

**A Novel Framework for Maritime Security
Assessments and its Applications on the Shipping
Industry. Cyber security examples.**

Panayiotis Papageorgiou

**A Thesis submitted in partial fulfilment of the requirements of
Liverpool John Moores University for the degree of Master of Philosophy**

January 2022

Abstract

Terrorism, piracy, robbery, cyber-threats on ships and port facilities, smuggling and drug trafficking through cargo and containers, etc., are some of the international security problems due to which the national maritime security services must provide solutions. Cyber-attack is considered particularly important due to the possibility to be combined with all the other security vulnerabilities in the shipping industry.

It is clear that the maritime supply chain is particularly vulnerable to malicious acts resulting from criminal and terrorist elements. It is therefore necessary for the national maritime security services to take appropriate security measures in order to reduce the threats posed by these malicious elements.

In fact there is no extensive and in-depth literature for the risk acceptance criteria concerning maritime security. Basic information is drawn from other areas, such as civil aviation. It is necessary to standardize these criteria, as is the case with the Formal Safety Assessment, where practitioners know how to gather information, to make comparisons with previous experience and to make decisions that are often based on experience from the past.

Thus, the practice of security management in the maritime industry must be seen from a new perspective given the rapid changes that shipping is facing. **The aim of the proposed study is to address the issue of maritime security through the development of a method applicable to the maritime industry that evaluates and manages security related risks and specifically maritime cyber risk.**

The main **objectives** of this study are: i) **To critically analyse the existing maritime risk approaches.** ii) **To develop a method to address maritime cyber risk.** iii) **To illustrate through the application how this method could be used in practise.** iv) **To provide brief recommendation for future work.**

The proposed method uses the Bow-Tie diagram tool for the estimation of the risk. A risk computation procedure is described after the application of a set of prevention barriers, which is based mainly on the accuracy of the definition of the Probability P_i and the Contribution C_i of each Threat (i) as well as on the accuracy of the estimation of the Effectiveness value E_{ij} , of each Prevention Barrier (j) for the same defined Threat (i), by the user.

Similarly, the risk computation for each consequence, after the application of a set of mitigation barriers, is based mainly on the accuracy of the definition of the Risk Value RV_i of each Consequence (i) as well as on the accuracy of the estimation of the Effectiveness value E_{ij} , of each Mitigation Barrier (j) for the same defined Consequence (i), by the user.

The results of the risk computation appear in the Bow-Tie diagram providing a coloured scheme of the obtained risk values for top event and consequences, after the introduction of the necessary prevention and mitigation barriers.

The present work may be completed in the future, to perform cost benefit analysis, decision making procedures and training programmes.

Acknowledgements

The writer wishes to express his appreciation and thanks to the following individuals and groups who helped to make this dissertation possible:

- Prof. Zaili Yang and Dr. Christos Kontovas, for their support during my research study in Liverpool John Moores University.
- Prof. Stratos Papadimitriou of the Department of Maritime Studies - University of Piraeus, for his help in the framework applications concerning maritime cyber security examples.
- Dr. Zacharias Dermatis, member of the educational staff of the Department of Management and Technology - University of Peloponnese, for his help in the development of the required software in Visual Basic for the proposed framework.
- My Parents Christos and Vassilki Papageorgiou for their support and motivation during my research.

Contents

<i>Abstract</i>	iii
<i>Acknowledgements</i>	v
<i>Chapter 1. Introduction</i>	1
<i>Chapter 2. Literature Review – A Critical Analysis of the Existing Maritime Risk Approaches</i>	5
<i>2.1. Introduction</i>	5
<i>2.2. Maritime Safety vs Maritime Security - Basic Terminology</i>	5
<i>2.3. The concept of Maritime Security</i>	9
<i>2.4. Maritime Security Regulations</i>	11
<i>2.5. Vulnerabilities existing in the maritime industry concerning security</i>	13
<i>2.5.1. Terrorist Targeting of Ships and Ports</i>	14
<i>2.5.2. Piracy and Armed Robbery</i>	17
<i>2.5.3. Drug Smuggling</i>	19
<i>2.5.4. Cyber and Information Threats to Seaports, Ships etc</i>	22
<i>2.6. Maritime Security Assessment</i>	27
<i>2.6.1. ISO 31000 and ISO 27005 for risk management</i>	30
<i>2.6.2. Six Steps Quantitative Maritime Security Assessment (QMSA)</i>	33
<i>2.6.3. Existing tools for Risk Assessment</i>	34
<i>2.6.4. Existing methods for Risk Assessment</i>	38
<i>2.6.5. The Bow-Tie Method for Security Risk Assessment</i>	45
<i>2.7. Conclusions concerning Literature Review</i>	47
<i>Chapter 3. Development of a Risk-Based Method to Address Maritime Risk and Specifically Cyber-Risk</i>	51
<i>3.1. Introduction</i>	51
<i>3.2. Proposed Framework as a method for Security Risk Assessment</i>	51
<i>3.3. Contribution to knowledge and novelty of the research</i>	54
<i>3.4. Framework’s General Description</i>	55
<i>3.5. Required Calculations and Used Data</i>	58
<i>3.6. Software Description</i>	63
<i>3.7. Software printouts</i>	65

3.8. Conclusion.....	66
Chapter 4. Applied Examples, Results and Discussion – How this Method is Used in Practise.....	67
4.1. Introduction.....	67
4.2. A first application of cyber security – Malware related incident	67
4.3. A second application of cyber security – Unauthorized external user.....	82
4.4. Discussion.....	104
Chapter 5. Conclusions and Brief Recommendation for Future Work	105
Appendix 1: Programme presentation	109
Appendix 2: Programme printouts	119
References	123

Chapter 1. Introduction

The **aim** of the proposed study is **to address the issue of maritime security through the development of a method applicable to the maritime industry that evaluates and manages security related risks and specifically maritime cyber risk.** The challenge is the development of joint initiatives and relations between the stakeholders to secure maritime industry interests from threats such as terrorism and criminal activity. Thus, the core of maritime security is to minimise injuries, illnesses and economic losses due to terrorism and criminal activity, in order to ensure the flow of trade and the continuity of maritime business.

The main objectives of the study are the following: **i) To critically analyse the existing maritime risk approaches. ii) To develop a method to address maritime cyber risk. iii) To illustrate through the application how this method could be used in practise. iv) To provide brief recommendation for future work.**

The proposed work will address the issue of maritime security through the development of a method that assesses and manages security related risks applicable to the maritime industry. The research will be based on risk management methodologies that address safety-related risk, for example the so-called Formal Safety Assessment methodology proposed by the UN's International Maritime Organisation.

This research topics falls under the main research interests of LJMU and particularly the Liverpool Logistics, Offshore and Marine Research Institute (LOOM) at the Faculty of Engineering and Technology, as some of its members are performing world-leading research on the area of risk assessment; see for example Prof. Jin Wang, Prof. Zaili Yang and Dr. Christos Kontovas.

The practice of security management of ports and shipping must be seen from a new perspective given the rapid changes that shipping is facing, especially after the terrorist attacks in the United States in 2001. The issue of maritime security has mainly been addressed by the so-called ISPS code, which contains requirements concerning security, addressed to for Governments, port authorities and maritime companies in a first mandatory section (Part A), as well as many guidelines to meet these requirements in a second, non-mandatory section (Part B). However, the Code itself does not mention a specific tool or technique to be used in order to perform the

assessment of related risks. This is also apparent from the way that security assessments are being currently performed (Ng & Vaggelas, 2012).

The extended literature review that we performed is in line with the research performed by others, see for example Fransas et al. (2012) and Yang et al. (2016), which is indicated in the work of the later authors "*the existence of a significant research gap, requiring the development of systematic risk analysis methodologies with the support of novel and advanced risk modelling and decision-making techniques.*".

Given the complexity of the maritime industry and the need for a decision-making tool for use at the different stages of design and operation, a special risk-based assessment tool for security risk assessment, analysis and evaluation, which integrates several studies focusing on maritime security risk quantification is proposed for development, consisting of: i) Risk Identification, ii) Risk Analysis and iii) Security Mitigation Options.

The Bow-Tie visual risk assessment method will be applied using the Bow-Tie diagram technique by which both incident prevention barriers and consequence reduction barriers are identified. Security Cost-Benefit Analysis and Decision Making will be added to the software in the future when the previously mentioned three stages will be completed.

The development of the proposed tool is in line with the ISO guide on Risk Management (ISO 31000) and IMO's Formal Safety Assessment guidelines. Various proposals of security related frameworks such as that proposed in Yang et al. (2016) have also been taken into account.

The structure of the present dissertation has the following form:

Chapter 1. Introduction (current chapter)

Chapter 2. Literature Review – A Critical Analysis of the Existing Maritime Risk Approaches, which includes details about the concept of maritime security and the corresponding international regulations, the vulnerabilities existing in the maritime industry concerning security, the existing maritime security evaluation & assessment procedures, included in the ISO 31000 and ISO 27005 standards for risk management, the Six Steps Quantitative Maritime Security Assessment (QMSA), the existing tools for risk assessment, the existing methods for risk assessment and finally, the Bow-Tie method for security risk assessment and management.

Chapter 3. Development of a Risk-Based Method to Address Maritime Risk and Specifically Cyber-Risk, where the proposed method to address maritime security risk and specifically cyber risk is presented, illustrating through the application how this method could be used in practise and mentioning the contribution to knowledge and novelty of the research, the framework's general description, the required calculations, the used software's description and the software's printouts.

Chapter 4. Applied Examples, Results and Discussion, where two applied examples are presented: A first example of cyber security for a malware related incident and a second example of cyber security for unauthorized external user. The obtained results are presented numerically and graphically, while the discussion of the obtained results is included in this chapter too.

Chapter 5. Conclusions and Brief Recommendation for Future Work, where the final conclusions for this study are presented, followed by some recommendations for future work.

Chapter 2. Literature Review – A Critical Analysis of the Existing Maritime Risk Approaches

2.1. Introduction

The main objective of maritime security is to minimise loss, destruction, damage, injury, death, delay injuries, illnesses and economic losses, due to criminal activity, affecting people, environment, assets and reputation, in order to ensure the flow of trade and the continuity of maritime business. The literature review contributes to the understanding of the current security situation in the maritime industry and will highlight existing gaps and the need for further research.

As a first step to approach the concept of maritime security it is necessary to compare it with maritime safety and to define carefully the different terms used for risk assessment. The concept of maritime security and the corresponding maritime security regulations will be then presented in a critical manner. A brief overview of the existing different types of malicious acts resulting from criminal and terrorist elements, such as terrorism, piracy, robbery, cyber-threats on ships and port facilities, smuggling and drug trafficking through cargo and containers, etc. is the next part of literature review. Finally, the existing methods, tools and practices for maritime security risk assessment and the ISO 31000 and ISO 27005 systems for risk management will be presented.

2.2. Maritime Safety vs Maritime Security - Basic Terminology

According to Burns (2015), there is a variety of **risk areas** in port management and the maritime industry in general. Most of these risk areas are summarized in the following Figure 1. Different types of risks have different **impacts** and therefore need to be treated differently. Such impacts are loss, destruction, damage, injury, death, delay etc. (Rowbotham, 2014).

The concept of **maritime safety** deals with protection of life, health, marine environment, property and reputation from threats such as accidents that are unintentional.

According to the ship owner's view (Jones, 2006), the theme of **maritime security** is *“the state of a shipping company/vessel/crew/port, being of feeling*

secure“, or *“the safety of a shipping company/vessel/crew/port against such threats as terrorism, piracy, and other criminal activities”*. Thus, the scope of maritime security is to reduce human losses, injuries, illnesses and economic losses due to criminal activity, ensuring the flow of trade and the business continuity. Although piracy and theft are predicated on financial gain, in many cases terrorism at sea is driven by political motives (Psaros et. al., 2009).

Predicting the next accident, either intentional or unintentional accident is not the subject of safety or security risk management. Safety or security risk management aims to provide solutions in the form of an economically acceptable and appropriate proposal that will positively affect security and safety procedures. In addition, Mærli et al. (2009), identify the differences between safety and security, considering that unintentional and without certain target events are classified as safety events, while intentional, planned, and targeted events are security events. Figure 2 illustrates the differences between safety and security as described by Nyman et al. (2010) and Fransas et al. (2012).

Formal Safety Assessment (FSA) is the use of standardized methods (usually quantitative) of grading the existence of safety measures, i.e. the existence of measures for the protection against accidents or unintended hazards (such as unintentional accidents). According to the IMO definition: *“One way of ensuring that action is taken before a disaster occurs is the use a process known as formal safety assessment. This has been described as ‘a rational and systematic process for assessing the risks associated with shipping activity and for evaluating the costs and benefits of IMO's options for reducing these risks.’ It can be used as a tool to help evaluate new regulations or to compare proposed changes with existing standards. It enables a balance to be drawn between the various technical and operational issues, including the human element and between safety and costs.”* (IMO, 2019). FSA was originally developed after the offshore platform Piper Alpha explosion of 1988 in the North Sea. It was introduced in 1997 with the Interim Guidelines for the application of FSA to the IMO rule-making process by MSC/Circ.829-MEPC/Circ.335 (IMO, 1997) in order to support decision making. In 2002, IMO issued the Guidelines for FSA for use in the IMO rule-making process by MSC/Circ.1023-MEPC/Circ.392 (IMO, 2002). The Guidelines have since been amended by MSC/Circ.1180-MEPC/Circ.474 (IMO, 2005) and MSC-MEPC.2/Circ.5 (IMO, 2009), revised by

MSC-MEPC.2/Circ.12 (IMO, 2013) and MSC-MEPC.2/Circ.12/Rev.1 (IMO, 2015) and now have been superseded by MSC-MEPC.2/Circ.12/Rev.2 (IMO, 2018).

Similarly, and according to the opinion of the author, **Formal Security Assessment (FSecA)** could be defined as “*the use of standardized methods of grading the existence of security measures, i.e. the existence of measures for the protection against deliberate and intentional accidents and for evaluating the costs and benefits of options for reducing these risks.*”

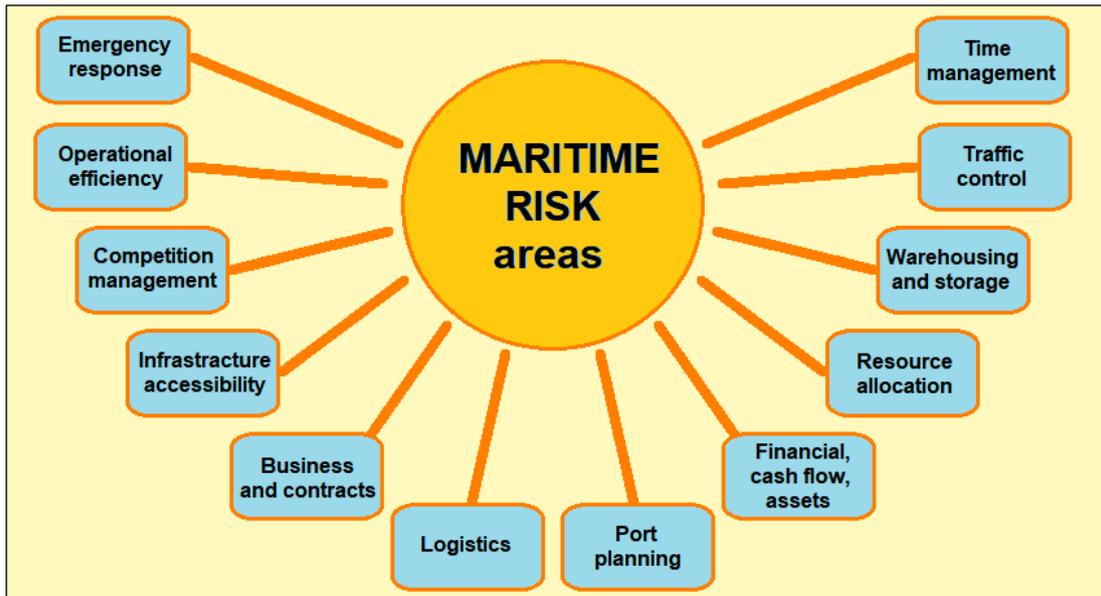


Figure 1. Maritime risks areas.
Source: Created by the author, based on Burns (2015).

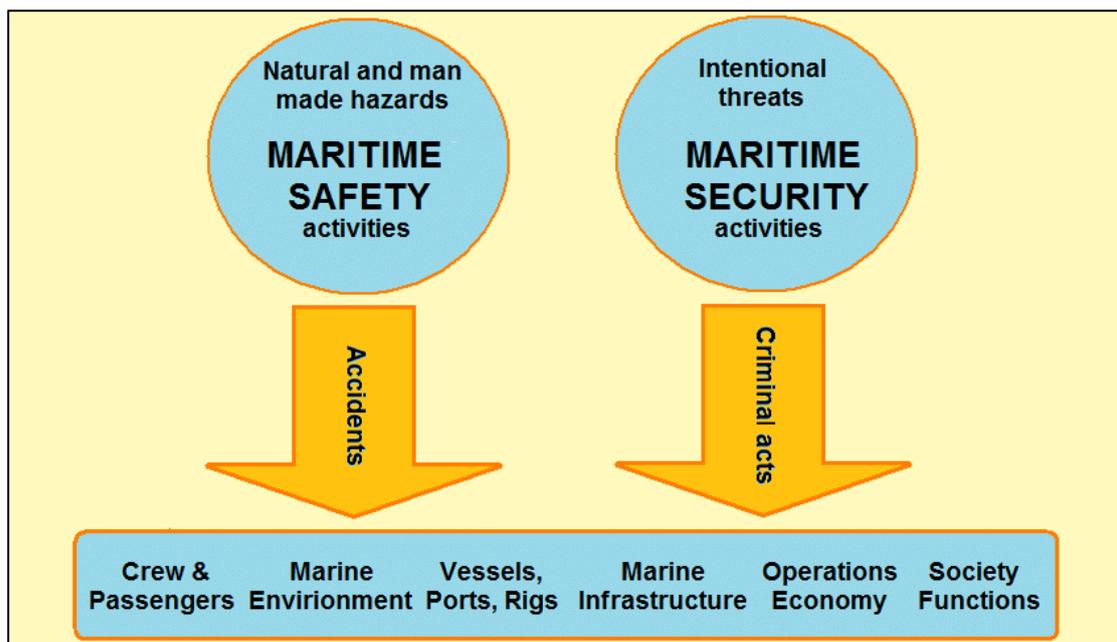


Figure 2. The sketch of the maritime total safety, showing the differences between safety and security.
Source: Created by the author, based on Nyman et al. (2010) and Fransas et al. (2012).

The European Commission's "Guidance of risk assessment at work" defines **hazard** as "*the intrinsic of property or ability of something (e.g. work materials, equipment, work methods and practices) with the potential to cause harm.*" (European Commission, 1996). Actually, hazard may be defined as a condition which includes a potential for human injury and damage either to property or to the environment, and in some cases, to both of them (IMO, 2002).

Also the European Commission's "Guidance of risk assessment at work" defines **risk** as "*the likelihood that potential for harm will be attained under the conditions of use and/or exposure, and the possible extent of the harm.*" (European Commission, 1996). It is a combination of the probability of an adverse event occurring and the magnitude of its possible consequences, or a combination of the probability of a particular adverse event occurring and the severity of its effects. Risk is in fact the possibility of injury or loss of life due to the likelihood of the adverse event and its adverse consequences. It is measured as a threat size that is calculated as a combination of the probability and the results of the adverse event, known as threat (IMO, 2002). For the numerical calculation of the expected risk, the product of these values is calculated taking into account the uncertainty. Essentially for security, risk identification is based on the analysis and aggregation of three key factors: threat, vulnerability and consequence (IMO, 2002).

Threat is considered as an indication or event that may cause loss of life or injury, damage to the environment, loss of an asset or negative effects on reputation. To assess security risk, threat is explored in terms of the intent and ability of a malicious third party to cause damage to property, populations or the environment through its actions (Threat Analysis Group, 2019).

Vulnerability is considered to be a possible problem in the design, construction or operation of a structure or infrastructure as well as in the behaviour of employees, which may be the reason for probable loss of life or injury, damage to the environment, loss of an asset or negative effects on reputation. In the case of security, vulnerabilities can be exploited by malicious individuals, in order to affect negatively human lives, environment, assets and reputation as well as to cause other consequences (Threat Analysis Group, 2019).

Consequence is the result of an event, which includes all direct, short-term and long-term losses or damages, caused due to intentional or non-intentional actions

(IMO, 2002). Losses may include human life losses or injuries, financial losses and environmental impacts, and even less visible and less quantitative impacts, including political impacts, as well as the reduction of reputation and operational efficiency of the involved parties (IMO, 2002).

Also, trying to distinguish between safety and security we may say that **safety** is “*the protection against mishaps that are unintended*” (such as accidents). That means that safety is “*protection against hazards*” (accidents that are unintentional). On the other hand, **security** is “*the protection against deliberate accidents*” (such as attacks from miscreants). That means that security is “*a state of feeling protected against threats that are deliberate and intentional*” (Psaros et al., 2009; Fransas et al. 2012).

Finally, trying to distinguish between formal and informal assessment we may say that **formal assessment** is “*the use of standardized methods (usually quantitative methods) of grading the existence of safety [or security] measures*”, while **informal assessment** is “*the use of non-standardized tools (usually qualitative methods) of grading the existence of safety [or security] measures*”. Specifically, the definition of Formal Safety Assessment was given in the beginning of § 2.2 (IMO, 2019).

2.3. The concept of Maritime Security

When the term security is used, it includes all intentional acts. In contrast, when the term safety is used, it refers to unintentional events. The traditional approach to safety mainly deals with accidental and unintended failures, unintentional errors and malfunctions, as well as all possible damages or losses arising from them. On the contrary, the analysis of intentional and planned actions aimed at harmful results in specific targets, is the subject of security. With this approach, any act of piracy, vandalism, terrorism, theft, espionage etc., are considered as a security issue. In addition, the concept of security includes organized crime, such as smuggling, human trafficking, tax evasion, blackmail, etc., which benefit criminals while harming people, property and the state (Nyman et al., 2010; 14). In this chapter we discuss the definitions of maritime security, as well as threats and related security risks. Threats are defined and classified in the existing literature, and are described in more detail in this context.

Also, based on who uses the term or in what context it is used, there are many definitions for the terms general "security" and especially "maritime security" (Klein,

2011). In Natalie Klein's book *Maritime Security and the Law of the Sea* (2011, 4) defines security in many ways from an academic point of view. Thus, for example the Copenhagen School (Bradford, J. 2004, according to Klein, 2011, 4) defines security as: *“Security is a socially constructed concept and that discourse is a key element in the construction and identification of security issues. Based on the discourse which surrounds it, a public policy issue can be classified as non-politicized, politicized or securitized. [...] A securitized issue is identified as a potential threat to the continued existence of the state. Once securitized, issues are perceived to be of such immediate importance that they are elevated above the ordinary norms of the political debate and the state acquires special rights to adopt extraordinary measures in order to protect itself”*.

Moreover, Genserik Reniers (2011) has defined security as: *“taking all preventive measures in order to avoid harmful incidents caused by unauthorized (internal or external) persons who intend to seriously damage the company, as well as controlling such incidents and their adverse effects”*.

Also, the concept of security is defined by The Finnish Ministry of Defence as follows: *“The comprehensive concept of security comprises security issues which, if exacerbated, may turn into threats that can jeopardize or seriously harm Finland, Finns or the functions vital to Finnish society. Wide-ranging threats include premeditated action such as the use of military force, terrorism or interference with information networks. They can also occur spontaneously, such as widespread failures of the electric grid or extreme forces of nature”* (Finnish Ministry of Defence, 2011).

Natalie Klein (2011, 8) finds that those working in different fields use the term "maritime safety" differently. Thus, the army treats the concept of maritime security differently than the companies in the shipping industry. For example, the US Naval Operations Concept uses the following phraseology when referring to shipping security business issues: *“ensuring the freedom of navigation, the flow of commerce and the protection of ocean resources, as well as securing the maritime domain from nation-state threats, terrorism, drug trafficking and other forms of transnational crime, piracy, environmental destruction and illegal seaborne immigration”* (US Navy, 20067, ref. to Klein, 2011).

On the other hand, ship-owners believe that the existence of maritime security is primarily necessary to ensure the transport of cargo without any problems related to criminal activity (Raymond & Morrien, 2008, according to Klein, 2011, 8). Regarding this view of ship-owners, Steven Jones (2006), in his book *Maritime Security* considers that the importance of security for them is “*the state of a shipping company/vessel/crew/port, being of feeling secure*“, or “*the safety of a shipping company/vessel/crew/port against such threats as terrorism, piracy, and other criminal activities*”. Moreover, the UN Secretary-General concludes that there is no commonly accepted definition of maritime security, and seeks to identify actions that are commonly considered to deliberate threats to maritime security, rather than clearly defining the term "security" (UNGA, 2008).

Especially after the terrorist attacks in the United States in 2001, the practice of maritime security needs to be examined in a new context, which is undergoing rapid changes. It is necessary to find new ways to develop initiatives and cooperation between the private and public sectors in order to overcome terrorist acts and criminal activities. Therefore, minimizing life losses, injuries, financial losses and environmental degradation due to terrorism and criminal activity, are priorities that will ensure their smooth operation and continuity of maritime business. However, as mentioned earlier, while piracy and theft are based on economic benefits, terrorism at sea is often appear due to political reasons (Psaros et al., 2009). Piracy and theft are essentially aimed at maintaining maritime trade, as a means of enrichment that will result from criminal activities, while the terrorisms due to political reasons are aimed at destroying it as a way of enforcing power. However, in recent decades, there has been a widespread perception that there is a conflict between piracy and terrorism, which creates further problems in how to address security issues at sea (Bakir, 2007; King, 2005; Crist, 2003; Chalk, 2008; Talley & Rule, 2008).

2.4. Maritime Security Regulations

In response to the events of September 11, 2001 in the United States, as well as a host of ongoing problems in maritime transport of people and cargo, due to rising terrorism, crime, piracy, etc., several regulations have been drawn up that are mandatory or voluntary, aiming at security of the maritime industry (Bichou 2008; Chalk, 2008).

The main regulatory measures that have been adopted and implemented are included in the IMO security package, including a new Chapter XI-2 on the Convention on the Safety of Life at Sea (SOLAS) Convention (1974/1988), which specifically mentions measures to achieve security in maritime transport. This is the of International Ships and Port Facilities Security (ISPS) Code (IMO, 2003) which describes the minimum security measures for vessels, port facilities and public organizations, to identify security threats and take the necessary preventive measures to deal with incidents that affect vessels or ports. The Code is a two-part document. The first part includes mandatory requirements, while the second part provides instructions for implementation. The Code was adopted by 108 members of the SOLAS Convention at a meeting in London on 12 December 2002. The Code entered into force on 1 July 2004, with application for ships for international travel, such as passenger ships, cargo ships with a total capacity of 500 or more, mobile offshore drilling, as well as in port facilities for such ships.

The ISPS code aims to: a) Cooperation between governments, public services, local governments and shipping industry companies to identify security threats and implement security measures. b) Determine the relevant roles and responsibilities of collaborating governments, public services, local government and shipping companies, nationally and internationally to achieve maritime security. c) The timely and effective collection and exchange of information related to security. d) The preparation of a procedure for security evaluation, by creating plans and procedures for the various forms of security. e) Create the necessary confidence for taking appropriate and specialized security measures at sea.

There are three categories of Security Levels. Security Level 1 is the main level applied under normal circumstances. In the case of medium security alert, the Level 2 will be applied. In exceptional cases, the high Level 3 will be applied. Therefore, there are different requirements imposed by the ISPS Code, corresponding to different risk levels. There are no specific measures specified by the ISPS Code that each port and each ship must take, in order to ensure the security against terrorism. There are only standardized, consistent frameworks for evaluating risk, which enable governments to estimate the required changes for ships and port facilities.

It is clear that this code aims to create appropriate collaborations for a timely and effective collection and exchange of security information, through a security

assessment process, with appropriate plans and procedures for the various forms of security (IMO 2003). The Automatic Identification System (AIS) and the Long Range Identification and Tracking (LRIT) can be used in the context of IMO, which improve navigation security levels and the marine industry security in general. These systems are designed to provide useful information (such as identity, type, location, course, speed, navigation status) of the ship to other ships and to port authorities (IMO, 2004; IMO, 2009b).

Additionally, another important set of security measures exists in various states, with that of the United States being considered particularly important. This includes the Container Security Initiative (CSI), the Customs- Trade Partnership Against Terrorism (C-TPAT) and others (Bichou, 2008; Crist, 2003; Chalk, 2008). The most important change is the increased demand for information, documentation, control and exchange of information on cargo maritime transport.

However, the previously mentioned procedures for the implementation of security measures have not been introduced in a scientific way and scientific justification, while the issue of cost and benefit assessment has not been estimated systematically and in advance. In addition, the contribution of security measures to reduce risk should be made clearer. Given that both the proposed security measures and their implementation are based on procedures and criteria for assessing the acceptable level of risk (IMO 2002), it is clear that a risk-based approach is needed to assess the effectiveness of security measures.

2.5. Vulnerabilities existing in the maritime industry concerning security

Terrorism, piracy, robbery, cyber-threats on ships and port facilities, smuggling and drug trafficking through cargo and containers, etc., are some of the international security problems due to which the national maritime security services must provide solutions. **Cyber-attack is considered particularly important due to the possibility to be combined with all the other security vulnerabilities in the shipping industry.**

It is clear that there is a range of vulnerabilities in the maritime supply chain, which makes it particularly vulnerable to malicious acts resulting from criminal and terrorist elements. It is therefore necessary for the national maritime security services to take appropriate security measures in order to reduce the threats posed by these

malicious elements. Figure 3 shows the vulnerabilities in maritime transport and port facilities.

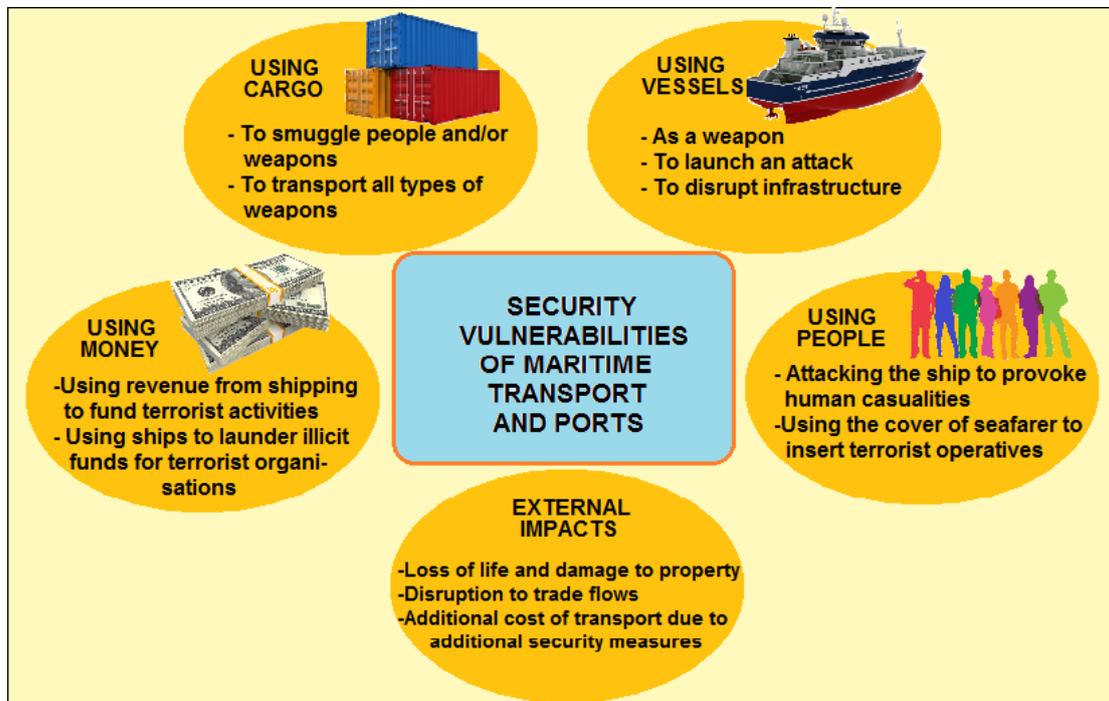


Figure 3. Security vulnerabilities of maritime transport and ports.
 Source: Created by the author, based on OECD (2003) and Mc Nicolas (2016).

2.5.1. Terrorist Targeting of Ships and Ports

During the recent decades, terrorist groups have targeted and attacked ships and port facilities and used merchant ships and coastal transport ships as means of transport for terrorists and illegal weapons and cargo worldwide. During the same period, the Islamic State expanded, and the number of terrorist organizations extending from West Africa to Southwest Asia, which use military weapons in naval terrorist attacks, increased, creating a bleak prospect for shipping industry. The alleged "operational alliance" between various forms of terrorist organizations in the form of a network for economic gain, includes drug traffickers, smugglers, pirates and cooperating states friendly to this alliance, which facilitate their activities. It is precisely these criminal alliances with their threatening terrorist activities against the maritime sector that are the subject of concern for maritime security scholars (Mc Nicolas, 2016; Prodan, 2017). A list of attacks on ships and ports after year 2001 is given in Table 1 (Safety4Sea, 2017).

Each port or a harbour is a specialized case for security risk assessment, where many different parameters and shipping activities and functions are taken into account. There are also differences in the location of the port or harbour, given that different locations also have different commercial profiles and obviously different security problems. There are also differences due to the flow of passengers or due to their distance from environmentally sensitive areas.

Table 1. Attacks on ships and ports after 2001.
Source: Safety4Sea (2017).

Attacks on Ships			
Date	Ship	Area	Result
06.10.2002	LIMBURG tanker	From Iran to Malaysia	1 person lost his life
27.02.2004	SUPERFERRY 14	Philippines	116 persons lost their lives
28.08.2005	DON RAMON	Philippines	30 passengers wounded
27.07.2010	M STAR tanker	Straits of Hormuz	1 person injured
31.08.2013	COSCO ASIA	Suez Canal	Limited damages

Attacks on ports		
Date	Port	Result
14.03.2004	Port of Ashdod	10 people were killed and 16 others injured
11.12.2016	Port of Mogadishu	16 people were killed and 48 others injured

Therefore, dealing with security issues for ports or harbour requires a broad knowledge of the specific maritime business activities that are carried out, in order to better assess the risks. It is therefore necessary, when assessing the risks in a port or harbour, to use all the existing knowledge relevant to all existing activities for each port or harbour. There should be a database that can be supplemented with both new data and feedback that will make it easier for the practitioner to gain a better understanding of what is going on in the field.

Also, **special information** is necessary to be taken into account, which will include but not be limited to, the information given in the following Table 2 (McNicolas, 2016). Also, the port or harbour then needs to be categorised into appropriate **areas for specific security care**, as shown in the next Table 3 (McNicolas, 2016).

Table 2. Special information required for the security of ports or harbour.
 Source: McNicolas (2016).

Special information required
◦ Vessel sizes and types using the port or harbour
◦ Nature of leisure activities
◦ Passenger movements
◦ Traffic density and types of traffic involved at busiest times
◦ The tidal regime, wave height and periodicity
◦ Non tidal oceanography (long period waves; surging, etc.)
◦ Navigational channel width, depth and route/heading needed for each transit
◦ Hydrographic information and sea bed morphology
◦ Weather limitations
◦ Types of berths/securing and fendering arrangements
◦ Types of cargoes being handled
◦ Disposition of navigational aids
◦ Communication or radar black spots
◦ Pilotage system and pilotage criteria
◦ Status of operating manuals and limitations on movements
◦ Available incident and accident data

Table 3. Areas of specific security care in a port or harbour.
 Source: McNicolas (2016).

Areas of specific security care in a port or harbour
◦ All gates and access points (functional or otherwise)
◦ Restricted areas on the port facility
◦ Ship berths
◦ Emergency equipment and emergency shutdown controls
◦ Parking areas
◦ Security checkpoints
◦ Building/structures within the facility
◦ Traffic flow, including emergency vehicle lanes
◦ Storage areas for dangerous materials
◦ Critical port facility assets

2.5.2. Piracy and Armed Robbery

The International Maritime Bureau (IMB) defines piracy and armed robbery against ships as follows:

“An act of boarding or attempting to board any ship with the apparent intent to commit theft or any other crime and with the apparent attempt or capability to use force in the furtherance of that act.”

And, Article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) defines Piracy as follows:

“(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the Crew or the passengers of a private ship or a private aircraft, and directed (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) Any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).”

The IMO defines Armed Robbery in Resolution A.26/Res.1025 (IMO, 2010) as:

“Armed robbery against Ships means any of the following acts:

(a) Any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State’s internal waters, archipelagic waters and territorial sea;

(b) Any act of inciting or of intentionally facilitating an act described above.”

In recent years there has been a significant increase in the number of pirate attacks on ships, particularly in the Gulf of Aden, the Somali Basin and the Indian Ocean. Large water areas are affected by the challenge of preventing maritime piracy. Figures 4, 5 and 6 illustrate the number of piracy attacks globally and per area. The good news is that piracy overall has dropped to its lowest level since 1998, according to data from the International Maritime Bureau’s (IMB) Piracy Reporting Centre’s yearly piracy report and IMO yearly reports (IMB, 2020; IMO, 2020).

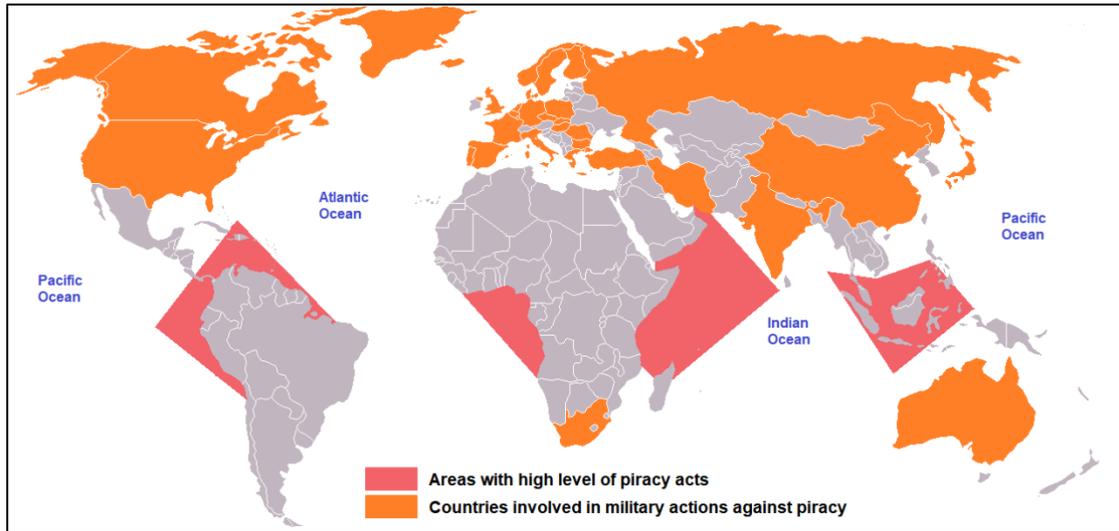


Figure 4. Piracy areas, countries involved in the international military fight against piracy and countries where prosecutions have been engaged. Source: Created by the author, based on data from IMO (2020).

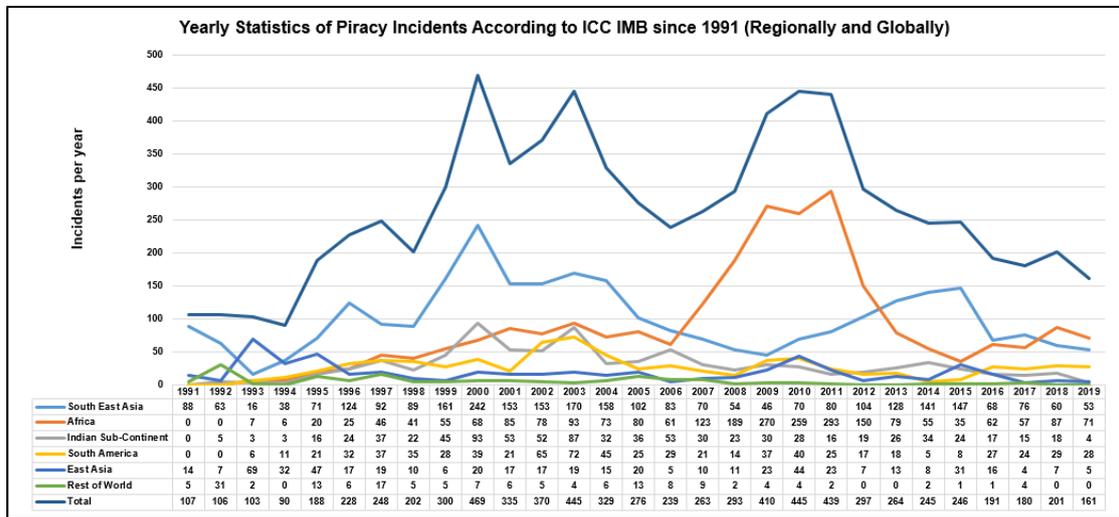


Figure 5. Yearly Statistics of Piracy Incidents According to ICC IMB since 1991 (Regionally and Globally). Source: Created by the author using data from IMB (2020).

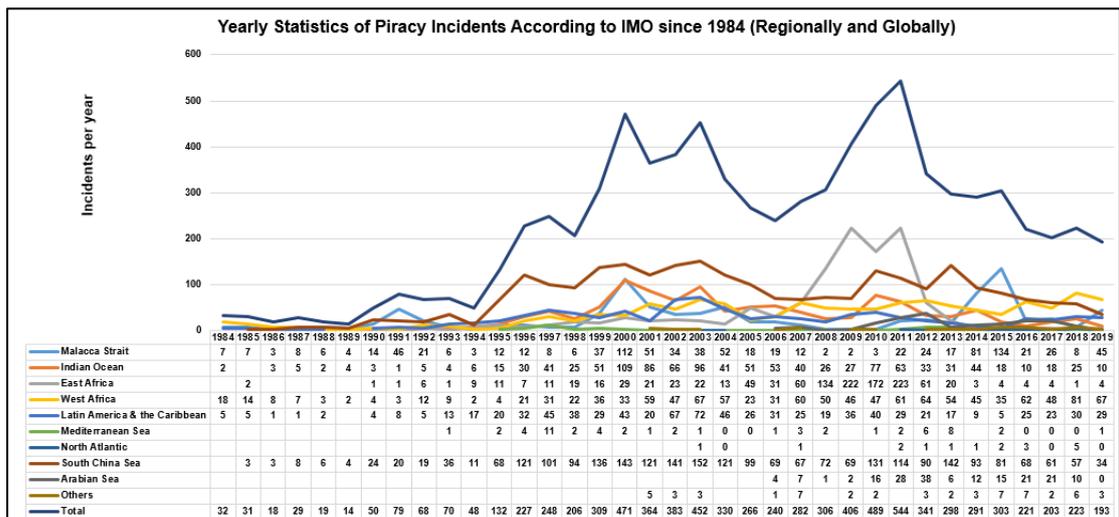


Figure 6. Yearly Statistics of Piracy Incidents According to IMO since 1991 (Regionally and Globally). Source: Created by the author using data from IMO (2020).

Maritime piracy affects large docks and jeopardizes the life of seafarers and merchant seafarers from around the world. Among them, some hundreds are arrested each year (see Table 4). At the same time, millions of dollars are being paid as piracy ransom. There is a general belief that some of this money is distributed among pirates, those who guide them and those who finance them. However, part of the ransom seems to be being invested abroad by Somali immigrants.

Table 4. Piracy attacks, Seafarers affected and Piracy cost by area.

Source: Created by the author using data from: *The State of Maritime Piracy (2014, 2015, 2016, 2017, 2018, 2019, 2020)*.

	2012	2013	2014	2015	2016	2017	2018	2019
EAST AFRICA AND SOMALIA								
Attacks	47	23	18	16	27	54	9	12
Seafarers affected	851	486	320	306	545	1,102	175	270
Piracy Cost (billions \$)	5.7	3.0	2.3	1.3	1.7	1.4	N/A	N/A
WEST AFRICA AND GUINEA								
Attacks	43	100	67	54	95	97	112	98
Seafarers affected	966	1,871	1,035	1,225	1,921	1,726	2,012	1,689
Piracy Cost (millions \$)	845	623	983	720	794	818	N/A	N/A
SOUTH EASTERN ASIA								
Attacks			185	199	129	99	98	89
Seafarers affected			3,654	3,674	2,283	1,908	1,730	1,503
Piracy Cost (millions \$)			N/A	9.7	4.5	31.9	N/A	N/A
LATIN AMERICA & CARRIBEAN								
Attacks					27	71	85	84
Seafarers affected					527	854	858	783
Piracy Cost (millions \$)					0.3	0.9	N/A	N/A

2.5.3. Drug Smuggling

Drugs and weapons trafficking takes place by sea due to the opportunities presented for large-scale transportation from producing countries to consuming

countries. It is often linked to organized crime groups and in some cases may be linked to the collection of money for terrorism.

Merchant shipping, unfortunately, can unwittingly play an important role in transporting illicit drugs to the places where they are consumed. The shipping industry therefore has a common collective responsibility to help combat this illicit traffic. This requires shipping companies and ship crews to be constantly aware of the possibility that the ships and cargo they are carrying could be used as cover for drug trafficking (International Chamber of Shipping, 2021).

Thus, drugs and weapons trafficking are connected with other types of vulnerabilities concerning maritime security, such as terrorism, robbery and cyber threats. International Chamber of Shipping explains how cyber-enabled trafficking is accomplished, through the access to sensitive data, regarding the cargoes being transported, code-locks and other devices used to restrict entry, electronic devices, such as CCTV fitted on the vessel covering all places around the vessel, using sometimes social engineering as the mean for this access (International Chamber of Shipping, 2021, Chapter 6).

The main types of illicit drugs trafficked to the United States and Europe through international maritime trade are cocaine, heroin and marijuana. Most illegal drugs are transported by sea. The United Nations estimates that drug transport by sea at a global level during 2014 accounts for more than 60% of all seized drugs. However, it is very likely that this figure is actually "understated" and the actual rate is much higher.

The smuggling routes for Afghan heroin extend beyond the traditional "Balkan Route" and the "Northern Route" (see Figure 7). By 2010, the Balkan route was the main route for Afghan heroin to reach Western Europe. However, according to the UNODC, during the recent years there has been a sharp shift to the "Southern Route" due to improved law enforcement and border control operations along the route in Central Europe and as a result of the conflict in Syria (Dawn, 2015). The newer South Road emerges as an increasingly important maritime route for Afghan heroin destined for Canada, North Europe, Oceania and Africa (Dawn, 2015).

Cocaine smuggling to the United States and Europe from Colombia follows the route shown in Figure 8. However, for maritime transport, it is preferred to use transshipment ports in Central America and Ecuador and, to a lesser extent, through West Africa.

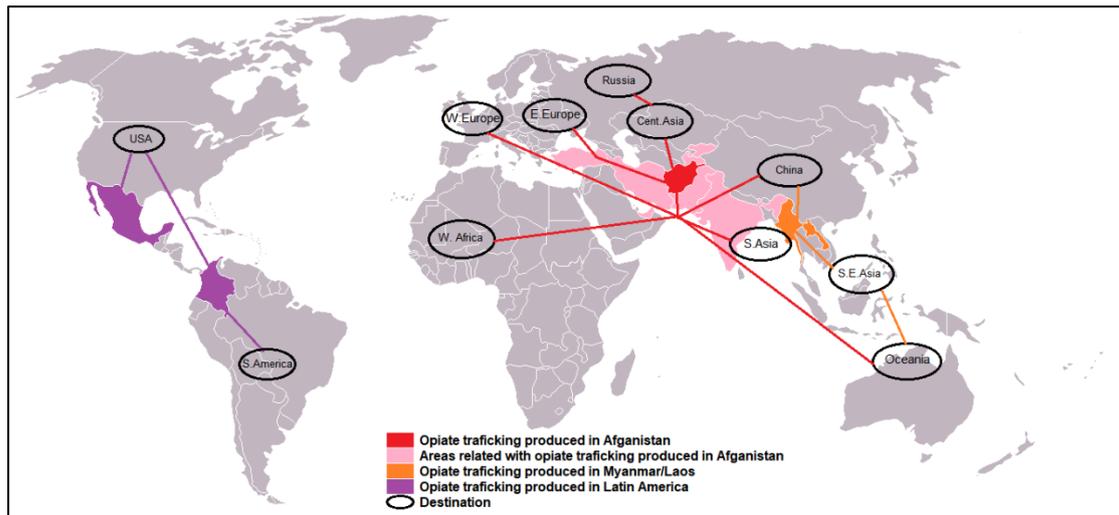


Figure 7. Heroin flow from/to countries or regions.
 Source: Created by the author, based on data from UNODOC (2015).

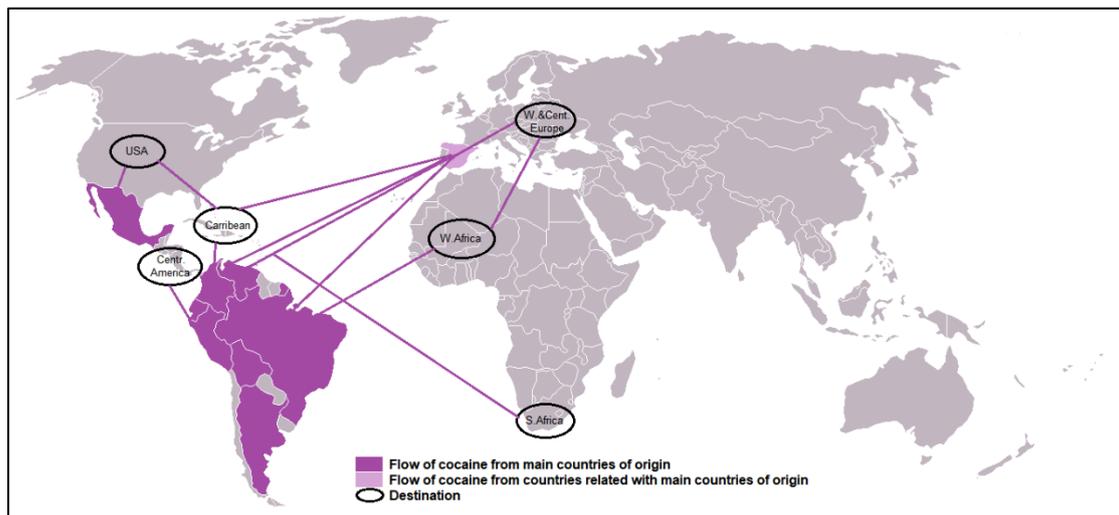


Figure 8. Cocaine flow from/to countries or regions.
 Source: Created by the author, based on data from UNODOC (2015).

It is known in drug law enforcement circles that major drug trafficking organizations in locations such as Colombia and Mexico have teams of "surgeons" in staff, which are engineers, chemists, scientists and logistics experts, who are developing improved new methods, techniques and tactics to mitigate security measures and to discover security "holes", in order to achieve their goals.

Resolution A.20/Res.872 was adopted by IMO on 27 November 1997 (IMO, 1997b), containing Guidelines for the "Prevention and Suppression of the Smuggling of Drugs, Psychotropic Substances and Precursor Chemicals on Ships engaged in International Maritime Traffic". This resolution was replaced by resolution

MSC.82/24/Add.2 for the revision of these guidelines, on 7 December 2006 (IMO, 2006) and by resolution FAL.34/9 for a newer revision of these guidelines, on 30 March 2007 (IMO, 2007).

2.5.4. Cyber and Information Threats to Seaports, Ships etc.

For a long time, cyber threats were not included in the high-risk categories (Jensen, 2015). At the beginning only a small number of companies had drawn up prevention plans to protect against cyber threats or to recover from an attack, minimizing losses. Therefore, the arising hypotheses are whether these companies are overreacting or whether there is a serious risk of cyber-attacks that other companies are unaware of or underestimate.

As a result of the increasing innovation and automation technology, there has been a similar growth in the shipping sector in automatic navigation and communication technology, which has made the shipping industry more vulnerable to cyber-attacks if the appropriate security measures have not been taken.

The threat of cyber-attacks has been taken seriously by some national organizations (American Bureau of Shipping, 2016; BIMCO et al., 2020) and the International Maritime Organization (IMO, 2017). Thus, the cyber risk management sector is now a necessary complement to the security planning of shipping companies by 2021. The non-compliance of shipping companies now carries serious risks of loss of time, money and reputation, given that the risks through malware are constantly increasing.

The following Figure 9 presents the results of a survey conducted in 2016 by IHS Maritime & Trade in collaboration with BIMCO (IHS Maritime & Trade, 2016). The survey found that 65 of the 300 shipping companies, i.e. 21% of shipping companies, admitted to have a successful cyber-attack through their computer and navigation systems, 57% of them did not accept any attack, and the remaining 22% did not reply.

Figure 10 shows that malware was the most common form of cyber-attack by 77%, while phishing was the second with 57%. Also, as shown in Figure 11, of those who admitted to being attacked by cyber-attacks, 67% said they were IT downtime, 48% said they had lost stored data, e-mails, personal data, payroll, human resources information etc., and 21% said they had some financial losses.

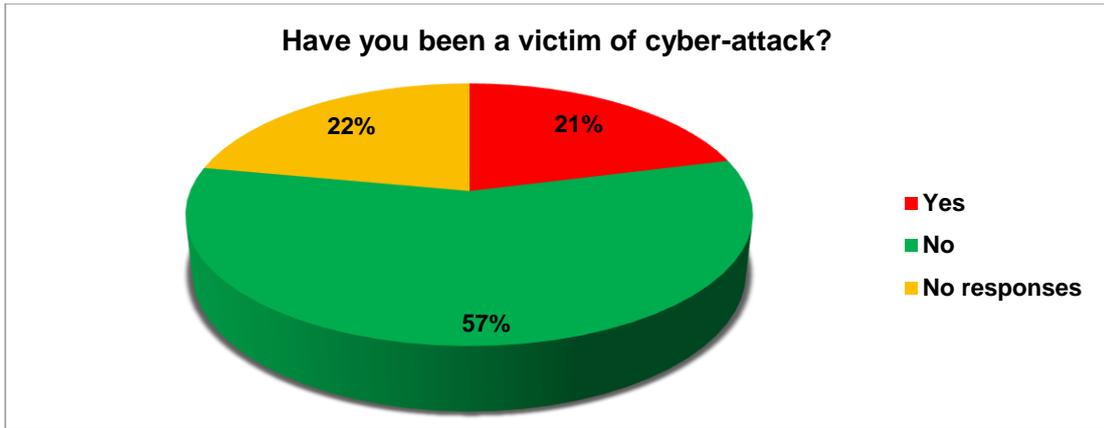


Figure 9. Answers to the question: 'Have you been a victim of cyber-attack?'.
Source: Graph created by the author using data from IHS Maritime & Trade (2016).

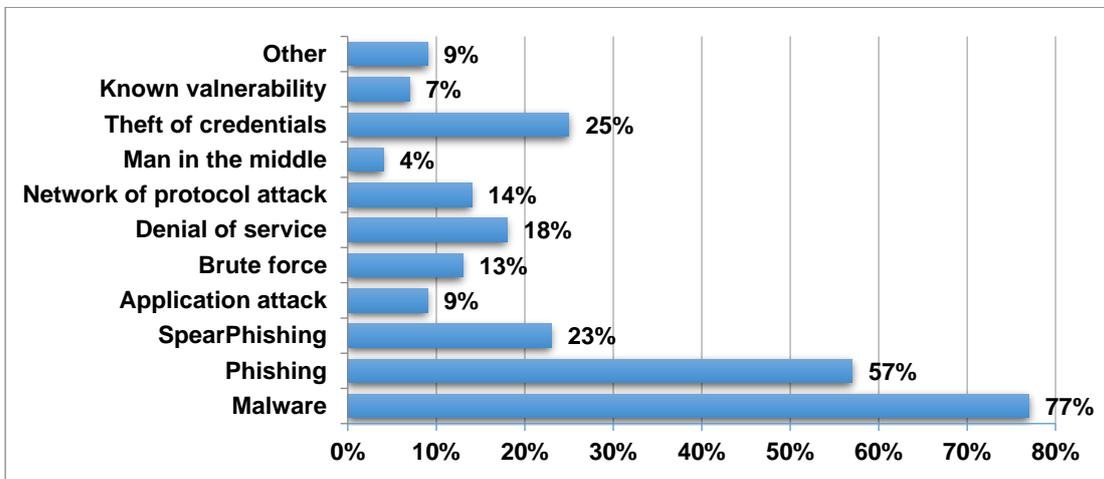


Figure 10. Nature of cyber-attack.
Source: Graph created by the author using data from IHS Maritime & Trade (2016).

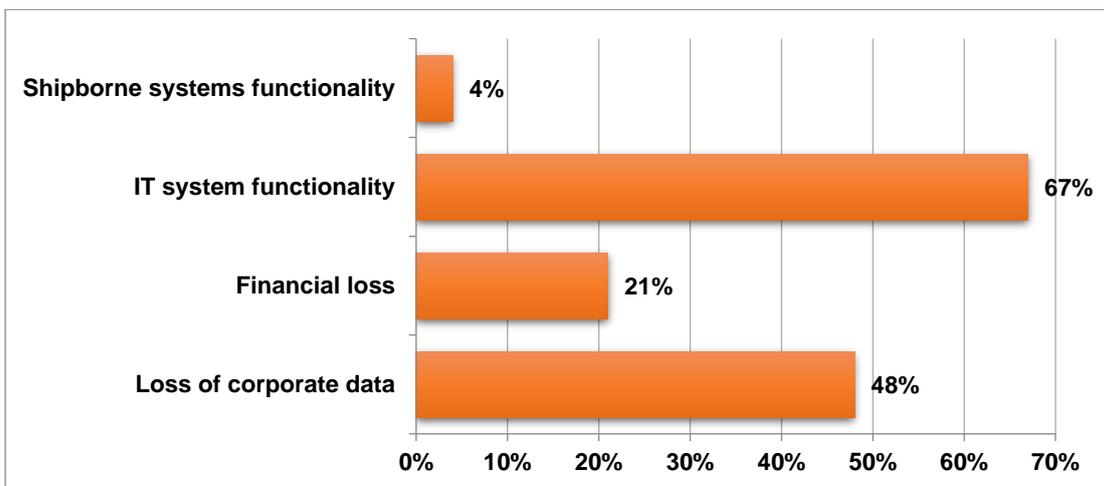


Figure 11. Extend of cyber-attack.
Source: Graph created by the author using data from IHS Maritime & Trade (2016).

In terms of cost, about 50% of those who had a cyber-attack, had financial losses of less than \$ 5,000 and 25% between \$ 5,000 and \$ 50,000. Two of those who responded positively reported economic losses of more than \$ 500,000 (IHS Maritime & Trade, 2016).

Nowadays cyber security is a matter of necessity. Cyber security threats are progressing and becoming a part of our daily business. According to the FBI, *“There are only two types of companies: those that have been hacked, and those that will be.”* Also, according to a 2020 survey of marine professionals, 77% of respondents view cyber-attacks as a high or medium risk. But yet only 64% said that their company has a business continuity plan in order to follow the event of a cyber-security incident. Moreover, only 24% of respondents claimed it was tested every three months, and only 15% said that it was tested every six to 12 months. Additionally, only 40% of the respondents said that their company protects vessels from operational technology (OT) cyber threats, while some of them describe their company policy to OT cyber risk as “careless” (Mission Secure, 2021).

According to Brendan Saunders (2016), Maritime Cyber Threats have increased due to: i) Increasing connectivity of ships, ii) Ever-greater integration of ICS into on board networks, iii) Pre-Internet systems and protocols wrapped in IP, iv) Widespread use of USB memory devices for data sharing, v) Greater use of remote access capability, vi) Attackers increasingly targeting non-conventional IT, vii) Lack of Leadership in the Maritime Cyber Security. Attack surface overview is shown in Figure 12, for ships, harbour, navigation and rigs. Also, according to O’ Neil (2016), the range of attacks is: i) Sealing/Destroying Key Data Bases, ii) Impairing Vessel Operation/Safety Systems, iii) Immobilizing Ports, iv) Tracking/Diverting Vessels & Cargo.

Threats and cyber-attacks on ports, ships, rigs and navigation are now a reality, and the damage they cause can be enormous (see Table 5). It should also be understood that an internet connection is not necessary for cyber-attack. Malware can be transferred via USB units or through upgrades to existing software. So, either through this path or through the internet, the spread of malware may cause significant negative effects.

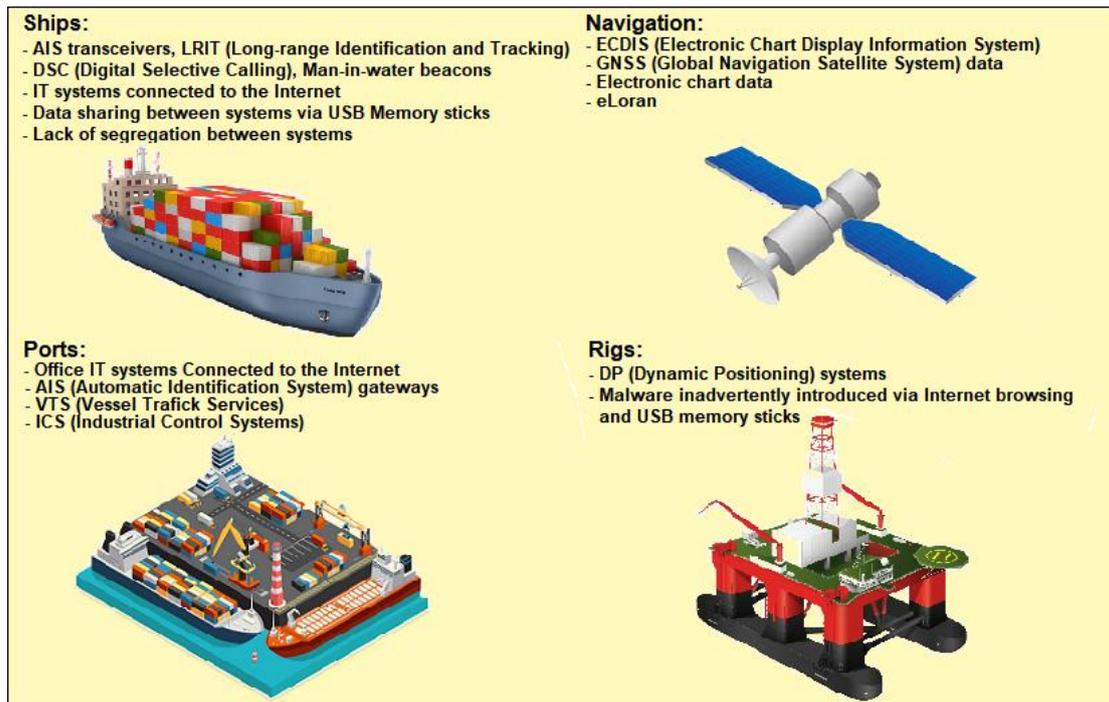


Figure 12. Cyber-attack surface overview.
Source: Created by the author, based on Brendan Saunders (2016).

Satellite or other wireless internet connections, such as SATCOM, VOIP, WLAN, WiFi, may create suitable conditions for cyber-attacks, resulting in the operation failure of a number of electronic communication systems. Also, electronic navigation systems, such as Electronic Chart Display (ECDIS), are usually not accompanied by anti-virus protection software, making it impossible to prevent cyber-attacks resulting to system control loss.

Disruption of the smooth operation of navigation could also be caused by deleting important information. Also, access through cyber-attacks to sensitive data can be obtained, regarding the cargoes being transported, and / or the lists with personal data of passengers and crews, which can then be used by the attackers for illegal activities.

Passenger services and management systems, crew networks and basic infrastructure systems could also be affected, causing effective business stops and financial losses.

Figure 13 shows the complex automation and digital communication systems of modern commercial ships, highly vulnerable to hostile hackers (McNicolas, 2016). *“It really doesn’t matter who the bad guy is” in hacking the vessel itself, from propulsion to navigation systems, port management, terminal capacity of cargo, to a*

maintenance facility's work schedule because "all of these systems are connected together." (Grady, 2020).

Table 5. Reported Cyber Attack cases.

Cyber Attack Reported Cases
Between 2011 and 2013 the Port of Antwerp was subject to cyber criminals to smuggle drugs. They installed physical devices, such as key loggers, and sent malware attached to emails, to infiltrate the computerized cargo tracking system of different companies within the port. In this way, they could identify the shipping containers in which the drugs were hidden. When these containers were located, they dispatched their own drivers to retrieve their containers and covered their tracks afterwards (HLN.be, 2013).
In the summer of 2013 a 'friendly' experiment was performed by researchers from the department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin. They created false civil GPS signals to gain control of the GPS receivers of a superyacht. This technique, called spoofing, did not trigger alarms on the ship's navigation equipment and allowed the research team to change the course of the vessel (The University of Texas in Austin, 2013).
In 2014, the Danish Maritime Authorities discovered they had been attacked in 2012. The attack was carried out through the transmission of a PDF document with an embedded virus. Consequently, this was spread throughout the networks of the organizations as well as other Danish government institutions (Seafocus, 2016).
Off the coast of Africa an oil rig was tilted to one side. This action, caused by hackers, shut the production down for a week. Another incident occurred to an oil rig on its way from South Korea to Brazil. In this case malware had taken the rig's system offline, none of the workers knew the ins and outs of the computer system they were using to operate the rig, which contributed to a delayed response (CSIS, 2016).
The company Verizon mentions a maritime case in their report 'Data breach digest. Scenarios from the field'. In this case, they were contacted by a shipping company who noticed a change in the way pirates operated. These pirates attacked specific vessels and, once on board, they headed for certain cargo containers and then departed the vessel without further incident. After investigation, it became apparent that hackers could access the CMS of the shipping companies, which led them to get insight in the shipping inventories and bills of lading for future shipments (Verizon, 2016).
Personal data of over 134.000 US navy personnel was retrieved by computer hackers. They were able to do so via an access point of the company Hewlett Packard, who are responsible for the automation of the US navy.
The company Fox-IT presented recent 'maritime' cases during Digital Ship Maritime Cyber Resilience Forum Rotterdam (2017).
During 2017, Danish AP Moller-Maersk, the world's largest container shipping line, experienced a large-scale cyber-attack on June 27th. It resulted in the shutdown of IT systems across multiple sites and business units with 17 terminals being hacked. This cost the company between \$250 million and \$300 million (Leovy, 2017).

Resolution MSC.98/428 was adopted by IMO on 16 June 2017 (IMO, 2017b), aiming to address cyber risks in the shipping industry. Cyber risks were effectively addressed by the IMO resolution as a part of safety management systems included in the ISM Code. By this resolution it is necessary to ensure that the existing safety management systems address appropriately cyber risks and cybersecurity for ships by

their 2021 annual verification. It summarizes key parts of the IMO 2021 cyber security measures in shipping industry, connected to ISO/IEC 27001 and the Guidelines on Cyber Security on Board Ships, providing also information and a framework for the cyber security of ports (Mission Secure, 2020).

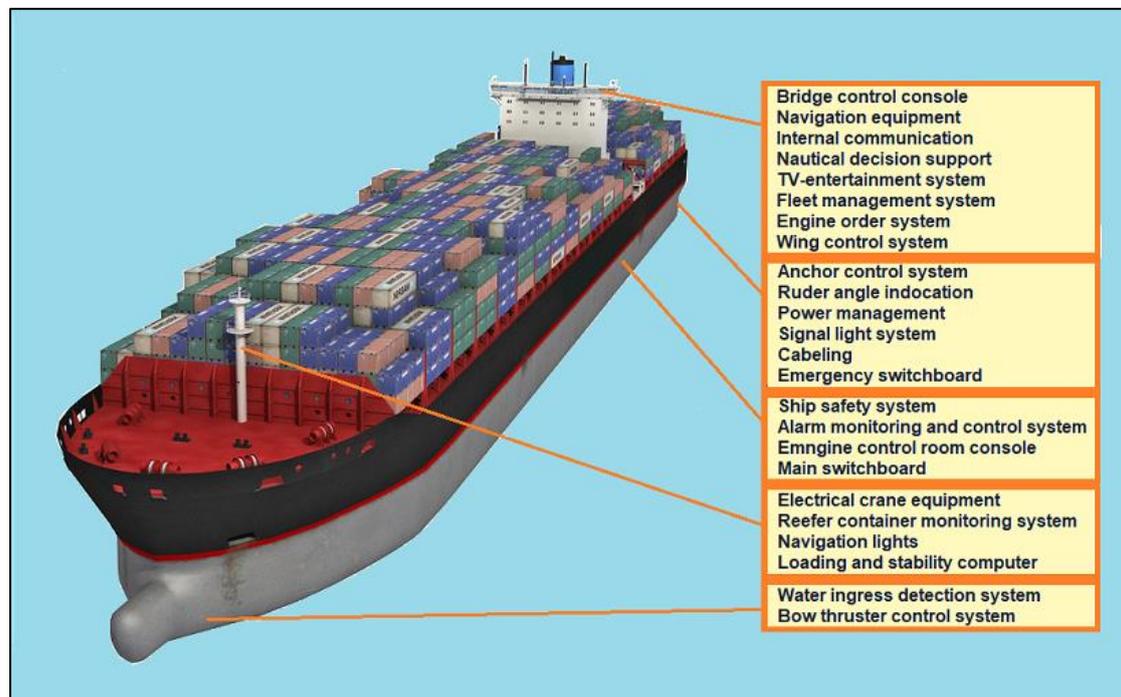


Figure 13. The complex automation and digital communication systems on most modern commercial ships, highly vulnerable to hostile hackers.

Source: Created by the author, based on information given by McNicolas (2016).

2.6. Maritime Security Assessment

The historical past of maritime safety in terms of regulations, methods and guidelines goes back to IMO research and methodology specifically for the Formal Safety Assessment (FSA) procedure. This is a systematic methodology structured to use risk assessment and economic analysis in order to improve maritime safety, which includes the protection of human life and health, as well as the protection of property and the marine environment (IMO, 2018; IMO, 2019).

However, it seems necessary to develop a similar security risk management process to be combined with that of the security risk management. Bichou (2008), and Brooks & Pelot (2008) consider that the safety risk assessment and management procedures could also be used as security risk assessment and management procedures. Also, Parnell et al. (2007) argue that it is possible to assess, evaluate and

manage together security and safety risks, which can be implemented in a common framework that generally covers the social, environmental and economic dimensions. In addition, Lambert (2007) examines the possibility of combined actions and the allocation of financial resources to address both security and safety in the maritime industry, given their interdependence. It is therefore logical to use similar approaches and practices to address both security and safety issues in the shipping industry.

In fact there is no extensive and in-depth literature for the risk acceptance criteria concerning maritime security. Basic information is drawn from other areas, such as civil aviation. It is necessary to standardize these criteria, as is the case with the FSA, where practitioners know how to gather information, to make comparisons with previous experience and to make decisions that are often based on experience from the past. However, risk acceptance criteria may be based on political or subjective assessments, while risk identification should be based on objective assessments and be performed prior to the FSA. Their usefulness is especially important for final decision making. Both risk acceptance criteria and decision-making determine the measurable risk assessment, as well as the level of necessary financial cost to reduce the risk.

Risk acceptance criteria are used when deciding to implement Risk Control Options (RCOs). However, according to some scholars, they are not applicable in cases of saving human life or reducing marine pollution, while they can be used only when making decisions about choosing, for example, rescue equipment and not the rescue operation itself. This is because in a rescue operation, all resources for human lives must be available without considering the cost (Skjong et al. 2007).

Based on previous discussion, the FSA procedure, developed systematically by the IMO as a Risk Assessment Methodology and Cost Effectiveness Analysis (CEA) can therefore be used as a decision making support tool in the assessment of security risks and in the preparation of new regulations for both safety and security at sea as an extension. In this way, a balance could be obtained between the various technical and operational issues used, which would contribute to the protection of human life and health, the reduction of economic losses, the protection of the marine environment and the maintaining of maritime companies reputation.

Taking into account the ISPS Code, the evaluation of risk scenarios depending on the size of the threat is carried out using a scale from 1 to 3, with a rating from a

simple threat to a serious threat respectively. This scale was adopted through the provisions of the ISPS code of the United States Coast Guard MARitime SECURITY (MARSEC). In both of the previously mentioned models, the risks are identified, assessed and prioritized using a combination of probability and impact. In practice, risk management is a procedure for decision-making where measures are taken based on the outcome of the risk assessment. Well-known standard risk prevention procedures aim either to reduce the probability of an accident (pre-accident intervention) or to minimize the probability of negative effects in the event of an accident (post-accident intervention).

Cost-benefit Analysis (CBA) is usually added to these processes for the best possible decision making. It is essentially a basic complement to the process for the optimization of the result. The FSA process introduced the CBA through its official guidelines approved by the IMO in 2001 and incorporated into many well-known maritime security assessment systems (US Maritime Transportation Security Act, 2002; OECD, 2003; UK Regulatory Impact Assessment, 2004).

Therefore, regarding maritime security, it is necessary to set specific and specially defined risk criteria, as the security risk assessment is not comparable to the traditional risks of maritime safety. Thus, as with the FSA case (IMO 2018), it is proposed by some researchers (Psaros et al., 2009) “*a five-step risk assessment process for the maritime security case:*

- i) Hazards identification (HAZID)*
- ii) Risk assessment (RA),*
- iii) Risk management with alternative risk control options (RCOs),*
- iv) Cost-benefit analysis (CBA) and*
- v) Recommendations for decision making.”*

Several other studies in maritime security have been carried out, either generally (Yang & Wang, 2009; Yang et al., 2011; Yang, 2014; Yang & Qu, 2016) or specifically for containers supply chains (Yang et al., 2010), seaports and port facilities (Orosz et al., 2009; Yang et al., 2013b, Yeo et al., 2013), infrastructures (Patterson & Apostolakis, 2007), piracy and robbery (Pristrom et al., 2016) etc.

2.6.1. ISO 31000 and ISO 27005 for risk management

Risk management regulations were implemented in the United Kingdom in the 1970s and in the European Union and Australia in the 1990s, and have been incorporated into ISO 31000 standard. Many high-risk industries use this risk management standard and through this, they develop, implement and improve their risk management framework, following the provided guidance (ISO, 2018). Also, ISO 20858 for Maritime port facility security assessments and security plan development was developed (ISO, 2007).

Additionally, the ISO 27000 family of standards provides a complete system for **information security risk management**. It uses the existing experience from other existing quality system standards, but in the same time it introduces new approaches for the management of complex cases of cyber and information security (Risk Review, 2018).

ISO 27005 standard was prepared by the ISO / IEC JTC1 Joint Technical Committee, Information Technology, SC 27 subcommittee, IT Security Techniques. ISO 27005 and includes guidance for security Risk Management (ISO/IEC 27005, 2011). This standard includes both qualitative and quantitative risk analysis options, but does not provide detail about methods and their application (Agrawal, 2017).

Although ISO 31000 and ISO 27005 risk management processes does not specify any specific risk management method, they imply a continual information risk management process based on six key components:

1. Context establishment
2. Risk assessment
3. Risk treatment
4. Risk acceptance
5. Risk communication and consultation
6. Risk monitoring and review

Figure 14 provides an overview of ISO 31000 and ISO 27005 for “Information technology – security techniques – information security risk management” (ISO, 2018; ISO/IEC 27005, 2011).

Also, Figure 15 provides a risk management programme according to ISO 31000 and ISO 27005 for “Information technology – security techniques – information security risk management”.

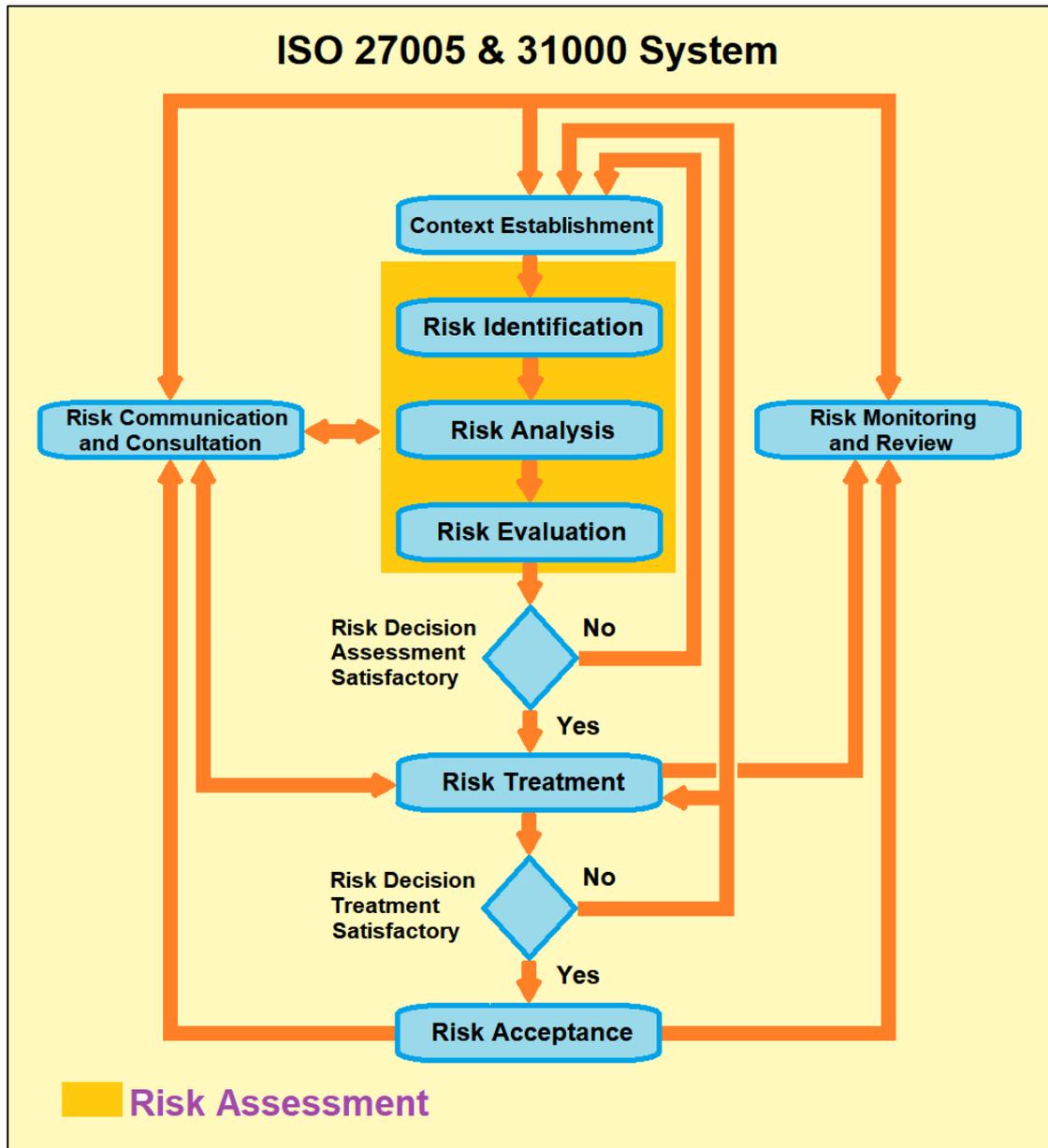


Figure 14. Overview of ISO31000 and 27005.
 Source: Created by the author, based on ISO (2018) and ISO/IEC 27005 (2011).

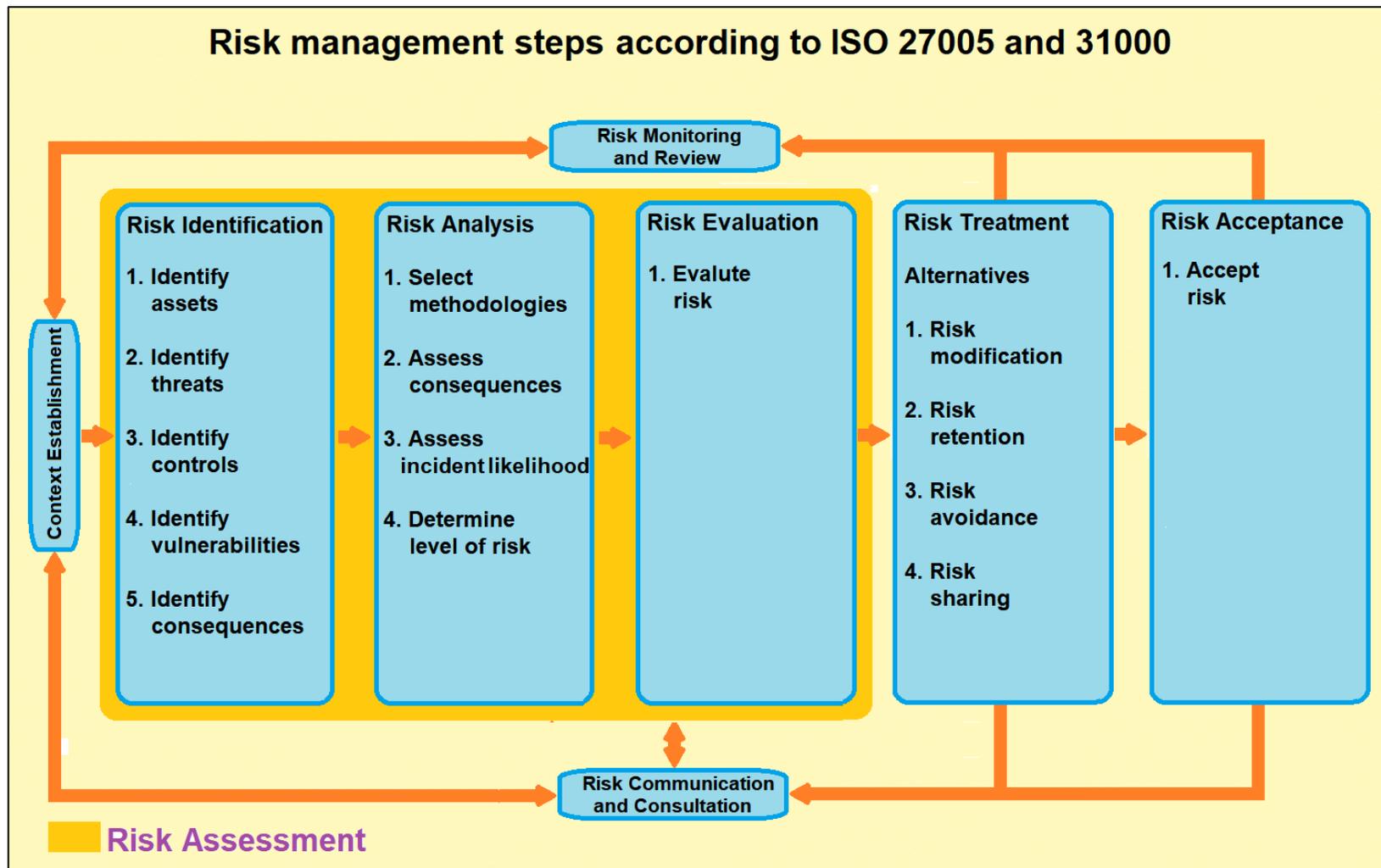


Figure 15. Risk management programme according to ISO 31000 and ISO 27005.
 Source: Created by the author based on ISO (2018) and ISO/IEC 27005 (2011).

2.6.2. Six Steps Quantitative Maritime Security Assessment (QMSA)

Yang et al. (2016) proposed a six steps Quantitative Maritime Security Assessment (QMSA), i.e.: “*i) identification of threats and vulnerabilities, ii) subjective security risk estimation, iii) security risk mitigation and protection, iv) security cost and benefit analysis, v) dynamic security-economic evaluation and vi) security inspection and maintenance, provided a general structure to facilitate security risk-based operations of large and complex marine systems.*”.

After the definition of RCMs in the previous step, the security benefits resulting from the reduction of risk, causing the increase of accountability and the reduction of customers’ revenue must be compared with the required costs from security equipment investment, shipping time etc. in order to identify the “optimal” security RCMs. A cost–benefit analysis is required and it is proposed to use the Evidential Reasoning (ER) approach. It is a generic evidence-based Multi-Criteria Decision Analysis (MCDA) approach to deal with uncertainty problems, ignorance and randomness, having both types of criteria: quantitative and qualitative. It is used during decision, evaluation and assessment procedures for the creation of a decision making model, representing an MCDA uncertainty problem, with evidence-based algorithms in order to measure the degree of ignorance (Yang & Xu, 2002; Srivastava, 2010; Xu, 2012; Ruspini et al., 1992).

Although the previously selected RCMs can improve the security levels, the required measures can increase costs and required shipping time. Additionally, possible negative economic effects for supporting rational security policymaking need to be investigated. It is necessary to use System Dynamic (SD) in order to simulate the cost-benefit analysis of security by creating optical causal loops that link the cost of security and the required benefits generated. Thus, the objective of this part is to synthesize the previous steps and present them in a way that could be useful to the decision makers, since it will be useful for a successful prediction of the required security level, while keeping an optimal productivity level of maritime operation (Yang et al. 2016).

2.6.3. Existing tools for Risk Assessment

For **risk assessment**, the main tools that could generally be used are given below. The third of them focuses on events that may occur after a critical incident, while the fourth works in the opposite direction, taking into account all possible scenarios that can lead to a critical event, while the fifth is a combination of the mentioned two diagrams.

1. **Bayesian Network (BN) Influence Diagrams**, which is a probabilistic graphical model where given the symptoms, the probabilities of the presence of various diseases could be estimated (see Figure 16).
2. **Fault Tree analysis (FTA)**, which gives the direct cause and initiating events (see Figure 17).
3. **Event Tree analysis (ETA)**, which gives event trees for consequences (see Figure 18).
4. **Risk Contribution Tree (RCT)**, which is a combination of FTA and ETA, providing a conceptual model of the risk (see Figure 19).

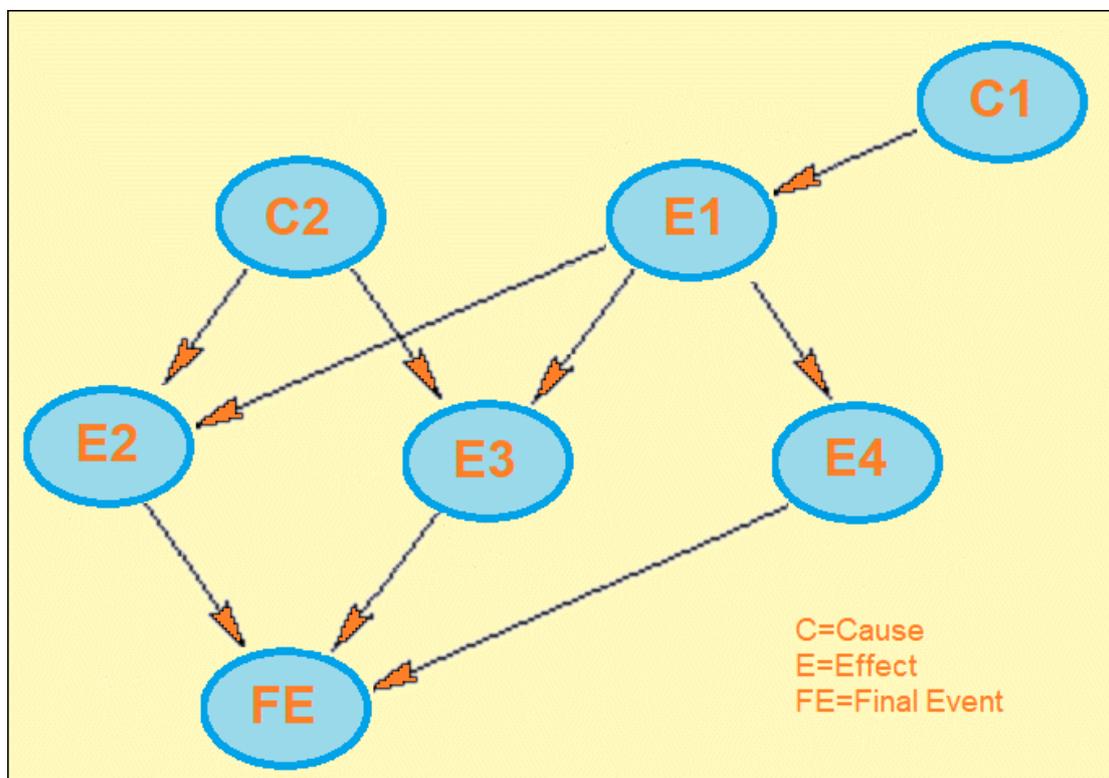


Figure 16. Example of a Bayesian Network influence diagram for risk analysis for piracy.
Source: Created by the author.

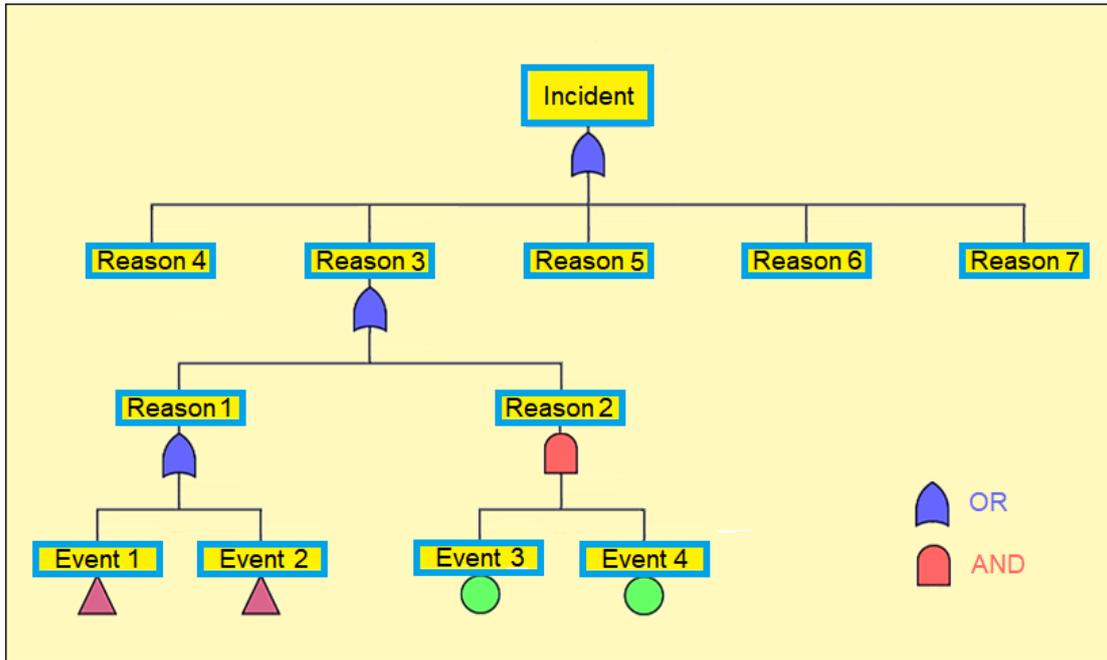


Figure 17. Example of a Fault Tree Analysis.
Source: Created by the author.

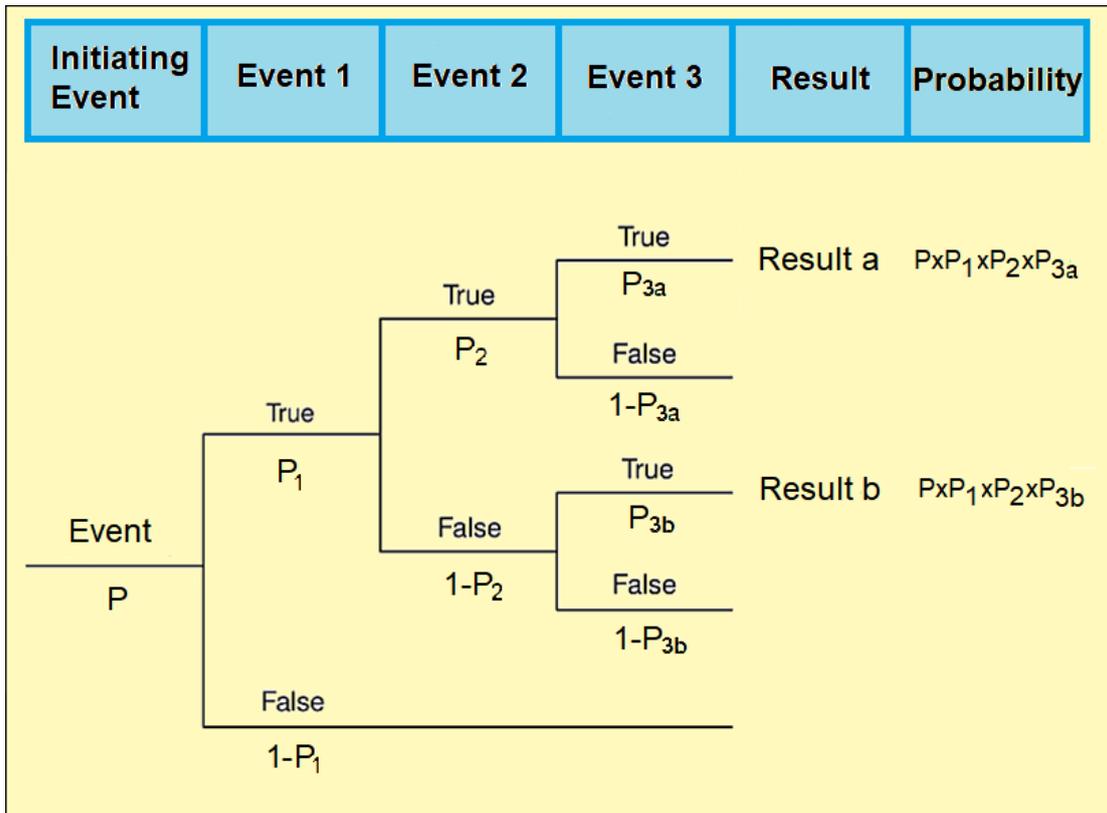


Figure 18. Example of an Event Tree Analysis.
Source: Created by the author.

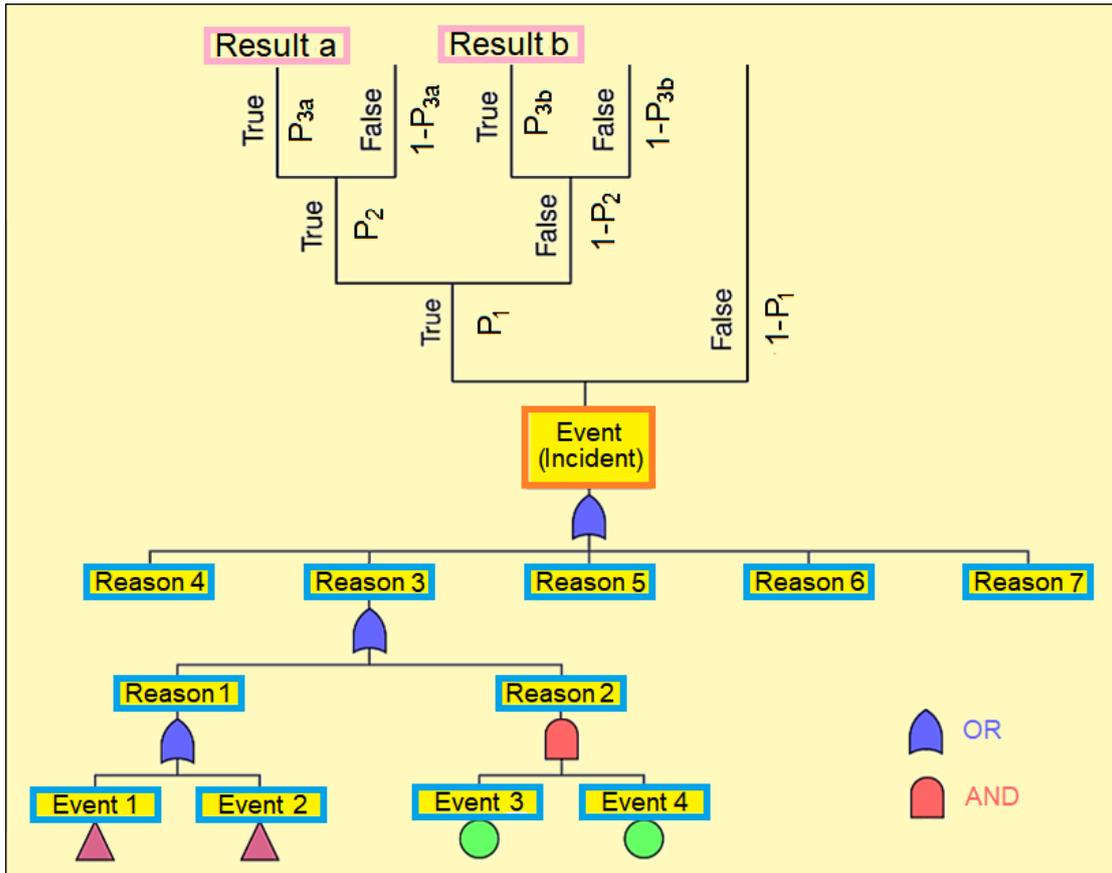


Figure 19. Example of a Risk Contribution Tree.
Source: Created by the author.

The RCA may be presented as a conceptual model of the risk, combining frequency and consequence, as shown in Figure 20, which actually is a vertical presentation of the Bow-Tie model presented in § 2.6.6.

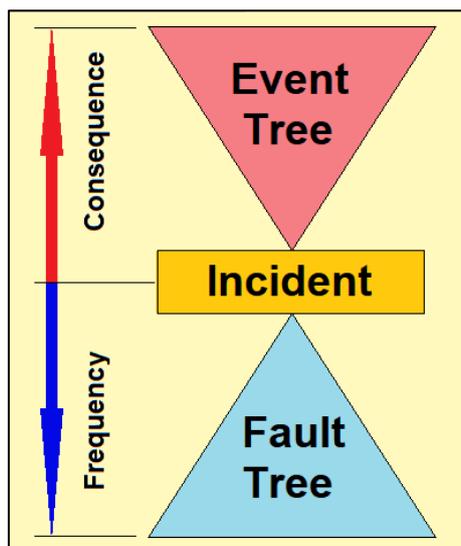


Figure 20. The connection between Fault and Event Trees.
Source: Created by the author.

In this step, the **SWOT security analysis** could be useful, since it is a suitable tool for assessing the strengths and weaknesses of a business or activity, providing information about the opportunities, as well as the threats that arise from it, as is shown in the following Figure 21 & Table 6. Strengths and weaknesses are considered as internal factors, while opportunities and threats, are considered as external factors. That means that businesses or activities can influence strengths and weaknesses but do not have the tools to influence opportunities and threats but only to react to them.

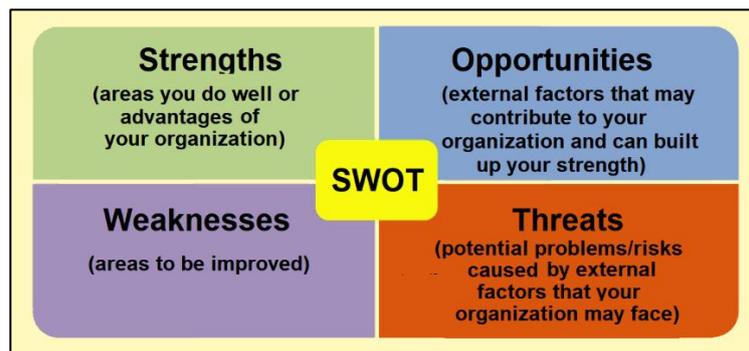


Figure 21. The SWOT Analysis.

Source: Created by the author, based on a typical SWOT Analysis.

Table 6. Definition of Strengths, Weaknesses, Opportunities and Threats in a SWOT Analysis.

Source: Created by the author, based on a typical SWOT Analysis.

Internal	Strengths: attributes, characteristics and factors that give competitive advantage to the business. For example, considerable brand value of the business, cash reserves, first mover advantage and exclusive access to unique resources are major strengths that contribute to competitive advantage of the business.
	Weaknesses: attributes, characteristics and factors that weaken competitiveness of the business in the market place. A history of defective products, presence of huge debts and high employee turnover are examples of major weaknesses that a company may have.
External	Opportunities: favourable situations and factors that can strengthen competitive advantage of the business or provide the business with new sources of competitive advantage. The list of major opportunities for a business may include new product development, finding new customer segment for existing products, opportunities for further cost reductions thanks to creativity and technological innovations and others.
	Threats: unfavourable situations and factors that could create problems for the business compromising its competitive advantage to a certain extent. The most noteworthy threats faced by businesses include, but not limited to the loss of key members of workforce, increase in the prices of raw resources, patent infringement and other lawsuits against the company and others.

2.6.4. Existing methods for Risk Assessment

In relation to the ISPS Code, a procedure for maritime security would be to identify risks and use a scalable risk system to categorize threats.

Hazard identification, categorization, and grading of risk scenarios according to their overall threat capabilities using a rating scale system, are a standard application for maritime security related to the ISPS code.

In all proposed systems (models), risks are identified, assessed, evaluated and prioritized through a combination of probability and impact, affecting usually **people, environment, assets** and **reputation**. According to the definition given by the IMO, risk is the combination of the frequency (likelihood or probability) and severity (consequence). **Frequency** and **Severity indices** are defined on a logarithmic scale in order to facilitate the ranking and validation of ranking. **Risk Index** is established by adding the frequency and severity indices, i.e.:

$$\mathbf{Risk} = \mathbf{Threat} \times \mathbf{Vulnerability} \times \mathbf{Severity} \quad (1)$$

or

$$\mathbf{Risk} = \mathbf{Frequency} \times \mathbf{Severity} \quad (2)$$

or

$$\mathbf{Log (Risk)} = \mathbf{Log (Frequency)} + \mathbf{Log (Severity)} \quad (3)$$

or

$$\mathbf{RI} = \mathbf{FI} + \mathbf{SI} \quad (4)$$

where:

RI = Risk Index = Log (Risk)

FI = Frequency Index = Log (Frequency)

SI = Severity Index = Log (Severity)

Some authors consider that frequency of events is not the same as probability of an accident/incident, due to changes in conditions and due to the fact that the sample of the historical events is not large enough. Thus, they use the term “Probability” instead of the term “Frequency” (Kontovas, Psaraftis, 2009). Some others take into account some limitations of Eq. (1) for Risk Analysis of Terrorist Attacks (Cox, 2008).

A 4×7, 5×5 or 3×3 (high, medium, low) (International Standard, 2007) or any other type of Risk Index Matrix (or Severity/Frequency Matrix) for initial ranking of different scenarios, is constructed. A 5×5 Risk Index Matrix is shown in Figure 22.

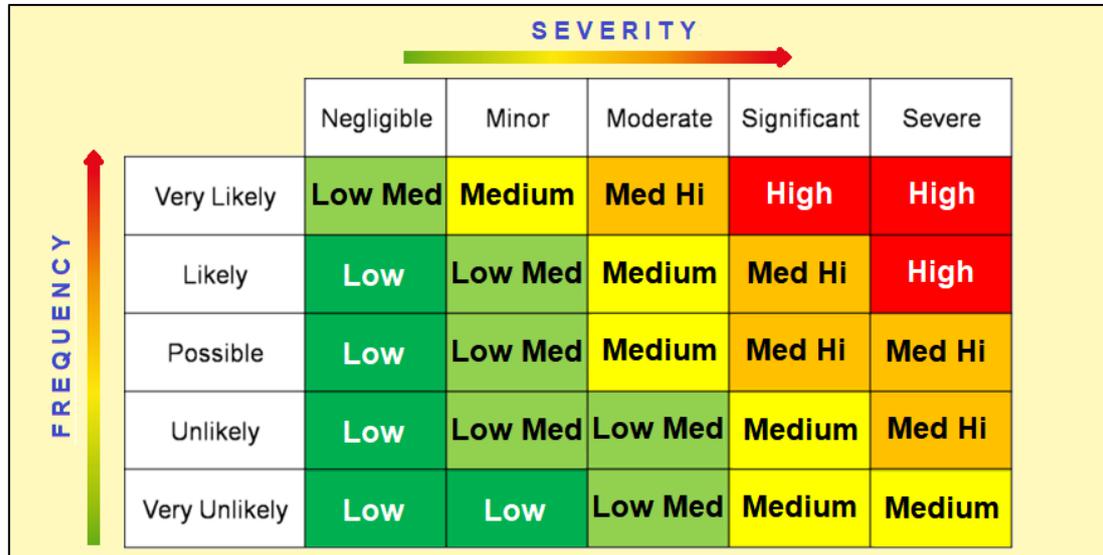


Figure 22. Example of calculated Risk Index Matrix of type 5X5.
Source: Created by the author.

The IMO uses a Failure Mode Effect Analysis (FMEA) and has introduced a 7 x 4 Risk Index Matrix, for initial ranking of accident scenarios in ships, which gives greater potential variation for frequencies than that for consequences. Indices for severity and frequency are written in a logarithmic form (IMO 2018). The next Tables 7 & 8 give examples of logarithmic frequency indices and severity indices respectively scaled for a maritime safety issue. For oil spill specifically, an example of severity indices is shown in Table 9. Taking into consideration Equation 4, an example of a Risk Index matrix (RI) can be constructed, as shown in Table 10, using Equations 5 & 6.

$$FI = \log_{10}(F) + 6 \quad (5)$$

and

$$SI = \log_{10}(S) + 3 \quad (6)$$

Table 7. Frequency Index.
Source: IMO (2018), MSC-MEPC.2/Circ.12/Rev.2.

Frequency Index (FI)			
FI	FREQUENCY	DEFINITION	F (per ship-year)
7	Frequent	Likely to occur once per month on one ship	10
5	Reasonably probable	Likely to occur once per year in a fleet of 10 ships	10 ⁻¹
3	Remote	Likely to occur once per year in a fleet of 1.000 ships	10 ⁻³
1	Extremely remote	Likely to occur once in the lifetime of a world fleet of 5.000 ships	10 ⁻⁵

Table 8. Severity Index.
Source: IMO (2018), MSC-MEPC.2/Circ.12/Rev.2.

Severity Index (SI)				
SI	SEVERITY	EFFECTS ON HUMAN SAFETY	EFFECTS ON SHIP	S (eq. fatalities)
1	Minor	Single or minor injuries	Local equipment damage	0.01
2	Significant	Multiple or severe injuries	Non-severe ship damage	0.1
3	Severe	Single fatality or multiple severe injuries	Severe damage	1
4	Catastrophic	Multiple fatalities	Total loss	10

Table 9. Severity Index for oil spill.
Source: IMO (2018), MSC-MEPC.2/Circ.12/Rev.2.

Severity Index (SI)		
SI	SEVERITY	DEFINITION
1	Category 1	Oil spill size < 1 tonne
2	Category 2	Oil spill size between 1-10 tonnes
3	Category 3	Oil spill size between 10-100 tonnes
4	Category 4	Oil spill size between 100-1.000 tonnes
5	Category 5	Oil spill size between 1.000-10.000 tonnes
6	Category 6	Oil spill size >10.000 tonnes

Table 10. Example of calculated Risk Index.
Source: IMO (2018), MSC-MEPC.2/Circ.12/Rev.2.

Risk Index (RI)						
			SEVERITY INDEX (SI)			
			1	2	3	4
			Minor	Significant	Severe	Catasatrophic
FREQUENCY INDEX (FI)	7	Frequent	8	9	10	11
	6		7	8	9	10
	5	Reasonable probable	6	7	8	9
	4		5	6	7	8
	3	Remote	4	5	6	7
	2		3	4	5	6
	1	Extremely remote	2	3	4	5

To meet the requirements for risk criteria, different types of risk expression are commonly used. However, the “**As Low As Reasonably Practicable**” (ALARP) principle is considered to be the commonly accepted principle, which accepts a maximum level of risk as a limit above which the risk is considered “intolerable”, cannot be justified and should be limited, regardless of economic cost.

There is also a lower limit where, according to the same principle, the level of risk is considered as “broadly accepted”, so the risk is considered negligible and no reduction is required. Between these two extreme limits of this principle, and based on the economically permissible possibility, the risk must be reduced to reasonable levels (see the following Figure 23). It is noted that the proposed risk reduction measures should have a technical basis for their implementation, while, as mentioned above, there should be a balance between the benefits of risk reduction and the financial costs required. This is usually examined during the CBA.

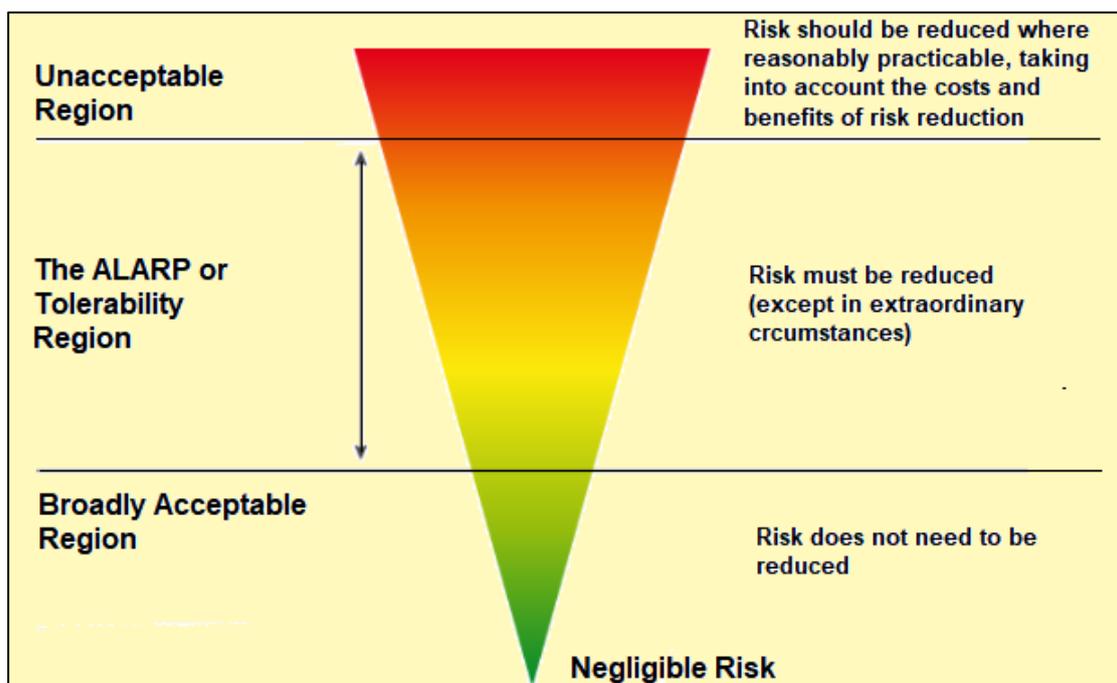


Figure 23. The ALARP principle.
Source: Common carrot diagram, modified graphically and descriptively by the author.

Suitable techniques for the risk modelling could be used in this step. The estimation of the risk related to a hazard identified is the estimation of **Frequency (F)**. For ships it is given by the following Equation 7:

$$F = \frac{\text{No of Casualties}}{\text{Shipyears}} \quad (7)$$

Additionally, consequences are estimated using the **Potential Loss of Life (PLL)**, which is defined according to the following Equation 8:

$$PLL = \frac{\text{No of Fatalities}}{\text{Shipyears}} \quad (8)$$

Individual risk (IR) is defined as the frequency for an individual fatality per year. Usually R is considered as the risk of death and is used for the maximum exposition of individuals. IR is considered as person and location specific (IMO 2018) and is calculated using the following Equation 9.

$$IR = F \times P \times E \quad (9)$$

Where:

F = Frequency

P = Resulting casualty Probability

E = Fractional exposure to that risk

Societal risk (SR) is used for the estimation of risks of accidents that affect many persons. SR denotes the risk to every person, even if the person is exposed briefly to that risk (IMO, 2018). PLL estimation may be used for that reason. Also, societal risk could be measured using the **FN diagram** where the relationship between the number of fatalities and the cumulative frequency of an accident are shown in a multidimensional log-log diagram as shown in Figure 24. Usually, a scheme that evaluates risk in a qualitative way may be more useful than another that uses quantitative methods, unless the latter is highly improved and sophisticated. Thus, “*a qualitative approach may be better than a problematic quantitative one*” (Kontovas, Psaraftis, 2009).

Defining **Risk Control Options (RCO)** and identifying potential **Risk Control Measures (RCM)** is the next important step. This step strongly relies on expert opinion (Kontovas, Psaraftis, 2009). According to the IMO (2018) the purpose of step 3 is: “*to propose effective and practical Risk Control Options comprising the following four principal stages:*

1. *Focusing on risk areas needing control;*
2. *Identifying potential Risk Control Measures;*

3. Evaluating the effectiveness of the RCMs in reducing risk by re-evaluating step 2;
4. Grouping RCMs into practical regulatory options.”

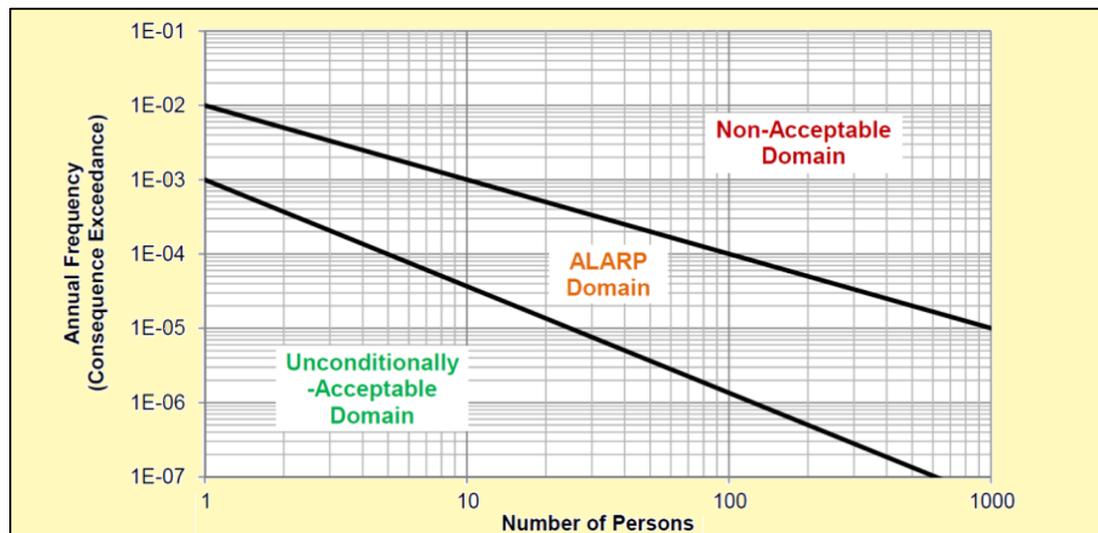


Figure 24. Typical FN diagram.
 Source: Typical FN diagram, modified graphically and descriptively by the author.

The main aspects of the first stage are to review risk levels, taking into account the frequency of occurrence and the severity of outcomes, to review the probability, by identifying the areas of the risk model with the highest probability of occurrence, to review the severity, by identifying the areas of the risk model with the highest severity outcomes and to review the confidence, by identifying areas where the risk model has considerable uncertainty either in risk, severity or probability.

The main aspects of the second stage are to introduce new RCMs for risks that are insufficiently controlled by the applied measures, i.e. to address both the existing risks and the risks resulted either from new technology or from new methods of operation and management. Attributes of RCMs are provided by IMO (2018) in appendix 6 of MSC-MEPC.2/Circ.12 and their assignment helps for a logical procedure to understand how an RCM works, using causal chains of the form:

causal factors → failure → circumstance → accident → consequences

In order to include any potential side effects due to the introduction of the RCM, it is necessary to evaluate of the effectiveness of the RCMs, by re-evaluating the previously mentioned step 2.

The aspect of the final stage is to organize the RCMs into a certain number of Risk Control Options (RCOs). Such grouping is achieved by:

1. A **General Approach** to mitigate the likelihood of incidents occurring. They seem to provide positive results in preventing a number of incidents.
2. A **Distributed Approach** to control the escalation of accidents as well as other subsequent relevant or unrelated incidents.

A qualitative evaluation of RCO interdependencies must be performed before the adoption a group of RCOs without a previous quantitative assessment of their effects. This evaluation is possible to take the form of a matrix similar to that shown in the next Table 11.

Table 11. Example of interdependencies of RCOs.
Source: IMO (2018), MSC-MEPC.2/Circ.12/Rev.2.

Interdependencies of RCOs				
RCO	1	2	3	4
1		Strong	No	Weak
2	Weak		Weak	No
3	No	Weak		No
4	Weak	No	No	

It should be noted that the Risk Control Options are broadly divided into five categories. As shown in the following Table 12 (Kishore, 2013).

Table 12. Categories of Risk Control Options.
Source: Kishore (2013).

Categories of Risk Control Options	
Elimination	If the activity is redesigned or the substance concerned is eliminated so as to remove the hazard, then the redesigned method should not prove less effective or cause unacceptable results from the activity. Then this is a risk control option.
Substitution	If some material or process is substituted with alternative means, which results in a lesser hazards, then this means becomes a risk control option.
Engineering Controls	If employing additional automation or machinery or separating and enclosing dangerous items results in mitigating the hazards, then exercising these options forms an engineering risk control option.
Administrative Controls	If some rules are framed such as avoid smoking, limiting the workers continuous exposure time to the hazard etc. reduce hazards, then these are the administrative risk control options.
Use of PPE	If the hazards associated with the activity are minimised if the personnel involved use appropriate personal protective equipment (PPE), then providing personnel such gear constitute a risk control option. Examples of PPE are Safety Helmet, Cover alls, Visor or Goggles, Gloves, Safety Shoes etc.

The results of the procedure for defining **risk control options**, should be (IMO 2018): “i) a list of RCOs, with their effectiveness in reducing risk, including the method of analysis, ii) a list of interested entities affected by the identified RCOs, iii) a table stating the interdependencies between the identified RCOs and iv) results of analysis of side effects of RCOs”.

2.6.5. The Bow-Tie Method for Security Risk Assessment

The Bow-Tie visual risk assessment method is nowadays applied using the Bow-Tie diagram technique by which both incident prevention barriers and consequence reduction barriers are identified (DNV-GL, 2016, Rheinboldt, 2014). The proposed barriers follow the well-known James Reason’s Swiss Cheese Model of Accident Causation model shown in the following Figure 25 below (Reason, 1990).

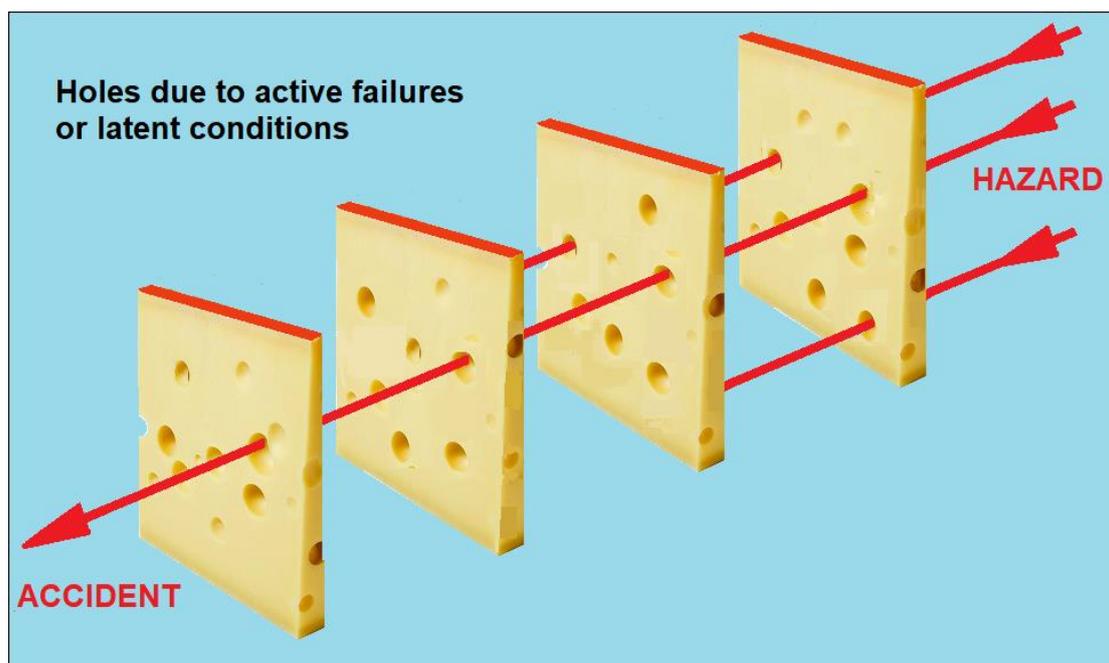


Figure 25. Successive Layers of defence using James Reason's Swiss Cheese Model of Accident Causation.
Source: Created by the author, based on James Reason’s Swiss Cheese Model (Reason, 1990).

The exact origin of the Bow-Tie method is not known, but it is thought to have originated in the late 1970s by ICI. Bow-Tie was used as a business practice by the Royal Dutch / Shell Group. Today, however, the Bow-Tie method has been widely used by countries, companies and industries, such as the French Government, the Australian State Regulator, the New Zealand Land Transport Safety Authority, the Abu Dhabi National Oil Company (ADNOC), the UK Health and Safety Executive,

the International Standards (e.g. ISO 17776: 2000), the International Association of Drilling Contractors (IADC), etc.

Specifically, Bow-Tie software is a risk assessment software that enables the creation of bowties to assess risk. **This software has the ability to represent visually multiple risks in a comprehensible way, while at the same time allowing the preparation of detailed plans for dealing with risks. A Bow-Tie diagram (see Figure 26) provides a visual overview of the risks, while facilitating a clear differentiation between prevention and risk reaction in risk management. In particular, Bow-Tie visually provides an overview of many possible scenarios of events and at the same time the proposed barriers that limit the negative effects of the risk scenarios (Aust & Pons, 2020).**

Bow-Tie software will get us started to identify and manage our risks (DNV-GL, 2016; Aust & Pons, 2020) *“in simple steps:*

- 1. Define the Hazard and the Top Event which is the initial consequence, i.e.: What happens when the danger is released?*
- 2. Identify the Threats which cause the Top Event, i.e.: What causes the release of danger? and How can control be lost?*
- 3. Identify the existing Protection Barriers for each Threat, in order to prevent the Top Event occurrence i.e.: How can controls fail? and How can their effectiveness can be compromised?*
- 4. Identify the consequences of the Top Event, i.e.: What happens after the danger is released?*
- 5. Identify the Recovery Measures for each Consequence, in order to minimise its effects, i.e.: How can we limit the severity of the event? and How can we minimise the effects?*
- 6. For each Barrier, Recovery Measures identify the Critical Safety Tasks.”*

Bow-Tie method has been used widely for many issues of maritime security during the last few years. Figure 26 illustrates a general form of a Bow-Tie diagram.

Bow-Tie risk analysis tools can be used together with ISO 31000 (and 27005 for “Information technology – security techniques – information security risk management”) for qualitative or quantitative analysis (see Figures 14 & 15). Identification of hazard, threats and consequences etc. are supported by a good Bow-

Tie analysis, which provides the risk expert with a better visual illustration of how the risk event can be controlled.

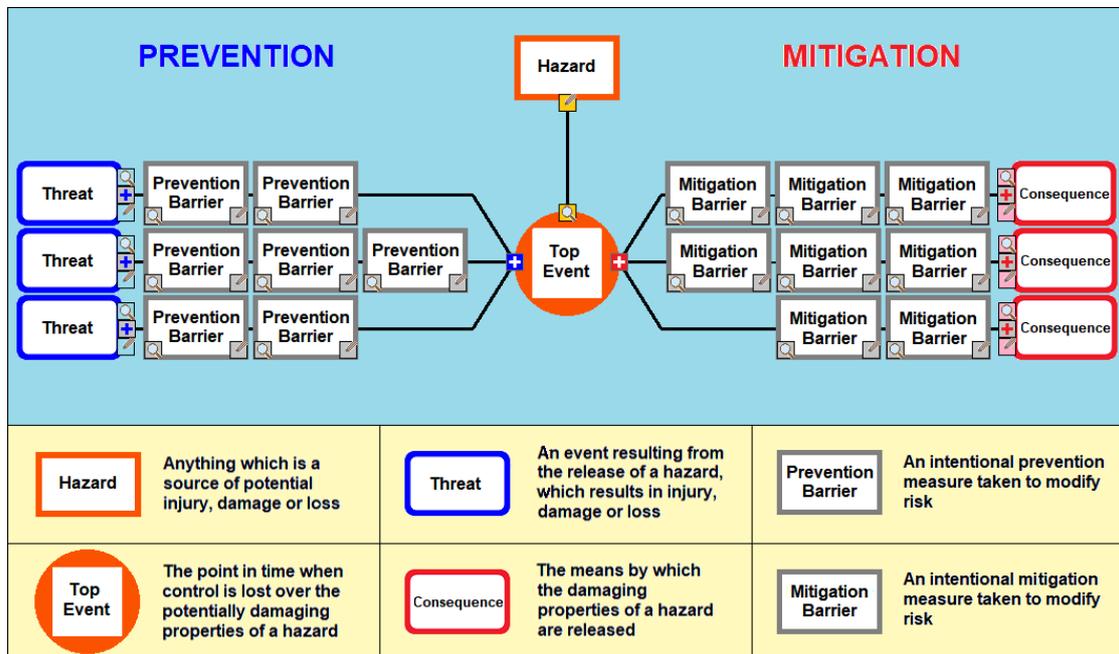


Figure 26. Bow-Tie Diagram.
Source: Created by the author, based on Bow-Tie method (DNV-GL, 2016).

2.7. Conclusions concerning Literature Review

The main objective of maritime security is to minimize losses, injuries, illnesses and economic losses due to intended criminal activities, ensuring the flow of trade and the business continuity.

In the area of maritime safety the regulations, guidelines and methods have a history and culture of systematic research, development and implementation. Particularly, a Formal Safety Assessment (FSA) procedure has been developed by IMO as a structured and systematic methodology by using risk assessment and cost effectiveness analysis, in the context of enhancing maritime safety, including protection of life, health, the marine environment and property.

It seems necessary to develop a similar security risk management process. Some scholars consider that the safety risk assessment and management procedures could also be used as security risk assessment and management procedures. Some others argue that it is possible to assess, evaluate and manage together security and safety

risks, which can be implemented in a common framework that generally covers the social, environmental and economic dimensions. Some of them examine the possibility of combined actions and the allocation of financial resources to address both security and safety in the maritime industry, given their interdependence. It is therefore logical to use similar approaches and practices to address both security and safety issues in the shipping industry.

Thus, the FSA procedure, developed systematically by the IMO as a Risk Assessment Methodology and Cost Effectiveness Analysis (CEA) can therefore be used as a decision making support tool in the assessment of security risks and in the preparation of new regulations for both safety and security at sea as an extension. In this way, a balance could be obtained between the various technical and operational issues used, which would contribute to the protection of human life and health, the reduction of economic losses, the protection of the marine environment and the maintaining of maritime companies reputation.

However, the implementation of security measures have not been introduced in a scientific way and scientific justification, while the issue of cost and benefit assessment has not been estimated systematically and in advance. In addition, the contribution of security measures to reduce risk should be made clearer. Given that both the proposed security measures and their implementation are based on procedures and criteria for assessing the acceptable level of risk (IMO 2018), it is clear that a risk-based approach is needed to assess the effectiveness of security measures.

Actually, there is no extensive and in-depth literature for the risk acceptance criteria concerning maritime security. Basic information is drawn from other areas, such as civil aviation. It is necessary to standardize these criteria, as is the case with the FSA, where practitioners know how to gather information, to make comparisons with previous experience and to make decisions that are often based on experience from the past. However, risk acceptance criteria may be based on political or subjective assessments, while risk identification should be based on objective assessments and be performed prior to the FSA. Their usefulness is especially important for final decision making. Both risk acceptance criteria and decision-making determine the measurable risk assessment, as well as the level of necessary financial cost to reduce the risk.

Given the complexity of the maritime industry and the need for a decision-making tool for use at the different stages of design and operation, a special risk-based assessment tool for security risk assessment, i.e. for risk identification, risk analysis and risk evaluation, which integrates several studies focusing on maritime security risk quantification is proposed for development. **The Bow-Tie method will be used since it has the ability to represent visually multiple risks in a comprehensible way, while at the same time allowing the preparation of detailed plans for dealing with risks. It actually provides an overview of many possible scenarios of events and at the same time the proposed barriers that limit the negative effects of the risk scenarios. The development of the proposed framework as a method of security risk assessment, will be in line with the ISO guide on Risk Management (ISO 31000 and ISO 27005) and IMO's Formal Safety Assessment methodology guidelines.**

Chapter 3. Development of a Risk-Based Method to Address Maritime Risk and Specifically Cyber-Risk

3.1. Introduction

As explained in § 2.7, a special framework as a **method** for security risk assessment, i.e. for risk identification, risk analysis and risk evaluation, which integrates several studies focusing on maritime security risk quantification is proposed for development, in line with the ISO guide on Risk Management (ISO 31000 and ISO 27005) and IMO's Formal Safety Assessment **methodology** guidelines.

The proposed framework is accompanied by the appropriate software, the combination of which will help the user graphically and friendly, to carry out Risk Identification by identifying hazard and top event, adding threats and consequences and adding prevention and mitigation barriers, to carry out Risk Analysis, by estimating top event risk and consequence risk, and to carry out Risk Evaluation by the calculation of the effectiveness of prevention and mitigation barriers.

The Bow-Tie visual **Risk Assessment** method will be applied using the Bow-Tie diagram technique, i.e. a user friendly method for **Risk Identification, Risk Analysis and Risk Evaluation**, which is developed with the end-user in mind, making it one of the most visually helpful risk assessment tools. It also reduces complexity to a manageable size without losing context and focus on the critical elements. **Risk Assessment (i.e. Risk Identification, Analysis and Evaluation) method is based mainly on the definitions and calculations of Risk Values and Threat Indices, leading to the evaluation of all Barriers' Effectiveness, and the resulting Final Risk Values, as it is described by the author in § 3.5, following the steps shown in Figures 27 and 28.**

Security Cost-Benefit Analysis and Decision Making will be added in the future.

3.2. Proposed Framework as a method for Security Risk Assessment

Taking into account that maritime industry is complex and the necessity for a decision-making tool for use at the different stages of design and operation is obvious, a special risk-based assessment tool is proposed, following Yang et al. (2016), ISO 31000 and ISO 27005 and IMO's Formal Safety Assessment guidelines based on

several studies focusing on maritime security risk quantification. This framework will include **Risk Assessment** which is the procedure for risk identification, analysis, and evaluation (Makrodimitris et al., 2016).

Risk Identification typically begins with consideration of what could go wrong. As part of this step, potential threat actors are identified and the significance of the threat they pose is assessed against the potential target, whether it be a ship, port, facility, or region (Edgerton, 2013). Threats and vulnerabilities are identified using a pairwise analysis. Different attack modes, i.e. different threats define the criticality level of the vulnerabilities. For each vulnerability the relevant threats are identified, while the priority of its criticality is considered taking into account these threats (Yang et al., 2013; Yang, et al., 2016). Then, a first approach is made to the required prevention measures. Similarly, all consequences of the main (top) event are identified and a first approach is made to the required mitigation measures.

Risk Analysis is required to answer the three primary questions of security risk: “*i) What can happen? ii) How likely is it to happen? iii) What are the consequences if it does happen?*” Threat and vulnerability together will be considered to determine likelihood, while consequence captures the effects of interest to the appropriate decision-makers (Edgerton, 2013). Thus, after the previous screening process of risk identification, an in-depth prioritization analysis is needed for the vulnerabilities with high criticality (Yang et al., 2009; Yang, et al., 2016). This step helps in decision making as a result of risk analysis, taking into account which risks affecting **people, environment, assets** and **reputation** need treatment and ending with the prioritization of the implementation (DNV-GL, 2016).

Risk Evaluation is used to evaluate the effectiveness of security prevention and mitigation measures. After a security risk pair of threat-vulnerability is identified in the risk identification step, and the required prevention and mitigation measures are proposed, the evaluation step is needed to estimate the effectiveness of the proposed prevention and mitigation measures, in order to complete the risk assessment procedure, from technical point of view.

For our research work the Bow-Tie visual risk assessment method will be applied using the **Bow-Tie diagram** technique by which both incident prevention barriers and consequence reduction barriers are identified (DNV-GL, 2016). Specifically: “*A Bow-Tie diagram visualizes the risk and creates a clear differentiation between the*

proactive and reactive side of risk management. Specifically, the bowtie diagram provides an overview of multiple plausible incident scenarios and shows the barriers controlling these scenarios. Bow-Tie software will get us started to identify and manage our risks in 6 simple steps:

- 1. Add a Hazard*
- 2. Add a Top Event*
- 3. Add Threats*
- 4. Add Consequences*
- 5. Add Prevention Barriers*
- 6. Add Mitigation Barriers”*

A **specially developed software** will be used, that enables the creation of bowties to assess risk in Visual Basic 6 programming language. This software was developed with the help of Dr. Zacharias Dermatis, member of the educational staff of the Department of Management and Technology - University of Peloponnese, in Greece (Schneider, 2020).

Security Cost-Benefit Analysis will be required in the future and it is proposed to use the Evidential Reasoning (ER) approach. It is a generic evidence-based Multi-Criteria Decision Analysis (MCDA) approach to deal with uncertainty problems, ignorance and randomness, having both types of criteria: quantitative and qualitative. It is used during decision, evaluation and assessment procedures for the creation of a decision making model, representing an MCDA uncertainty problem, with evidence-based algorithms in order to measure the degree of ignorance (Yang & Xu, 2002; Srivastava, 2010; Xu, 2012; Ruspini et al., 1992).

A **Decision Making** procedure is also required in the future, since the required measures can increase costs and required shipping time and additionally, possible negative economic effect for supporting rational security policymaking needs to be investigated. The System Dynamic (SD) may be used in order to simulate the cost-benefit analysis of security by creating optical causal loops that link the cost of security and the required benefits generated. It could help the decision makers, since it will be useful for a successful prediction of the required security level, while keeping an optimal productivity level of maritime operation (Yang et al. 2016).

3.3. Contribution to knowledge and novelty of the research

The design of a new tool for security assessment, able to handle the new and more complex demands of maritime security, such as Cyber Security, Ship Security, Port Security effects on maritime security, looks promising to assess and manage security related risks applicable to the maritime industry and to cover the existing gaps in this area. The new scenario-based risk model, and the corresponding mitigation measures will be recorded as a ‘live’ database (Yang et al., 2016). Specifically, the proposed ‘scenario-based’ framework:

- Provides the user with quick results and informations, while requires a limited amount of data from him.
- Provides the possibility of immediate changes in the data provided if the user so wishes.
- Provides the ability to create and maintain a history of changes that the user can refer to.
- The way of calculating the effectiveness of the prevention and mitigation barriers is direct and understandable by the user, thus enabling him to make improvements whenever required.
- Compared with the existing frameworks (mainly for safety risk assessment), it is easier and flexible.

Additionally, the novelty of using the Bow-Tie technique for risk identification, which will contribute to knowledge in the field of security risk assessment (DNV-GL, 2016) “*lies in the fact that:*

- *It is developed with the end-user in mind, making it one of the most visually helpful risk assessment tools.*
- *It reduces complexity to a manageable size without losing context and focus on the critical elements.*
- *Filters allow users to decide which information they want to display on their diagram, without deleting any information.*
- *Allows users to link their management systems to their bowtie diagram by creating activities and document links.*
- *Enables users to maintain the diagram so it will always represent the current status of safety barriers.*
- *It is possible to run reports based on users’ customized template.”*

3.4. Framework's General Description

The **special risk-based assessment tool is proposed for development**, which performs **security risk assessment, through risk identification, risk analysis and risk evaluation**, integrating studies related with the quantification of maritime security risk, is shown descriptively and schematically in Figure 27. As it is shown:

Risk Identification consists of:

1. Hazard identification (Hazard addition in the Bow-Tie diagram).
2. Top Event identification (To Event addition in the Bow-Tie diagram).
3. Threats identification (Threats addition in the Bow-Tie diagram).
4. Consequences identification (Consequences addition in the Bow-Tie diagram).
5. Prevention measures identification (Prevention barriers addition in the Bow-Tie diagram).
6. Mitigation measures identification (Mitigation barriers addition in the Bow-Tie diagram).

Risk analysis consists of:

1. Top Event risk estimation separately for People, Environment, Assets and Reputation (Top Event risk estimation using a 5×5 risk matrix in the Bow-Tie diagram – see Table 13, § 3.4).
2. Consequences risk estimation separately for People, Environment, Assets and Reputation (Consequences risk estimation using a 5×5 risk matrix in the Bow-Tie diagram – see Table 13, § 3.4).

Risk evaluation consists of:

1. Check prevention barriers effectiveness (Prevention barriers effectiveness calculations in the Bow-Tie diagram – see § 3.4).
2. Check mitigation barriers effectiveness (Mitigation barriers effectiveness calculations in the Bow-Tie diagram – see § 3.4).

Also, Figure 28 represents graphically the compatibility of the proposed Risk Assessment procedure using the Bow-Tie method, with ISO 31000 and ISO 27005. This Figure could be compared with Figure 15, illustrating graphically a Risk management programme according to ISO 31000 and ISO 27005.

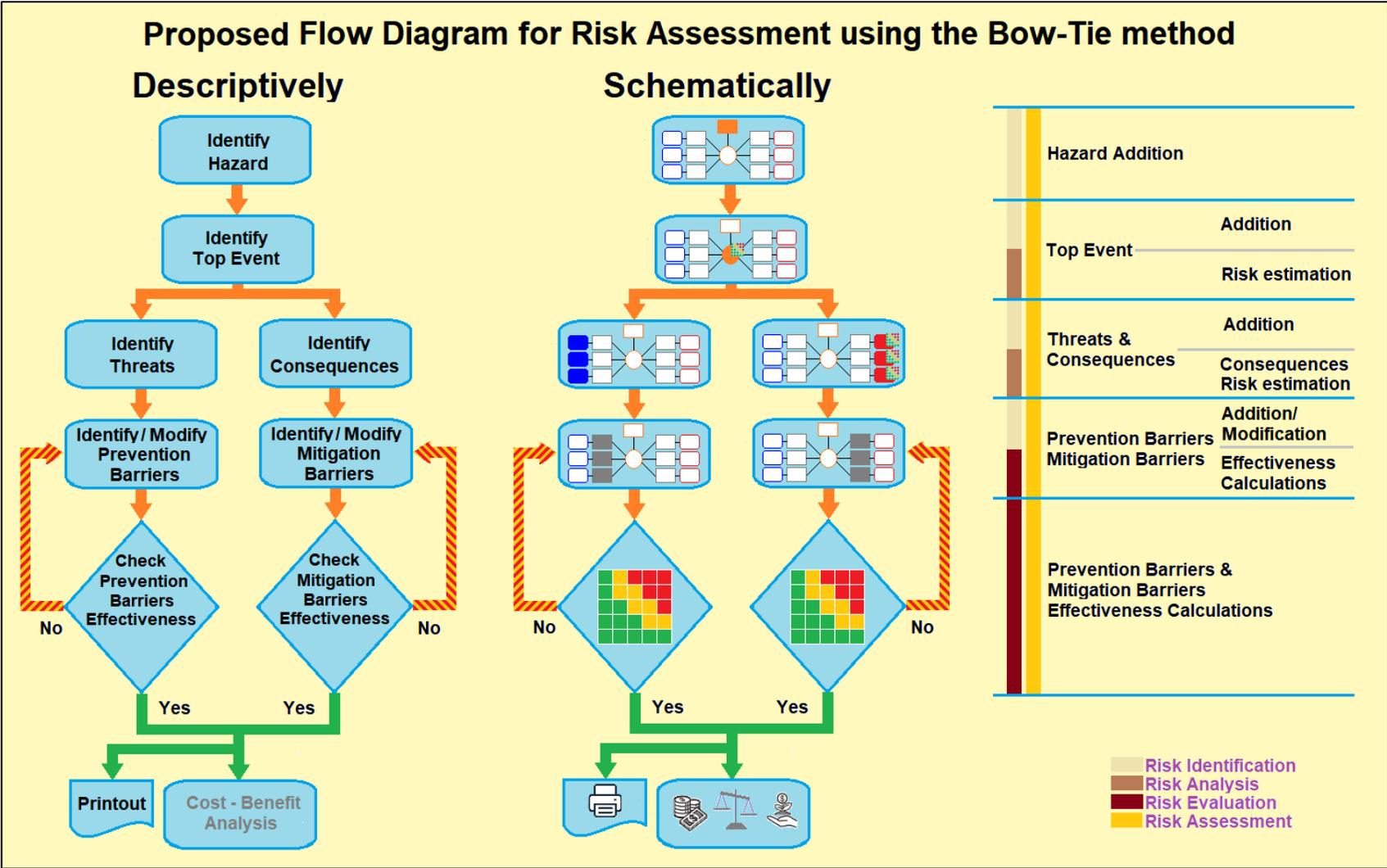


Figure 27. Proposed flow diagram for risk assessment using the Bow-Tie method.

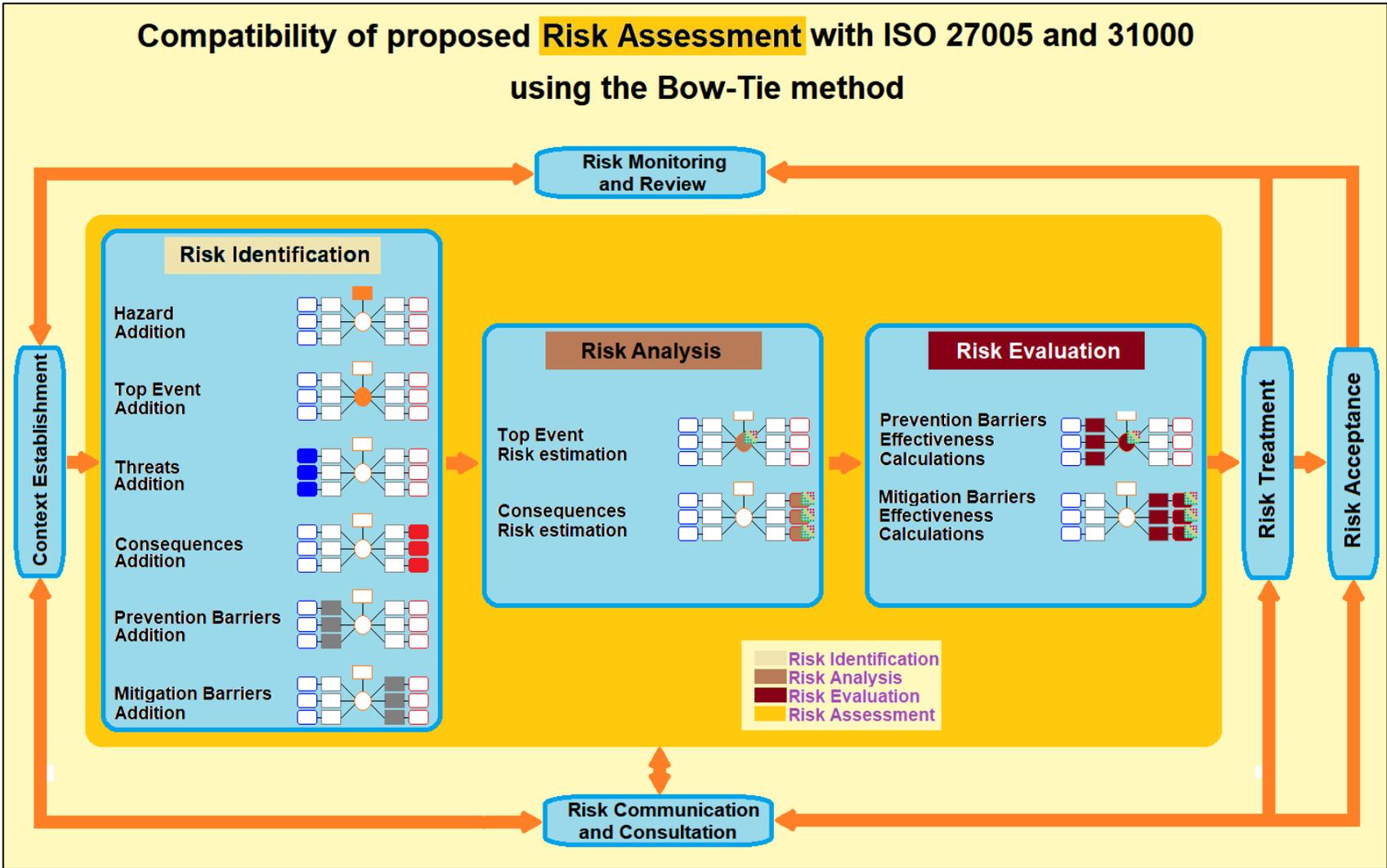


Figure 28. Compatibility of proposed Risk Assessment procedure with ISO 31000 and ISO 27005, using the Bow-Tie method.

3.5. Required Calculations and Used Data

For the purpose of this study, we define the following:

- The **Risk Value (RV)**, which includes information about the Frequency and the Severity of the main unwanted event (Top Event) and all resulting Consequences. For this scope we use a 5×5 risk matrix (see Table 13). Thus, the range of arithmetic values of Risk Value is [1 – 25].
- The **Threat Index (TI_i)** for each Threat (i), which express the partial effect of each Threat (i) on the Top Event, resulting from the Probability and Contribution of each Threat (i) (see Table 14). Arithmetic values of probabilities given by the user are integer numbers within the range [1 – 6], while arithmetic values of contributions given also by the user are integer numbers within the range [1 – 3]. The Threat's Probability values vs the described verbally probability is almost logarithmic (see diagram in Table 14). Obviously, the sum of all Threat Indices expressing the total effect of all Threats on the Top Event is one (1). It is clear that there are no similar indices for the Consequences.
- The **Risk Value Reduction coefficient (R_{redi})** for each Threat (i), which represents the degree of the reduction of the Risk Value, resulting from the Effectiveness (i,j) of all added Prevention Barriers (j) to each Threat (i) (see Table 15). Arithmetic values of Effectiveness given by the user are integer numbers within the range [1 – 6]. The Barrier's Effectiveness values vs the described verbally Effectiveness is assumed as linear (see diagram in Table 15). Similarly, there are separate **Risk Value Reduction coefficients (R_{red})** for each Consequence (i), resulting from the Effectiveness (i,j) of all added Mitigation Barriers (j) to each Consequence (i).

The main purpose of the proposed framework is to reduce the Risk Value RV of the Top Event and the Consequences to acceptable (green) levels, by adding prevention and mitigation barriers in the Bow-Tie Diagram and recalculating the new values of Risk Value RV (i.e. by calculating the Prevention and Mitigation Barriers effectiveness), in the Risk Evaluation procedure, to ensure that these new values for the Top Event and the Consequences are within the acceptable (green area) range. The sequence of the applicable procedure is the following:

Risk Identification procedure includes Hazard, Top Event, Threats, Consequences, Prevention Barriers and Mitigation Barriers additions in the Bow-Tie Diagram. **Risk Analysis** procedure – which is carried out in the same time with Top Event and Consequences additions during Risk Identification procedure – provides the Top Event risk estimation and the Consequences risk estimation, separately for People, Environment, Assets and Reputation, by the **Risk Value *RV*** calculation, combining **Frequency** and **Severity**, as follows:

$$RV = Frequency \times Severity \quad (10)$$

Obviously the selection of the proper Frequency and the proper Severity depends on the user's experience. As shown in the following Table 13, the range of Risk Values is [1 – 25]. The range of the acceptable green area is [1 – 6], the range of the tolerable yellow area is (6 – 15) and the range of the unacceptable red area is [15 – 25].

Table 13. Risk Analysis for Top Event and Consequences, using 5X5 Risk Matrix

Risk Analysis using 5X5 Risk Matrix			
	Frequency	Severity	5X5 Risk Matrix
People	A: Very Unlikely B: Unlikely C: Possible D: Likely E: Very Likely	1: Slight Injury 2: Minor Injury 3: Major Injury 4: Single Death 5: Multiple Deaths	<p>Colours Description</p> <ul style="list-style-type: none"> ■ Low Risk ■ Medium Risk ■ High Risk
Environment	A: Very Unlikely B: Unlikely C: Possible D: Likely E: Very Likely	1: Slight Effect 2: Minor Effect 3: Moderate Effect 4: Major Effect 5: Massive Effect	
Assets	A: Very Unlikely B: Unlikely C: Possible D: Likely E: Very Likely	1: Slight Damage 2: Minor Damage 3: Moderate Damage 4: Major Damage 5: Extensive Damage	
Reputation	A: Very Unlikely B: Unlikely C: Possible D: Likely E: Very Likely	1: Slight Impact 2: Minor Impact 3: Moderate Impact 4: National Impact 5: Global Impact	
Arithmetic values for Frequencies			A: 1, B: 2, C: 3, D: 4, E: 5
Arithmetic values for Severities			1: 1, 2: 2, 3: 3, 4: 4, 5: 5
Risk Value (RV) = Frequency × Severity			Range: [1 – 25]
Green Area: [1 – 6],			Yellow Area: (6 – 15),
			Red Area: [15 – 25]

During the Threats addition, user must define by his experience, the **Probability** P_i and the **Contribution** C_i of each **Threat** (i), using the probability and contribution scaling presented in Table 14. Also, during the Prevention Barriers addition, user must define by his experience, the **Effectiveness** value E_{ij} , of each **Prevention Barrier** (j) for the same defined **Threat** (i), using the effectiveness scaling presented in Table 15. It is clear that risk evaluation is based mainly on the accuracy of the definition of the **Probability** P_i and the **Contribution** C_i of each **Threat** (i) as well as on the accuracy of the definition of the **Effectiveness** value E_{ij} , of each **Prevention Barrier** (j) for the same defined **Threat** (i), set by the user and based on his experience.

Risk Evaluation for the Top Event is the next step, by calculating the Prevention Barriers Effectiveness. For the Top Event Risk Evaluation we define **Threat Index** TI_i as the partial effect of each **Threat** (i) on the Top Event. Thus, the **Threat Index** TI_i for each **Threat** (i), is expressed as:

$$TI_i = \frac{P_i \times C_i}{\sum_{i=1}^n [P_i \times C_i]} \quad (11)$$

i.e.

$$TI = TI_1 + TI_2 + TI_3 + \dots + TI_n = 1 \quad (12)$$

To estimate the Top Event **resulting Risk Value** RV_{final} , for People, Environment, Assets and Reputation, after the introduction of prevention barriers, we use the **Prevention Barrier** (j) **Effectiveness value** E_{ij} , for **Threat** (i) to calculate the **Risk Value Reduction coefficient** R_{redi} of **Threat** (i) as follows:

$$R_{redi} = TI_i \times \left[\sum_{j=1}^{k_i} E_{ij} \right] / k_i \quad (13)$$

where (k_i) is the total **Number of Prevention Barriers** for **Threat** (i).

Then the total Top Event **Risk Value Reduction coefficient** R_{red} is calculated from:

$$R_{red} = \sum_{i=1}^n R_{redi} \quad (14)$$

And the resulting **Final Top Event Risk Value** RV_{final} , for People, Environment, Assets and Reputation, after the introduction of all prevention barriers is:

$$RV_{final} = (1 - R_{red}) RV \quad (15)$$

Table 14. Threat's Probability and Contribution

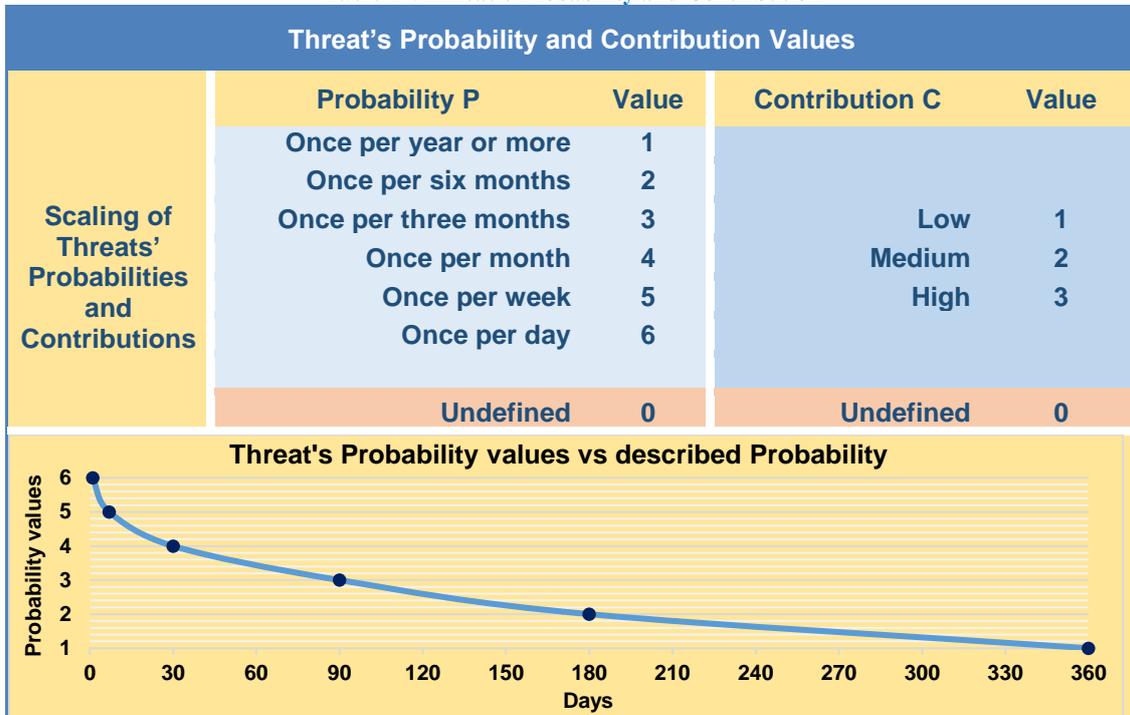
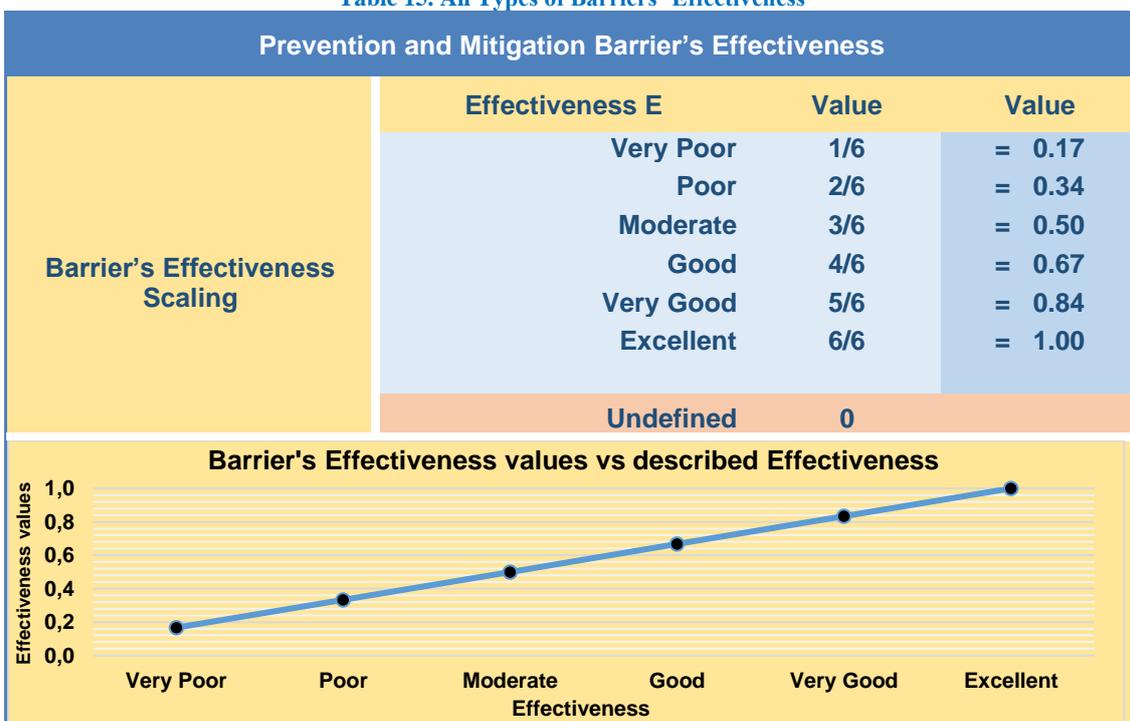


Table 15. All Types of Barriers' Effectiveness



During the Consequences addition, user must define by his experience, the **Concern** N_i of each **Consequence** (i), using the concern scaling presented in Table 16. This value for each **Consequence** (i) will be used for Cost-Benefit Analysis later. Also, during the Mitigation Barriers addition, user must define by his experience, the **Effectiveness** value E_{ij} , of each **Mitigation Barrier** (j) for the same defined **Consequence** (i), using the effectiveness scaling presented in Table 15. It is clear that risk evaluation is based mainly on the accuracy of the definition of the **Effectiveness** value E_{ij} , of each **Mitigation Barrier** (j) for the same defined **Consequence** (i), set by the user and based on his experience.

Table 16. Consequence's Concern.

Consequences Concern Values		
Graduations of Consequences' Concerns	Concern	Value
	Minor	1
	Medium	2
	Major	3
	Undefined	0

Risk Evaluation for each one of the Consequences is the next step by calculating the Mitigation Barriers Effectiveness. To estimate the **resulting Consequence Risk Value** RV_{finali} , for People, Environment, Assets and Reputation, for **Consequence** (i), after the introduction of mitigation barriers, we use the **Mitigation Barrier** (j) **Effectiveness** value E_{ij} , for **Consequence** (i) to calculate the **Risk Value Reduction coefficient** R_{redi} of **Consequence** (i) as follows:

$$R_{redi} \left[\sum_{j=1}^k E_{ij} \right] / k_i \quad (16)$$

where (k_i) is the total **Number of Mitigation Barriers** for **Consequence** (i).

And the resulting **Final Consequence Risk Value** RV_{finali} , for People, Environment, Assets and Reputation, for **Consequence** (i), after the introduction of all mitigation barriers is:

$$RV_{finali} = (1 - R_{redi}) RV_i \quad (17)$$

Obviously, in the case of undefined probabilities and contributions of threats, undefined levels of effectiveness of prevention and mitigation barriers and undefined risk levels of the Top Event and Consequences, risk evaluation could not be carried out and Bow-Tie Diagram remains as an information diagram only.

Since the use of primary data would not provide the ability to check the accuracy of the results of the framework used, secondary data will be used, mainly from similar frameworks, such as the information and details provided by DNV-GL (2016) for similar cases, so that the accuracy of the obtained results can be checked and compared with results obtained for similar cases. DNV-GL (2016) provides hints for the way of identification of threats and consequences and lists with details for what prevention and mitigation barriers may include, specifically for cyber-security resilience management for ships and mobile offshore units in operation.

3.6. Software Description

The following software in Visual Basic language is proposed, using Bow-Tie method and taking into account the impact of a **Top Event** and the **Consequences** on **People, Environment, Assets** and **Reputation** as presented in Appendix 1 (see Fig. 57). This software in Visual Basic was developed with the help of Dr. Zacharias Dermatis, member of the educational staff of the Department of Management and Technology of the University of Peloponnese, following the required steps of the proposed framework (Schneider, 2020). The name of this software is **MarSec** resulting from the first three letters of each one of the words **Maritime Security**.

The programme starts with the appearance of a **Main Menu** for Bow-Tie diagram generation (see Fig. 58a). The same main menu may be used by the user to **Edit** an existing Bow-Tie diagram stored in a file, or the stored auxiliary data files, containing information about previous cases of maritime security (see Fig.58b). Also, the same main menu may be used to **View** an existing Bow-Tie diagram, or the auxiliary data files, containing information about activities, responsibilities and reports (see Fig. 58c). Main menu screen will provide tools to make a Cost-Benefit Analysis as the next step to the currently proposed framework (see Fig. 58d).

When the user starts to develop a Bow-Tie diagram (see Fig. 59), a **Hazard Identification** block and a **Top Event** block appear in the screen. At the same time

the Hazard Identification and Top Event definition form appears (see Fig. 60). Hazard may be defined or selected from a list which includes cases such as: terrorism, cargo theft, extortion, robbery, vandalism, trafficking of people, drugs, stolen goods, weapons or money, stowaways, smuggling, piracy, corruption, embargo violations, customs violations, destroying the marine environment and cyber-attack. The user may also select to define the **Top Event's Risk Value** by clicking the corresponding square for people, environment, assets and reputation. Then a risk matrix form appears, in order to select the frequency and severity of the Top Event for each one of the affected cases, i.e., people, environment, assets, reputation (see Figs. 61, 62, 63, 64). Some authors (Bernsmed et al, 2018), prefer to assess the risk of top event through the assessment of the Threat Actors, Window of Opportunity, Vulnerabilities and Security Countermeasures in the left side of the Bow-Tie diagram. Such assessment does not provide the frequency and severity of the top event for each one of the previously mentioned affected cases, i.e. people, environment, assets, reputation.

After Hazard and Top Event identification is completed, the user may add **Threats** and **Prevention Barriers**. Each time the plus (+) sign in the threat side of the Top Event block of the Bow-Tie diagram screen is clicked, a new threat block appears and the threat identification and description form appears too, where the user will add a new Threat and its description. The user may also select to define **Probability** of Threat, as is shown in the following Table 13, by marking the corresponding circle. User must also define the **Contribution** of Threat, as it is shown in the following Table 13, by marking the corresponding square (see Fig. 65).

Each time the plus (+) sign in the right side of the threat block of the Bow-Tie diagram screen is clicked, a new **Prevention Barrier** block appears in the Bow-Tie diagram form and the prevention barrier identification and description form appears too, where the user will identify a new prevention barrier and its description (see Fig. 66). The user may also select to define **Effectiveness** of the Prevention Barrier, as is shown in the following Table 14, by marking the corresponding circle (see also Fig. 66) and to select the proper **Activities** and **Responsibilities** from a given list or to define new activities and responsibilities for the certain Prevention Barrier (see Fig. 69 and Fig. 70).

When all Threats' identifications have been completed, the user may introduce **Consequences** and **Mitigation Barriers**. Each time the plus (+) sign in the consequence side of the Top Event block of the Bow-Tie diagram screen is clicked, a new consequence block appears and the consequence identification and description form appears too, where the user will identify a new Consequence and its description. The user may also select to define the **Consequence's Risk Value** by clicking the corresponding square for people, environment, assets and reputation. Then a risk matrix form appears, in order to select the frequency and severity of the consequence for each one of the affected cases, i.e., people, environment, assets, reputation (see Figs. 61, 62, 63, 64). User must also define the **Concern** of Consequence, as it is shown in the following Table 16, by marking the corresponding square (see Fig. 67), which will be used for Cost-Benefit Analysis as the next step to the currently proposed framework.

Each time the plus (+) sign in the left side of the consequence block of the Bow-Tie diagram screen is clicked, a new **Mitigation Barrier** block appears in the Bow-Tie diagram form and the mitigation barrier identification and description form appears too, where the user will identify a new mitigation barrier and its description (see Fig. 68). The user may also select to define **Effectiveness** of the Mitigation Barrier, as is shown in the following Table 14, by marking the corresponding circle (see also Fig. 68) and to select the proper **Activities** and **Responsibilities** from a given list or to define new activities and responsibilities for the certain barrier (see Fig. 69 and Fig. 70).

A complete **Help Menu** is included in this software (see Fig. 71), containing information about the framework.

3.7. Software printouts

As it is presented in Appendix 2, the programme MarSec outputs are the following:

1. A complete Bow-Tie diagram schematically, defining Threats, Consequences, Prevention Barriers and Mitigation Barriers, having the form shown in Fig. 43 (Appendix 1).
2. A Main Printout providing general information about Threats and Consequences, having the form shown in Table 19 (Appendix 2).

3. A Printout of Activities and Responsibilities, as a result of the defined Prevention and Mitigation Barriers, having the form shown in Table 20 (Appendix 2).

The programme may be completed in the future by adding routines to accomplish:

1. A Cost-Benefit Analysis.
2. Decision Making.
3. Training Programme.

It is important to mention that the printouts can be modified according to the desire of the user.

3.8. Conclusion

The proposed framework as a method of visual Risk Assessment is in line with the ISO guide on Risk Management (ISO 31000 and ISO 27005) and IMO's Formal Safety Assessment guidelines and it is accompanied by the appropriate software, the combination of which will help the user graphically and friendly, to carry out Risk Assessment.

The Bow-Tie visual Risk Assessment method will be applied using the Bow-Tie diagram technique, i.e. a user friendly method for Risk Identification, Risk Analysis and Risk Evaluation. Using the Bow-Tie visual Risk Assessment method, the user may identify Top Event, Threats and Consequences. User may also define the Risk Value of the Top Event and of each one of the Consequences, and may also define the probability and contribution of each Threat.

The main purpose of the proposed framework is to reduce the Risk Value of the Top Event and the Consequences to acceptable (green) levels, by adding Prevention and Mitigation Barriers in the Bow-Tie Diagram and recalculating the new values of Risk Value (i.e. by calculating the Prevention and Mitigation Barriers effectiveness), in the Risk Evaluation procedure, to ensure that these new values for the Top Event and the Consequences are within the acceptable (green area) range.

Chapter 4. Applied Examples, Results and Discussion – How this Method is Used in Practise

4.1. Introduction

Two specific applications for the use of the framework to perform Risk Assessment, for cyber security in ports, ships, rigs and offshore units, are presented in this chapter. The first is related to malware attacks (malware related incidents as the Top Event). The second is related to unauthorized external users getting online access (unauthorized external user as the Top Event). Some ideas for cyber security cases were also taken from DNV-GL (2016).

The author received important information about cyber security applications, both from Dr. Christos Kontovas of Liverpool John Moores University, as well as from Prof. Stratos Papadimitriou of the Department of Maritime Studies - University of Piraeus, especially for details concerning the required prevention and mitigation measures and the required activities and responsibilities during the application of prevention and mitigation measures.

4.2. A first application of cyber security – Malware related incident

This application is related to malware attacks and thus, malware related incidents are the Top Event of our example. Threats are related to the way that the malware can get into the system. Normally, there are mainly three ways: i) through the network (worms), ii) through removable storage media and iii) through ways based on user's behaviour. In this example, the barriers to prevent a worm are network segregation and antivirus software. Blocking USB ports and the use of antivirus software are barriers to prevent malware through removable storage media, but also awareness training is considered as a prevention barrier too. Lastly, e-mail washing and proper antivirus software are the proper barriers to avoid malware.

The consequence of these malware related incidents is the system malfunction or stop. To avoid this consequence, a system disconnection procedure is required, as well as a backup and restore system and an antivirus alarm as mitigation barriers.

The complete Bow-Tie diagram for this application is shown in the following Figure 29, as generated by the previously described software MarSec.

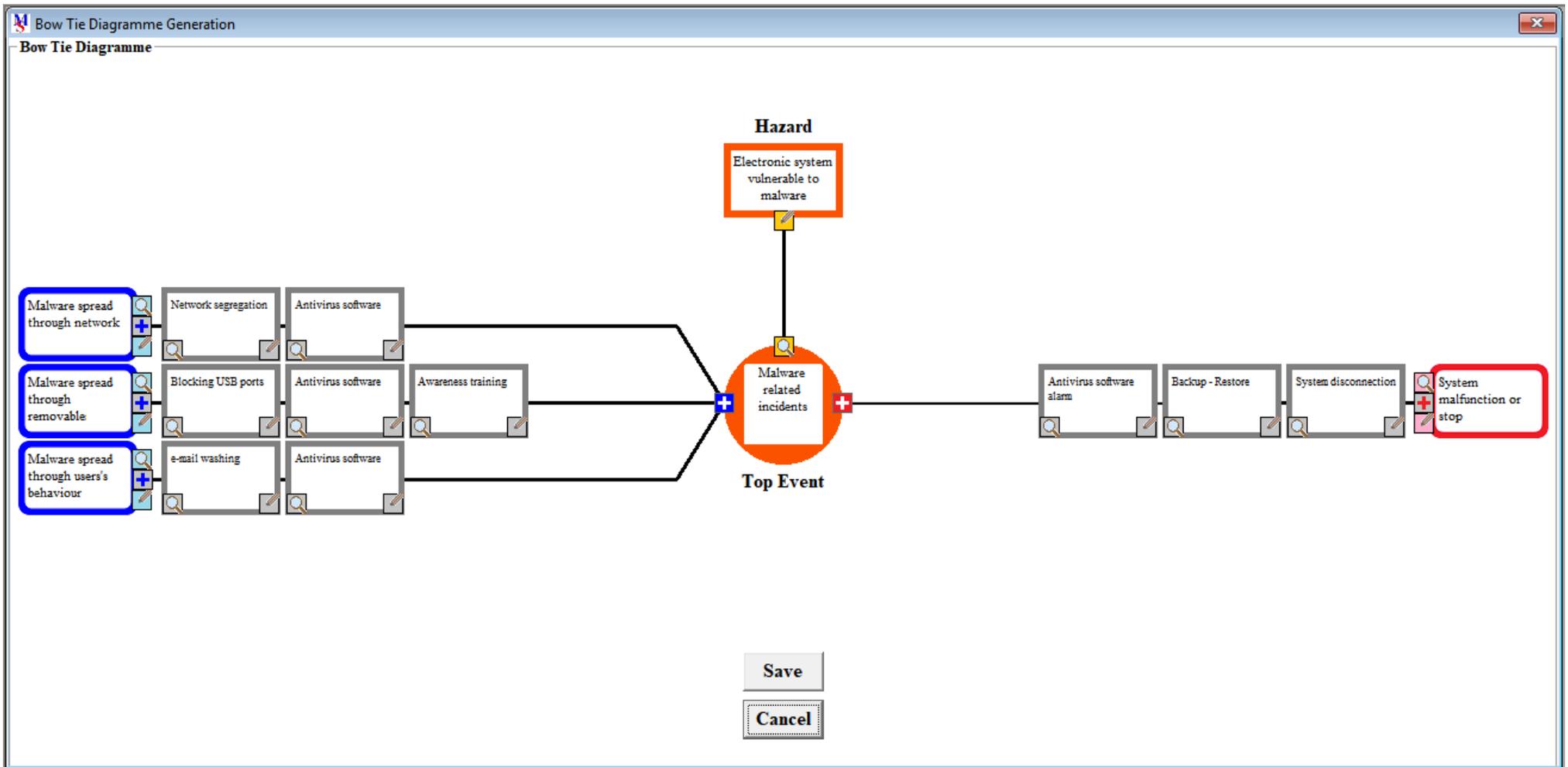


Figure 29. Bow-Tie diagram for electronic systems vulnerable to malware.

Hazard and Top Event are defined using the form of Figure 30.

Figure 30. Hazard identification and Top Event Form before the introduction of Threat Barriers.

For the Top Event, the **Frequency** and **Severity** of each one of People Environment, Assets and Reputation is selected from the corresponding Risk Matrix form, as shown in Figure 31 (see also Table 13), by clicking the proper square in the Risk Matrix.

Risk Matrix for People

Frequency	Severity	Matrix
A: Very Unlikely	1: Slight Injury	5: [Yellow, Yellow, Red, Red, Red]
B: Unlikely	2: Minor Injury	4: [Green, Yellow, Yellow, Red, Red]
C: Possible	3: Major Injury	3: [Green, Green, Yellow, Red, Red]
D: Likely	4: Single Death	2: [Green, Green, Green, Yellow, Yellow]
E: Very Likely	5: Multiple Deaths	1: [Green, Green, Green, Green, Green]

Risk Matrix for Environment

Frequency	Severity	Matrix
A: Very Unlikely	1: Slight Effect	5: [Yellow, Yellow, Red, Red, Red]
B: Unlikely	2: Minor Effect	4: [Green, Yellow, Yellow, Red, Red]
C: Possible	3: Moderate Effect	3: [Green, Green, Yellow, Red, Red]
D: Likely	4: Major Effect	2: [Green, Green, Green, Yellow, Yellow]
E: Very Likely	5: Massive Effect	1: [Green, Green, Green, Green, Green]

Risk Matrix for Assets

Frequency	Severity	Matrix
A: Very Unlikely	1: Slight Damage	5: [Yellow, Yellow, Red, Red, Red]
B: Unlikely	2: Minor Damage	4: [Green, Yellow, Yellow, Red, Red]
C: Possible	3: Moderate Damage	3: [Green, Green, Yellow, Red, Red]
D: Likely	4: Major Damage	2: [Green, Green, Green, Yellow, Yellow]
E: Very Likely	5: Extensive Damage	1: [Green, Green, Green, Green, Green]

Risk Matrix for Reputation

Frequency	Severity	Matrix
A: Very Unlikely	1: Slight Impact	5: [Yellow, Yellow, Red, Red, Red]
B: Unlikely	2: Limited Impact	4: [Green, Yellow, Yellow, Red, Red]
C: Possible	3: Moderate Impact	3: [Green, Green, Yellow, Red, Red]
D: Likely	4: National Impact	2: [Green, Green, Green, Yellow, Yellow]
E: Very Likely	5: International Impact	1: [Green, Green, Green, Green, Green]

Figure 31. Risk Matrices Forms for the selection of Frequency and Severity for each one of People, Environment, Assets and Reputation,

The proper colour and place appears in the lower part of the Hazard identification and Top Event Form of Figure 30. The **Risk Value** for each one of People, Environment, Assets and Reputation is calculated using Equation 10:

$$RV = Frequency \times Severity$$

	<i>Frequency</i>	<i>Severity</i>	<i>Risk Value RV</i>
People	1	1	1
Environment	1	1	1
Assets	4	4	16
Reputation	4	3	12

i.e.:

$$RV_P = A1 = 1 \times 1 = 1$$

$$RV_E = A1 = 1 \times 1 = 1$$

$$RV_A = D4 = 4 \times 4 = 16$$

$$RV_R = D3 = 4 \times 3 = 12$$

Three threats are then defined, using the forms of Figures 32, 33 and 34. From the described three threats (**n = 3**) and their **Probabilities** P_i and **Contributions** C_i (see Figures 32, 33 and 34 – see also Table 14), the **Threat Index** TI_i values for each of Threat (i) of the three defined threats, are calculated using Equation 11:

$$TI_i = \frac{P_i \times C_i}{\sum_{i=1}^n [P_i \times C_i]}$$

<i>Threat i</i>	<i>Probability P_i</i>	<i>Contribution C_i</i>	<i>Threat Index TI_i</i>
1	1	3	0.25
2	1	3	0.25
3	2	3	0.50

Threat Identification

Threat Malware spread through network

Description

Frerquency

- Once per year or less
- Once per 6 months
- Once per 3 months
- Once per month
- Once per week
- Once per day
- Undefined

Contribution

- Low
- Medium
- High
- Undefined

Cancel

Figure 32. 1st Threat identification.

Threat Identification

Threat Malware spread through removable storage

Description

Frerquency

- Once per year or less
- Once per 6 months
- Once per 3 months
- Once per month
- Once per week
- Once per day
- Undefined

Contribution

- Low
- Medium
- High
- Undefined

Cancel

Figure 33. 2nd Threat identification.

Threat Identification

Threat Malware spread through users's behaviour

Description

Frerquency

- Once per year or less
- Once per 6 months
- Once per 3 months
- Once per month
- Once per week
- Once per day
- Undefined

Contribution

- Low
- Medium
- High
- Undefined

Cancel

Figure 34. 3rd Threat identification.

i.e.:

$$TI_1 = (1 \times 3) / 12 = 0.25$$

$$TI_2 = (1 \times 3) / 12 = 0.25$$

$$TI_3 = (2 \times 3) / 12 = 0.50$$

and:

$$TI = TI_1 + TI_2 + TI_3 = 0.25 + 0.25 + 0.50 = 1$$

The prevention barriers for each threat are then defined, using the forms of Figures 35a, 35b, 36a, 36b, 36c, 37a and 37b. From the values of the **Effectiveness** E_{ij} of each Barrier (j) for each Threat (i) (see Figures 35a, 35b, 36a, 36b, 36c, 37a and 37b – see also Table 15), the **Risk Value Reduction coefficient** R_{redi} of each Threat (i) are calculated using Equation 13:

$$R_{redi} = TI_i \times \left[\sum_{j=1}^{k_i} E_{ij} \right] / k_i$$

<i>Threat i</i>	<i>Barrier j</i>	<i>Threat Index TI_i</i>	<i>Effectiveness E_{ij}</i>	<i>Number of Barriers k_i</i>	<i>Reduction Coeff. R_{redi}</i>
1	1	0.25	0.84	2	0.2100
	2		0.84		
2	1	0.25	0.67	3	0.1817
	2		0.84		
	3		0.67		
3	1	0.50	0.84	2	0.4200
	2		0.84		

i.e.:

$$R_{red1} = 0.25 \times (0.84 + 0.84) / 2 = 0.25 \times 0.8400 = 0.2100$$

$$R_{red2} = 0.25 \times (0.67 + 0.84 + 0.67) / 3 = 0.25 \times 0.7267 = 0.1817$$

$$R_{red3} = 0.50 \times (0.84 + 0.84) / 2 = 0.50 \times 0.84 = 0.4200$$

Then, the total Top Event **Risk Value Reduction coefficient** R_{red} is calculated using Equation 14:

Prevention Barrier Identification

Prevention Barrier: Network segregation

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Operations for network segregation
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 35a. 1st Barrier for 1st Threat.

Prevention Barrier Identification

Prevention Barrier: Antivirus software

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Application of antivirus software
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 35b. 2nd Barrier for 1st Threat.

Prevention Barrier Identification [X]

Prevention Barrier: Blocking USB ports

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Activities for blocking USB ports
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 36a. 1st Barrier for 2nd Threat.

Prevention Barrier Identification [X]

Prevention Barrier: Antivirus software

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Application of antivirus software
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 36b. 2nd Barrier for 2nd Threat.

Prevention Barrier Identification

Prevention Barrier: Awareness training

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Training in computer systems awareness
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 36c. 3rd Barrier for 2nd Threat.

Prevention Barrier Identification

Prevention Barrier: e-mail washing

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Operations to clean-up e-mails files
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 37a. 1st Barrier for 3rd Threat.

The screenshot shows a software dialog box titled "Prevention Barrier Identification". It has a close button (X) in the top right corner. The "Prevention Barrier" text box contains "Antivirus software". Below it is an empty "Description" text box with scroll arrows. The "Effectiveness" section has radio buttons for "Very Poor", "Poor", "Moderate", "Good", "Very Good" (which is selected), "Excellent", and "Undefined". The "Activities and Responsibilities" section has a dropdown menu showing "ACTIVITY: Application of antivirus software" and "RESPONSIBILITY: Computer Engineering Manager". A "Cancel" button is located at the bottom right.

Figure 37b. 2nd Barrier for 3rd Threat.

$$R_{red} = \sum_{i=1}^n R_{redi}$$

i.e.:

$$R_{red} = 0.2100 + 0.1817 + 0.4200 = 0.8117$$

Then the resulting **Final Top Event Risk Value** RV_{final} , for People, Environment, Assets and Reputation is calculated using Equation 15:

$$RV_{final} = (1 - R_{red}) RV$$

i.e.:

$$RV_{finalP} = (1 - 0.8117) \times 1 = 0.1883 \text{ (Green Area)}$$

$$RV_{finalE} = (1 - 0.8117) \times 1 = 0.1883 \text{ (Green Area)}$$

$$RV_{finalA} = (1 - 0.8117) \times 16 = 3.0128 \text{ (Green Area)}$$

$$RV_{finalR} = (1 - 0.8117) \times 12 = 2.2596 \text{ (Green Area)}$$

The resulting Hazard Identification and Top Event form, after the introduction of the Threats Barriers, takes the form of Figure 38, with all Final Top Event Risk Values colours in green.

Hazard Identification and Top Event

Define Hazard Electronic systems vulnerable to cyber security incidents

Define Top Event Malware related incidents

Description

Risk Value	Start	Final
People	A1	█
Environment	A1	█
Assets	D4	█
Reputation	D3	█

Cancel

Figure 38. Hazard identification and Top Event after the introduction of all Threat Barriers.

Similarly, the single consequence is defined using the form of Figure 39.

Consequence Identification

Consequence System malfunction or stop

Description

Risk Value	Start	Final	Concern
People	A1	█	Minor <input type="checkbox"/>
Environment	A1	█	Medium <input type="checkbox"/>
Assets	D4	█	Major <input checked="" type="checkbox"/>
Reputation	D3	█	Undefined <input type="checkbox"/>

Cancel

Figure 39. 1st Consequence identification before the introduction of Consequence Barriers.

For the single Consequence, the **Frequency** and **Severity** of each one of People Environment, Assets and Reputation is selected from the corresponding Risk Matrix form, as shown in Figure 31 (see also Table 13), by clicking the proper square in the Risk Matrix. Also a Concern level is selected (see Table 16) for the single Consequence.

The proper colour appears in the lower part of the single Consequence identification of Figure 39. The **Risk Value** for each one of People, Environment, Assets and Reputation is calculated using Equation 10:

$$RV = Frequency \times Severity$$

	<i>Frequency</i>	<i>Severity</i>	<i>Risk Value RV</i>
People	1	1	1
Environment	1	1	1
Assets	4	4	16
Reputation	4	3	12

i.e.:

$$RV_P = A1 = 1 \times 1 = 1$$

$$RV_E = A1 = 1 \times 1 = 1$$

$$RV_A = D4 = 4 \times 4 = 16$$

$$RV_R = D3 = 4 \times 3 = 12$$

The mitigation barriers for the single consequence are then defined, using the forms of Figures 40a, 40b, 40c. From the values of the **Effectiveness** E_{ij} of each Barrier (j) for the single Consequence (see Figures 40a, 40b, 40c – see also Table 15), the **Risk Value Reduction coefficient** R_{redi} of the single Consequence are calculated using Equation 16:

$$R_{redi} \left[\sum_{j=1}^k E_{ij} \right] / k_i$$

<i>Conseq. i</i>	<i>Barrier j</i>	<i>Effectiveness E_{ij}</i>	<i>Number of Barriers k_i</i>	<i>Reduction Coeff. R_{redi}</i>
1	1	0.84	3	0.6700
	2	0.67		
	3	0.50		

Mitigating Barrier Identification [X]

Mitigating Barrier: System disconnection

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Operations to disconnect the system
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 40a. 1st Barrier for 1st Consequence.

Mitigating Barrier Identification [X]

Mitigating Barrier: Backup - Restore

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Operations for backup and restore
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 40b. 2nd Barrier for 1st Consequence.

Figure 40c. 3rd Barrier for 1st Consequence.

i.e.:

$$R_{red1} = (0.84 + 0.67 + 0.50) / 3 = 0.6700$$

Then the resulting **Final Consequence Risk Value** RV_{final} , for people, environment, assets and reputation, is calculated using Equation 17:

$$RV_{finali} = (1 - R_{redi}) RV_i$$

i.e.:

$$RV_{finalP} = (1 - 0.6700) \times 1 = 0.3400 \text{ (Green Area)}$$

$$RV_{finalE} = (1 - 0.6700) \times 1 = 0.3400 \text{ (Green Area)}$$

$$RV_{finalA} = (1 - 0.6700) \times 16 = 5.4400 \text{ (Green Area)}$$

$$RV_{finalR} = (1 - 0.6700) \times 12 = 4.0800 \text{ (Green Area)}$$

The resulting Consequence form, after the introduction of the Consequence Barriers, takes the form of Figure 39, with all Final Risk Values colours in green.

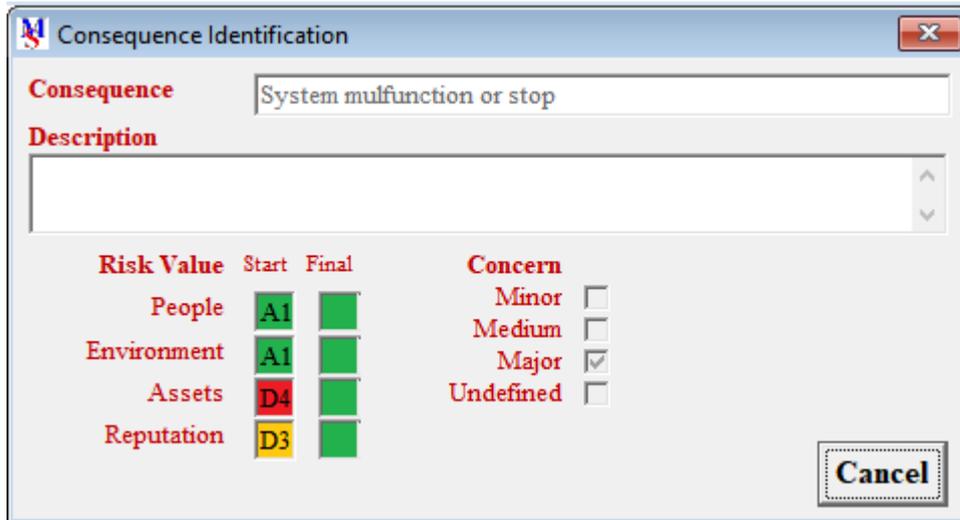


Figure 41. 1st Consequence identification after the introduction of Consequence Barriers.

Finally, the resulting printouts are presented in the following Table 17 (Main Printout about Threats and Consequences) and Table 18 (Printout of Activities and Responsibilities resulting from Prevention & Mitigation Barriers).

Table 17. Main Printout about Threats and Consequences.

Main Printout about Threats and Consequences		
Hazard: Electronic systems vulnerable to cyber security incidents		
Top Event: Malware related incidents		
Risk Values		
People ■	Environment ■	Assets ■
		Reputation ■
Threats		
Description	Frequency	Contribution
1. Malware spread through network	Once per year or less	High
2. Malware spread through removable storage	Once per year or less	High
3. Malware spread through users' s behaviour	Once per 6 months	High
Consequences		
Description	Risk Value for	Concern
1. System malfunction or stop	P ■ E ■ A ■ R ■	Major

Table 18. Printout of Activities and Responsibilities resulting from Prevention & Mitigation Barriers.

Printout of Activities and Responsibilities for Prevention and Mitigation Barriers			
Hazard: Electronic systems vulnerable to cyber security incidents			
Top Event: Malware related incidents			
Risk Values			
People 	Environment 	Assets 	Reputation 
1st Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. Network segregation	Very good	Operations for network segregation	Computer Engineering Manager
2. Antivirus software	Very good	Application of antivirus software	Computer Engineering Manager
2nd Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. Blocking USB ports	Good	Activities for blocking USB ports	Computer Engineering Manager
2. Antivirus software	Very good	Application of antivirus software	Computer Engineering Manager
3. Awareness training	Good	Training in computer awareness	Computer Engineering Manager
3rd Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. e-mail washing	Very good	Operations to clean-up e-mail files	Computer Engineering Manager
2. Antivirus software	Very good	Application of antivirus software	Computer Engineering Manager
1st Consequence Mitigation Barriers			
Description	Effectiveness	Activities	Responsibilities
1. System disconnection	Very good	Operations to disconnect the system	Computer Engineering Manager
2. Backup - Restore	Good	Operations for backup and restore	Computer Engineering Manager
3. Antivirus software alarm	Moderate	Keep antivirus alarm in operation	Computer users

4.3. A second application of cyber security – Unauthorized external user

This application is related to unauthorized external users getting online access and thus, unauthorized external user is the Top Event of our example. An external attacker uses hacking techniques to gain online access to the electronic system on board. Thus the threats are related to the ability of the attacker to gain online access. Such threats are: i) credential theft, eaves dropping etc., ii) modification or replaying control

sequences, iii) wrong activities of unsuspecting authorized users. Typical prevention barriers to prevent such incidents are firstly the implementation of multifactor authentication so that the user could be identified, while the risk for compromised passwords will be reduced. Additionally, the network connection should be encrypted, while the communication endpoints should be authenticated. Connection of user must be for a limited time, then the session from the user client should be terminated in a jump-server and a new session from the jump-server is then established with new required authentication. Also, antivirus software and awareness training for personnel are required and e-mail and web filtering should also be implemented.

The usual consequences of unauthorized external users' online access are the system malfunction and the system unavailability. Backup/ restore procedures, event alarming and software whitelisting are considered as the proper mitigation barriers.

The complete Bow-Tie diagram for this application is shown in the following Figure 43, as generated by the previously described software MarSec.

Hazard and Top Event are defined using the form of Figure 42.

Risk Value	Start	Final
People	A1	
Environment	A1	
Assets	D3	
Reputation	D4	

Figure 42. Hazard identification and Top Event Form before the introduction of Threat Barriers.

For the Top Event, the **Frequency** and **Severity** of each one of People Environment, Assets and Reputation is selected from the corresponding Risk Matrix form, as shown in Figure 31 (see also Table 13), by clicking the proper square in the Risk Matrix.

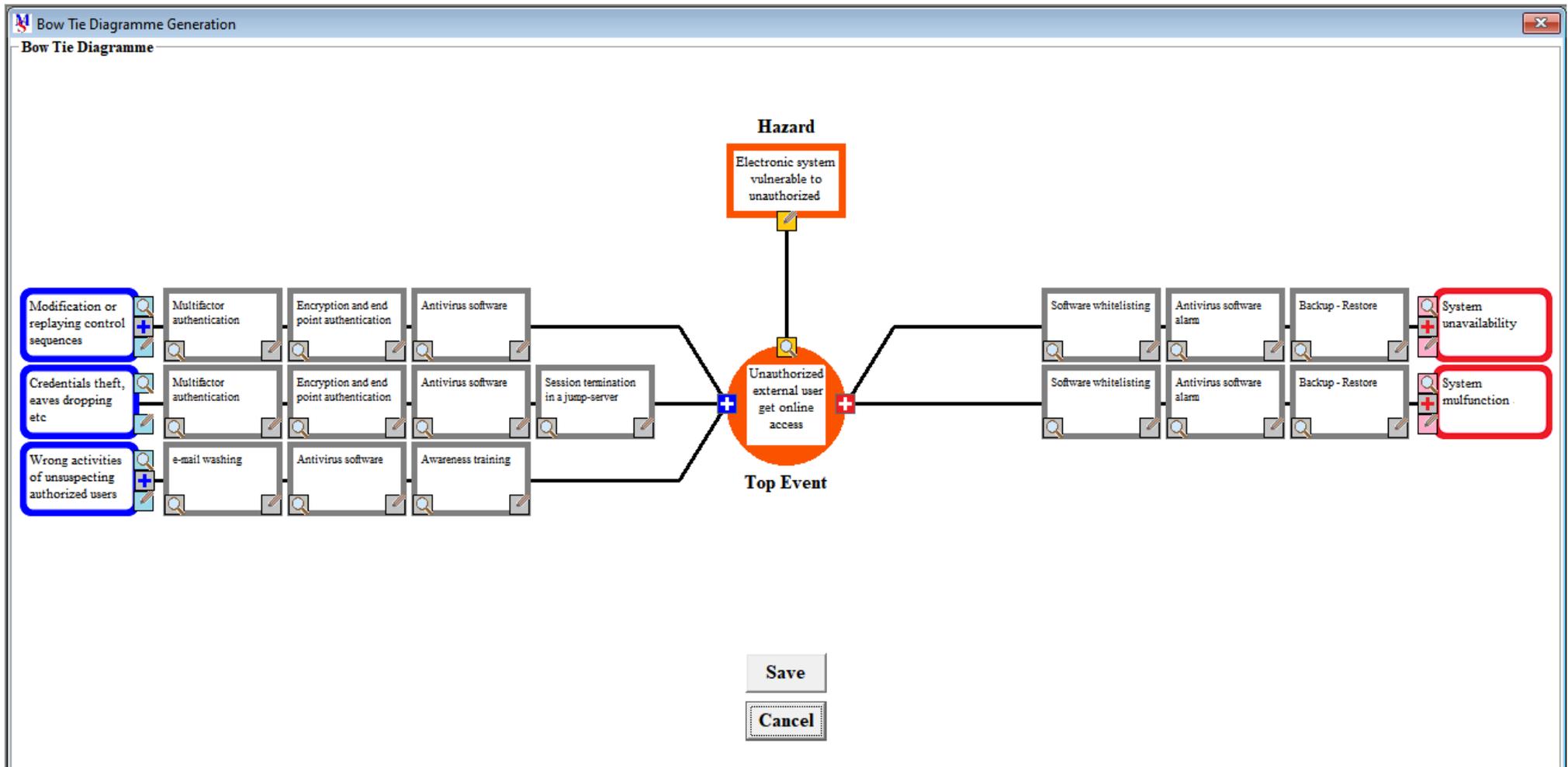


Figure 43. Bow-Tie diagram for electronic systems vulnerable to unauthorized external user.

The proper colour appears in the lower part of the Hazard identification and Top Event Form of Figure 42. The **Risk Value** for each one of People, Environment, Assets and Reputation is calculated using Equation 10:

$$RV = Frequency \times Severity$$

	<i>Frequency</i>	<i>Severity</i>	<i>Risk Value RV</i>
People	1	1	1
Environment	1	1	1
Assets	4	5	20
Reputation	4	4	16

i.e.:

$$RV_P = A1 = 1 \times 1 = 1$$

$$RV_E = A1 = 1 \times 1 = 1$$

$$RV_A = D5 = 4 \times 5 = 20$$

$$RV_R = D4 = 4 \times 4 = 16$$

Three threats are then defined, using the forms of Figures 44, 45 and 46. From the described three threats (**n = 3**) and their **Probabilities P_i** and **Contributions C_i** (see Figures 44, 45 and 46 – see also Table 14), the **Thread Index TI_i** values for each of Threat (i) of the three defined threats, are calculated using Equation 11:

$$TI_i = \frac{P_i \times C_i}{\sum_{i=1}^n [P_i \times C_i]}$$

<i>Threat i</i>	<i>Probability P_i</i>	<i>Contribution C_i</i>	<i>Threat Index TI_i</i>
1	1	3	0.25
2	1	3	0.25
3	2	3	0.50

Threat Identification

Threat Modification or replaying control sequences

Description

Frerquency

- Once per year or less
- Once per 6 months
- Once per 3 months
- Once per month
- Once per week
- Once per day
- Undefined

Contribution

- Low
- Medium
- High
- Undefined

Cancel

Figure 44. 1st Threat identification.

Threat Identification

Threat Credentials theft, eaves dropping etc

Description

Frerquency

- Once per year or less
- Once per 6 months
- Once per 3 months
- Once per month
- Once per week
- Once per day
- Undefined

Contribution

- Low
- Medium
- High
- Undefined

Cancel

Figure 45. 2nd Threat identification.

Threat Identification

Threat Wrong activities of unsuspecting authorized users

Description

Frerquency

- Once per year or less
- Once per 6 months
- Once per 3 months
- Once per month
- Once per week
- Once per day
- Undefined

Contribution

- Low
- Medium
- High
- Undefined

Cancel

Figure 46. 3rd Threat identification.

i.e.:

$$TI_1 = (1 \times 3) / 12 = 0.25$$

$$TI_2 = (1 \times 3) / 12 = 0.25$$

$$TI_3 = (2 \times 3) / 12 = 0.50$$

and:

$$TI = TI_1 + TI_2 + TI_3 = 0.25 + 0.25 + 0.50 = 1$$

The prevention barriers for each threat are then defined, using the forms of Figures 47a, 47b, 47c, 48a, 48b, 48c, 48d, 49a, 49b and 49c. From the values of the **Effectiveness** E_{ij} of each Barrier (j) for each Threat (i) (see Figures 47a, 47b, 47c, 48a, 48b, 48c, 48d, 49a, 49b and 49c – see also Table 15), the **Risk Value Reduction coefficient** R_{redi} of each Threat (i) are calculated using Equation 13:

$$R_{redi} = TI_i \times \left[\sum_{j=1}^{k_i} E_{ij} \right] / k_i$$

<i>Threat I</i>	<i>Barrier j</i>	<i>Threat Index TI_i</i>	<i>Effectiveness E_{ij}</i>	<i>Number of Barriers k_i</i>	<i>Reduction Coeff. R_{redi}</i>
1	1	0.25	0.84	3	0.2100
	2		0.84		
	3		0.84		
2	1	0.25	0.84	4	0.1994
	2		0.84		
	3		0.84		
	4		0.67		
3	1	0.50	0.84	3	0.3917
	2		0.84		
	3		0.67		

i.e.:

$$R_{red1} = 0.25 \times (0.84 + 0.84 + 0.84) / 3 = 0.25 \times 0.8400 = 0.2100$$

$$R_{red2} = 0.25 \times (0.84 + 0.84 + 0.84 + 0.67) / 4 = 0.25 \times 0.7975 = 0.1994$$

$$R_{red3} = 0.50 \times (0.84 + 0.84 + 0.67) / 3 = 0.50 \times 0.7833 = 0.3917$$

Prevention Barrier Identification [X]

Prevention Barrier:

Description:

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Application of multifactor authentication
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 47a. 1st Barrier for 1st Threat.

Prevention Barrier Identification [X]

Prevention Barrier:

Description:

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Encryption and end point authentication
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 47b. 2nd Barrier for 1st Threat.

Prevention Barrier Identification [X]

Prevention Barrier:

Description:

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Application of antivirus software
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 47c. 3rd Barrier for 1st Threat.

Prevention Barrier Identification [X]

Prevention Barrier:

Description:

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Application of multifactor authentication
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 48a. 1st Barrier for 2nd Threat.

Prevention Barrier Identification [X]

Prevention Barrier Encryption and end point authentication

Description

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Encryption and end point authentication
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 48b. 2nd Barrier for 2nd Threat.

Prevention Barrier Identification [X]

Prevention Barrier Antivirus software

Description

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Application of antivirus software
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 48c. 3rd Barrier for 2nd Threat.

Prevention Barrier Identification [X]

Prevention Barrier

Description

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Session termination in a jump-server
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 48d. 4th Barrier for 2nd Threat.

Prevention Barrier Identification [X]

Prevention Barrier

Description

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Operations to clean-up e-mails files
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 49a. 1st Barrier for 3rd Threat.

Prevention Barrier Identification [X]

Prevention Barrier:

Description:

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Application of antivirus software
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 49b. 2nd Barrier for 3rd Threat.

Prevention Barrier Identification [X]

Prevention Barrier:

Description:

Effectiveness

- Very Poor
- Poor
- Moderate
- Good
- Very Good
- Excellent
- Undefined

Activities and Responsibilities

- ACTIVITY: Training in computer systems awareness
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 49c. 3rd Barrier for 3rd Threat.

Then, the total Top Event **Risk Value Reduction coefficient** R_{red} is calculated using Equation 14:

$$R_{red} = \sum_{i=1}^n R_{redi}$$

i.e.:

$$R_{red} = 0.2100 + 0.1994 + 0.3917 = 0.8014$$

Then the resulting **Final Top Event Risk Value** RV_{final} , for People, Environment, Assets and Reputation is calculated using Equation 15:

$$RV_{final} = (1 - R_{red}) RV$$

i.e.:

$$RV_{finalP} = (1 - 0.8014) \times 1 = 0.1986 \text{ (Green Area)}$$

$$RV_{finalE} = (1 - 0.8014) \times 1 = 0.1986 \text{ (Green Area)}$$

$$RV_{finalA} = (1 - 0.8014) \times 20 = 3.9720 \text{ (Green Area)}$$

$$RV_{finalR} = (1 - 0.8014) \times 16 = 3.1776 \text{ (Green Area)}$$

The resulting Hazard Identification and Top Event form, after the introduction of the Threats Barriers, takes the form of Figure 50, with all Final Top Event Risk Values colours in green.

	Risk Value	Start	Final
People	A1	Green	Green
Environment	A1	Green	Green
Assets	D5	Red	Green
Reputation	D4	Red	Green

Figure 50. Hazard identification and Top Event after the introduction of all Threat Barriers.

Similarly, the 1st consequence is defined using the form of Figure 51.

Figure 51. 1st Consequence identification before the introduction of Consequence Barriers.

For the 1st Consequence, the **Frequency** and **Severity** of each one of People Environment, Assets and Reputation is selected from the corresponding Risk Matrix form, as shown in Figure 31 (see also Table 13), by clicking the proper square in the Risk Matrix. Also a Concern level is selected (see Table 16) for the 1st Consequence.

The proper colour appears in the lower part of the 1st Consequence identification of Figure 51. The **Risk Value** for each one of People, Environment, Assets and Reputation is calculated using Equation 10:

$$RV = Frequency \times Severity$$

	<i>Frequency</i>	<i>Severity</i>	<i>Risk Value RV</i>
People	1	1	1
Environment	1	1	1
Assets	4	4	16
Reputation	4	4	16

i.e.:

$$RV_P = A1 = 1 \times 1 = 1$$

$$RV_E = A1 = 1 \times 1 = 1$$

$$RV_A = D4 = 4 \times 4 = 16$$

$$RV_R = D4 = 4 \times 4 = 16$$

The mitigation barriers for the 1st consequence are then defined, using the forms of Figures 52a, 52b, 52c. From the values of the **Effectiveness** E_{ij} of each Barrier (j) for the single Consequence (see Figures 52a, 52b, 52c – see also Table 15), the **Risk Value Reduction coefficient** R_{redi} of the 1st Consequence are calculated using Equation 16:

$$R_{redi} \left[\sum_{j=1}^k E_{ij} \right] / k_i$$

<i>Conseq.</i> <i>i</i>	<i>Barrier</i> <i>j</i>	<i>Effectiveness</i> <i>E_{ij}</i>	<i>Number of</i> <i>Barriers k_i</i>	<i>Reduction</i> <i>Coeff. R_{redi}</i>
1	1	0.67	3	0.6700
	2	0.50		
	3	0.84		

i.e.:

$$R_{red1} = (0.67 + 0.50 + 0.84) / 3 = 0.6700$$

Then the resulting **1st Consequence Risk Value** RV_{final} , for people, environment, assets and reputation, is calculated using Equation 17:

$$RV_{finali} = (1 - R_{redi}) RV_i$$

i.e.:

$$RV_{finalP} = (1 - 0.6700) \times 1 = 0.3300 \text{ (Green Area)}$$

$$RV_{finalE} = (1 - 0.6700) \times 1 = 0.3300 \text{ (Green Area)}$$

$$RV_{finalA} = (1 - 0.6700) \times 16 = 5.2800 \text{ (Green Area)}$$

$$RV_{finalR} = (1 - 0.6700) \times 16 = 5.2800 \text{ (Green Area)}$$

Mitigation Barrier Identification

Mitigation Barrier: Backup - Restore

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Operations for backup and restore
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 52a. 1st Barrier for 1st Consequence.

Mitigation Barrier Identification

Mitigation Barrier: Antivirus software alarm

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Keep antivirus alarm in operation
- RESPONSIBILITY: Computer users

Cancel

Figure 52b. 2nd Barrier for 1st Consequence.

Mitigation Barrier Identification

Mitigation Barrier: Software whitelisting

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Check software whitelisting
- RESPONSIBILITY: Computer Engineering Manager
- ACTIVITY: Check software whitelisting
- RESPONSIBILITY: Computer users

Cancel

Figure 52c. 3rd Barrier for 1st Consequence.

The resulting 1st Consequence form, after the introduction of the Consequence Barriers, takes the form of Figure 53, with all Risk Values colours in green.

Consequence Identification

Consequence: System unavailability

Description:

	Risk Value	Start	Final	Concern
People	A1		Green	Minor <input type="checkbox"/>
Environment	A1		Green	Medium <input type="checkbox"/>
Assets	D4		Green	Major <input checked="" type="checkbox"/>
Reputation	D4		Green	Undefined <input type="checkbox"/>

Cancel

Figure 53. 1st Consequence identification after the introduction of Consequence Barriers.

Similarly, the 2nd consequence is defined using the form of Figure 54.

For the 2nd Consequence, the **Frequency** and **Severity** of each one of People Environment, Assets and Reputation is selected from the corresponding Risk Matrix form, as shown in Figure 31 (see also Table 13), by clicking the proper square in the

Risk Matrix. Also a Concern level is selected (see Table 16) for the single Consequence.

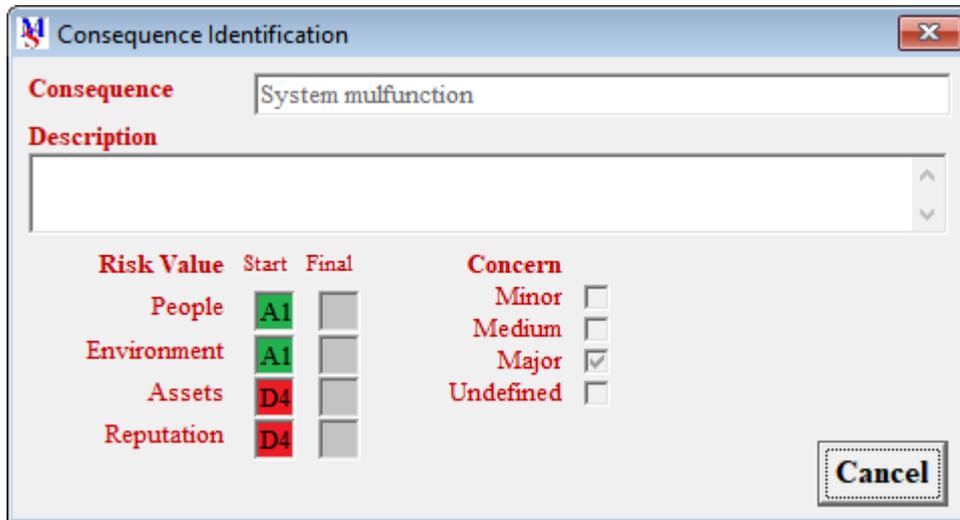


Figure 54. 2nd Consequence identification before the introduction of Consequence Barriers.

The proper colour appears in the lower part of the 2nd Consequence identification of Figure 54. The **Risk Value** for each one of People, Environment, Assets and Reputation is calculated using Equation 10:

$$RV = Frequency \times Severity$$

	<i>Frequency</i>	<i>Severity</i>	<i>Risk Value RV</i>
People	1	1	1
Environment	1	1	1
Assets	4	4	16
Reputation	4	4	16

i.e.:

$$RV_P = A1 = 1 \times 1 = 1$$

$$RV_E = A1 = 1 \times 1 = 1$$

$$RV_A = D4 = 4 \times 4 = 16$$

$$RV_R = D4 = 4 \times 4 = 16$$

Mitigation Barrier Identification

Mitigation Barrier: Backup - Restore

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Operations for backup and restore
- RESPONSIBILITY: Computer Engineering Manager

Cancel

Figure 55a. 1st Barrier for 2nd Consequence.

Mitigation Barrier Identification

Mitigation Barrier: Antivirus software alarm

Description:

Effectiveness:

- Very Poor
- Poor
- Moderate
- Good
- Very good
- Excellent
- Undefined

Activities and Responsibilities:

- ACTIVITY: Keep antivirus alarm in operation
- RESPONSIBILITY: Computer users

Cancel

Figure 55b. 2nd Barrier for 2nd Consequence.

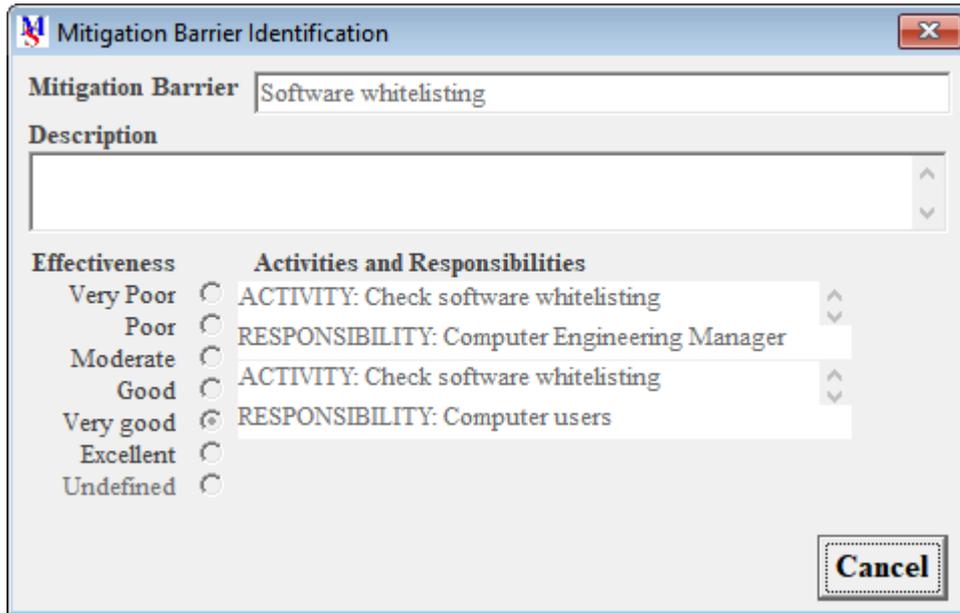


Figure 55c. 3rd Barrier for 2nd Consequence.

The mitigation barriers for the 2nd consequence are then defined, using the forms of Figures 55a, 55b, 55c. From the values of the **Effectiveness** E_{ij} of each Barrier (j) for the single Consequence (see Figures 55a, 55b, 55c – see also Table 15), the **Risk Value Reduction coefficient** R_{redi} of the 2nd Consequence are calculated using Equation 16:

$$R_{redi} [\sum_{j=1}^k E_{ij}] / k_i$$

<i>Conseq.</i> <i>i</i>	<i>Barrier</i> <i>j</i>	<i>Effectiveness</i> <i>E_{ij}</i>	<i>Number of</i> <i>Barriers k_i</i>	<i>Reduction</i> <i>Coeff. R_{redi}</i>
1	1	0.67	3	0.6700
	2	0.50		
	3	0.84		

i.e.:

$$R_{red1} = (0.67 + 0.50 + 0.84) / 3 = 0.6700$$

Then the resulting 2nd **Consequence Risk Value** RV_{final} , for people, environment, assets and reputation, is calculated using Equation 17:

$$RV_{finali} = (1 - R_{redi}) RV_i$$

i.e.:

$$RV_{\text{finalP}} = (1 - 0.6700) \times 1 = 0.3300 \text{ (Green Area)}$$

$$RV_{\text{finalE}} = (1 - 0.6700) \times 1 = 0.3300 \text{ (Green Area)}$$

$$RV_{\text{finalA}} = (1 - 0.6700) \times 16 = 5.2800 \text{ (Green Area)}$$

$$RV_{\text{finalR}} = (1 - 0.6700) \times 16 = 5.2800 \text{ (Green Area)}$$

The resulting 2nd Consequence form, after the introduction of the Consequence Barriers, takes the form of Figure 56, with all Risk Values colours in green.

Risk Value	Start	Final	Concern
People	A1	Green	Minor <input type="checkbox"/>
Environment	A1	Green	Medium <input type="checkbox"/>
Assets	D4	Green	Major <input checked="" type="checkbox"/>
Reputation	D4	Green	Undefined <input type="checkbox"/>

Figure 56. 2nd Consequence identification after the introduction of Consequence Barriers.

Finally, the resulting printouts are presented in the following Table 19 (Main Printout about Threats and Consequences) and Table 20 (Printout of Activities and Responsibilities resulting from Prevention & Mitigation Barriers).

Table 19. Main Printout about Threats and Consequences.

Main Printout about Threats and Consequences			
Hazard: Electronic systems vulnerable to unauthorized external user			
Top Event: Unauthorized external user get online access			
Risk Values			
People 	Environment 	Assets 	Reputation 
Threats			
Description	Frequency	Contribution	
1. Modification or replaying control sequences	Once per year or less	High	
2. Credentials theft, eaves dropping etc.	Once per year or less	High	
3. Wrong activities of unsuspecting authorized users	Once per 6 months	High	
Consequences			
Description	Risk Value for		Concern
1. System unavailability	P  E  A  R 		Major
2. System malfunction	P  E  A  R 		Major

Table 20. Printout of Activities and Responsibilities resulting from Prevention & Mitigation Barriers.

Printout of Activities and Responsibilities for Prevention and Mitigation Barriers			
Hazard: Electronic systems vulnerable to unauthorized external user			
Top Event: Unauthorized external user get online access			
Risk Values			
People 	Environment 	Assets 	Reputation 
1st Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. Multifactor authentication	Very good	Application of multifactor authentication	Computer Engineering Manager
2. Encryption and end point authentication	Very good	Encryption and end point authentication	Computer Engineering Manager
3. Antivirus software	Very good	Application of antivirus software	Computer Engineering Manager
2nd Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. Multifactor authentication	Very good	Application of multifactor authentication	Computer Engineering Manager
2. Encryption and end point authentication	Very good	Encryption and end point authentication	Computer Engineering Manager
3. Antivirus software	Very good	Application of antivirus software	Computer Engineering Manager
4. Session termination in a jump-server	Good	Session termination in a jump-server	Computer Engineering Manager
3rd Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. e-mail washing	Very good	Operations to clean-up e-mail files	Computer Engineering Manager
2. Antivirus software	Very good	Application of antivirus software	Computer Engineering Manager
3. Awareness training	Good	Training in computer awareness	Computer Engineering Manager
1st Consequence Mitigation Barriers			
Description	Effectiveness	Activities	Responsibilities
1. Backup - Restore	Good	Operations for backup and restore	Computer Engineering Manager
2. Antivirus software alarm	Moderate	Keep antivirus alarm in operation	Computer users
3. Software whitelisting	Very good	Keep antivirus alarm in operation	Computer Engineering Manager/Computer users
2nd Consequence Mitigation Barriers			
Description	Effectiveness	Activities	Responsibilities
1. Backup - Restore	Good	Operations for backup and restore	Computer Engineering Manager
2. Antivirus software alarm	Moderate	Keep antivirus alarm in operation	Computer users
3. Software whitelisting	Very good	Keep antivirus alarm in operation	Computer Engineering Manager/Computer users

4.4. Discussion

The proposed Framework for Risk Assessment and Analysis, uses the Bow-Tie for quantitative analysis, where, our likelihood is defined in terms of probability and contribution and our consequence in terms of quantitative Risk Value (pre-defined by the users). Bow-Tie integrates several approaches focusing on the quantification of the maritime security risk, consisting mainly of Risk Identification, Risk Analysis and Risk Evaluation.

Through the user friendly software in Visual Basic, the results of the risk computation appear in the Bow-Tie diagram providing the user with a coloured scheme of the obtained risk values for top event and each consequence, after the introduction of the necessary prevention and mitigation barriers by the user.

Additionally, the user can obtain some programme printouts: i) A Bow-Tie diagram providing schematically, Threats, Consequences, Prevention Barriers and Mitigation Barriers. ii) A Main Printout providing general information about Threats, and Consequences, iii) A Printout of Activities and Responsibilities, as a result of the defined Prevention and Mitigation Barriers.

All obtained results were checked and compared with similar results from other commercial frameworks, such as DNV-GL (2016) and we found that they were in line with them.

As a general conclusion, the proposed framework provides the user optically with all necessary information concerning threats and consequences, all necessary prevention and mitigation barriers, all related actions to reduce risk and all responsible persons and finally, all necessary related printouts. Risk computation is carried out easily in a completely understandable way and the results are presented immediately and optically in a Bow-Tie type diagram.

The framework is open for further additions, such as Cost-Benefit Analysis and Decision Making.

Chapter 5. Conclusions and Brief Recommendation for Future Work

The traditional concept of safety mainly deals with accidents, failures, mistakes, accidental malfunctions and any possible damage due to them. The security view leads to the examination of planned and appropriate actions aimed at adversely affecting the selected target. Therefore, the practice of maritime security must be examined in a new context, facing rapid changes, especially after the terrorist attacks in the USA in 2001. The challenge is to develop joint initiatives and relations between private sector and public sector to secure maritime industry when affected by the threats of terrorism and criminal activity. Therefore, the main goal of maritime security is to minimize losses, accidents, injuries and financial losses resulting from terrorism and criminal activity, enabling the flow of trade and business continuity.

Given the complexity of the maritime industry and the need for a decision-making tool for use at the different stages of design and operation, a special risk-based assessment tool is proposed for development, which performs security risk assessment, analysis and evaluation, integrating several studies related with the quantification of maritime security risk

Assessments of security using Bow-Tie type diagrams provide a useful visual presentation of the main risks and the proposed method for their control. This technique is already known and used by many industries, and among them the maritime industry plays an important role.

The proposed Framework for Risk Assessment and Analysis, uses the Bow-Tie for quantitative analysis, where, our likelihood is defined in terms of probability and contribution and our consequence in terms of quantitative Risk Value (pre-defined by the users). Bow-Tie integrates several approaches focusing on the quantification of the maritime security risk, consisting of Risk Identification, Risk Analysis and Risk Evaluation. The framework is open for further additions, such as Cost-Benefit analysis and Decision Making.

The user identifies Threats and he also may define Probability and Contribution for each defined threat. Then the user introduces Prevention Barriers and he may also select to define Effectiveness of the prevention barrier, if he wants to obtain the actual effect of the described barriers on the reduction of the predetermined Risk Value of

the top event. He also may select the proper Activities and Responsibilities for the activation of the introduced barrier in order to obtain a Report of Activities and Responsibilities.

The user also identifies Consequences and he also may select to make a Risk Assessment and to define the Concern of each consequence. Then the user introduces Mitigation Barriers and he may also select to define Effectiveness of the mitigation barrier, if he wants to obtain the actual effect of the described barriers on the reduction of the predetermined Risk Value of each consequence. He also may select the proper Activities and Responsibilities for the activation of the introduced barrier in order to obtain a Report of Activities and Responsibilities.

A risk computation procedure is described after the application of a set of prevention barriers, which is based mainly on the accuracy of the definition of the Frequency F_i and the Contribution C_i of each Threat (i) as well as on the accuracy of the estimation of the Effectiveness value E_{ij} , of each Prevention Barrier (j) for the same defined Threat (i), by the user.

Similarly, the risk computation for each consequence, after the application of a set of mitigation barriers, is based mainly on the accuracy of the definition of the Risk Value RV_i of each Consequence (i) as well as on the accuracy of the estimation of the Effectiveness value E_{ij} , of each Mitigation Barrier (j) for the same defined Consequence (i), by the user.

Through the user friendly software in Visual Basic, the results of the risk computation appear in the Bow-Tie diagram providing the user with a coloured scheme of the obtained risk values for top event and each consequence, after the introduction of the necessary prevention and mitigation barriers by the user.

Additionally, the user can obtain important programme outputs as reports: i) A Bow-Tie diagram providing schematically, Threats, Consequences, Prevention Barriers and Mitigation Barriers. ii) A Main Printout providing general information about Threats and Consequences, iii) A Printout of Activities and Responsibilities, as a result of the defined Prevention and Mitigation Barriers.

All obtained results were checked and compared with similar results from other commercial frameworks, such as DNV-GL (2016) and we found that they were in line with them.

As a general conclusion, **the aim of the proposed study, to address the issue of maritime security through the development of a method applicable to the maritime industry that evaluates and manages security related risks and specifically maritime cyber risk, was achieved.** The research has achieved the **objectives set out** in the Introduction chapter. Specifically, in Chapter 2 **the author has critically analysed the existing maritime risk approaches** (objective 1). In Chapter 3, **the author has developed a method to address maritime cyber risk, which was tested using cyber security examples** (objective 2). In Chapter 4, **the author illustrated through the application how this method could be used in practise** (objective 3). The proposed framework provides the user optically with all necessary information concerning threats and consequences, all necessary prevention and mitigation barriers, all related actions to reduce risk and all responsible persons and finally, all necessary related reports. Risk computation is carried out easily in a completely understandable way and the results are presented immediately and optically in a Bow-Tie type diagram. In Chapter 5, **the author provides brief recommendation for future work** (objective 4). It is recommended to use the existing input and output data in order to complete the programme in the future by adding routines to accomplish:

i) A Cost-Benefit Analysis. The security benefits resulting from the reduction of risk, causing the increase of accountability and the reduction of customers' revenue must be compared with the required costs from security equipment investment, shipping time etc. in order to identify the "optimal" security Risk Control Measures. Thus, a cost-benefit analysis is required and sometimes the Evidential Reasoning (ER) approach may be used.

ii) A Decision-making procedure. Decision-making is necessary in order to synthesize the previous steps and present them in a way that could be useful to the decision makers, since it will be useful for a successful prediction of the appropriate security level, while keeping an optimal productivity level. Sometimes it is necessary to use the Dynamic System (SD) in order to simulate the cost-benefit analysis of security by creating optical causal loops that link the cost of security and the required benefits generated.

iii) A Training Programme. In order to accomplish the decided procedure it is necessary to develop a training programme in which all responsible persons must be

included and all required procedures must be defined accurately, in order to avoid misunderstandings and unnecessary actions.

Appendix 1: Programme presentation

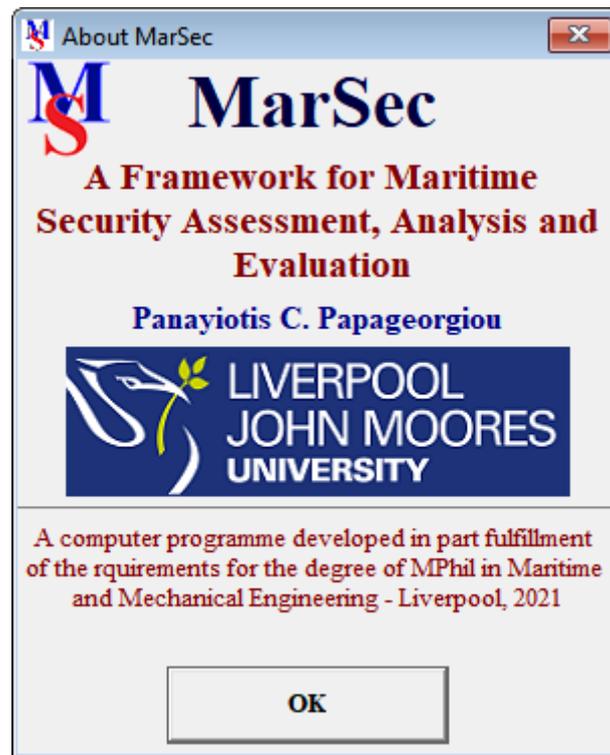


Figure 57. About the Programme

Main Screen

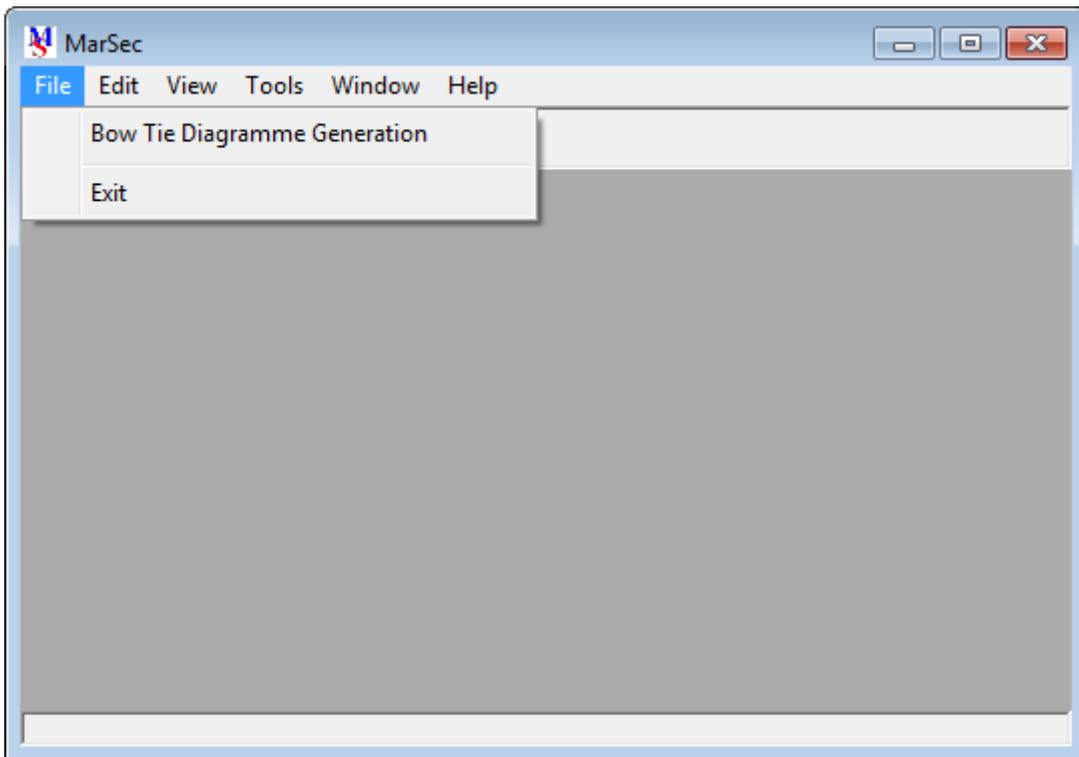


Figure 58a. Main menu screen for Bow-Tie diagram generation.

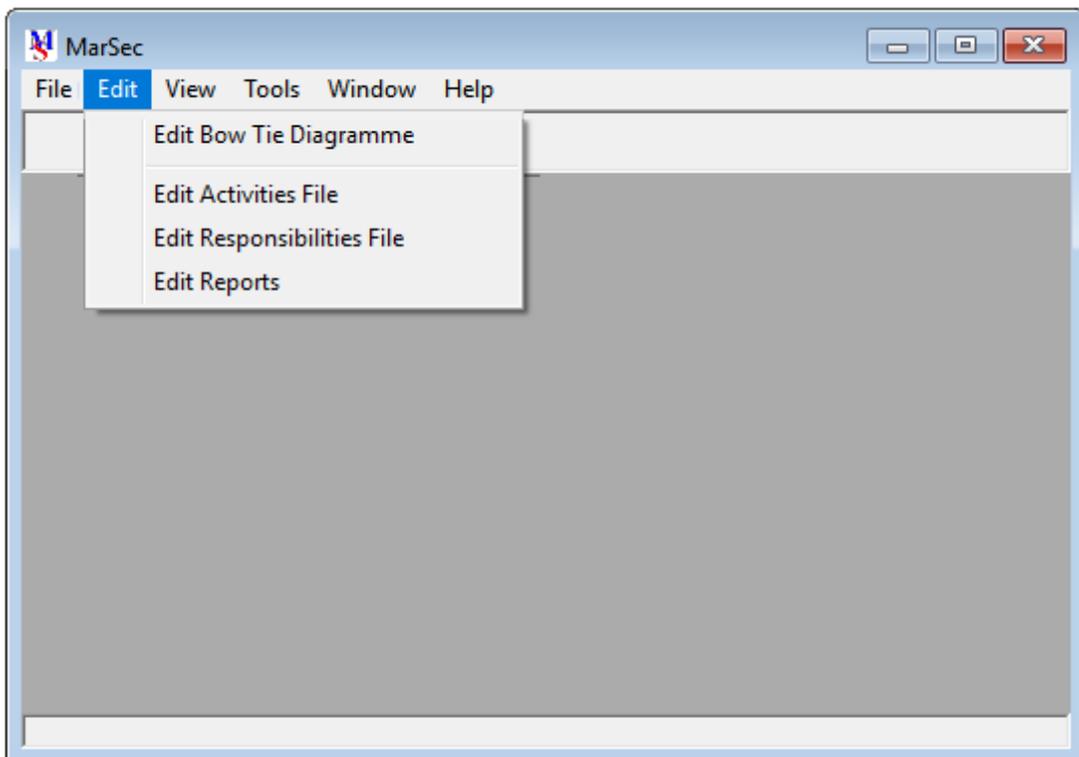


Figure 58b. Main menu screen to edit an existing Bow-Tie diagram, or to edit an auxiliary data file, containing information about previous cases of maritime security.

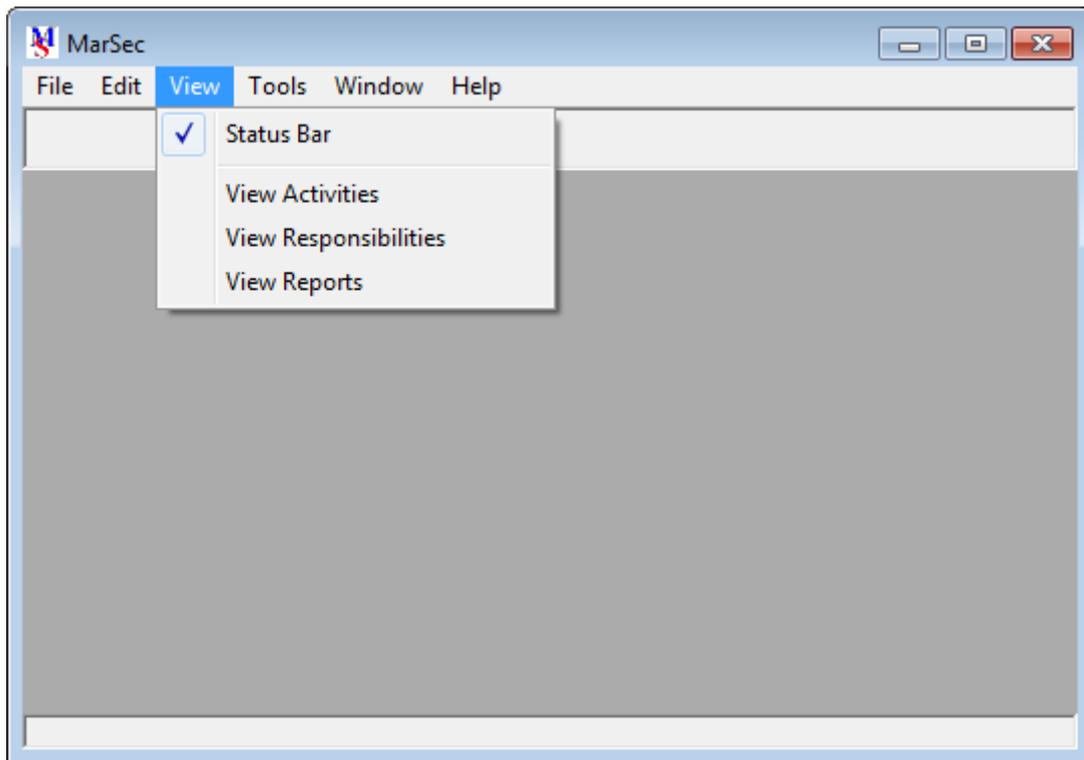


Figure 58c. Main menu screen to view an existing Bow-Tie diagram, or to view auxiliary data files, containing information about activities, responsibilities and reports.

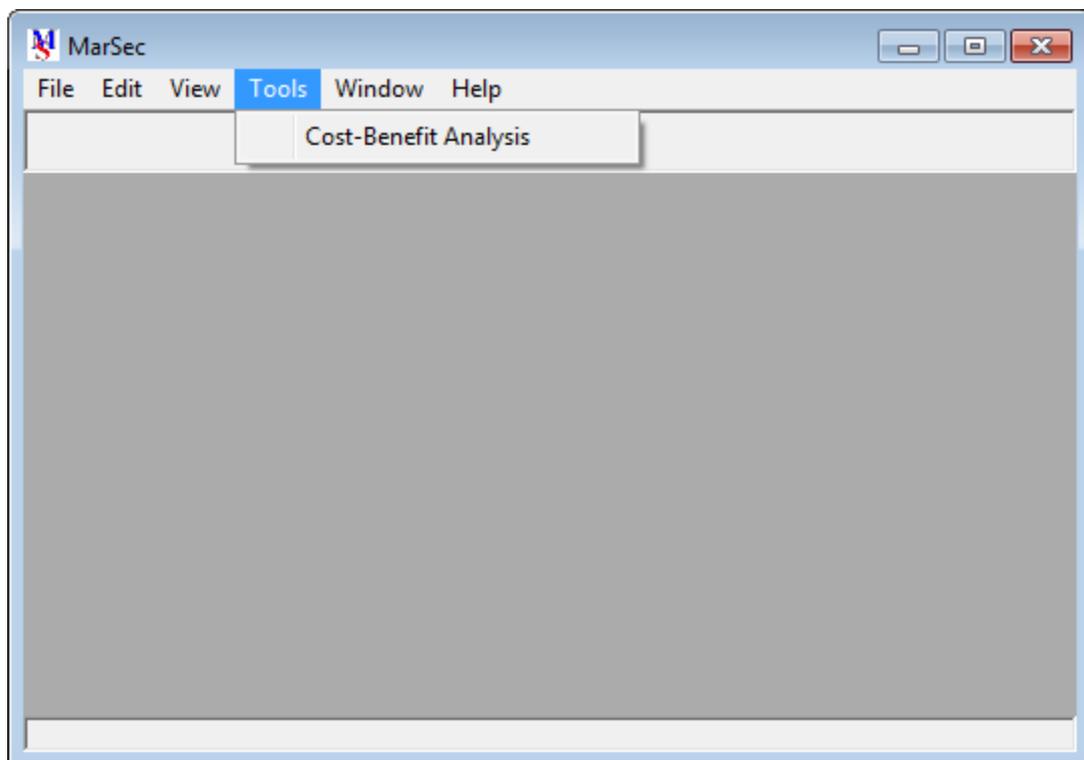


Figure 58d. Main menu screen to edit providing tools to carry out a cost benefit analysis for the whole procedure shown in the Bow-Tie diagram.

Bow-Tie Diagram Generation Screen

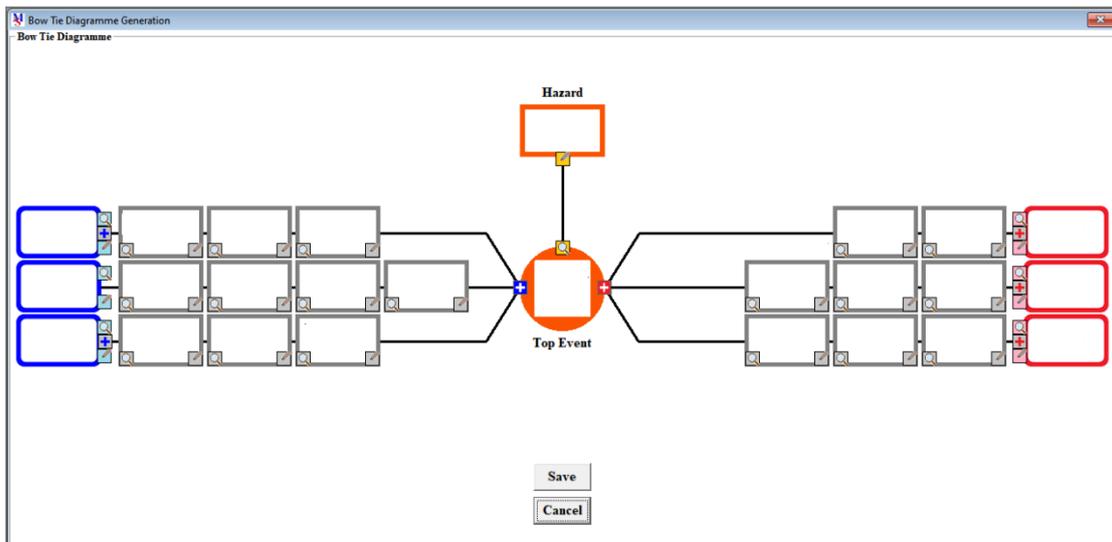


Figure 59. Example of Bow-Tie diagram generation.

Risk Value	Start	Final
People	<input type="text"/>	<input type="text"/>
Environment	<input type="text"/>	<input type="text"/>
Assets	<input type="text"/>	<input type="text"/>
Reputation	<input type="text"/>	<input type="text"/>

Figure 60. Hazard Identification and Top Event definition form. Hazard may be defined or selected from a list which includes cases such as: terrorism, cargo theft, extortion, robbery, vandalism, trafficking of people, drugs, stolen goods, weapons or money, stowaways, smuggling, piracy, corruption, embargo violations, customs violations, destroying the marine environment and cyber-attack. If Risk Assessment is selected, then a risk matrix form appears, in order to select the frequency and severity of the event for each one of the affected cases, i.e. people, environment, assets, reputation (see Figs. 61, 62, 63, 64).

Four Types of Risk Matrices

Risk Matrix for People

Description of Matrix Elements

<u>Frequency</u>	<u>Severity</u>
A: Very Unlikely	1: Slight Injury
B: Unlikely	2: Minor Injury
C: Possible	3: Major Injury
D: Likely	4: Single Death
E: Very Likely	5: Multiple Deaths

Colours description

■	Low Risk
■	Medium Risk
■	High Risk

Matrix

5					
4					
3					
2					
1					
	A	B	C	D	E

Cancel

Figure 61. Risk Matrix form for people, for the selection of the frequency and the severity of the event.

Risk Matrix for Environment

Description of Matrix Elements

<u>Frequency</u>	<u>Severity</u>
A: Very Unlikely	1: Slight Effect
B: Unlikely	2: Minor Effect
C: Possible	3: Moderate Effect
D: Likely	4: Major Effect
E: Very Likely	5: Massive Effect

Colours description

■	Low Risk
■	Medium Risk
■	High Risk

Matrix

5					
4					
3					
2					
1					
	A	B	C	D	E

Cancel

Figure 62. Risk Matrix form for environment, for the selection of the frequency and the severity of the event.

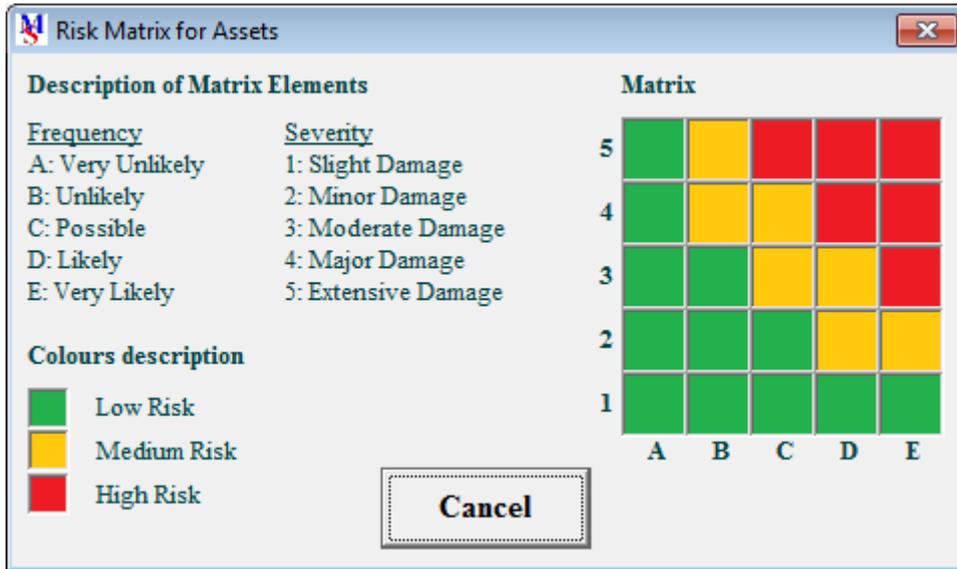


Figure 63. Risk Matrix form for assets, for the selection of the frequency and the severity of the event.

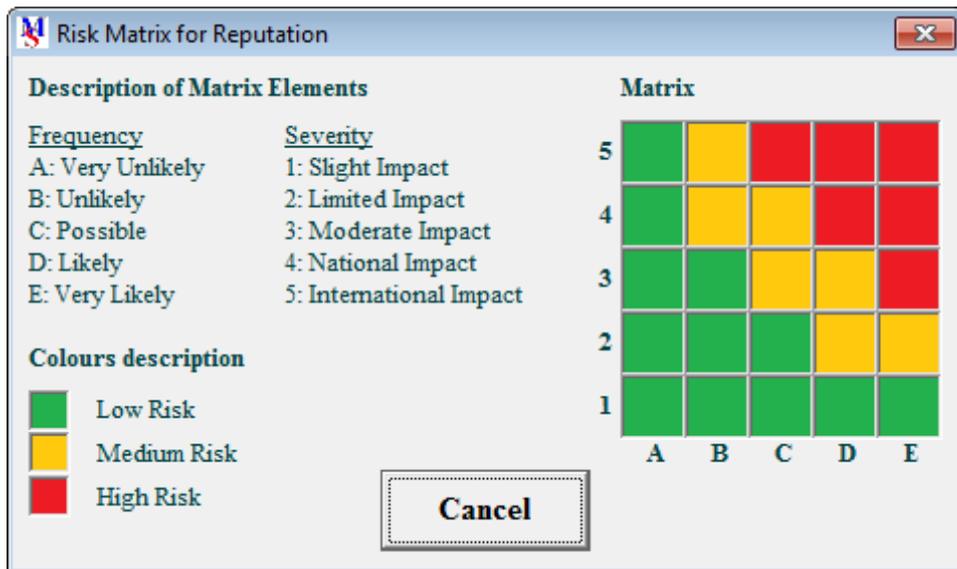


Figure 64. Risk Matrix form for reputation, for the selection of the frequency and the severity of the event.

Threats and Prevention barriers Identification

Figure 65. Threat identification and description form. Each time the plus (+) sign in the threat side of the Top Event block of the Bow-Tie diagram screen is clicked, a new threat block appears and the current form appears too, where user will identify a new threat and its description. User may also select to define frequency and contribution of threat, by marking the corresponding square.

Figure 66. Prevention barrier identification and description form. Each time the plus (+) sign in the right side of the threat block of the Bow-Tie diagram screen is clicked, a new prevention barrier block appears in the Bow-Tie diagram form and the current form appears too, where user will identify a new prevention barrier and its description. User may also select to define effectiveness of the prevention barrier, by marking the corresponding circle.

Consequences and Mitigation barriers Identification

Figure 67. Consequence identification and description form. Each time the plus (+) sign in the consequence side of the Top Event block of the Bow-Tie diagram screen is clicked, a new consequence block appears and the current form appears too, where user will identify a new consequence and its description. User may also select to assess risk and to define concern of consequence, by clicking and marking the corresponding square. If Risk Assessment is selected, then a risk matrix form appears, in order to select the frequency and severity of the consequence for each one of the affected cases, i.e. people, environment, assets, reputation (see Figs. 61, 62, 63, 64).

Figure 68. Mitigation barrier identification and description form. Each time the plus (+) sign in the left side of the consequence block of the Bow-Tie diagram screen is clicked, a new mitigation barrier block appears in the Bow-Tie diagram form and the current form appears too, where user will identify a new mitigation barrier and its description. User may also select to define effectiveness of the mitigation barrier, by marking the corresponding circle.



Figure 69. List of Activities.

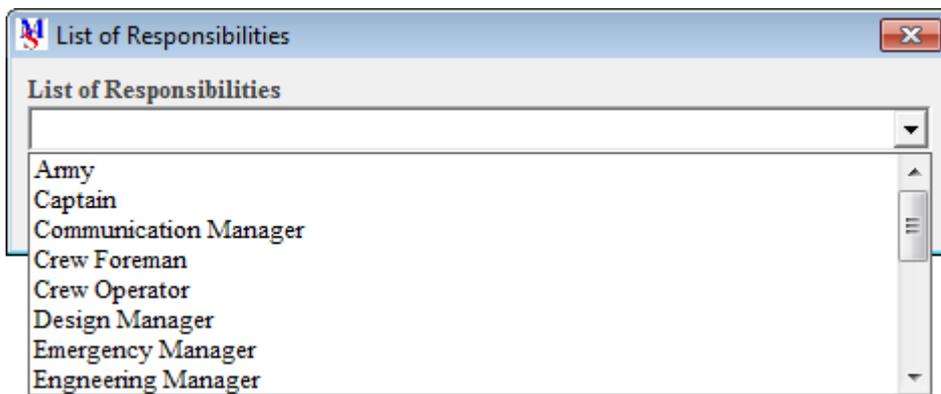


Figure 70. List of Responsibilities.

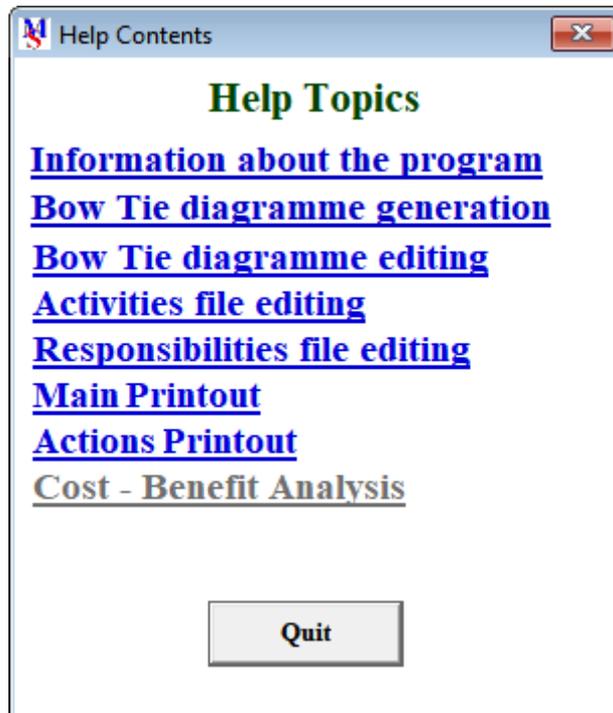


Figure 71. Help Topics form.

Appendix 2: Programme printouts

Table 21. Main Printout about Threats and Consequences.
Main Printout about Threats and Consequences

Hazard _____			
Top Event _____			
Risk Assessment			
People □	Environment □	Assets □	Reputation □
Threats			
Description	Frequency	Contribution	
1. _____	_____	_____	
2. _____	_____	_____	
3. _____	_____	_____	
:			
Consequences			
Description	Risk for	Concern	
1. _____	P □ E □ A □ R □	_____	
2. _____	P □ E □ A □ R □	_____	
3. _____	P □ E □ A □ R □	_____	
:			

Table 22. Printout of Activities and Responsibilities resulting from Prevention & Mitigation Barriers.

Printout of Activities and Responsibilities for Prevention and Mitigation Barriers			
Hazard: _____			
Top Event: _____			
Risk Assessment			
People □	Environment □	Assets □	Reputation □
1st Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
2. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
3. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
:			
2nd Threat Prevention Barriers			
Description	Effectiveness	Activities	Responsibilities
1. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
:			
:			
1st Consequence Mitigation Barriers			
Description	Effectiveness	Activities	Responsibilities
1. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
2. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
3. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
:			
2nd Consequence Mitigation Barriers			
Description	Effectiveness	Activities	Responsibilities
1. _____	_____	a. _____ b. _____ :	a. _____ b. _____ :
:			
:			

References

- American Bureau of Shipping (2016). The application of cyber security principles to marine and offshore operations. *American Bureau of Shipping*, Houston
- Agrawal, V. (2017). A framework for the information classification in ISO 27005 standard. Department of Information Security and Communication Technology Norwegian University of Science and Technology, NTNU Gjøvik.
- Aust, J., Pons, D. (2020). A Systematic Methodology for Developing Bowtie in Risk Assessment: Application to Borescope Inspection. *Aerospace*, 7(7), 86. <https://doi.org/10.3390/aerospace7070086>
- Bakir, N.O. (2007). A brief analysis of threats and vulnerabilities in the maritime domain. In: Linkov I et al. (eds), *Managing critical infrastructure risks*, Springer, Dordrecht, pp 17–49
- Bernsmed, K., Frøystad, Ch., Meland1, P.H., Nesheim, D.A., Rødseth, Ø.J. (2018). Visualizing Cyber Security Risks with Bow-Tie Diagram. Springer International Publishing AG 2018 P. Liu et al. (eds.): *GramSec 2017*, LNCS 10744, pp. 38–56, 2018. https://doi.org/10.1007/978-3-319-74860-3_3
- Bichou K. (2008). Security and risk-based models in shipping and ports: review and critical analysis. *OECD International Transport Forum*; Discussion Paper No. 2008-20
- BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC) (2020). *The Guidelines on Cyber Security on board Ships*, Version 4
- Bradford, J. F. (2004). Japanese Anti- Piracy Initiatives in Southeast Asia: Policy Formulation and the Coastal State Responses. *Contemporary Southeast Asia*, 26(3), 480–505. <https://doi.org/10.1355/cs26-3e>
- Brooks, M., Pelot, R. (2008). Port Security: A Risk-Based Approach. In book: Wayne & Talley (ed.) *Maritime Safety, Security and Piracy - Chapter: 11*, Publisher: Informa
- Burns, M. (2015). *Port Management and Operations*, CRC Press, Boca Raton
- Chalk, P. (2008). *International security: terrorism, piracy, and challenges for the United States*, Center for Terrorism Risk Management Policy, Santa Monica, RAND

- Cox, Jr, L. A. T. (2008). Some Limitations of “Risk = Threat × Vulnerability × Consequence” for Risk Analysis of Terrorist Attacks. *Risk Analysis*, 28(6), 1749–1761. <https://doi.org/10.1111/j.1539-6924.2008.01142.x>
- Crist, P. (2003). *Security in maritime transport: risk factors and economic impact*, OECD Directorate for Science, Technology and Industry–Maritime Transport Committee, Paris
- DAWN (2015). Over 200 tonnes of heroin is smuggled via Pakistan a year. *DAWN*. <http://www.dawn.com/news/731994/over-200-tonnes-of-heroin-is-smuggled-via-pakistan-a-year>;
- DNV-GL (2016). *Cyber security resilience management for ships and mobile offshore units in operation*, DNV-GL AS, September 2016
- Edgerton, M. (2013). *A Practitioner's Guide to Effective Maritime and Port Security*, John Wiley & Sons, Inc. New Jersey, USA
- European Commission (1996). Guidance of risk assessment at work. European Commission, Luxembourg. URL: <http://osha.europa.eu/en/topics/riskassessment/guidance.pdf>
- Fransas, A. Nieminen E., Salokorpi M., Rytönen J. (2012). *Maritime safety and security: Literature review*, Kymenlaakso University of Applied Sciences
- Grady, J. (2020). Experts: Maritime Industry Remains Vulnerable to Cyber Attacks. *USNI News*, September 28, 2020. URL: <https://news.usni.org/2020/09/28/experts-maritime-industry-remains-vulnerable-to-cyber-attacks>
- IHS Maritime and Trade (2016). IHS Fairplay Maritime Cyber-security Survey – the results. URL: <https://fairplay.ihs.com/article/4275151/ihs-fairplay-maritime-cyber-security-survey-the-results>
- IMO (1997). Interim Guidelines for the Application of Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process, MSC/Circ.829-MEPC/Circ.335, 17 November 1997
- IMO (1997b). Guidelines for the Prevention and Suppression of the Smuggling of Drugs, Psychotropic Substances and Precursor Chemicals on Ships Engaged in International Maritime Traffic, A20/Res.872, 5 December 1997
- IMO (2002). Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-Making Process, MSC/Circ.1023-MEPC/Circ.392, 5 April 2002
- IMO (2003). International ship and port facility security (ISPS) code and SOLAS amendments, adopted on 12 December 2002. Electronic edition, *Sales number: E116E*, London

-IMO (2004). Guidance to Masters, Companies and Duly Authorized Officers on the Requirements Relating to the Submission of Security-related Information Prior to the Entry of a Ship into Port, MSC/Circ.1130, 14 December 2004

-IMO (2005). Amendments to the Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-Making Process (MSC/Circ.1023-MEPC/Circ.392), MSC/Circ.1180-MEPC/Circ.474, (MSC 80), 25 August 2005

-IMO (2006). Revised Guidelines for the Prevention and Suppression of the Smuggling of Drugs, Psychotropic Substances and Precursor Chemicals on Ships Engaged in International Maritime Traffic, MSC82/24/Add.2, 7 December 2006

-IMO (2007). Revised Guidelines for the Prevention and Suppression of the Smuggling of Drugs, Psychotropic Substances and Precursor Chemicals on Ships Engaged in International Maritime Traffic, FAL34/9, 30 March 2007

-IMO (2009). Amendments to the Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-Making Process (MSC/Circ.1180-MEPC/Circ.474), MSC-MEPC.2/Circ.5, (MSC 82), 2009

-IMO (2009b). Revised Guidance to Masters, Companies and Duly Authorized Officers on the Requirements Relating to the Submission of Security-related Information Prior to the Entry of a Ship into Port, MSC.1/Circ.1305, 9 June 2009

-IMO (2010). Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships, A.26/Res.1025, 18 January 2010

-IMO (2013). Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process, MSC-MEPC.2/Circ.12, 8 July 2013

-IMO (2015). Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process, MSC-MEPC.2/Circ.12/Rev.1, 18 June 2015

-IMO (2017). Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3, 5 July 2017

-IMO (2017b). Maritime Cyber Risk Management in Safety Management Systems, MSC.98/428/Add.1, 16 June 2017

-IMO (2018). Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process, MSC-MEPC.2/Circ.12/Rev.2, 9 April 2018

-IMO (2019). Maritime Safety – Safety Topics – Formal Safety Assessment. URL: <https://www.imo.org/en/OurWork/Safety/Pages/FormalSafetyAssessment.aspx>

-IMO (2020). Reports on Acts of Piracy and Armed Robbery Against Ships, MSC.4/Circ.264, 27 April 2020

-IMB (2020). Piracy and Armed Robbery against Ships, Report for the Period 1 January – 31 December 2019, London: ICC IMB, 1990 -2020

- International Chamber of Shipping (2021). *Drug Trafficking and Drug Abuse On Board Ship – Guidelines for Owners and Masters on Preparation, Prevention, Protection and Response*, 6th Edition, Witherbys
- ISO/IEC 27005 (2011). Information technology - Security techniques - Information security risk management. *Technical rep.* (2011). URL: http://www.iso.org/iso/catalogue_detail?csnumber=56742
- ISO 20858 (2007). Ships and marine technology — Maritime port facility security assessments and security plan development. URL: <https://www.iso.org/standard/46051.html>
- ISO 31000 (2018). Risk management ISO 31000, ISO, Geneva, 2018. URL: <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf>
- Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, April 2015
- Jones, S. (2006). *Maritime security: a practical guide*, London: Nautical Institute
- King, J. (2005). The security of merchant ship-ping. *Marine Policy* 29: 235–45
- Klein, N. (2011). *Maritime security and the law of the sea*, Oxford University Press, Oxford & New York
- Kontovas, C., Psaraftis, H. (2009). Formal Safety Assessment: A Critical Review. *Marine Technology*, Vol. 46, No. 1, January 2009, pp. 45–59
- Kishore, E.A. (2013). Formal Safety Assessment in Maritime Industry - Explanation to IMO Guidelines. *Class Notes for MTech NA&OE 1st Year*
- Lambert, J.H. (2007). Risk-cost-benefit analysis for port environmental security investments. In: Linkov, I. et al (eds), *Managing critical infrastructure risks*. Springer, Dordrecht, pp 299–307
- Leovy, L. (2017). Cyberattack cost Maersk as much as \$300 million and disrupted operations for 2 weeks. *Los Angeles Times*, Aug 17
- Mærli, M.B., Barø, R., Paaske, B.J., Vahr, H.R., Lia, B. (2009). *Energy supply chain threat assessment and generic security guidance*, COUNTERACT Project Deliverable 3
- Makrodimitris, G., Polemi, N., Douligeris. C. (2014). Security Risk Assessment Challenges in Port Information Technology Systems. *Springer*, DOI: 10.1007/978-3-319-11710-2_3
- McNicholas (2016). *Maritime Security - An Introduction*, Elsevier Inc.

-Ministry of Defence of Finland (2011). Security Strategy for Society. Government Resolution 16.12.2010. Ministry of Defence, Helsinki

-*Mission Secure* (2020). Complying with the IMO 2021 Cybersecurity Regulations - Ensuring the safe and secured operation of vessels at sea and onshore. *Mission Secure*, Regulatory Overview, URL: <https://www.missionsecure.com/hubfs/Assets/Collateral/complying-with-imo-cybersecurity-overview-mission-secure.pdf>

-*Mission Secure* (2021). A Comprehensive Guide to Cyber Security for Ships. *Mission Secure*, Ship Cyber Security. URL: https://www.missionsecure.com/ship-cyber-security-risk-management?utm_term=cyber%20security%20for%20ships&utm_campaign=Maritime+Cyber+Security&utm_source=adwords&utm_medium=ppc&hsa_acc=9936888968&hsa_cam=11247064448&hsa_grp=117076417669&hsa_ad=497697627976&hsa_src=g&hsa_tgt=kwd-860161525364&hsa_kw=cyber%20security%20for%20ships&hsa_mt=b&hsa_net=adwords&hsa_ver=3

-Ng, A.K.Y., Vaggelas, G.K. (2012). Port security: the ISPS Code. In Talley, W.K. (Ed.): *The Blackwell Companion to Maritime Economics*, pp.674–700, Blackwell, Hoboken, NJ

-Nyman, T., Tuominen, R., Rytönen, J., Kujala, P. & Ylitalo, T. (2010) Itämeren meriturvallisuusmenetelmä- ja tutkimussuunnitelman laadinta (Preliminary study of developing a new method to control maritime safety and security risks together). Electronical report, not published. Espoo: The Finnish Transport Agency, Ministry of Defence, The Finnish Border Guard, Aalto University, Kymenlaakso University of Applied Sciences and Technical Research Centre of Finland. Presented by Fransas A., Nieminen E., Salokorpi M., Rytönen J. (2012). Maritime safety and security Literature review. Kymenlaakson ammattikorkeakoulu. University of Applied Sciences

-OECD (2003). Security in maritime transport: Risk factors and economic impact OECD – Maritime Transport Committee, Directorate for science, technology and industry, July 2003

O'Neil, M., Gates, K.&L (2016). Maritime Cyber Security. URL: <http://www.cmashipping2016.com/postprogram/Wednesday/Michael%20Neil.pdf>

-Orosz, M., Southwell, C., Barrett, A., Bakir, O., Chen, J., Maya I. (2009). PortSec: Port Security Risk Management and Resource Allocation System. *12th IFAC Symposium on Transportation Systems*, Redondo Beach, CA, USA, September 2-4

-Parnell, G., et al. (2007). Decision Analysis Tools for Safety, Security, and Sustainability of Ports and Harbors. In book: *Managing Critical Infrastructure Risks*, January 2007 NATO Security through Science Series C: Environmental Security. DOI: 10.1007/978-1-4020-6385-5_13

- Patterson, S.A., Apostolakis, G.E. (2007). Identification of critical locations across multiple infrastructures for terrorist actions. *Reliability Engineering & System Safety*, Vol. 92, No. 9, pp.1183–1203
- Raymond, C.Z., Morriën, A. (2008). Security in the Maritime Domain and Its Evolution Since 9/11. In Rupert Herbert-Burns, Sam Bateman and Peter Lehr (eds), *Lloyd's MIU Handbook of Maritime Security* (CRC Press, London 2008) 3
- Reniers, G. (2011). Security of multimodal dangerous freights: the way forward. In Guarascio, M., Reniers, G., Brebbia, C.A., Garzia, F. (eds.), *Safety and Security Engineering*, pp. 327 – 335
- Rowbothan, M. (2014). *Introduction to Marine Cargo Management*, Lloyd's Practical Shipping Guides, Informa Law from Routledge, 2nd ed.
- Pristrom, S., Li, K., Yang, Z., Wang, J. (2013). A study of maritime security and piracy. *Maritime Policy & Management* 2013 Vol. 40, No. 7, 675–693
- Pristrom, S., Yang, Z., Wang, J., Yan, X. (2016). A novel flexible model for piracy and robbery assessment of merchant ship operations. *Reliability Engineering and System Safety* 155 (2016) 196-211
- Prodan, T. (2017). Maritime Terrorism and Resilience of Maritime Critical Infrastructures. *National Security and the Future* 1-2 (18)
- Psarros, G., Rolf, S., Magnus, E. (2009). The acceptability of maritime security risk. *J Transp Secur* (2009) 2:149–163
- Reason, J. (1990). The Contribution of Latent Human Failures to the Breakdown of Complex Systems. *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences*. 327 (1241): 475–484. Bibcode:1990RSPTB.327.475R. doi:10.1098/rstb.1990.0090. JSTOR 55319. PMID 1970893
- Rheinboldt, P. (2014). Bow-tie Risk Analysis. Instituto des Enginieros de Minas di Peru, DNV, Business Assurance, 02 Dec. 2014. URL: <https://www.slideshare.net/PeruminOficial/0910-paulorheinbolt>
- Risk Review* (2018). Cyber security risk assessments: using bowtie analysis with ISO 27000. URL: <https://www.meercat.com.au/risk-management-blog/risk-management-news/cyber-risk-assessments-bowtie-analysis/>
- Ruspini, E., Lowrance, J. (1992). Understanding Evidential Reasoning. *International Journal of Approximate Reasoning* 1992; 6:401-424
- Safety4Sea* (2017). Rethinking maritime security. 25 October 2017. URL: <https://safety4sea.com/rethinking-maritime-security-2/>
- Saunders, B. (2016). Maritime Cyber Security - Threats and Opportunities. Maritime Lead, Transport Cyber Security Practice, nccgroup, URL:

https://www.ahcusa.org/uploads/2/1/9/8/21985670/maritime_cyber_security__threats_and_opportunities.pdf

-Schneider, D. (2020). *An Introduction to Programming Using Visual Basic*, 11th ed. Pearson Education, Inc., Greek language edition: Psaromiligos, J., Lazakidou, A., Dermatis, Z. (editors), (2020), Broken Hill Publishers Ltd, Nicosia

-Skjong, R., Vanem, E., Endresen, Ø. (2007). Risk evaluation criteria. Technical report. Safedor -D-4.5.2-2007-10-24-DNV-RiskEvaluationCriteria-rev-3.0., URL: <http://www.safedor.org/resources/SAFEDOR-D-04.05.02-2005-10-21-DNVRiskEvaluationCriteria-rev-3.pdf>

-Srivastava, R. (2010). An Introduction to Evidential Reasoning for Decision Making under Uncertainty: Bayesian and Belief Functions Perspectives. *International Journal of Accounting Information Systems*, Vol. 12: 126–135

-*The State of Maritime Piracy 2013* (2014). One Earth Future, Broomfield CO, USA

-*The State of Maritime Piracy 2014* (2015). One Earth Future, Broomfield CO, USA

-*The State of Maritime Piracy 2015* (2016). One Earth Future, Broomfield CO, USA

-*The State of Maritime Piracy 2016* (2017). One Earth Future, Broomfield CO, USA

-*The State of Maritime Piracy 2017* (2018). One Earth Future, Broomfield CO, USA

-*The State of Maritime Piracy 2018* (2019). One Earth Future, Broomfield CO, USA

-*The State of Maritime Piracy 2019* (2020). One Earth Future, Broomfield CO, USA

-Threat Analysis Group (2019). Threat, vulnerability, risk – commonly mixed up terms. TAG, URL: <https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/>

-Talley, W.K., Rule, E.M. (2008). Piracy in shipping. In: Talley, W.K. (ed), *Maritime safety, security and piracy*, Informa, London, pp 89–101

-UK Regulatory Impact Assessments: 1st July to 31st December 2004 (2004). Presented to Parliament by the Minister for the Cabinet Office, May 2005

-United Nations (2008). *General Assembly Resolutions*

-*UNODOC* (2015). World Drug Report. URL: <http://www.unodc.org/wdr2015/>

-US Maritime Transportation Security Act of 2002 (2002). Protecting America's Ports, Homeland Security

- US Navy (2007). US Marine Corps, US Coast Guard. *The Commander's Handbook on the Law of Naval Operations* (July 2007)

- Xu, D.-L. (2012). An introduction and survey of the evidential reasoning approach for multiple criteria decision analysis. *Ann Oper Res* (2012) 195:163–187
- Yang J.B., Xu D.L. (2002). On the evidential reasoning algorithm for multiple attribute decision analysis under uncertainty. *IEEE Transactions on Systems, Man and Cybernetics Part A: Systems and Humans*, 32 (3): 289–304
- Yang, Z. (2014). Formal security assessment-new approaches to maritime security risk quantification. *International Association of Maritime Economics Conference 2014 (IAME2014)*, July 15–18, Norfolk, USA.
- Yang, Z., Bonsall, S., Wang, J. (2009). Use of fuzzy evidential reasoning in maritime security assessment. *Risk Anal.*, 29, 95–120.
- Yang, Z., Bonsall, S., Wang, J. (2010). Facilitating Uncertainty Treatment in the Risk Assessment of Container Supply Chains. *Journal of Marine Engineering and Technology*, A17, 23–36.
- Yang, Z., Ng, A., Wang, J. (2013). Prioritizing security vulnerabilities in ports. *Int. J. Ship. Transp. Logist.*, 5, 622–636.
- Yang, Z., Ng, A., Wang, J. (2013b). A new risk quantification approach in port facility security assessment. *Transportation Research A* 59, 72–90
- Yang, Z., Ng, A., Wang, J. (2011). Incorporating Quantitative Risk Analysis in Port Facility Security Assessment. *International Association of Maritime Economics Conference 2011 (IAME2011)*, Santiago, October 26–28.
- Yang, Z., Qu, Z., (2016). Quantitative maritime security assessment: a 2020 vision. *IMA Journal of Management Mathematics* (2016) 00, 1–18
- Yang, Z. & Wang, J. (2009). Quantitative Analysis of Maritime Security Assessment in ISPS. *European Safety and Reliability Association Conference 2009 (ESRELO9)*, 7–10 September, Prague: Czech Republic.
- Yang, Z., Wang, J., Ng, A. (2016). Toward Robust Management of Maritime Risk and Security. In *Dynamic Shipping and Port Development in the Globalized Economy*, pp 122-149, Palgrave Macmillan UK
- Yeo, G.T., Pak, J.Y., Yang, Z. (2013). Analysis of dynamic effects on seaports adopting port security policy. *Transportation Research A* 49, 285–301