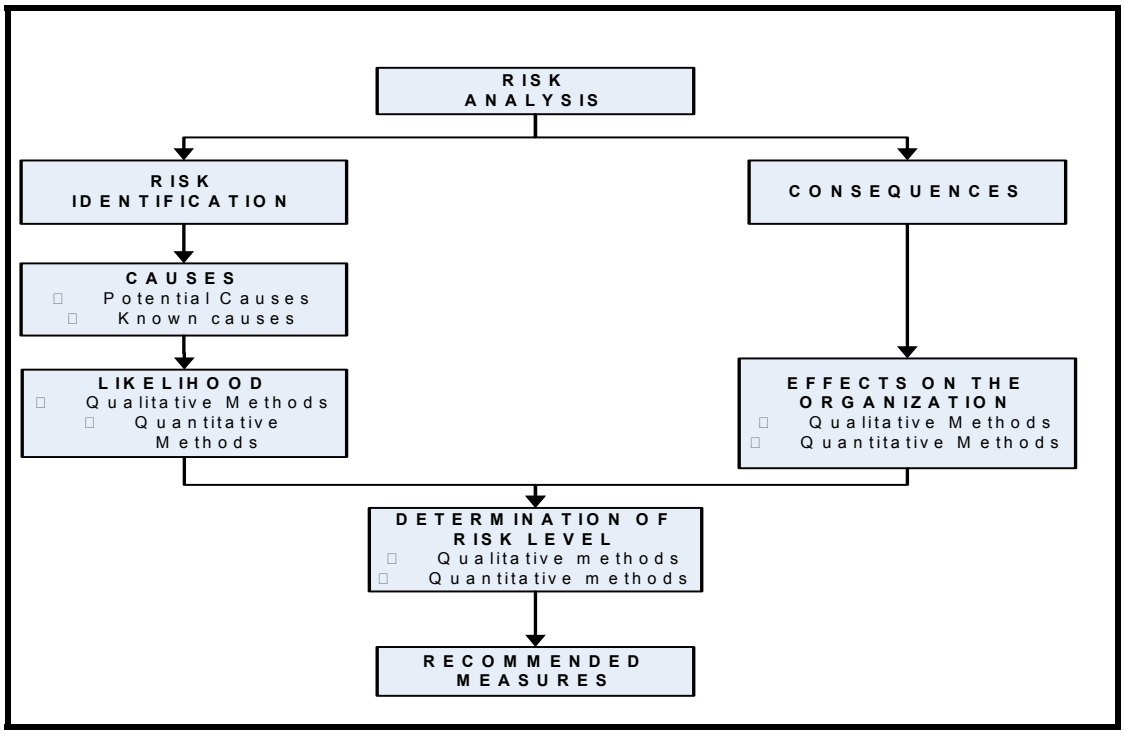


Figure 3.2. Risk Analysis process.

Figure 3.2 shows the entire process of risk analysis, highlighting particularly those stages where the use of methodologies based on quantitative or qualitative techniques are necessary. Most of these techniques are currently used for safety purposes and the selection of quantitative or qualitative methods will depend on the availability of information and the degree of sophistication or variety of processes to

be evaluated. This process of risk analysis will now be analysed with particular reference to these techniques to start looking at the feasibility to use them also in security assessments.

3.3.1.1 Risk Identification

Risk Identification is the process of systematically identifying those factors that are able to produce risks to any organization. Sometimes these factors by themselves do not constitute risks but in combination with other factors inside and outside the organization and the likelihood of occurrence, they may become risks. In a safety context these factors are usually referred to as hazards and should not be confused with risk. In security they are generally referred to as threats (Waring &Glendon, 1998, p. 5). Therefore, there are two important elements in risk identification. First the identification of the causes of risks and second the estimation of the likelihood of occurrence. These two factors will be analysed next:

Causes

In a safety example, identification of hazards is the first step of the “Safety Case Approach” proposed by Kuo (1998). Some principles of hazard identification are defined in this approach to determine what can go wrong. Basically it is necessary to understand the general and particular objectives of the organization and then identify the possible deviations from what is planned to achieve those objectives. Finally these possible deviations should be listed and recorded for future analysis.

Risks are caused by one factor or some factors. In the methodology mentioned in the previous paragraph, to be able to identify deviations from the intended purpose it is first necessary to recognize their possible causes. These causes of risks are hazards or threats that, depending on the situation, may represent a certain level of risk. Hazards or threats are factors (situations, components, conditions, operations, etc) that may be dangerous and will represent a degree of risk depending on their likelihood of occurrence and the level of consequences on the installation or organization.

There are several techniques that provide a systematic approach for identifying potential hazards in sophisticated systems. Among these techniques we have: (a) Hazard and Operability Studies (HAZOP); (b) Failure Mode and Effect Analysis (FMEA); (c) Fault Tree Analysis (FTA). Some of these techniques, like HAZOP and FMEA, are qualitative techniques and they are not mainly aimed to assess likelihood, while FTA is a quantitative technique that can be used for the assessment of likelihood as well.

In a security context, identification of threats, as we have already said before, will require information. Sometimes this information is available as in the case of the locally restricted maritime security issues like Piracy or Stowaways. However, in the case of terrorism, there is not always enough information available to identify the threats. Important elements to know in this regard are, for example, previous incidents, existence of the threat, capability and intention of terrorist groups (USCG, 2003, p.39244). This is why qualitative and simple quantitative risk assessment methods are looked at.

Likelihood

Once hazards have been identified it is necessary to estimate the likelihood that those hazards can occur. This estimation may be done through quantitative or qualitative methods. The selection of the adequate technique will depend basically on the availability of information. Quantitative estimation of risk requires statistical information related to the analysed system however this information is not always available or is not complete enough to produce acceptable results. This is why sometimes it is necessary to use the so-called Heuristic or qualitative techniques or "Rule of Thumb".

Qualitative techniques are based mainly on an individual's collective judgment. This means a group of experienced people with high expertise on the system or organization analysed, who decide what is the level of risk of the identified hazards based on the information available. In this sense a hazard can be deemed simply as likely or unlikely, or maybe frequent, reasonably probable, remote, extremely

remote. The point here is that whatever the scale decided, the judgement will be purely subjective.

The problem in terms of security is the identification and determination of likelihood mainly of those locally unrestricted security issues such as terrorism that do not create patterns. However, what we can do is to be prepared for the event that a terrorist attack happens, identifying vulnerabilities, critical points and potential consequence in order to develop the necessary measures to deter terrorists and, in the case of an attack, react timely to mitigate the effects. Therefore techniques like HAZOP, FMEA or FTA cannot be useful for identification of security threats but they might be useful for the identification of vulnerabilities and critical points.

3.3.1.2 Risk Consequences

When a safety hazard occurs there will always be an effect on the organization or installation, say ship or port facility. Therefore consequences have to be not only identified but also measured in some way. Techniques like HAZOP or FMEA identify hazards and also the potential consequences of those hazards, but they do not assess consequences in a structured way. According to Frame (2003), to assess these consequences a process of risk impact analysis is necessary that can be developed by qualitative or quantitative analysis.

In terms of safety, the outcome of a hazard could involve injury to personnel, damage to property, pollution of the environment or a combination of all three (Kuo, 1998, p. 48), hence the estimation of the consequences is developed in this context. However, with respect to security, one additional element should be taken into account: Criticality. This element is for example mentioned by GAO (2001) that bases its risk management approach on enhancing the level of preparedness for terrorist threats, on assessments of threat, vulnerabilities, and criticality. Criticality involves some specific operations, assets or functions where the impact of a threat will affect not only that component but also the entire system and for that reason are deemed as critical. Therefore, the impact on these particular points should be especially analyzed in a security case to prioritize the measures to protect them.

3.3.1.3 Determination of Risk level

The final step of risk analysis is constituted by the assessment of risk level. Our basic equation to define risk is now complete with the likelihood and the consequences of the hazard already determined. Either qualitative or quantitative, the values assigned to likelihood and consequences can be placed in a likelihood-impact matrix or Risk Matrix. Figure 3.3 shows a risk matrix for qualitative data.

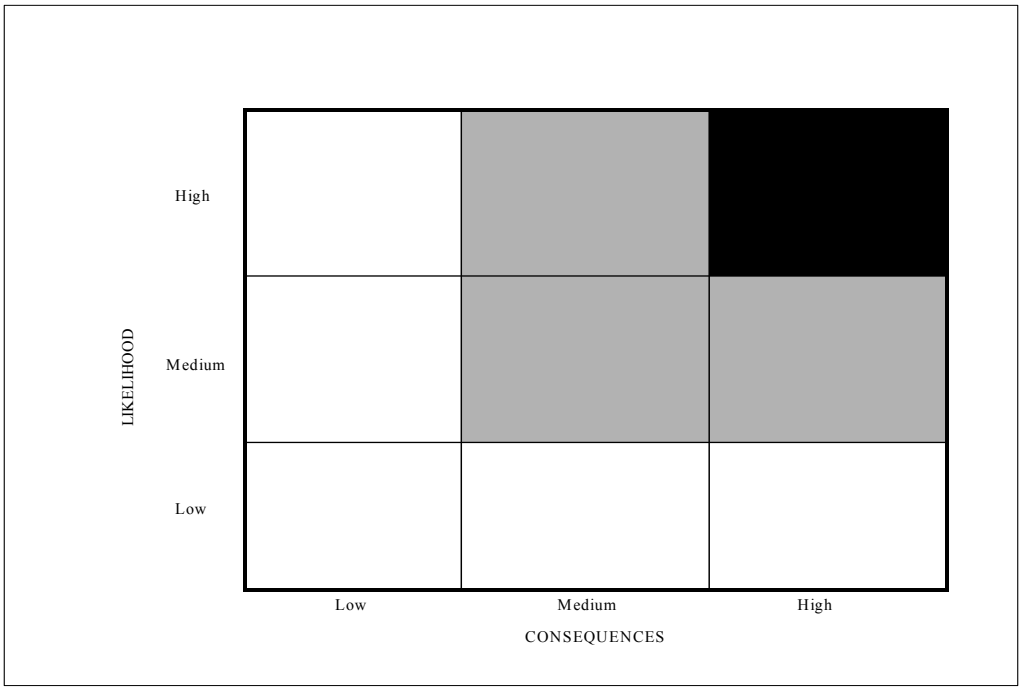


Figure 3.3. Risk Matrix to categorize risk events qualitatively

Source: Davidson Frame, 2003, p.76

It can be seen in figure 3.3 how risk is categorized in function of likelihood and consequence. The outcome of this matrix establishes the level of risk that the identified hazards impose. For instance the black zone represents a high level of risk because the likelihood is high and the consequences are high as well, therefore it should attract especial attention for the implementation of measures to reduce its level of risk. This matrix has been constructed with qualitative information, however, if quantitative data is available the risk matrix can be built in the same way. The

most important thing in this analysis is that the level of risk that a hazard imposes on the organization is known.

Defining a level of risk in terms of security is, however most complicated due to the several elements involved and to the degree of uncertainty that threats like terrorism represent. Four elements should be taken into account: Threat, Vulnerability, Consequences and Criticality. If threat is uncertain then one possibility to assess it is defining subjectively what are the most credible threat scenarios for the specific target. Then the level of security risk is defined by vulnerability and consequences. Another possibility is to give a qualitative value to the relation threat-vulnerability and compare these results with the potential consequences. Different approaches to deal with the determination of security risks will be shown in the description of the current security assessment approaches of the USCG and the NSA.

Finally, with the level of risk estimated, some preliminary recommendations can be made to mitigate or reduce this level of risk. The next phase then involves the evaluation and management of risk in economical and technical terms. The level of risk that we are able to accept is the most important question. As we have said at the beginning of this chapter risk is part of our lives and is also true that it is almost impossible to reduce it to zero. In terms of safety some risks can be deemed as negligible but in terms of security this can be at least debatable. The next section will analyses this problem in more detail.

3.3.2 Risk evaluation/ management

Now that the risk analysis phase is finished with the outcome of the level of risk defined, it is time to take decisions. First of all we have to define which risks are acceptable and which are not. Some of them should be obviously unacceptable due to their high likelihood and adverse effects. However, those that are in the so-called grey zone could be accepted to some degree. Therefore an intolerable, tolerable and negligible region is established for safety risks.
An intolerable risk implies that the presence of the hazard in the system cannot be accepted. A tolerable risk means hazards in the system that may give rise to

accidents and therefore they should be reduced only if it is economically justifiable. Finally a negligible risk is one that is unlikely to lead to accidents and any effort to reduce it is worthless.

With the level of acceptance defined then the next step will be to analyse if the existent control measures are adequate. If they are adequate then no further actions are necessary, however hazards should be evaluated regularly in order to identify changes in the level of risk they impose. On the other hand, in case control measures are inadequate or nonexistent, then adequate reduction measures should be developed.

At this point one important thing emerges. Risk reduction measures should be developed on the basis of some criteria to be able to decide if they are acceptable. Acceptability of a measure will imply that it must be feasible and also affordable. This situation is faced in safety with a principle known as “ALARP” (As Low as Reasonable Practicable).

According to the ALARP principle, as much effort as is reasonably practicable needs to be made to reduce safety risks to an acceptable level. According to Kuo (1998) “reasonably” implies that the appropriate effort is made to achieve reduction of risk, and “practicably” means that if a reduction measure is not practical then it is not possible to be applied. The effort may be represented in economical terms or in time and balanced against the reduction of risk level. In case the reduction of risk is insignificant in relation to the cost of implementing the measure to obtain that reduction, then it is not reasonably practicable to implement that measure. Several other considerations, of course, are involved in the process; some of them are political and social while others lie in the context of private interests.

Another methodology to evaluate the acceptability of risk control measures is known as Cost-Benefit Analysis. Kuo (1998) says that to utilize the cost-benefit approach it is necessary to compare the measures selected with an appropriate monetary valuation of risk reduction. One interesting example of this valuation can be found in risk assessments related to the protection of the environment. These studies

evaluate, for example, “costs per averted spill”, ranking the risk control options according to cost-effectiveness.[3]

The economic evaluation of risk reduction measures related to safety is a difficult task due to the number of factors involved, some of which are purely technical but others that lie in social and political aspects and indeed private interests play an important role. In a security context the economic considerations of risk reduction measures should be taken into account as well. However, as it will be shown in the next chapter, current approaches to the ISPS Code consider this marginally or do not consider it at all. What the acceptable risk level in security is something not mentioned in the ISPS Code but is necessary to discuss. The maritime industry is a business and therefore, as it has said in section 3.2, it should achieve the adequate balance among competitiveness, specification, cost- effectiveness, safety and now security.

3.4 An initial Security Assessment Framework

The previous sections have shown and analysed the basic theory of risk and have demonstrated the importance to manage risks in a structured way. Risk Management represents an invaluable tool to manage risks establishing a logical process for planning, assessing risks and controlling the efficiency of the measures implemented. Risk Assessment, as a main part of the Risk Management Process has been shown step-by-step as a detailed framework to identify risks, estimate their consequences, establish their level and develop risk reduction measures that are acceptable, feasible and affordable.

All these processes have been analysed mainly in a safety context, however, a number of particularities emerge with the application of the Risk Management framework to manage security risks. These can be summarized as follows:

[3] The complete information can be found in the report of Risk Analysis of Navigational Safety in Danish Waters, June 2002, < http://www.frv.dk/en/publikationer/risikovurdering/Summary.pdf> (July 6, 2004)

- Security risks involve elements external to the typical environment of the ship or port facility with the additional feature that they are intentional; therefore they are not possible to be controlled from the ship or port facility standpoint.
- Some security threats like terrorism do not generate statistical patterns, therefore it is difficult to assess likelihoods for these threats when there is insufficient information. In this sense to perform a Risk Security Assessment will be necessary to assume a certain level of threat represented for some credible threat scenarios and then focus the study to assess vulnerabilities, consequences and critical points in order to manage security from elements that are under the control of the ship or port facility.
- Techniques for identification of risk and the consequences are useful in identifying safety hazards in complex systems. In a security assessment, however, what is necessary is to identify vulnerabilities, consequences and criticality. Therefore it is in the identification of these factors where qualitative techniques like HAZOP, FMEA or FTA could be used.
- Risk reduction measures for security risks should take into account two important factors: one is concerns the level of security risk that should be accepted and the other is related to the economical considerations of the implementation of measures to reduce security risks.

Therefore, a risk security assessment framework that takes into account these considerations is necessary. Figure 3.4 suggests an initial framework for security assessment where all the particular elements related to security have been included. This initial security assessment framework focuses then on the assessment of threats either for likelihood or to fix some credible threat scenarios to work on; identifying these assets and operations that are critical for the ship or port facility; the assessment of the vulnerabilities of the security system related to the assumed threat scenarios; an estimation of security level based on the assessment of the existing measures and the evaluation of threat-vulnerability-consequences or vulnerability-consequences; finally the evaluation of the proposed measures based not only on technical factors but also on economical considerations.

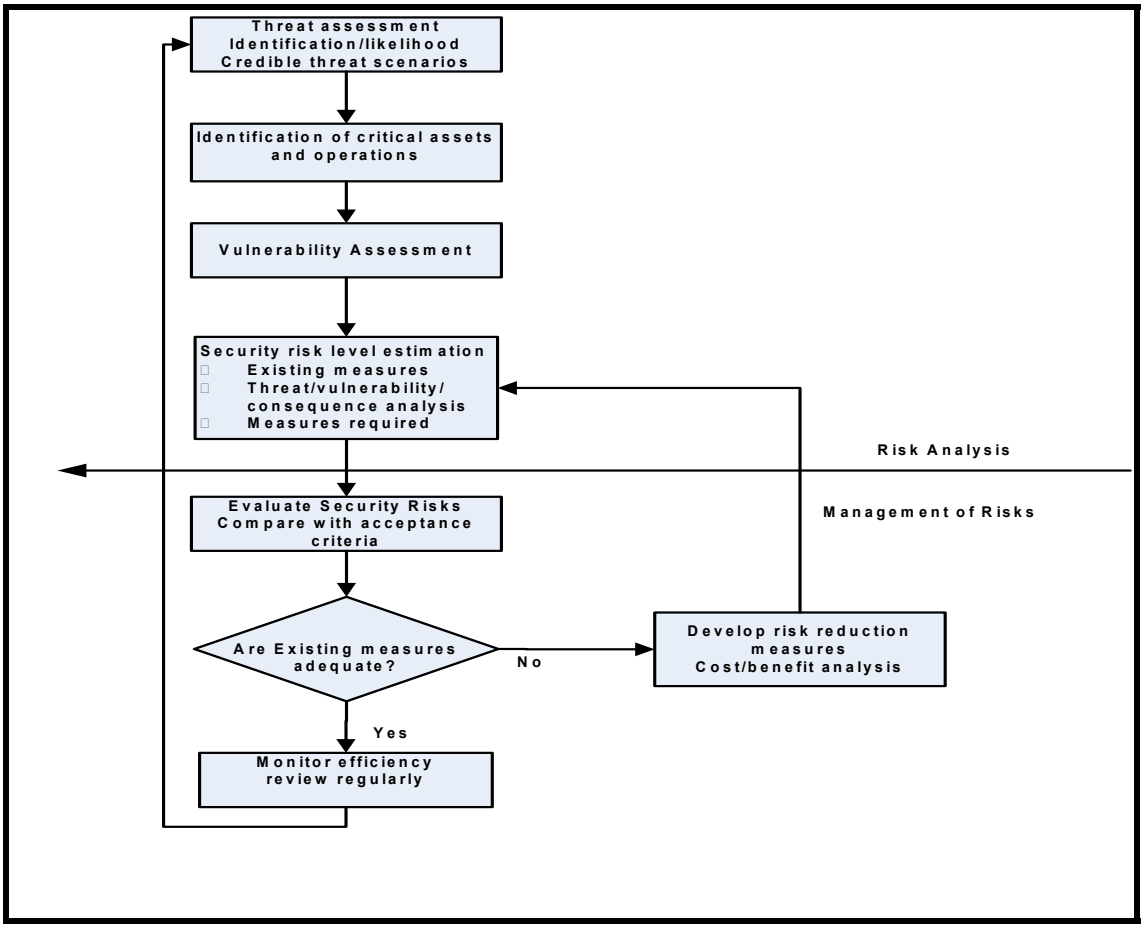


Figure 3.4. Initial Risk Security Assessment framework

Source: Adapted from Schröder, 2004 and Waring and Glendon, 1998

3.5 Conclusions

This chapter has highlighted the main particularities concerning risk from the security standpoint and has also shown how the risk management framework in general and the risk assessment framework in particular could be adapted for security purposes, taking into account these peculiarities. Moreover, an initial security assessment framework has been suggested based on the specific requirements that the security context implies.

The security assessment framework suggested will be used now as a general reference to analyse how the security assessment approaches proposed by the USCG and the NSA consider the specific requirements of security. Also some

hazard identification techniques used for safety risk assessments will be selected and analysed to identify their capabilities to fulfil the particular requirements of the security assessment framework introduced in this chapter. This task will be developed in the following two chapters.

CHAPTER 4 CURRENT APPROACHES FOR SECURITY ASSESSMENTS

The new maritime security framework, as it has been seen in chapter 2, is based on risk management principles. In particular the ISPS Code provides a basic methodology for security assessments in ships and port facilities. However, despite the efforts made by the IMO, the implementation process is a difficult task, mainly due to a lack of experience on the topic and the limited time available before the new regulations enter into force. With the intention to solve these problems two approaches were developed in order to carry out security assessments: The USCG Security Guidelines for Vessels and the NSA "Guideline for Performing Ship Security Assessment".

Both security assessment methodologies attempt to follow the risk-based approach given by the ISPS Code, but face the assessment of maritime security risks in a particular way. This chapter will analyse these two approaches with the objective of identifying their main features in reference to those issues previously highlighted in chapter 3, with regard to the application of risk management for security purposes.

4.1 The United States Coast Guard approach

One of the approaches for security assessments established by the ISPS Code has been developed by the United States Coast Guard (USCG) through its Navigation and Vessel Inspection Circular 10-02 Security Guidelines for Vessels (NVIC 10-02) and Navigation and Vessel Inspection Circular 09-02 Guidelines for Port Security Committees and Port Security Plans required for U.S. Ports (NVIC 09-02). NVIC are used internally by the USCG to ensure that inspections and other regulatory actions conducted by its field personnel are adequate, complete and consistent.

Additionally, seafarers and the shipping industry normally use NVIC as a means of determining how the USCG will be enforcing certain regulations.[1]

4.1.1 Ship Security Assessment

Guidance on Performing Security Assessments for vessels is given in Appendix B of the NVIC 10-02. This security assessment approach is based on a Risk-based decision-making concept, which is a "systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function and to identify actions to reduce the vulnerability and mitigate the consequences of a security breach"(USCG, NVIC 10-02, Appendix B). In this context NVIC 10-02 suggests a simplified risk-based security assessment consisting of five steps that can be seen in Figure 4.1.

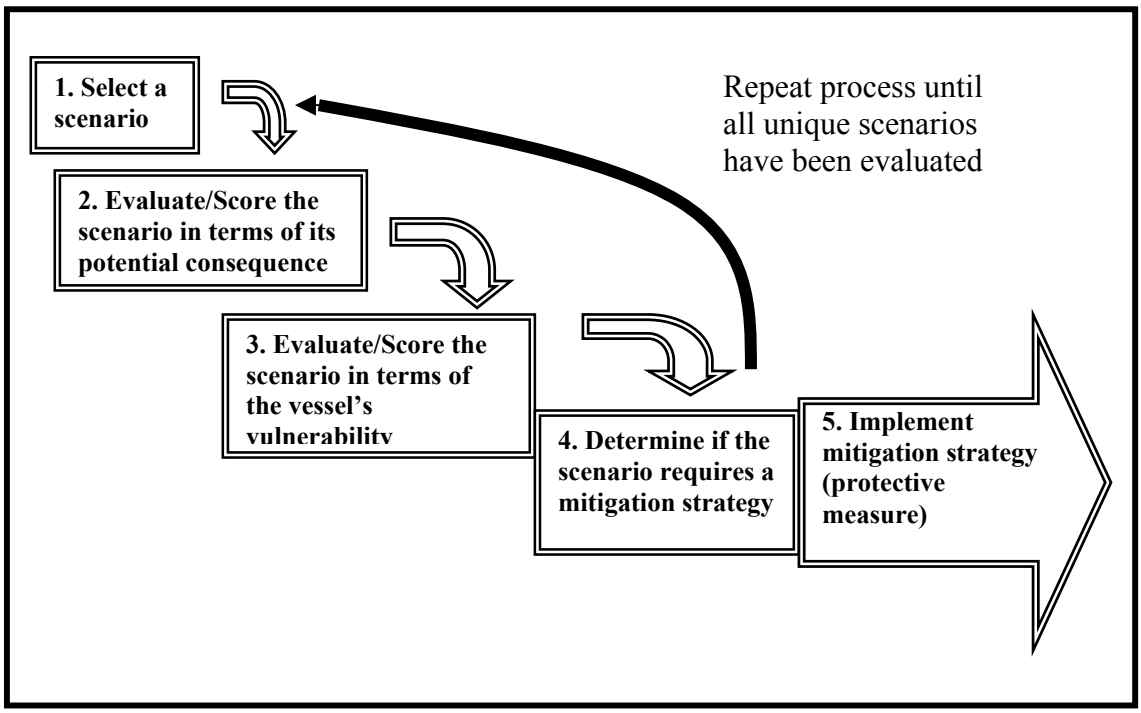


Figure 4.1: Simplified risk-based security assessment process
Source: NVIC 10-02

[1] NVIC provides detailed guidance about the enforcement or compliance with certain US Federal marine safety regulations and USCG marine safety programs. An overview about NVIC's can be found in http://www.uscg.mil/hq/gm/nvic/index.htm

Step 1 in this process implies a threat assessment. Attack scenarios should be developed based on the potential threats to the vessel under specific situations. For example, a terrorist group to be considered a threat must not only exist, but also have the intention and capability to launch attacks (GAO, 2001). This step therefore requires an important element of intelligence information that is not always available. For this reason the model recommends that an initial evaluation should at least consider three types of scenarios:

- Intrude and/or take control of the vessel
- Externally attack the vessel
- Use the vessel as a means of unlawful activities.

Step 2 evaluates each scenario in terms of consequences. For this purpose death and injury, economic impact and environmental impact, are the basic parameters to assess the consequences of an attack. The consequences are then scored in three levels: catastrophic (3), significant (2) and moderate (1). Usually the appropriate rating at these levels is assigned taking into account the worst scenario, which means that if the consequence of the attack in terms of death and injury is low but the environmental impact is high the overall consequence score should be assigned the highest level.[2]

In Step 3 each scenario created in Step 1 is evaluated in relation to the ship's vulnerability to an attack. This process implies the following general elements of vulnerability (USCG, 2003):

- Availability. – The availability of a target measures its presence and predictability as it relates to an enemy's ability to plan and conduct an attack.

[2] Hazard Severity Categories from Military Standard STD-882C have been used as a reference for these type of evaluations in: US General Accounting Office Report to Congressional Requestors: *Combating Terrorism: Threat and Risk Assessments can help prioritize and target Program Investments,* April 1998. (GAO/NSIAD-98-74) (http://www.gao.gov/archive/1998/ns98074.pdf, accessed on 19 June 2004)

- Accessibility. – Evaluates if the target is physically accessible to be attacked. It evaluates its physical deterrence against different attack modes in terms of physical and geographic barriers that deter the threat without organic security.
- Organic Security. – Assesses the ability of the target's security measures to deter an attack. It includes security plans, communication capabilities, guard forces, intrusion detection systems, and ability of outside law enforcement to prevent an attack.
- Target Hardness. – It is a measure of the ability of a target to withstand attack. It is based on the complexity of target design and material construction characteristics.

The model given by the NVIC 10-02 only considers the Accessibility and Organic Security elements for the vulnerability assessment because they are under the control of the company.[3] Then each scenario is assessed with reference to these two elements and placed according to the following categories:

- No deterrence (Category 3)
- Good deterrence (Category 2)
- Excellent deterrence (Category 1)

In Step 4 the consequence and vulnerability scores of each scenario are correlated to determine which of them needs to develop mitigation strategies. For this purpose three mitigation categories are defined: mitigate, consider and document. Mitigate means that protective measures should be developed to reduce the current level of risk. Consider means that the specific scenario should be taken into account but protective measures may or may not be developed based on the analysis of each particular case. Document means that the scenario does not require immediate protective measures and therefore only should be documented in order to be considered in future evaluations. Table 4.1 shows the matrix result of this step.

[3] According to SOLAS Chapter XI-2 Regulation 1 Company means a Company as defined in regulation IX/1: The owner of the ship or any other person who has assumed the responsibility for the operation of the ship. The author is using this term in the same meaning.

Table 4.1: Vulnerability & Consequence Matrix

		Total Vulnerability Score Accessibility + Organic Security= Total Score		
		2	**3-4**	**5-6**
Consequence Score	**3**	**Consider**	**Mitigate**	**Mitigate**
	2	**Document**	**Consider**	**Mitigate**
	1	**Document**	**Document**	**Consider**

Source: NVIC 10-02

Finally in Step 5 mitigation strategies are implemented for those necessary scenarios. In this step the model also gives a model table with the purpose to help companies evaluate the effectiveness and feasibility of each specific mitigation strategy. The idea is to evaluate if the mitigation strategy reduces the risk and if its implementation is feasible in cost-benefit terms.

4.1.2 Port Security Assessment

Guidance to Port Security Assessment is given in enclosure (3) of NVIC 9-02. This model follows the same risk-based decision making process of NVIC 10-02. However, one step is added in order to define which assets or infrastructure is necessary to protect. Figure 4.2 shows the process suggested by this model.

A step for a Criticality Assessment is considered in this model with the purpose to identifying activities, operations and infrastructure that are critical to a port. The criticality of these key elements is evaluated in the function of 3 parameters:

- Mission
- Effect of Target Destruction
- Ability to Recover

Based on these parameters criticality is rated in three scales:

- Critical
  - Support multiple missions

- Several consequence effects
- Difficult or impossible to recover in a timely manner

- Moderate
  - Support one or two missions
  - One or two consequence areas
  - Reasonable ability to recover
- Marginal
  - Do not support any mission
  - Limited to minimal effects
  - Back up or redundant systems in place.

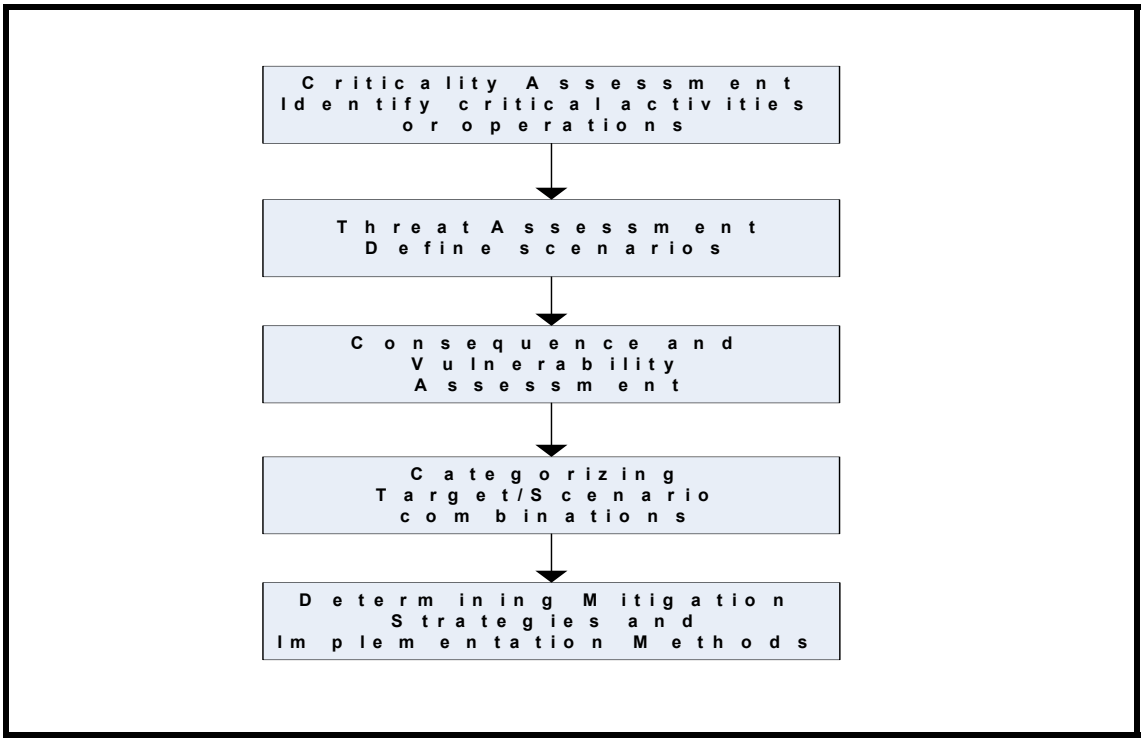


Figure 4.2: Port Security Assessment Process

Source: Adapted from NVIC 9-02

The rest of the process considered in this model is almost the same as the NVIC 10-02 methodology for vessel security assessments but tailored for the purpose and particularities of ports in general and port facilities specifically. Therefore it is not necessary to repeat the process described in the previous section. An analysis of the whole approach is made in the following section.

4.1.3 Considerations related to the USCG Security Assessment Approach

The USCG Security Assessment approach is focused mainly on the analysis of consequences and the vulnerabilities of the vessel or port facility in order to determine what measures are necessary to implement. This approach does not include any judgment about likelihood of threats and use of basic foreseeable scenarios to start the security assessment. This is understandable since there is always the possibility of lack of specific and credible intelligence to assess the level of threat. In those cases therefore, for the purpose of the assessment, it is better to fix the threat at a certain level consistent with the security levels to be set by the government and then changes in security levels will be the reference for future modifications of the assessed threat levels.[4] The advantage of this approach is that it is not necessary frequent updates of the security assessment (Schröder, 2004a).

This characteristic, however, has the disadvantage that could generate too many mitigation measures because the security assessment team will have the tendency to cover all the possibilities in the subjective limits of the security levels. The problem is that this situation weakens the essence of the Risk Based Decision Making model which seeks to avoid mitigation measures based on worst case scenarios and is therefore out of balance with the threat. [5]

Another interesting observation in relation to the USCG Security Assessment approach is that this model only touches marginally on the important role of cost-benefit evaluation. Mitigation measures not only have to be effective but also feasible, and feasibility implies the fact that the costs of the implementation of the mitigation measures should be affordable. In this context the question of what level of security risk is acceptable becomes important because different designated

[4] This concept has been extracted from the approach for threat assessment commented upon by the USCG in Department of Homeland Security, Implementation of National Maritime Security Initiatives. 1 July 2003, p. 39245.

[5] The US General Accounting Office has issued several documents related to the application of Risk Management for the design of countermeasures against terrorism. The RBDM model used by the USCG is based on these recommendations, which emphasize the necessity to prioritize risk to develop countermeasures in balance with the risk to avoid unnecessary costs. GAO reports can be found on its web page www.gao.gov.

authorities in different countries could have different criteria in this respect. The real problem is whether or not the USCG will accept these other criteria in case the current discussion at the US Congress with regard to a measure requiring ships calling at US ports to be equipped with SSP approved by the USCG, succeeds (Mc Laughlin, 2004).

One final observation concerning the USCG approach refers to the vessel security assessment model. The simplified process offered by the USCG does not follow the ISPS Code methodology. In particular there is no mention related to the Identification of Key Shipboard Operations, a criticality factor that is only considered for port security assessments.

4.2 The Norwegian Shipowners' Association approach

The Norwegian Shipowners' Association developed in 2003, with the support of Det Norske Veritas, a "Guideline for Performing Ship Security Assessment" (NSA, 2003) conceived as a practical tool to help shipowners/operators in the task of carrying out ship security assessments according to the ISPS Code. As is stated in the Guideline itself, it has been prepared in direct concordance with Part A and Part B of the ISPS Code taking into account the recommendations given in the USCG NVIC 10-02.

In this model the ship security assessment (SSA) process has been divided into 8 steps. The first three steps have the objective to identify and evaluate the current situation of the ship in relation to factors concerning motivation to threaten the ship, key shipboard operations and existing security measures. The result of this phase is mainly a matrix that links two categories of critical operations (High /Low) with two options for security measures (Yes-implemented/ No-implemented). The matrix then identifies those highly critical operations for which no security measure has been implemented. Figure 4.3 shows the matrix.

Steps 4 and 5 are a threat and vulnerability assessment. The objective of this phase is to identify, on the basis of the information obtained in the previous steps, the vital few scenarios that imply the highest risk. In this sense, regardless of whether a

motivation exists or not, a set of possible threats and consequences are defined and finally a matrix compares two categories of scenarios (unlikely/not unlikely) with three categories of consequences (moderate, high, extreme). The matrix outcome then identifies those not unlikely scenarios with high and extreme consequence that is necessary to take into account in the development of new security measures. Figure 4.4 shows this result.

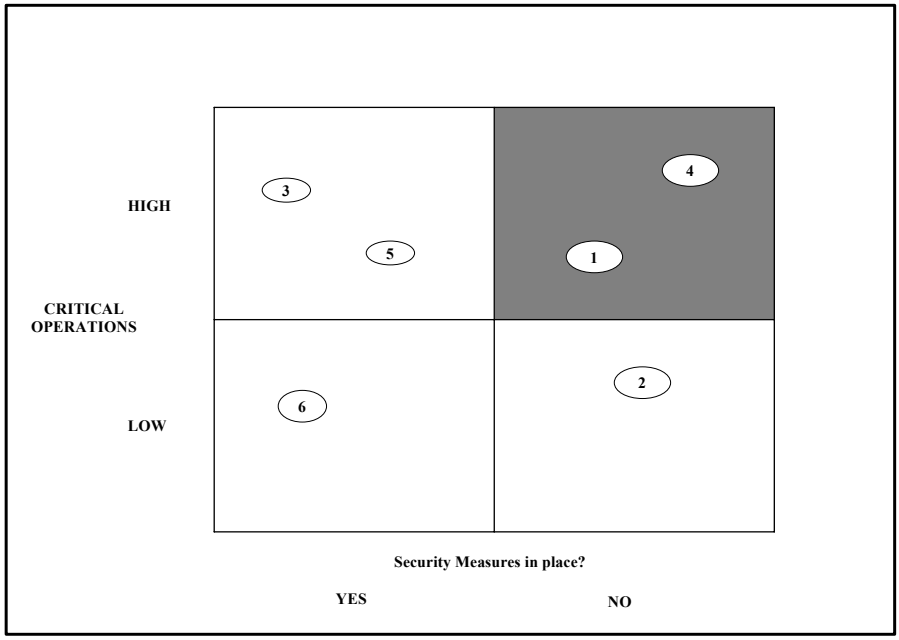


Figure 4.3: Identification of security measures necessary to implement.
Source: NSA Guidelines for Performing SSA

Steps 6 and 7 develop a process to carry out an onboard security audit. In that sense an onboard ship security survey checklist is created on the basis of the information gathered in the previous phases. This ship security survey checklist consists of a number of issues to check, which will permit the identification of the most important security measures necessary to implement and also those security measures already in place that present some degree of conflict with safety, for example.

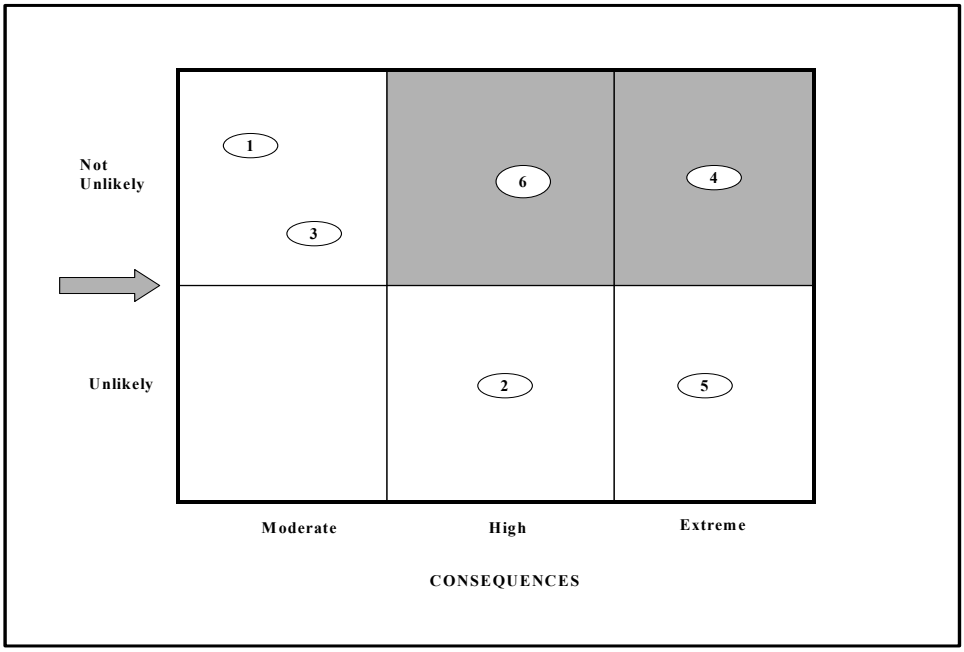


Figure 4.4: Identification of not unlikely scenarios/high and extreme consequences
Source: NSA Guidelines for Performing SSA

Finally, Step 8 identifies weaknesses in the system and therefore those issues where it is necessary to improve security measures or fill some possible gaps. Figure 4.5 shows these 3 final steps whose outcome forms the basis for the Ship Security Plan.

4.2.1 Considerations related to the NSA approach

The NSA approach follows closely all the provisions established in the ISPS Code concerning the ship security assessment and includes detailed cross-references to these provisions. This approach has the virtue to give an order to the sometimes-confused diversity of provisions of Part A and Part B of the code helping in this way to keep always an overview of the whole process. For example Part A section 8.4.2 of the Code establishes the process for identification of key shipboard operations, however the guidance given in part B section 8 does not precise exactly what are these operations. Step 2 of the NSA approach establish clearly that sections 8.3, 8.6

and 8.8 of Part B should be taken into account to prepare a list of security-critical operations, systems, areas, and personnel onboard.

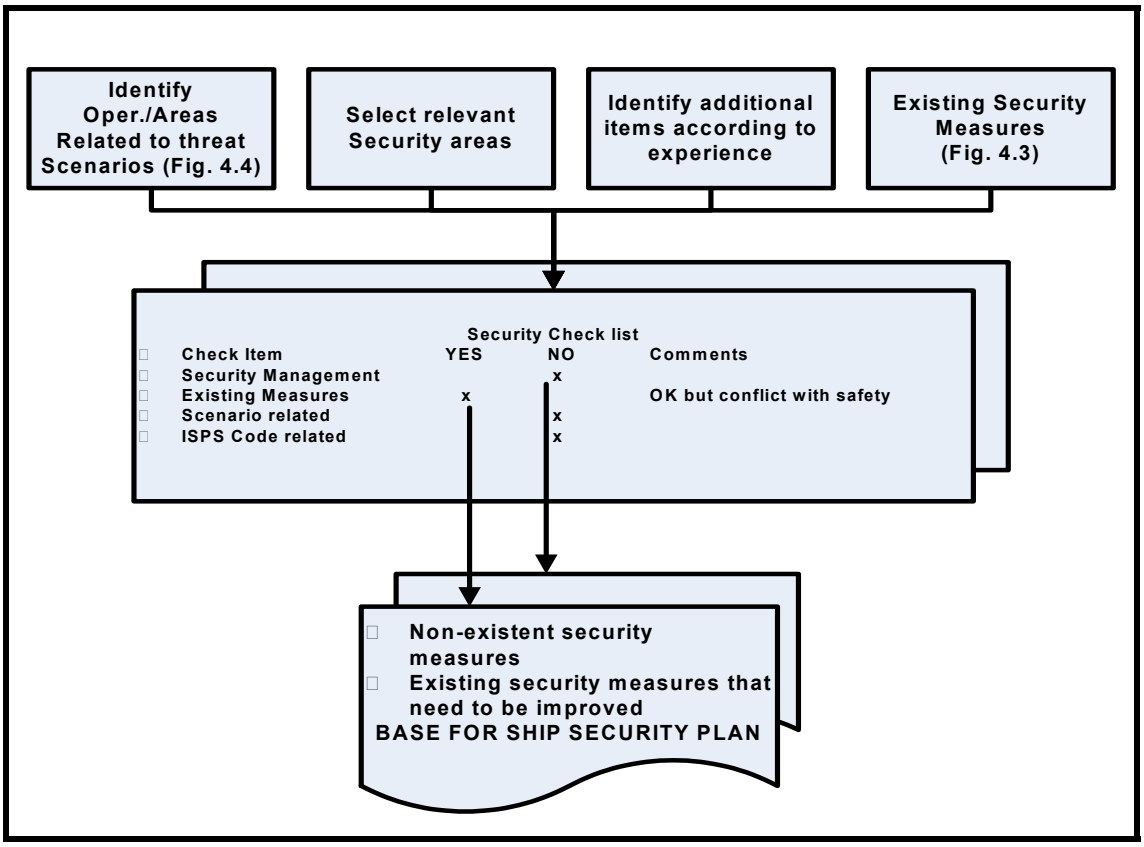


Figure 4.5: Onboard audit process and identification of security measures to be implemented.

Source: Adapted from NSA Guideline for performing SSA

One more specific observation concerning this approach is that cost benefit analysis is not taken into account in the process. Cost benefit analysis is, however, an issue that should be considered because these new security measures imply additional costs for companies. One of the objectives of the ISPS Code is to ensure confidence that adequate and proportionate maritime security measures are in place. This means that the security measures should be proportional to the assessed risk and therefore should include their economic impact. The level of security risk that is acceptable is again the key concept in this issue.

Another observation of the NSA approach is that contrary to the USCG approach, this model deals with likelihoods. Step 5 assesses ship vulnerability to threats in terms of likelihood and potential consequences, identifying those “not unlikely” scenarios with high and extreme consequences. This model has the advantage that the selected security measures will be focused only in those most probable risks leaving aside those that are not likely, meaning a significant saving in costs and effort. However, being the model based in likelihoods, the problem is that the assessment should be continuously revised when changes in the likelihood of threats have been detected. This disadvantage unfortunately could offset the advantage mentioned above.

4.3 Conclusions

The main advantages and disadvantages of these two approaches have been already highlighted in the respective section. However, in these conclusions it is necessary to remark on one characteristic of both approaches that has been observed as a deficiency: the lack of mention of the economical implications related to security measures. The impact of these measures in economical terms should be put in balance with the threats we are facing. How real are these threats in practice to justify the security measures that security studies recommend is an important question. The application of the correct methodologies and tools available to perform security studies must be the answer. We are going to analyse in the next two chapters the implications of the application of different tools for risk security analysis.

CHAPTER 5 CURRENT APPROACHES TO SAFETY RISK ASSESSMENT TECHNIQUES

It has been shown in Chapter 4 the USCG and NSA approaches for the compliance of the ISPS Code. Even though they attempt to be more detailed tools to help in the development of security assessments, in practice they are still guidelines. In fact they say what to do but not too much how to do the study. Therefore, more specific and structured tools are required to systematically analyse security of complex systems like port facilities or ships, no matter what methodology you decide to use.

In Chapter 3 it was mentioned some current approaches for safety risk assessments. Techniques like HAZOP, FMEA and FTA are used mainly for risk identification in safety assessments in the chemical, nuclear and offshore industry, looking for possible causes of safety risks and the potential consequences that those risks could produce. These techniques are therefore support tools that help to develop some of the main stages of the risk assessment process. Sometimes more than one technique could be necessary to fulfil the necessities of evaluation of a complex system.

It has been seen also, the problems that the context of security implies: lack of information in most of the cases and the uncertainty of the threats faced. This situation brings about the necessity to assess security focusing our attention on criticality, vulnerabilities and consequences in function of the identified potential threats. This approach is reflected in the introductory security assessment framework proposed in Chapter 3.

The objective of this chapter, in this sense, is to analyse in some detail the mentioned risk identification techniques in order to identify their strengths and weaknesses in relation to the specific requirements of the proposed preliminary security assessment framework. Identification of critical operations and assets and

identification of vulnerabilities are some of the steps where it could be anticipated that these techniques can be applied. HAZOP, FMEA and FTA techniques have been selected for this purpose.

5.1 Hazard and Operability Studies (HAZOP)

The Hazard and Operability Study (HAZOP) is a qualitative method for risk identification, which is usually employed in the chemical and petroleum industries where complex systems are involved. Imperial Chemical Industries (ICI), a very large international company based in the United Kingdom, developed HAZOP, but the technique only started to be more widely used in the chemical industry after the Flixborough disaster in which a chemical plant explosion killed twenty-eight people in 1974.[1]

HAZOP is a systematic approach for identifying potential hazards in complex systems and uses "guide words" in order to identify deviations from the design objective of a system and its components (Kuo, 1998). HAZOP basically analyse all the operations of an industrial plant, which for that purpose is divided in several more manageable parts. Then, each part is analysed in detail to identify hazards related to its operation. (Dickson, 1991, p. 57).

5.1.1 Definition of Hazard

Prior to describe and analyse HAZOP, it is necessary to define Hazard in order to be clear with respect to the meaning of this term in a safety context. According to Kuo (1998), hazard is "an undesirable outcome in the process of meeting an objective, performing a task or engaging an activity" (p. 48). In safety, the undesired outcome could involve: Injury to personnel, damage to property, pollution of the environment or a combination of these events. This means that and event or situation only can be

[1] This disaster led to a significant tightening of the UK government's regulations covering hazardous industrial processes. For complete information see:
< http://www.wordiq.com/definition/Flixborough-disaster> (12 July 2004)

deemed as a hazard in case it leads to an undesirable outcome and therefore there is a risk level associated with that hazard.

In this sense, to identify a hazard firstly it is necessary to define the objective of the system or subsystem under analysis. Secondly, the possible deviations from that objective should be identified. Thirdly, the causes of these deviations should be deducted; and lastly, the potential consequences of the deviations are assessed. This process must be developed systematically and for that purpose is carried out in a number of sequential steps.

5.1.2 The Security Context for a HAZOP study: Vulnerability and Criticality

The preliminary security assessment framework shown in chapter 3 requires the identification and evaluation of vulnerabilities related to a selected threat scenario as an important part to estimate the security level of a ship or port facility. Also this framework considers the identification of critical assets and operations in order to focuses our attention on those points whose failure could represent a major damage to the whole system. The development of this task requires a structured and systematic analysis of the ship or port facility that could be addressed by a HAZOP study.

Vulnerability has been defined in chapter 3 as a system's property that evaluates the adequacy and effectiveness of safeguards against external threats. Also, Hawkes (1989) has said that maritime security are those measures employed to protect the ship or port facility from piracy, terrorism, sabotage, etc. HAZOP, therefore, could help to identify weaknesses in those security measures implemented for ships or port facilities in the same way it identifies safety hazards: identifying deviations from the design intention, their causes and consequences.

5.1.3 Selection of a Multidisciplinary Team

HAZOP is best carried out by a team, which jointly will derive the intention of the system under analysis (Dickson, 1991, p. 57). This team should be multidisciplinary

in order to cover the different technical skills necessary to analyse the diverse components of a system. Moreover, the team leader should be a person who is very familiar with the HAZOP technique, and also should act as a facilitator to keep the team on track. The other members do not need to have experience in HAZOP but must be familiar with the design and operation of the system. A good mixture of experience and expertise should be achieved (Bahr, 1997). HAZOP results, therefore, are highly dependant on the performance of this team, which has to use as much as possible its expertise and experience for the benefit of the study.

5.1.4 Security Assessment Team

HAZOP studies require the participation of a team in a way that is highly convenient for the identification of vulnerabilities and criticality of ships or port facilities. The employment of a team to develop a security assessment of a port facility or a ship is the better way to perform this kind of studies. This is because ships and port facilities are complex systems that are better assessed by a group of persons with the adequate expertise and experience not only in matters concerning ship or port operations but also in security matters. This situation has been recognized in the ISPS Code where provisions for the appropriate skills of the persons carrying out security assessments are established in part B.

5.1.5 Division of the system in more manageable subsystems

Once the team has been appointed, the next step is to prepare the necessary data, converting the data to a suitable form, planning the study sequence, and arranging the meetings. Also, in complex systems could be necessary to revise manual operations, operating instructions, logic diagrams, etc. (UOL, 2001). HAZOP requires, likewise, that the system under study be divided in a number of subsystems for which an intention should be defined in relation to some specific aspect or property. This task is important in order to focus the evaluation in those system's properties that are more likely to present hazards in case of deviation from the designed intention.

5.1.6 A Security System to assess

In a safety study, HAZOP analyses a system to identify hazards related to its operation. In a security assessment, it is necessary to analyze the physical and operational measures established to protect the installation (ship or port facility). These physical and operational measures to protect the ship or port facility constitute the Security System of the ship or port facility. Therefore, the system that HAZOP will analyze is the specific security system of the ship or port facility in order to identify vulnerabilities and criticality.

HAZOP also requires a clear definition of the intention of the system and subsystems in order to identify deviations. In that sense, the intention of the security system should be clearly defined. An example of definition could be: " Protect the ship/port facility from unauthorized access, introduction of unauthorized weapons, incendiary devices or explosives; and rise the alarm in reaction to security threats, according to an structured security plan."

This system then should be divided for the HAZOP study in subsystems with a defined intention. Some examples could be the following:

Physical Security. – Physical measures designed to safeguard personnel, prevent unauthorized access to facilities, equipments and documents, and protect it against sabotage, damage and theft (Schultz, 1978). These physical measures can be fences, lights, alarms, locks, surveillance systems, etc.

Operational Security. – Operational measures, procedures, human resources and personnel training to prevent unauthorized access. These measures include investigation of antecedents, restricted access to documents, measures for the control of access (ID cards), measures to control visitors, cargo inspections, etc.

Security Management. – These are measures concerning policies, decisions, organizational arrangements, plans to implement security measures, training

personnel in security aspects and making the whole organization involved in the security of the ship or port facility.

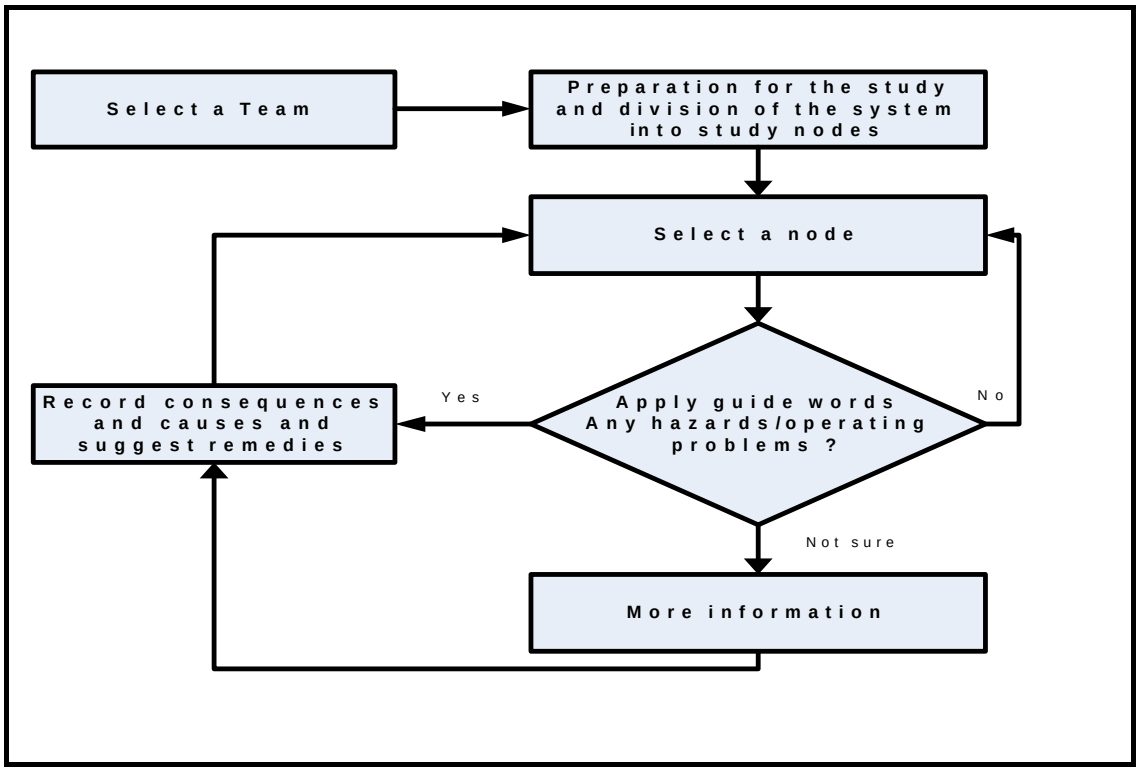


Figure 5.1. The HAZOP Process

Source: Adapted from: *Hazard and Operability (HazOp) Studies*. Retrieved July 12, 2004, from University of Florida, Unit Operation Laboratories Web site: http://pie.che.ufl.edu./guides/hazop/

5.1.7 Application of the Guide Words

Figure 5.1 shows the entire process of HAZOP and particularly the application of the specialized guidewords. Guidewords are designed with the purpose to provide the team with a structured approach to systematically identify all the deviations from the defined intention. They are applied to the parameters of the system previously defined and assist the team to identify not only if some property of the system is deviating from the intention but also if this deviation is complete, partial or in some way the qualitative conditions of the property have been altered. In table 5.1 we can see typical guidewords used for HAZOP studies, however new and case specific

words can be developed to suit the particular needs of a study, type of system and objectives.

Once the potential deviations are identified, the team should evaluate all possible causes, even those less obvious ways in which a deviation may occur (Lihou, 2004). This is an important feature because it allows the team to identify not only known causes but also unknown causes of hazards. Consequences also are considered in the HAZOP study. They can be produced by the deviation or by the cause itself. This situation highlights the fact that some conditions that by themselves are not deemed as hazards can produce together deviations with adverse consequences and therefore should be taken into account in the study.

Table 5.1 – Typical HAZOP Guidewords.

Guide Words	**Meanings**
No or Not	This is the complete negation of the intention
More Less	There is an increase or a decrease in the quantity of the property
As well as	There is a qualitative increase in the property
Part of	There is a qualitative decrease in the property
Reverse	The logical opposite of the intention
Other than	The complete substitution of the intention

Source: Dickson G.C.A. (1991). *Risk Analysis*. London: Witherby for the Institute of Risk Management

5.1.8 Guidewords to analyze a Security System

Since we are looking for vulnerabilities, then, the HAZOP guidewords will help to identify those parts where the system presents weaknesses. For example, if the physical security system is analyzed in relation to a piracy scenario for a ship, some physical measures to consider could be: high-powered strobe lights, alarm systems, water hoses, etc. The parameter to identify deviation from the planned intention is in this case (as in the majority of security threats) preventing unauthorized access to the ship. Then, applying the adequate guidewords it can be found, for example, whether or not there is an alarm system implemented, if it is working well, the possible causes for that situation and the potential consequences. The overall study

of this subsystem will give then a complete and comprehensive measure of the level of vulnerability of the ship in terms of physical security for the specific threat scenario.

5.1.9 Record the results

The outcome of the previous step is a list of causes and consequences from the deviations evaluated with the guidewords. Also some actions to eliminate or mitigate the hazard are suggested during the study taking into account the level of risk it imposes and whether appropriate control measures are already in place or not. This information then should be recorded in a systematic and structured way.

Table 5.2 – Form for recording HAZOP results

Subsystem: Physical Security **Subsystem: piracy alarm system** **Intention: Prevent unauthorized access to the ship**						
Guide Words	**Deviation**	**Causes**	**Consequences**	**Actions**	**Accessibility**	**Organic Security**
No or Not	There is not warning in case of a piracy attack	1. There is not alarm system in place. 2. The alarm system is not working.	1. Unauthorized access to the ship. 2. The ship hijacked by pirates	1. Installation of an alarm system for piracy. 2. Reparation of the alarm system already in place.	Not applicable	No deterrence capability
Part	The alarm signal does not reach all crew compartments	1. System failure 2. The system only considers signal to the bridge.	1. The crew is not alerted timely. 2. Possibility of unauthorized access increased.	1. Repair the system 2. Consider the adequacy of a system that considers signals in all crew compartments.	Not applicable	Limited deterrence capability

Source: Adapted from Dickson G.C.A. (1991). *Risk Analysis*. London: Witherby for the Institute of Risk Management

5.1.10 Recording the results for a Security case

Table 5.2 shows the record of the application of HAZOP for a vulnerability assessment. The physical security subsystem of a ship is assessed in relation to a pirate scenario and the HAZOP guidewords are applied to the piracy alarm subsystem. Then, the possible deviations of the intention of the subsystem (prevent unauthorized access) are recorded, as well as the potential causes and consequences. Note that two columns have been added to the basic HAZOP format in order to record vulnerability factors related to accessibility and organic security. This record represents a “living document” because it should be updated periodically helping in the management of the security system in a similar way that a Safety Management Plan with respect to a Safety Management System. In this manner, the necessary information to assess the vulnerability of the whole system is recorded systematically.

5.2 Failure Mode and Effect Analysis (FMEA)

The FMEA methodology was developed initially in the United States Military. The Military procedure MIL-P-1629, titled “Procedures for performing a Failure Mode, Effects and Critically Analysis” was issued on November 9, 1949. Some years later a working group representing Chrysler Corporation, Ford Motor Company and General Motors Corporation developed a Quality Management System based on ISO 9000 standards, which included the use of FMEA as part of its compliance requirements. In 1993 the American Automotive Industry Group and the American Society for Quality Control copyrighted FMEA standards widely used in the industry and they were presented in a FMEA manual approved and supported by the already mentioned automakers (FMECA.COM, 2003).

The United States Military Standard MIL-STD-1629A, 1980, defines Failure Mode and Effect Analysis as a “ procedure by which each potential failure mode in a system is analyzed to determine the results or effects thereof on the system and to classify each potential failure mode according to its severity”. This analysis can be performed in any stage of design and operation of the system, however the benefit

of its application is better in early stages of the design process to avoid difficulties to rectify faults later (Wilcox, 2002).

The FMEA should be carried out by a team of professionals with expertise and experience in all the necessary fields concerning the operation of the system under study. In this technique, as in HAZOP studies, the success or failure of the study is highly dependent on a balanced composition of the team with proportional degrees of knowledge and experience.

An FMEA study is usually performed in several sequential steps constituting a structured and systematic procedure. The following description of these steps together with the related security assessment aspects will give a clear idea about this technique and its application on vulnerability and criticality assessment.

5.2.1 Definition of the System to be assessed

The system to be analysed should be clearly defined for which all the internal functions and interfaces of the system are identified and its expected performance are established. Block diagrams illustrating the operation, functions, interrelationships and interdependencies can help in this stage presenting the system as a breakdown of its major functions.

In a security assessment using FMEA, like in a HAZOP study, the system to be defined is the security system of the ship or port facility. This is because we are looking for the identification of weaknesses on the measures taken to protect the installation against security threats. For that purpose, as it has been done for the HAZOP study, the subsystems concerning physical security, operational security and security management should be defined in detail as the major functions of the system in order to be analyzed by this technique.

5.2.2 Identify Failure Modes and Causes

A Failure Mode describes the way in which a system or subsystem could fail to perform its desired function or previously defined expected performance. In that sense, all predictable and potential failure modes should be identified and described. For this purpose, and with the intention to assure that a complete analysis is performed, those systems or subsystems are analysed in relation to the following basic failure conditions or categories:

- Complete failure
- Partial failure
- Intermittent failure
- Failure overt time (Failure to cease or operate at a prescribed time)
- Over performance of function
- Other conditions of failure can be established based on particular systems characteristics or operational requirements.

Once identified the failure modes, their causes should be identified as well. In this process it is necessary to take into account that more than one cause could exist behind each identified failure mode and that these causes can cover several aspects of the systems like for example engineering, operations or management problems. It is also possible that a failure mode in one component can serve as the cause of a failure mode in another component. Likewise, a probability factor could be assigned (if that information is available) to each cause in order to indicate what is the likelihood of occurrence of that cause.

The application of the technique for the identification of weaknesses and critical points in a security system, then, could be made quite smoothly. It has been already defined the security system of the ship or port facility as a breakdown of its main functions: physical security, operational security and security management. Now, the FMEA team has to “brainstorm” the potential failure modes of each component or subsystem using the basic failure conditions given by the methodology or finding the particular conditions that, according to the experience, better suit with the system. After that, the potential causes of the failure mode should also be identified.

As an example, it can be taken one of the common maritime security issues that a port facility faces: unauthorized access to vessels. As Hawkes (1989) says the problem of physically secure a port facility is a big task, because it involves a large area that include several piers, warehouses, storage areas, access points, etc. So, we can start analyzing the fencing and lightning system. The general function of the system will be then physical security and the particular function of the fencing and lightning system is to prevent unauthorized access to the port facility. Now, the FMEA team can analyze in detail the fence and lightning system identifying potential failures in different categories like complete failure of the lightning system, inadequate fences, access points with no or inadequate control etc.; and of course determine the potential causes for this failures that could involve also operational and security management measures.

5.2.3 Evaluating the effects on the system of each failure mode

The consequences of each assumed failure mode on the operation, function or status of a system shall be identified, evaluated and recorded. The impacts on the system analyzed as well as the effects in other system's levels and in the overall system should be considered. The identified effects in the overall system (end-effects) are then classified according with the following categories: (a) catastrophic; (b) hazardous; (c) major; and (d) minor (HSC Code, 1995). This categorization helps to prioritize the failures and then address the most important issues first.

In relation to the effects of failure modes on security systems it is necessary to remark that a careful assessment of the severity should be made. This is because a common issue like, unauthorized access, may produce different effects depending on the intention of the offenders. The unauthorized access could be done for robbery, drug smuggling, sabotage or maybe terrorism. Therefore, the subjective assessment of the effect should take into account the specific threat scenario assumed for the study.

5.2.4 Identifying Failure detection methods

A description of the methods by which occurrence of the failure mode is detected also shall be recorded. These can be mechanisms that prevent the failure mode from occurring or which detect the failure before it can produce any effect. Alarms, sensors or inspections procedures may be included at this stage.

5.2.5 Identify Failure Corrective Measures for Failure Modes

Provisions to mitigate the effect of the failure shall be identified and evaluated. Some provisions could be aimed to the design of the system while others could be related to specific procedures for operators. In this sense, some actions like specific inspections, redesign of items, monitoring mechanisms, preventive maintenance could be recommended. Also, in some cases when the effect of the failure in the overall system is very high, a back up system or redundancy may be necessary. The effects of these corrective measures should be evaluated in order to determine if any further actions are required.

Table 5.3 – Example of FMEA worksheet.

System _____
Indenture level _____
Reference drawing _____
Mission_____

FAILURE MODE AND EFFECT ANALYSIS

Date _____
Sheet _____
Compiled by _____
Approved by _____

Function	Failure Modes and Causes	Failure Effects	Failure detection method	Corrective Actions	Severity	Remarks

Source: Adapted from United States Military Standard MIL-STDA-1629A (1980)

5.2.6 Document the Analysis and prepare a FMEA report

A FMEA worksheet is usually utilized to record the detailed information of the analysis. Finally a summary of the main issues that could not be corrected by design and those special controls, which are necessary to reduce failure risks, should be prepared. Table 5.3 shows a model of a typical FMEA worksheet where the information obtained in the different steps of the FMEA process should be filled.

Table 5.4 – Example of FMEA application on Security Assessment

System: Operational Security
Mission: Prevent access of illegal immigrants

FAILURE MODE AN EFFECT ANALYSYS

FUNCTION	FAILURE MODE S	FAILURE EFFECTS	CAUSES	FAILURE DETECTION METHOD	CORRECTIVE ACTIONS	SEVERITY
Control of access to the port facility	Complete failure	I restricted Access of unauthorized people to the port facility and potentially to ships docked	• No access control established.	Physical inspections	Establishment of control measures for the access to the port facility	Major
	Partial failure	Eventual access of unauthorized persons to the port facility and potentially to ships docked	• Inadequate measures to control of access • Lack of training of security personnel.	Physical inspections	• Enhance access control measures. • Train security personnel.	Major
	Failure over time	Eventual access of unauthorized persons to the port facility and potentially to ships docked	• Inadequate watchkeeping system. • Lack of security personnel training • Lack of security personnel.	Physical inspections	• Enhance the watchkeeping system • Train security personnel • Increment the number of security personnel	Major

Source: Worksheet adapted from US Military Standard MIL-STDA-1629A (1980)

5.2.7 FMEA for the identification of vulnerabilities and criticality in security assessments

FMEA is a technique similar to HAZOP that, instead of identify deviation from the design intention, focuses on potential failure modes of systems or components in order to derive their causes and effects. However, this technique also focuses its attention on estimate qualitatively the severity of those effects. These features, then,

can help in a security assessment to the identification of vulnerabilities and the identification of critical points that is necessary to protect.

Table 5.4 shows the application of the FMEA for the operational security measures of a port facility related to an illegal immigration case scenario. The function of the operational security system will be, therefore, to prevent unauthorized access to the port facility. After that, the system is evaluated in relation to the basic failure conditions or categories; causes are identified; failure effects and their severity are estimated; and corrective actions are proposed. The outcome of the overall study will give us a clear idea o the points of the system where the impact of a failure is more severe helping on the identification of critical points, and the assessment of vulnerabilities throughout the identification of possible failures in the security system.

It can be seen that FMEA and HAZOP studies could be used for the identification of weaknesses and criticality throughout the analysis of the security system of the ship or port facility in a sort of “check list “ technique because we need a security system to analyze and therefore we have to define a system based on something written. This can be easily done taking into account the detailed guidance given by the ISPS Code related to the SSP or it can be done using some other checklist designed for experimented people in security matters like for example the models shown by Hawkes (1989). The advantage of this techniques, however, stem on the fact that they provide a systematical and structured way to do the task to assess vulnerabilities an criticality within our security assessment framework and with that, working with a team, the opportunity to analyze the security system in depth, leading to identify situations that are not so evident, going far beyond the limits of the check list used as a reference.

5.3 Fault Tree Analysis (FTA)

5.3.1 Definition

The FMEA technique studied in the last section can be deemed as an inductive method to analyse a system, because a FMEA study assumes some possible

component condition and try to determine the corresponding effect on the overall system. This means from the specific to the general. However, any system can also be analysed with a deductive approach, reasoning from general to specific. Fault Tree Analysis (FTA) is a deductive method where some particular system condition (usually a failure condition) is assumed and, based on this assumption, a chain of contributing faults to the undesired event are built up in a systematic way (Haals, Roberts, Vesely, Goldberg, 1981).

According to Dickson (1991) FTA " is a diagrammatic representation of all the events, which may give rise to some major event " (p. 66). This representation shows how the combination of a number of individual events may lead to a major hazardous event and in that process we should be able to identify all the factors involved in the problem. An example of a basic Fault Tree is shown in Figure 5.2, where a major event Q is produced by event A or event B, and event B for its part is caused by events C and D.

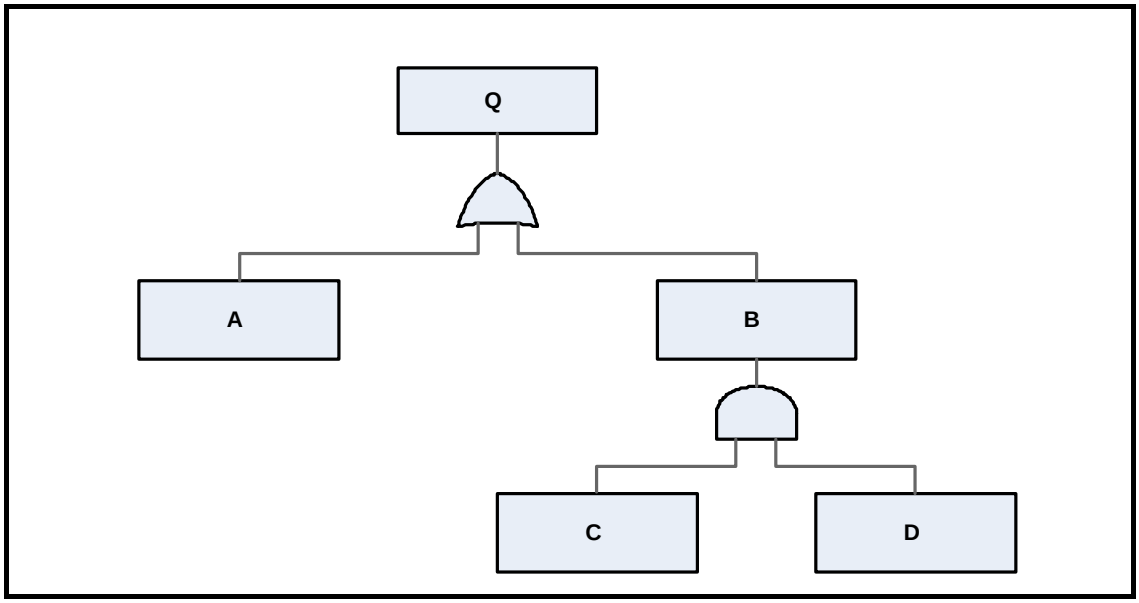


Figure 5.2 – Typical Fault Tree diagram

The basic methodology used by FTA is to define a system and then select a particular system failure mode, which constitute the top event of the system's fault tree. This approach has its basis in the fact that there are always a limited way a

system can fail with catastrophic effects. This means that, FTA only addresses those events above a point of maximum tolerable failure where an accident or adverse situation occurs, but the final objective or expected performance of the system is still achieved. The selected system failure mode, then, is an undesired event that generally consists of a complete or catastrophic failure. This undesired event should be selected and defined carefully in order to promote a complete and manageable analysis of the system (Haals, et al, 1981)

5.3.2 FTA in the context of Security Assessment

We have intentionally made the approach to the concept of FTA looking at this technique from the point of view of its deductive methodology rather than from its usual conceptualization as a quantitative technique. This is because we need this technique not as a quantitative but as a qualitative technique. As Dickson (1991) says: “Fault Trees are essentially quantitative in nature but they can certainly be used as a qualitative tool …” (p. 66). Therefore, for security assessments, we will attempt to use FTA to make qualitative analysis, taking also advantage of its deductive approach to mainly identify critical assets and operations and vulnerability.

As in the previous techniques analyzed, we will try to apply FTA to the study of the Security System of the ship defined by its three major functions in order to make the study more manageable. However, the difference will be that now we are going to deduce all the contributory aspects concerning a major adverse event on the system. These contributory elements may fall on the context of physical security, operational security or security management, since all the security system works in an integrated way. In this sense, we will be able to identify which system components have a more important role in relation to the top event and at the same time identify the weaknesses of the system.

5.3.3 Fault Tree Construction

Once the undesired event, that constitutes the top event, has been selected, the possible causes are deduced. In some cases more than one cause should occur at the same time to produce the failure, while in other cases a single particular cause could be responsible for the failure. These identified causes for its part can be consequence of other events in a lower level. The top event and its subsequent causes are then linked by logic gates: OR and AND. In this way, the contributory events are the inputs of the gates and the effects are the output of them.

5.3.4 Fault Tree Evaluation

Representing a Fault Tree through a number of events linked by logic gates allows to assign values to the input events and operate them using Boolean algebra. In that way, it can be possible to calculate the likelihood of occurrence of a top major event based on the likelihood of occurrence of the input events in a gate. For example, if it is assigned a value of probability to the input events in figure 5.2, then could be possible to calculate the likelihood of occurrence of the top event Q:

Q = A + B (OR Gate); B= C.D (AND Gate)
Q = A + (C.D)

To be able to generate these kinds of equations, of course, statistical information is necessary in order to determine the likelihood of the input events. Therefore, the accuracy of the result will depend largely on the accuracy of the information available.

According to Haals et al (1981) the evaluation of the Fault Tree can obtain qualitative and quantitative results. Among the qualitative results are:

- Minimal cut sets of the fault trees
- Qualitative component importance, which is evaluated making a qualitative ranking of each component with regard to its contribution to the system failure.

- Minimal cut sets potentially susceptible to common cause failures.

Representing a Fault Tree in terms of Boolean equations has the advantage that these equations can be used to determine the fault tree's associated "minimum cut sets". These "minimum cut sets" are the minimum number of ways a main event can occur, this means the minimum number of combinations of events which can bring about the main event (Dickson, 1991,p.73). This information is especially important in complex systems where there are a large number of events behind the main event, then if we have the possibility to identify the minimum number of events that can cause the top event, we will be able to identify what set of events are more likely to occur or produce the major effect on the top event.

Another valuable information, that is possible to obtain from the Fault Tree, is the identification of minimum cut sets potentially susceptible to common cause failures. These are multiple failures which can fail the system and which can originate from a common cause. Top events occur if all the primary failures in a minimum cut set occur, therefore, it is important to identify those common causes, which can trigger all these primary failures. This is made first, defining a common cause categories like human error, environment or energy sources. After that, component failures are codified according to these categories and then those minimal cut sets whose primary failures have the same element of a given category are identified.[2]

Quantitative results can also be obtained using probabilities, first determining the component failure probabilities, then calculating the minimum cut set probabilities and finally defining the top event probability. As it has been said before quantitative results depend on information and statistics related to the concerning components of a system which, in a security context is very limited or its treatment is more from a qualitative standpoint. For that reason, the analysis of the techniques used for quantitative evaluation in FTA will not be explained in detail.

[2] Primary failure is defined as any failure of a component that occurs in an environment for which the component is qualified. Component for its part can be a subsystem, sub subsystem, etc.

5.3.5 FTA evaluation of a security assessment application

Let us take an example applying FTA to a hypothetical situation. According to FTA we have to define first the system to be assessed and, after that, assume a catastrophic failure of that system. In this sense, it can be supposed a situation of a tanker ship carrying fuel hijacked by pirates while crossing the Malacca Strait. Figure 5.3 shows the construction of the Fault Tree related to that situation. It can be seen how a number of events that happen individually and in concurrence are inferred to be contributors to the top event. Also, it is necessary to highlight the fact that these contributory events belong to a different security functions falling in physical, operational and management measures.

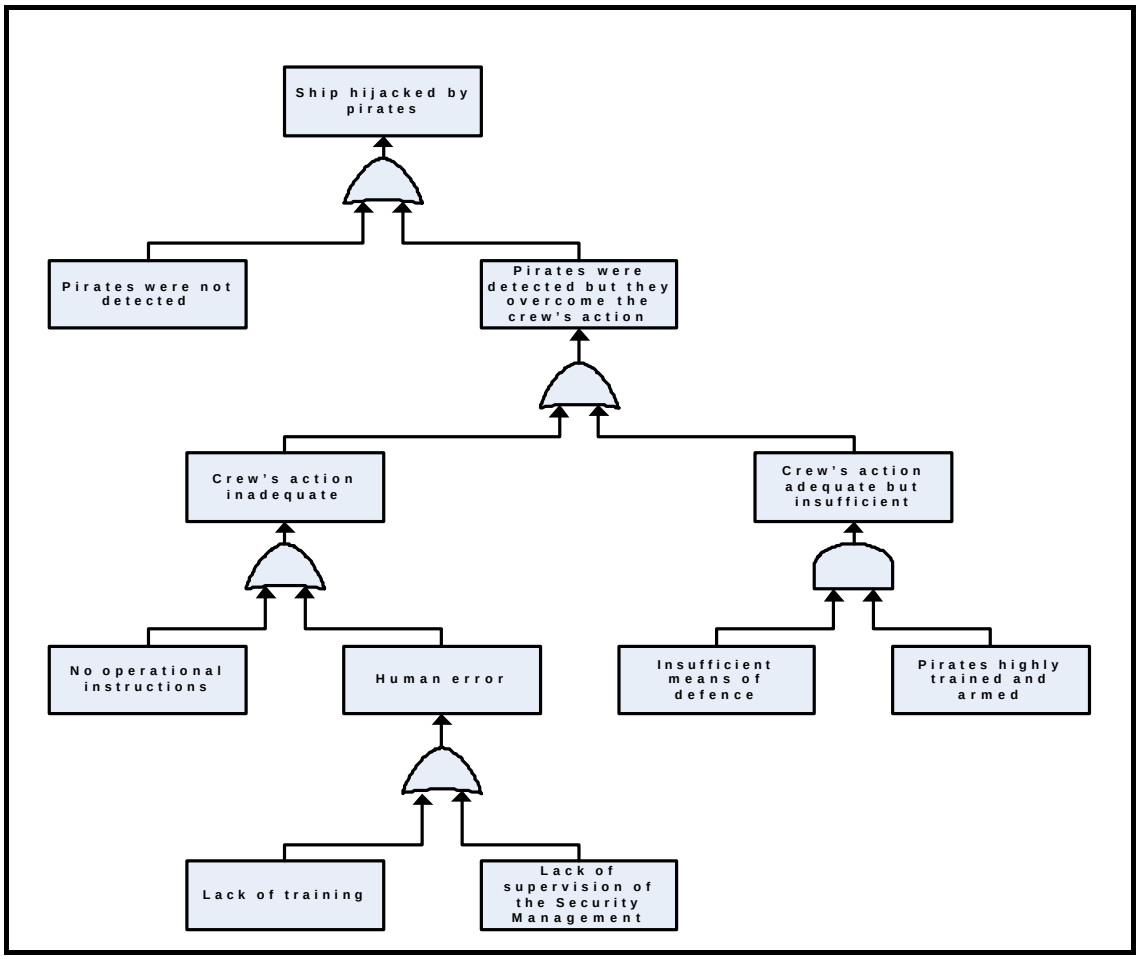


Figure 5.3 – Fault Tree Construction for a security event

The FTA construction shown is of course a simplification of a real construction that will imply much more space and detail. However, what it is necessary to remark is the evaluation of the fault tree, where it is possible to identify what set of events have major effect on the top event, both individually and in combination. In this regard, it could be identified in the example, the situation that a limited availability of means of defense of a ship in addition to pirates highly trained and armed lead to the hijack of the ship even if the crew is well trained. This is because means of defense against pirates like water hoses, strobe lights or dissuasive maneuvers are not enough to repeal a piracy attacks well planned and using modern weapons and fast boats.

FTA therefore, could be an interesting tool for the study of ship and port facility's security systems in order to identify vulnerabilities and critical points. This technique in this sense, has the virtue to assess the security system as a whole giving an excellent perspective of all interrelations that functions concerning operational, physical and management security measures involve. However, it is also clear that the construction of the fault trees represents a challenge for any security assessment team, especially in terms of time and the complication of the extension of the multiple diagrams that is necessary to draw.

5.4 Advantages and disadvantages of Safety Risk Assessment Techniques

5.4.1 Advantages

The techniques described on the previous sections have some common advantages that can be summarized as follows:

- The level of detail a system is analyzed guarantee that almost all possible failures in the system will be identified as well as (if such information is available) the likelihood of occurrence and consequences, defining in that way which parts of the system present a higher level of risk. Therefore, a system analyzed with these techniques becomes more reliable.

- Working with a team of experts allows examining a system in a more comprehensive way. Each member of the group has a different knowledge and experience with respect to the analyzed system, so the problems then can be seen from different point of views.
- One particular advantage concerning HAZOP and FMEA is that the different steps of these methodologies are recorded systematically in well-structured formats and reports, providing the necessary documentation for the requirements of the security management system.
- FTA can give us a better understanding of the security system operation. Vulnerabilities therefore can be identified in the process of building the trees and also critical components of the ship system, that are not so obvious, can be identified. The utility of FTA for security assessments arises when this technique is used qualitatively.

5.4.2 Disadvantages

There are also some disadvantages common to HAZOP, FMEA and FTA:

- One of them is that the teamwork could represent a disadvantage in case the right team is not achieved. If a correct balance between expertise and experience is not obtained the study could fail because the team will not be able to cover all the possibilities that a problem could involve.
- These studies are excessively time consuming. The team of experts needs extent meetings to develop the work and this imply high costs. The study's costs should be measured against the cost related to the occurrence of an undesired event.

5.6 Conclusions

Safety Risk Assessment techniques can be applied to assess security risks on ships and port facilities, focusing the studies on the identification of critical points, vulnerabilities and consequences under credible threat scenarios. Techniques like HAZOP, FMEA and FTA can therefore assess in a systematical and structured way

the ship and port facility's security systems. Of course they are excessively time consuming but the security risks that the maritime industry faces require well structured answers. In this sense, next chapter will show how these techniques could fit in a new security assessment framework based on the considerations identified throughout this work.

CHAPTER 6 SUGGESTION OF A NEW SECURITY ASSESSMENT FRAMEWORK

On the last chapter, it has been shown in some detail three of the most common risk assessment techniques developed by the industry. They were developed in response of the industry's necessity for comprehensive and structured techniques to assess the safety of complex systems like those of the chemical, nuclear and offshore industries.

Also, it has been shown those particularities that security risk assessments imply. Ships and Port facilities are complex systems that need to be protected from activities carried out with the express intention to damage the ship or port facility, use them as a mean for unlawful acts or simply pilfer cargo and any thing of some value onboard or in the port. This situation leads us to the need of a standardized security assessment framework that takes into account those particularities.

One preliminary approach for a new security assessment framework was suggested in chapter 3, to be used as a reference for the analysis of current safety risk assessment techniques, and also the security assessment approaches of USCG and NSA. However, this preliminary framework, even though based on well-known risk management approaches, suffers the lack of support of a methodology already proved on the maritime industry.

The first objective of this chapter is, in this sense, to suggest a new security assessment framework based on a methodology already in use in the maritime industry and the IMO for safety purposes. This methodology is the Formal Safety Assessment (FSA), which is an approach to manage safety risks presented in 1993 by the United Kingdom to IMO. The objective of FSA is to enhance maritime safety by using risk and cost/benefit assessments. The use of safety risk assessment

techniques for hazard identification and the cost benefit analysis are points of important coincidence with the preliminary security assessment framework suggested in chapter 3.

Having a more structured security assessment framework, the next objective of this chapter is to show, as a matter of summary, the main issues that the application of the methodologies analyzed in the last two chapters involve. It has already shown the main advantages and disadvantages of these methodologies, however, an overview of the whole problem is necessary in reference to the new security assessment framework proposed in this chapter.

Finally the economical considerations necessary to take into account in a security assessment will be analysed in some detail, especially in relation of one of the objectives of risk management, which is to develop risk reduction measures feasible not only technically but also economically. The special point to analyze then will be the fact that a certain level of security risk should be accepted by the industry and by the regulators.

6.1 Suggestion of a new Security Assessment Framework

6.1.1 Formal Safety Assessment (FSA)

It is not the intention of this work to describe in detail the FSA methodology but give an overview of its main steps and characteristics before the suggestion of a new security assessment framework is being made. For that purpose, the “Guidelines for Formal Safety Assessment for use in the IMO Rule-making process” (MSC/Circ.1023) will be used as a basic reference.

FSA involve the following steps:

- Identification of hazards;
- Risk analysis;
- Risk control options;
- Cost benefit assessment; and

- Recommendations for decision-making

Previously to the application of the steps indicated above, a generic model of the system under analysis is defined in order to describe the main functions and characteristics relevant to the particular situation subject to study. After that, the first step is applied and the safety hazards associated with a type of ship are identified using various techniques. These techniques can be FTA, Event Tree Analysis, FMEA, HAZOP, What if Analysis Technique, Risk Contribution Tree or Influence Diagrams (MSC/Circ. 1023, Appendix 3).

The second step, Risk Analysis, comprises the assessment of the causes and consequences of the hazard scenarios identified in step one. Then, the risk level that those main hazards impose is defined in order to prioritize those areas that need more attention. This step uses normally quantitative risk assessment techniques to take advantage of safety information available.

Step three implies the development of Risk Control Options (RCOs), which contain a limited number of Risk Control Measures (RCMs) for particular risk scenarios ranked by importance. These RCOs could be designed either to control the likelihood of initiation of accidents or control of escalation of accidents. The scope of this step is a set of RCOs assessed according to their effectiveness of reducing risk.

Step four of this methodology seeks to find the relation between the cost of the implementation of a RCO and the benefit obtained in terms of risk reduction. Costs are expressed as life cycle costs of the implementation of the measures and benefits normally use indicators like reductions in fatalities, injuries, casualties, and environmental damage. A number of techniques are used for this purpose.

Finally Step 5 establishes the recommendations to be presented to the decision makers. A list of RCOs and how they rate with respect to cost-benefit criteria is prepared and the decision makers select the best options according to the information shown and with their specific requirements.

6.1.2 New Security Assessment Framework

Based on the main features of the FSA methodology and on the preliminary security assessment framework introduced in chapter 3, now a new security assessment framework is developed. In this sense three main points have been extracted from the FSA: (a) the use of risk assessment techniques like HAZOP, FMEA and FTA for the identification of hazards; (b) The application of a risk acceptance criteria; and, (c) the cost-benefit analysis.

As it has been analyzed in previous chapters maritime security issues like terrorism do not create patterns and therefore it is not possible to estimate likelihood with an acceptable approximation. Additionally, those maritime security issues that create some kind of pattern such as piracy or stowaways, even though their likelihood can be estimated more precisely, there are not too much that a ship can do to eliminate these security threats. Therefore, it is necessary to focuses the security assessment on the identification of critical points, assessment of vulnerabilities and consequences with the objective to develop measures to protect those points that are more susceptible to security threats, reduce vulnerabilities of our security system in relation of specific threats and to minimize consequence in case a security risk arise.

Figure 6.1 shows the suggested new security framework, which reflects the requirements highlighted in previous paragraphs. This framework includes in principle the assessment of security threats, identification of critical assets and operations, and the assessment of vulnerabilities and consequences. Criticality, Vulnerability and consequences could be assessed with the help of the risk assessment techniques like HAZOP, FMEA and FTA, as it has been seen in chapter five. Based on the information gathered on these steps a level of security risk is estimated taking in to account existing security measures as well.

Moreover, a level of acceptance for security risks should be defined in order to determine what security risks require the development of security risk control options (SRCO). Then, cost benefit analysis is applied to these SRCO with the

purpose to identify which are economically feasible in relation to reduction of security risks. Finally, in any case the framework requires the record, monitor and control of the measures implemented in order to assess the security system periodically.

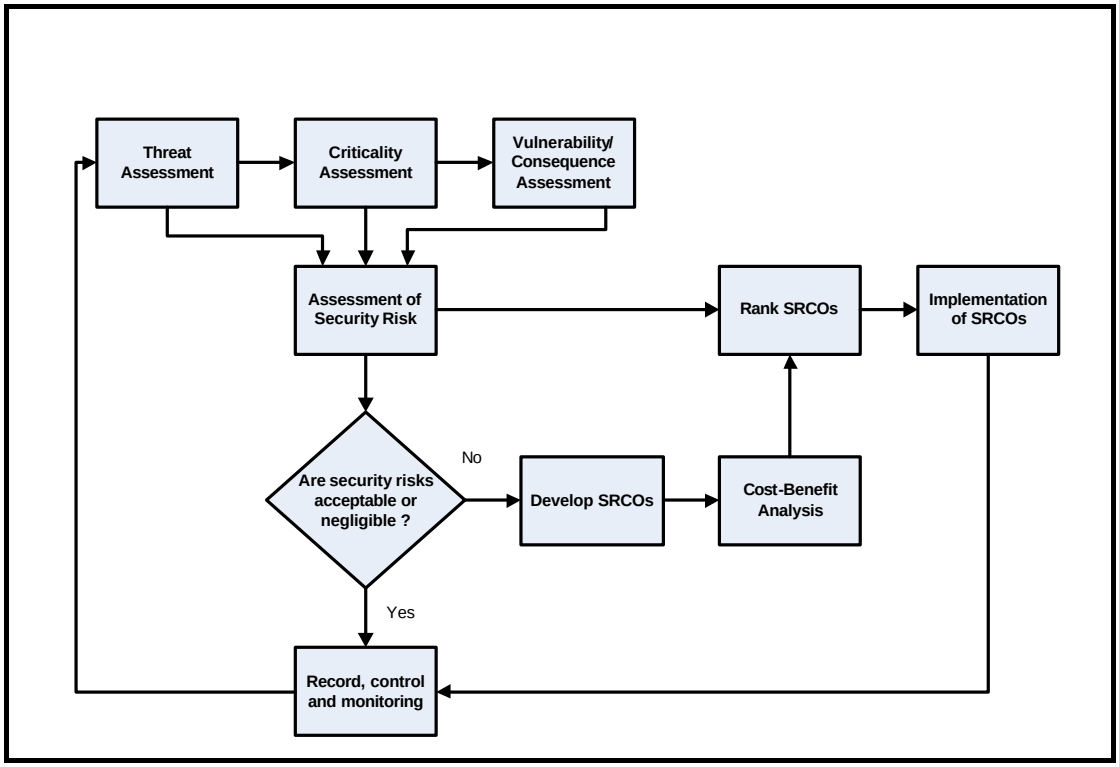


Figure 6.1 – New Security Assessment Framework.

6.2 Application of different methodologies to the new Security Assessment Framework

Throughout this work it has been shown how the new maritime security framework issued by IMO has created the necessity to develop methodologies to perform the requirements of the ISPS Code with respect of Ship and Port facility Security Assessments. Moreover, the particular characteristics of the main maritime security issues requires that the assessment of the level of security risk faced by a ship or port facility will not be based simply on likelihood and consequences, as it is usually done in safety, but in the interaction of security threats, vulnerabilities, criticality and the potential effects of those threats.

Additionally, once the level of security risk is estimated in some way, it is necessary to define which risks deserve more attention or require special measures to eliminate the risk or at least put the security risk in a level that can be considered acceptable. These measures indeed, should be feasible not only in technical but also in economical terms. That is why a cost-benefit analysis of the measures proposed should be carried out.

Table 6.1 – Application of different security and safety assessment methodologies to the suggested new security assessment framework.

Methodologies / Security Assessment	NVIC 10-02	NVIC 9-02	NSA	HAZOP	FMEA	FTA	FSA
Threat Assessment	Typical atack scenarios	Typical atack scenarios	Identification motives /threat scenarios	N/A	N/A	N/A	N/A
Criticality Assessment		Identify Critical Assets and Operations	Identification Key shipboard operations	Study of Security System	Analysis of Security System	Fault Tree for catastrophic top events	Safety Risk Assessment Techniques
Vulnerability Assessment	Score: Accessibility Org. Security	Score Accessibility Org. Security Availability Targ. Hardness	Identification Of Weaknesses	Study of Security System	Analysis of Security System	Fault Tree for catastrophic top events	Safety Risk Assessment Techniques
Consequence Assessment	Score: Catastrophic Significant Moderate	Score: Catastrophic Significant Moderate	Potential outcome of scenarios	Study of Security System	Analysis of Security System	Fault Tree for catastrophic top events	Safety Risk Assessment Techniques
Security Risk Estimation	Mitigation	Mitigation	Likelihood/ Consequences	N/A	N/A	N/A	Likelihood/ Consequences
Acceptance Criteria	Vulnerability/ Consequence Matrix	Vulnerability/ Consequence Matrix	Likelihood/ Consequences	N/A	N/A	N/A	Safety Acceptance Criteria
SRCOs	Mitigation Determination Worksheet	Mitigation Strategies	Identification of Remedial Actions based on vulnerabilities	Study of Security System	Analysis of Security System	N/A	RCOs for unacceptable risks
Cost-Benefit Analysis	Mitigation Implementation Worksheet	Mitigation Strategy Benefit Analysis	No	N/A	N/A	N/A	Cost-Benefit Analysis

The different methodologies analyzed in chapters 4 and 5 comply with some of the requirements of a complete and comprehensive security assessment. The problem

is that some of these methodologies or techniques may perform some tasks but not others or simply the methodology does not take into account certain key factors in a security context. The main characteristics, advantages and disadvantages of these techniques have been highlighted in chapters 4 and 5, however a general view of these techniques under the umbrella of the suggested new security assessment framework is necessary in order to identify clearly their utility for security assessments. I

In this sense table 6.1 shows all the methodologies analyzed previously compared with the different steps of the security assessment framework proposed in section 6.1. It can be seen in that way, which steps of the security framework are addressed by the selected methodologies and how they can be more useful in some stages than in others. Therefore, it could be possible to combine more than one of these techniques to carry out a security assessment. For example, the security assessment approach of NVIC 10-02 can be applied but at the same time using HAZOP to assess in detail the vulnerability of the ship's security system and the FSA approach for the cost benefit analysis.

6.3 Economical considerations in Security Assessments

The main reason why FSA was selected as a basis of the new security assessment framework proposed in section 6.1 was its risk assessment and cost benefit analysis approach. This approach will be necessary to create a workable and coherent security strategy (Alderton, 2002). This means that, as absolute security is not possible, some level of security risk should be accepted in order to keep the international world trade working.

The costs of implementation of security measures related to the ISPS Code, incurred by ship owners globally, have been estimated in US $1.3 billion (OECD, 2003). This situation shows the enormous impact that maritime security implies and the necessity to understand something mentioned before: shipping and port industry are business that have the goal, as professor Kuo says, "to be competitive in meeting the client's specifications with solutions that are cost-effective at an

acceptable level of safety". Security should be added now to this concept: we need security and safety but shipping and ports running as well.

As a result of a security assessment a number of measures are proposed in order to reduce the level of security risk that the ship or port facility face. These measures usually involve equipment or hardware, policies and procedures, management practices and new or retrained personnel. They have been already defined in chapter 5 as physical security, operational security and security management measures. Likewise, other options have been considered by the industry, like insurance coverage or simply accepting risks as a cost of doing business (ASIS, 2003).

In any case, the measures developed grouped in SRCOs should be evaluated to determine mainly their feasibility, in order to identify interference with the normal operation of the ship or port facility, and their affordability. The latter is necessary because, as we have seen before, these SRCOs imply costs. Therefore, "the challenge is to achieve high level of security and efficiency, while keeping costs at a minimum" (Kwek, Goswami, 2004, p. 202).

The costs of implementation of SRCOs should be compared with the benefit of the measures. This means that we have to "weigh the implementation costs against the impact of the loss, financially or otherwise" (ASIS, 2003). This process constitutes a cost benefit analysis and involves one major problem when attempt is made to quantify losses (consequences or effects of a security threats). No price can be placed on human life will say some people while others more pragmatic could say that this is done every day by insurers (Alderton, 2002). For example in the European Union the loss of one life is worth a million pounds (Kuo, 1998, p. 152).

This is therefore a difficult task that should be performed pragmatically but always keeping in mind that lives are in play. Politics and the social perception of the situation play, of course, a relevant part on the implementation of security measures globally. It is the common customer who will pay finally the overall costs of security

and from its perception of security will depend its willingness to pay those additional costs.

6.4 Conclusions

This chapter has proposed a new security assessment framework that attempt to combine the main requirements and features that the analysis of security on ships and port facilities involve. In that sense this methodology includes, for one hand, the necessary steps to assess threats, vulnerability, consequences and the identification of critical assets and operations, and on the other hand, this methodology also address the economical considerations concerning the implementation of security measures through the cost benefit analysis approach of the FSA methodology. Therefore, the proposed methodology seeks to be comprehensive in the sense of cover all the factors concerning the assessment of security of ships and port facilities.

The development of security assessments on ships and port facilities is a new task imposed by the ISPS Code. Chapter 4 has shown the security assessment approaches of the USCG and NSA, however, even though they try to be comprehensive, they still say more what to do than how to do some aspects of the study. These are the gaps that this study has attempted to fill with the introduction of techniques like HAZOP, FMEA and FTA, which normally used for safety purposes, it has been found that is possible to be applied for the detailed analysis of ship and port facility's security system with the objective to assess vulnerability and criticality. In this sense, this chapter has shown as a matter of summary how these techniques deal with the different steps of the security assessment framework proposed and how they could be complemented each other to fulfil a security assessment.

Finally, this chapter has shown, in general, the economical implications that the implementation of security measures involve and the necessity to assume the challenge to achieve a maritime industry with high level of efficiency, safety and security, but keeping costs at a reasonable level to allow the normal development of this industry which is one of the most important elements of the international trade.

CHAPTER 7 SUMMARY AND CONCLUSIONS

The main purpose of this dissertation was the selection of risk assessment techniques commonly used for safety with the intention to evaluate whether their application on security assessments is feasible or not. This analysis required a clear understanding of all the considerations that a security assessment of ships and port facilities involve and the development of a security assessment framework based on these considerations. This security assessment framework, then, served as an adequate reference for the application of safety risk assessment techniques and other methodologies specially developed for security assessments purposes.

Maritime Security and Maritime Safety were firstly compared and it was found that maritime security has a different dimension. It is related to intentional actions with the purpose to cause damage to the ship or port facility. In this sense, maritime security was defined as the measures used to protect ships and port facilities from those threats. The problem with this situation is that, the assessment of security threats is sometimes difficult because they do not always create patterns that allow predicting likelihood or behaviour. Some of them create patterns and can be deemed as locally restricted because they arise in specific locations of the world, but others such as terrorism do not create patterns and they can emerge in any part of the world, that is why they are called locally unrestricted maritime issues.

The IMO addressed maritime security with an approach based on risk management. In this sense, it was found that the methodology used by the ISPS Code for security assessments follow in general, the risk management methodology employed by the industry ashore. Moreover, from the analysis of common safety risk approaches and the particularities of the maritime security issues, it was also found that the assessment of risk in terms of security requires an analysis of elements beyond probability and consequences.

The assessment of security risks will involve the assessment of the potential threats, vulnerabilities, consequences and the identification of critical assets and operations. These requirements can be explained by the fact that maritime security issues are threats external to the ships and port facilities, so they cannot be eliminated by actions from that side. Therefore, the only possibility is to assume some probable threat scenarios and assess vulnerability and consequences related to that threat scenarios in order to develop measures to make the ship or port facility as hard to attack, as it is possible, and in case of an attack minimize its consequences.

Therefore, a complete security assessment should take into account the analysis of those factors mentioned on the previous paragraphs. However, one additional element should be assessed once the level of security risk is estimated: the economical considerations. Measures to protect a ship or port facility do not only be feasible in technical terms but also in economic terms. The reason is that shipping and ports are business to obtain profit and therefore they have to balance security, safety, competitiveness, efficiency and costs.

The current security assessment approaches developed by the USCG and the NSA were analyzed and it was found that they follow with different approaches the security assessment methodology established by the ISPS Code. However, economical considerations for the implementation of measures to mitigate security risks are not considered explicitly on the NVIC 10-02 and this topic is not considered at all on the NSA guidelines. Additionally, these two methodologies mostly explain what to do to perform a security assessment but not too much how to do the study. Consequently, given the complexity of ships and port facilities, more detailed, structured and systematic techniques should be identified to perform the assessment of vulnerabilities and consequences.

Techniques usually employed for safety assessments on the chemical, nuclear and offshore industries, such as HAZOP, FMEA and FTA, were identified and their application was analysed for vulnerability assessments and for the identification of critical assets or operations that is necessary to protect. This analysis found that these techniques might be applied smoothly for the assessment of vulnerabilities

and the identification of critical points. The security system of the ship or port facility is assessed in detail to find weaknesses in relation to potential threats. The advantages of these techniques are mainly that they perform the assessment using a team of experts which “brainstorm” all the possibilities that the security system could fail. This is done in a structured and systematic way in order to avoid not identifying certain problems that are not so obvious. The disadvantages of these techniques are mainly two: (a) they are excessively time-consuming and require long sessions and physical inspections of the ship or port facility and (b) the outcome of the study is highly dependent on the composition of the team, because a team with poor expertise or experience on the area will not assess the system adequately.

Finally, this study suggested a new security assessment framework based on a methodology such as FSA that is used by the IMO. It was made in this way because this methodology, employed for safety assessments, uses two important elements that match with the requirements of a security assessment: Risk Analysis and Cost-Benefit analysis. In this sense, a new security assessment framework was proposed attempting to consolidate all the requirements for security assessment that this study has identified. This framework helps to understand how the application of methodologies such as NVIC 10-02 or NSA could be done with the aid of techniques such as HAZOP, FMEA or FTA with respect of vulnerability and criticality assessment. Also the cost-benefit approach used by FSA could be applied for the assessment of the economical considerations concerning the implementation of security measures.

The implementation of the ISPS Code is still at its early stages and therefore it is necessary to obtain more experience in the process of security assessments and in the implementation of security measures through security plans. This experience will make possible to understand more clearly all the aspects concerning maritime security and in this way attempt to protect ships and port facilities more efficiently from security risks.

REFERENCES

Abyankar, J. (2004): *Maritime Crime.* Unpublished lecture handout, World Maritime University, Malmö, Sweden

Alderton, P. (2002). The Maritime Economics of Security. *Maritime Policy and Management, 29, 2, 105-106*

ASIS International (2003). *General Security Risk Assessment Guideline*. Retrieved on August 15, 2004, from: http://www.asisonline.org/guidelines/guidelines.pdf

Bahr, N. (1997). *System Safety and Risk Assessment: a practical approach*. Washington D.C.: Taylor & Francis.

Broadleaf Capital International PTY LTD (1999). *Tutorial Notes: The Australia and New Zealand Standard on Risk Management, AS/NZS 436.* Retrieved on June 28, 2004, from: http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf

Churchill, R., Lowe, A. (1999). *The law of the sea.* Manchester, Yonkers, N.Y.: Manchester University Press, Juris Publications, p. 211.

Convention for the Suppression of Unlawful Acts against the safety of Maritime Navigation, 1988, IMO, (1988).

Cooper, N. (1994, June). The ISPS Code: a serving shipmaster's perspective. *Seaways (June 1994), 3- 6*

Danish Maritime Authority. (2002, June). *Risk Analysis of Navigational Safety in Danish Waters*. Retrieved on July 6, 2004, from: http://www.frv.dk/en/publikationer/risikovurdering/Summary.pdf

Dickson, G.C.A. (1991). Risk Analysis. London: Witherby for the Institute of Risk Management

FMEA History (2003). Retrieved on July 15, 2004, from FMECA.COM Web Page: http://www.fmeca.com/ffmethod/history.htm

Fergus, N. (2004). *International Terrorism and the quest for more effective security*, ASIS International Annual Conference, Melbourne, Australia February 16, 2004. Retrieved on June 28, 2004, from: http://www.irisks.org/news/int_ter_quest_security.pdf

Frame, J. (2003). *Managing Risk in Organizations.* San Francisco, CA: Jossey Bass, p.14

Haals, D., Roberts, N., Vesely, W., Goldberg, F. (1981). *Fault Tree Handbook*. U.S. Nuclear Regulatory Commission. (Publication No. NUREG-0492). Retrieved

on August 15, 2004, from: http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/

Hawkes, K. (1989). *Maritime Security.* Centreville, Md.: Cornell Maritime Press

Hazard and Operability (HazOp) Studies. Retrieved on July 12, 2004, from University of Florida, Unit Operation Laboratories Web Site: http://www.pie.che.ufl.edu./guides/hazop/

Hesse, H. (2003). *Ships and Port Security: the IMO's response*. BIMCO Review 2003.

Hillson, D. (2003). *Risk Management: Best Practice and Future Developments*, II Congreso Nacional de Gerencia de Proyectos, Universidad Nacional de Ingenieria, Lima-Perú, (24-25, October, 2003). Retrieved on June 28, 2004, from: http://www.risk-doctor.com

IMO International Course and Workshop on Maritime Security. Montevideo, Uruguay, 28 October to November 1st, 2002.

International Code of Safety for High Speed Crafts, 2000, IMO (2001)

International Convention for the Safety of Life at Sea, 1974, IMO, (2001).

International Maritime Organization. (1983, November 17). *Measures to prevent acts of piracy and armed robbery against ships*. (A.545 (13)). London: Author

International Maritime Organization. (1985). *Measures to prevent unlawful acts which threaten to safety of ships and the security of their passengers and crews*. (A.584 (14)). London: Author

International Maritime Organization. (1987). *IMO Ship Identification Number Scheme*. (A.600 (15)). London: Author.

International Maritime Organization.(2002, April). *Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-making Process*. (MSC/Circ. 1023). London: Author

International Ship and Port Facility Code, (2003), IMO (2003).

Keng-Huat, K., Goswami, N. (2004). Cost and Productivity Implications of Increased Security in Sea Trade Process. *BIMCO Review 2004, 197-203*

Kuo, C. (1998). *Managing Ship Safety.* London; Hong Kong: LLP, 1998

Lihou, M. (2004). Hazard & Operability Studies. Retrieved on July 15, 2004, from Lihou Technical & Software Services Web Page: http://www.lihoutech.com/history.htm

Mc Laughlin, J. (2004). Congress faces battle over forcing coast guard to vet US port calls. Lloyd's List (10 May, 2004). Retrieved August 17, 2004, from: http://www1.lloydslist.com/NASApp/cs/ContentServer?pagename=LloydsList/Printer

Mejía, M. (2003). *Maritime Gerrymandering: Dilemmas in Defining Piracy, Terrorism and other Acts of Maritime Violence*. Journal of International Commercial Law 2, no. 2. p. 162.

Mensah, T. (2003). *The Place of the ISPS Code in the Legal International Regime*. WMU Journal of Maritime Affairs, 3, no. 1. p. 20.

Mitropoulous, E. (2004, May). Speech to the Singapore Shipping Association, Singapore, 25 May 2004. Retrieved on 11 June, 2004 from: http://www.imo.org/home.asp

Norwegian Shipowners' Association (2003). *Guideline for Performing Ship Security Assessment*, 2003. Retrieved on June 22, 2004, from: http://www.rederi.no/File.asp?File=Dokumenter/Vedlegg%20sirkulaerer/SSA%20Final%20060203.doc

Organization for Economic Cooperation and Development (2003, July). *Security in Maritime Transport: Risk Factors and Economic Impact*. Paris: Author.

Project Management Institute (2002), *A Risk Management Standard*, retrieved on 28 June 2004, from: http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Schröder, J. (2004). *An introduction to shipboard security risk assessment*. Manuscript in preparation.

Schröder, J., Ketchum, J., Mejía, M (2004). *Maritime Security: an overview of the new requirements*, in: Background to Shipping, Conference: Lloyd's Maritime Academy, 9-12 March 2004, London.

Schultz, D. (1978). *Principles of Physical Security*. Houston, Tex.: Gulf Pub. Co.

U.S. Coast Guard. (2002). Security Guidelines for Vessels (NVIC 10-02). Retrieved on 15 June, 2004, from: http://www.uscg.mil/hq/g-m/nvic/10-02.pdf

U.S. Military Standard STD-882C (1993, January). System Safety Programs Requirements. Retrieved on August 15, 2004, from: http://www.reliasoft.org/mil_std/mil_std_882c.pdf

U.S. Military Standard STD-1629A (1980, November). Procedures for Performing a Failure Mode, Effect and Criticality Analysis. Retrieved on 15 July, 2004, from: http://www.npoesslib.ipo.noaa..gov/techlib/doc178/doc178.pdf

United States Coast Guard. (July 1, 2003). *Implementation of National Maritime Security Initiatives, Temporary interim rule with request for comments and notice of meeting.* Federal Register, Vol. 68, 126. Retrieved June 27, 2004, from:http://a257.g.akamaitech.net/7/257/2422/14mar2000800/edocket.access.gpo.gov/2003/pdf/03-16186pdf

US Coast Guard. (2002). *Guidelines for Port Security Committees and Port Security Plans required for U.S*. Ports. (NVIC 9-02). Retrieved on June 19, 2004 from: http://www.uscg.mil/hq/g-m/nvic/9-02.pdf

US General Accounting Office (2001, October). *Homeland Security: Key Elements of a Risk Management Approach* (Publication No. GA0 –02-150T). Retrieved on June 29, 2004, from: http://www.gao.gov/new.items/d02150T.pdf

US General Accounting Office. (1998, April). *Combating Terrorism: Threat and Risk Assessments can help prioritize and target Program Investments* (Publication No. GAO/NSIAD-98-74). Retrieved on June 19, 2004, from: http://www.gao.gov/archive/1998/ns98074.pdf

US General Accounting Office. (2001, September). *Combating Terrorism: Selected Challenges and related recommendations. (*Publication No.*GAO*-01-822). Retrieved on June 15, 2004 from: http://www.gao.gov/new.items/d01822.pdf

Waring, A., Glendom, A.I. (1998), *Managing Risk.* London, Boston: International Thomson Business Press

Wells, A. (2001). *Commercial Aviation.*New York: Mc Graw-Hill

Wilcox, R. (2002). *Risk-Informed Regulation of Marine Systems using FMEA*. Retrieved on August 15, 2004, from U.S. Coast Guard Marine Safety Centre Web Page http://www.uscg.mil/hq/msc/fmea.pdf