LIVERPOOL JOHN MOORES UNIVERSITY

LJMU Research Online

Yang, ZL and Qu, Z

Quantitative maritime security assessment: a 2020 vision

http://researchonline.ljmu.ac.uk/id/eprint/7317/

Article

Citation (please note it is advisable to refer to the publisher's version if you intend to cite from this work)

Yang, ZL and Qu, Z (2016) Quantitative maritime security assessment: a 2020 vision. IMA Journal of Management Mathematics, 27 (4). pp. 453-470. ISSN 1471-678X

LJMU has developed **LJMU Research Online** for users to access the research output of the University more effectively. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LJMU Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain.

The version presented here may differ from the published version or from the version of the record. Please see the repository URL above for details on accessing the published version and note that access may require a subscription.

For more information please contact researchonline@ljmu.ac.uk

http://researchonline.ljmu.ac.uk/

Quantitative maritime security assessment: a 2020 vision

Abstract
Maritime security assessment is moving toward a proactive risk-based regime. This opens the way for security analysts and managers to explore and exploit flexible and advanced risk modelling and decision making approaches in maritime transport. In this article, following a review of maritime security risk assessment, a generic quantitative security assessment methodology is developed. Novel mathematical models for security risk analysis and management are outlined and integrated together to demonstrate their use in the developed framework. Such approaches may be used to facilitate security risk modelling and decision making in situations where conventional quantitative risk analysis techniques cannot be appropriately applied. Finally, recommendations on further exploitation of advances in risk and uncertainty modelling technology are suggested with respect to maritime security risk quantification and management.

Keywords: quantitative security assessment, maritime risk, risk quantification, port security, maritime transport, maritime security.

1. Introduction

In the post 9/11 era, anti-terrorism challenges have been seen from air transportation to maritime supply chains for rationalising the use of limited security resources to avoid the risks of terrorists attacking ships or hijacking them to attack other maritime infrastructure/assets such as ports. Maritime security issues have been clearly pushed to the forefront of the international agenda consecutively in the past decade, attracting active endeavour to improve security records through a culmination of a number of initiatives, research developments, regulations and innovations (Yang et al., 2014). Despite such developments, security studies, particularly those in scientific areas persistently occupied a backseat role within the risk literature being overwhelmed by other aspects involving safety (e.g. Zhang et al., 2016; Montewka et al., 2010), reliability (de Almeida et al, 2015; Wang 2010) and maintenance (Vu et al., 2015; Marquez et al, 2013). Furthermore, previous security research in the maritime sector is often presented piecemeal, wanting an integrated framework to accommodate them in a systemic manner for realising cost effective maritime security policy making. Furthermore, developments such as the International Ship and Port Facility Security (ISPS) Code proposed by the International Maritime Organisation (IMO), requiring security risk assessment and security level categorizing, usually incorporated little, if any, quantitative analysis, with analysis carried out largely based on professional experiences with high uncertainties. If the security assessment cannot be quantitatively assessed using mathematical modelling, the established security management system does not motivate industrial professionals for its implementation, possibly because their effects are not visible in a state-of-the-art risk assessment (Yang et al., 2014). Therefore, a significant research gap needs to be urgently filled, particularly when taking into account the significant benefits of the adoption of the formal safety assessment (FSA) methodology by the IMO in improving safety at sea.

With this in mind, this paper aims to propose a new conceptual methodology of maritime security assessment in which risks are addressed in a comprehensive and cost effective manner. Success in addressing this methodological issue will provide a paradigm shift in maritime security assessment and management and will advance the state-of-the-art to a point where robust quantitative security assessment is feasible. This study draws together pioneering research on security quantitative analysis, expertise in the use of mathematical modelling alongside maritime safety, and innovative use of economic evaluation in security management. The development of a quantitative maritime security

assessment (QMSA) methodology will promote the standardisation of the current diversified practices and standards regarding "secured" facilities from different states around the world. Furthermore, QMSA will also represent a fundamental maritime safety and security cultural change from a largely reactive regime to one which is proactive and soundly based upon the quantification of risk.

To tackle the above research challenges, in this paper, following a brief review of the current status of maritime security assessment, a conceptual QMSA methodology is generated by incorporating FSA into maritime security context. Novel mathematical risk modelling and decision-making approaches are then outlined to demonstrate their use in QMSA. Such approaches are presented on the basis of pioneering risk modelling research using uncertainty methods such as fuzzy logic, Bayesian networks, evidential reasoning and system dynamics, etc. Finally, recommendations on further exploitation of advances in technology are suggested with respect to risk based security decision making, particularly in situations where conventional risk analysis methods cannot be appropriately applied due to a high level of uncertainty in failure data.

2. **Literature review on maritime security assessment**

Maritime security studies as a new dimension of enhancing maritime safety are attracting growing attention from the international society. Maritime safety accidents are unintentional, while maritime security incidents are intentional. Although all of them may have the same risk outcomes – injuries and property damage--they are quite different in nature, thus leading to significant variations in the approaches for analysing them. Specifically, maritime safety relies on analysis of hazards. A hazard is a physical situation with the potential of human injury, property damage and damage to the environment. Maritime security risks are based on threats, which are defined as action or potential action with the potential of human injury, property damage and damage to the environment (Yang *et al.*, 2009b). The difference between hazard and threat definitions manifests itself in that hazard-based risks are more likely to be quantified with mechanistic probability distributions, while the threat-based are closely connected to behavioural probability distributions. Thus, the understanding of hazard-based risks may come from objective historical accident statistics, while threat-based may better be described and presented using expert judgements based on human knowledge and experience as well as objective data if available. Consequently, threat-based risks, which are inherently difficult to quantify may tend to be expressed in vague or qualitative terms. It is due to this reason that maritime security research in the literature largely focuses on qualitative analysis for addressing risk mitigation measures without appropriately quantifying risks of the threats. An analysis of 423 maritime security journal papers published from 2000 to 2016 on web of science indicates that majority of them address maritime security effort from political (e.g. de Nevers, 2015; Papa, 2013) , economic (e.g. Lewis, 2016; Hastings and Phillips, 2016) and cultural (e.g. Akrus et al., 2016) aspects, leaving few looking at the quantification of maritime security risks (Yang et al., 2009a; 2009b; 2010; 2013a; 2014; Yeo et al., 2013; Dabrowski et al., 2015). This analysis apparently reveals 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. Incorporating FSA in maritime security studies may provide a feasible solution to the challenge (Yang et al., 2013b).

2.1. Formal safety assessment

FSA has as its objectives the development of a framework of safety requirements for shipping in which risks are addressed in a comprehensive and cost effective manner. To achieve the above objectives, the IMO's guidelines on the application of FSA recommends a five-step approach, consisting of (IMO, 1997b):

1. Hazard identification
2. Risk estimation

3. Risk control options
4. Cost benefit analysis
5. Recommendations for decision making.

In recent years, research activities have taken place to improve ship design and operation. In the context of FSA, the following research findings, a selected list, have been reported (Yang et al., 2008):

1. Trial study on high-speed craft (IMO, 1997a).
2. Trial study on bulk carriers (IMO, 1998a; IMO, 2002a; IMO, 2002b).
3. Trial study on passenger RO-RO vessels with dangerous goods (IMO, 1998b).
4. Its (FSA) application to fishing vessels (Loughran *et al.*, 2003).
5. Its application to offshore support vessels (Sii, 2001).
6. Its application to cruising ships (Lois, 2004).
7. Its application to ports (Trbojevic, 2002).
8. Its application to containerships (Wang and Foinikis, 2001; Gerigk, 2007).
9. Its application to liner shipping (Yang *et al.*, 2005).
10. Its application to LNG ships (Vanem *et al.*, 2008).

Although showing much attractiveness, the methodology still reveals some problems in its practical applications. Those significant deficiencies derived from Psarafits (2012) and Yang and Wang (2008) include unavailable failure data, floating risk criteria, unjustified expert options, different values of human lives in cost benefit analysis and difficulties of integrating hazard screening throughout the FSA analysis, etc. (Yang et al., 2013b). Applying FSA in maritime security clearly requires risk modellers and assessors to appropriately address such deficiencies and to ensure the newly developed QMSA is adaptive to integrating various risk modelling and decision making techniques that are available in the current literature or to be developed in future.

2.2. Security risk assessment

With the nearly infinite number of attack scenarios and the persistent nature of the threats, choosing the best anti-terrorism efforts is however surely a difficult challenge (Dillion et al., 2009). Use of risk assessment has been advocated as the solution to managing security. Previous research of using risk assessment in counter-terrorism security management mainly focused on critical system analysis. The motivation for identifying the critical systems was to prioritize activities and resources on safety and security investments and risk reduction processes (Aven, 2009). Conventional initiatives to identify safety and security critical systems could be classified into two main categories, namely vulnerability analysis and risk models. The former considered a system to be critical if its failure or malfunction might result in severe consequences (Gorman et al., 2004; Latora and Marchiori, 2005; Jonsson et al., 2007). The latter, incorporating the traditional risk and reliability importance measures, defined criticality as the combination of probability and importance (risk contribution) (Jenelius et al., 2006; van der Borst and Schoonakker, 2001). With the presentation of the difficulty of determining probabilities that terrorists would actually exploit a given vulnerability, vulnerability analysis has recently shown a special focus on critical infrastructures (Gheorghe et al., 2006; Johnson, 2007; Patterson and Apostolakis, 2007; Balducelli et al., 2007). However, care has to be taken when using vulnerability alone as a criticality parameter given that it might significantly vary with initiating events (i.e. attack modes) defined differently (Aven, 2009). Consequently, the argument for incorporating probabilities and uncertainty dimension in the core of criticality analysis has been increasingly supported by researchers, though the interpretation of such an argument can be seen in different ways (Willis, 2007; Aven, 2007). Furthermore, the evaluation of the criticality parameters that depend on threat scenarios is a dynamic process. Traditional risk assessment methods, where risk was often described using historical failure data and the occurrence of accidents follows certain rules known/assumed, might not be competent to catch the non-linear relationship between the parameters and to estimate and manage the risks with vague and incomplete data. To address such challenges, new models need to be developed to support the establishment of the QMSA framework.

3. **Development of a novel formal security assessment methodology**

It has been recognized that a framework with a holistic nature is desirable for risk assessment of large engineering systems where appropriate risk modelling and decision-making tools can be selected for use at different stages of the design process and operations (Wang et al., 2006). This is particularly true for maritime security risk assessment given the complexity of maritime transport systems. The scope of maritime transport systems has been expanded from traditional shipping (port to port service) to modern logistics (door to door service) sectors involving transport vehicles (e.g. ships and trucks) and infrastructures (e.g. ports and warehouses) due to market demand and business competition. For instance, a typical door-to-door journey using a shipping container will involve the interaction of approximately 25 different participants, generate 30-40 documents, use 2-3 different modes and be handled at as many as 12-15 physical locations (OECD, 2003). A new QMSA methodology is proposed to integrate several studies focusing on maritime security risk quantification and safety management, consisting of (Yang, 2014a; Yang et al., 2014c):

1. Identification of threats and vulnerabilities (Yang et al., 2013a)
2. Subjective security risk estimation (Yang et al., 2009b)
3. Security risk mitigation and protection (Yang et al., 2010)
4. Security cost and benefit analysis (Yang et al., 2009a)
5. Dynamic security-economic evaluation (Yeo et al., 2013)
6. Security inspection and maintenance (Yang et al., 2014b)

In the initial stages of security risk assessment, threats and vulnerabilities needs to be identified as a pair and evaluated/screened in situations where a high level of uncertainty is associated with the estimates of probabilities and consequences due to incomplete data. An extended Analytical Hierarchy Process (AHP) approach (Yang et al., 2013a) is more appropriately used for the estimates where expert judgments may need to be used with confidence for conducting comparison instead of isolated evaluations. Once the threats and vulnerabilities of high security risks are screened, more precise quantitative risk assessment needs to be carried out with the introduction of detailed risk parameters in the model. A fuzzy evidential reasoning approach (Yang et al., 2009b) shows that to achieve a solution it is feasible to incorporate multiple risk parameters in security analysis and to infer the risk reasoning from input parameters to output security estimates. Such a method is best applied in situations where there is a nonlinear relation between input risk parameters and output security estimates and there is incomplete data to configure the evaluations with respect to the risk parameters. The use of fuzzy evidential reasoning enables to distinguish the pairs of threats and vulnerabilities that have the same/similar risk screening results from the extended AHP approach. Furthermore, it provides an opportunity for exploring root causes contributing to the risk parameters in a hierarchy using a top down approach and therefore of exploiting appropriate risk control measures (RCMs) with respect to the root causes. It is crucial to have a robust security inference mechanism capable of testing the effectiveness of each RCM in real time in terms of its capability of reducing security risk of the investigated threats and vulnerabilities. A new risk inference method using Bayesian networks (BNs) is therefore proposed to address this research challenge. Furthermore the BN can be used to model the interdependency of the cost and benefit attributes when selecting the most cost effective RCM using Technique for Order Preference by Similarity to an Ideal Solution (TOPSIS). Security management is a dynamic process, in which the fitness of the selected RCMs based on static security assessment needs to be further verified to ensure that their implementation will increase the profits while minimising the associated risks. System Dynamics (SD) simulation is used in this process to predict the right security level at which profits can be maximised. Finally, key security performance indicators (KSPIs) are developed for facilitating the standardisation of security auditing and creating a self-assessment tool for security managers to benchmark their security performance in a long term.

4. Mathematical modelling – the new development of maritime security risk analysis

All the methods described above and their associated mathematical models detailed in the relevant publications in the above six steps are integrated in the QMSA that forms a general structure to facilitate security risk-based operations of large and complex marine systems. It is still worth bearing in mind the fact that these techniques are still in their infancy and are not yet universally used in industries, although the use of some models such as SD and KSPIs in real cases evidenced that both security managers and decision makers can benefit from the potential of these approaches for security risk modelling and decision making in certain situations. To further improve the adaptation of QMSA in the maritime industry, new security risk analysis methods are developed to deal with the following research challenges.

- How to rationalise the security risk analysis based on subjective evaluations?
- How to synthesise the internal security risks and external security criticality for optimising security management from component to system levels?

4.1 Analysis of security risks of independent components in maritime transport systems

Pioneering research on QMSA (e.g. Yang et al., 2009b) reveals that linguistic variables are often used to tackle the unavailability or incompleteness of objective security risk data. Detailed risk parameters are defined using fuzzy logic due to the subjectivity of the input data. The threat-based risk parameters used to define subjective security estimates include those at both senior and junior levels. The senior parameter is "*Security estimate (SE)*", the single fuzzy output variable, which can be defuzzified to prioritise the risks. The variable is described linguistically and is determined by some junior parameters. In risk assessment, it is common to express a security risk level by degrees to which it belongs to such linguistic terms as "Poor", "Fair", "Average" and "Good" that are referred to as security expressions. To analyse the junior parameters, four fundamental risk parameters are identified and defined as "*Will*" *(W),* "*Damage capability*" *(D),* "*Recovery difficulty*" *(R)* and "*Damage probability*" *(P)* (Yang et al., 2009b). *W* decides the likelihood of a threat-based risk, which directly represents the lengths one goes to in taking a certain action. To estimate *W*, one may choose to use such linguistic terms as "Very weak", "Weak", "Average", "Strong" and "Very strong". The combination of *D* and *R* responds to the consequence severity of the threat-based risk. Specifically speaking, *D* indicates the destructive force/execution of a certain action and *R* hints the resilience of the system after the occurrence of a failure or disaster. The following linguistic terms can be considered as a reference to be used to subjectively describe the two sister parameters: "Negligible", "Moderate", "Critical" and "Catastrophic" for *D* and "Easy", "Average", "Difficult" and "Extremely Difficult" for *R*. *P* means the probability of the occurrence of consequences. It can be defined as the probability that damage consequences happen given the occurrence of the event. One may choose to use linguistic terms such as "Unlikely", "Average", "Likely" and "Definite" to describe it.

The defined senior and junior risk parameters can be modelled by using a fuzzy *IF-THEN* rule base system for security risk estimates. For example, the following is a fuzzy *IF-THEN* rule: *IF W* of a threat is "Very strong" AND *D* is "Catastrophic" AND *R* is "Extremely difficult" AND *P* is "Definite", *THEN SE* is "Poor". Obviously, a *IF-THEN* rule in this study has two parts: an antecedent that responds to the fuzzy input and a consequence, which is the result/fuzzy output. In classical fuzzy rule-based systems, such input and output are usually expressed by single linguistic variables with 100% certainty and the rules constructed are also always considered as single output cases. However, when observing realistic maritime security situations, the knowledge representation power of the fuzzy rule systems will be severely limited if only single linguistic variables are used to represent uncertain knowledge. Given a combination of input variables, *SE* may belong to more than one security expression with appropriate belief degrees. For example, a fuzzy rule with certain degrees of belief can be described as: *IF W* of a threat is "Very strong" AND *D* is "Catastrophic" AND *R* is "Extremely difficult" AND *P* is "Likely", *THEN SE* is "Poor" with a belief degree of 0.9, "Fair" with a belief degree of 0.1, "Average" with a belief degree of 0 and "Good" with a belief degree of 0. It is

noted that all the parameters and the belief degrees of the rules are usually assigned at the knowledge acquisition phrase by multiple experts on the basis of subjective judgements. In order to model general and complex uncertain problems in security assessment, classical fuzzy rule-based systems are extended to assign each rule a degree of belief. Assume that the four antecedent parameters, *W*, *D*, *R* and *P* can be described by linguistic variable A_{iJ_i}, where i=1, 2, 3, or 4 respectively and J_1 = 1, …, or 5, J_2, J_3 and J_4 = 1, …, or 4. One consequent variable *SE* can be described by 4 linguistic terms, D_1, D_2, D_3 and D_4. Let $A_{iJ_i}^k$ be a linguistic term corresponding to the i^{th} parameter in the k^{th} rule, with i=1, 2, 3 and 4. Thus, the generic k^{th} rule in the rule base can be defined as follows:

R_k: IF *W* is $A_{1J_1}^k$ AND *D* is $A_{2J_2}^k$ AND *R* is $A_{3J_3}^k$ AND *P* is $A_{4J_4}^k$, THEN *SE* is D_1 with a belief degree of $\beta^1{}_k$, D_2 with a belief degree of $\beta^2{}_k$, D_3 with a belief degree of $\beta^3{}_k$ and D_4 with a belief degree of $\beta^4{}_k$. (1)

Once a rule-based system is established, it can be used to perform inference for given fuzzy or incomplete observations to obtain the corresponding fuzzy output, which can be used to assess the security level of the pair of an identified threat and vulnerability from Step 1. During the estimation process, if all the evaluation of the identified pair with respect to each junior parameter is expressed by a single linguistic variable, then a single IF-THEN rule will be employed for security estimate. Risk input is however sometimes described by multiple linguistic variables with respect to a risk parameter. For example, *W* of a defined pair of threat and vulnerability may be evaluated as "Very strong" with a belief degree of 0.5 and "Strong" with a belief degree of 0.5. Multiple rules will be hired in this situation, which requires an advanced method capable of synthesising the rules without losing useful input information. An Evidential Reasoning (ER) approach is well suited to modelling subjective credibility induced by partial evidence and therefore used in the synthesis of relevant rules for security estimates. The kernel of this approach is an ER algorithm developed on the basis of the Dempster-Shafer (D-S) theory, which requires modelling the narrowing of the hypothesis set with the requirements of the accumulation of evidence (Yang and Xu, 2002).

Although attracting much research attention (the most frequently cited journal paper in the subject of maritime security on web of knowledge), the above research work has still revealed problems in its practical applications (Alyami et al., 2014; Qu et al., 2014), mainly including 1) the lack of a rational mechanism to assign degrees of belief in the process of developing fuzzy rule bases and 2) losing advances, visibility and easiness of the conventional risk analysis method due to the complicated calculation involved in the ER algorithm. To overcome such problems, AHP (Saaty, 1980) and fuzzy rule-based Bayesian reasoning (FuRBaR) (Yang et al. 2008) are combined in a complimentary manner, in which the former is employed to rationalised the assignment of degrees of belief in the IF-THEN fuzzy rule base while the latter is applied to simplify the process of rule synthesis.

In the new method, both the junior level (i.e. *W*, *D*, *R* and *P*) and senior level risk parameters (i.e. *SE*) risk level are defined on the same plane of a grade set of {very low, low, medium, high, very high}. The fuzzy rules in Eq. (1) will be converted as follows if the weights of *W*, *D*, *R* and *P* are assigned equally.

R_1: IF *W* is very low AND *D* is very low AND *R* is very low AND *P* is very low, THEN *SE* is very low with a belief degree of 100%, low with a belief degree of 0%, medium with a belief degree of 0%, high with a belief degree of 0% and very high with a belief degree of 0%.
R_2: IF *W* is low AND *D* is very low AND *R* is very low AND *P* is very low, THEN *SE* is very low with a belief degree of 75%, low with a belief degree of 25%, medium with a belief degree of 0%, high with a belief degree of 0% and very high with a belief degree of 0%.

R_3: IF W is medium AND D is very low AND R is very low AND P is very low, THEN SE is very low with a belief degree of 75%, low with a belief degree of 0%, medium with a belief degree of 25%, high with a belief degree of 0% and very high with a belief degree of 0%.
…

If the four junior level risk parameters are assigned different weights using AHP, the belief degrees associated with each grade of SE for all rules are then calculated by using Eq. (2)

$$\beta_i^j = \beta_{Wi}^j \cdot \delta_W + \beta_{Di}^j \cdot \delta_D + \beta_{Ri}^j \cdot \delta_R + \beta_{Pi}^j \cdot \delta_P \quad (2)$$

where i = (1, 2, …, 5) means a grade in the set of {very low, low, average, high, very high}; j is the j^{th} rule in the rule base; β_{Ti}^j (T ∈ (W, D, R or P)) equals one when Ti is presented in the j^{th} rule and otherwise it is zero. Consequently, the development of the rule base with a belief structure can be standardised and rationalised. For example, particular rules can be developed as follows.

R_1: IF W is very low (W_1) AND D is very low (D_1) AND R is very low (R_1) AND P is very low (P_1), THEN SE is very low (SE_1) with a belief degree of 100% ($\delta_W + \delta_D + \delta_R + \delta$), low with a belief degree of 0%, medium with a belief degree of 0%, high with a belief degree of 0% and very high with a belief degree of 0%.
R_2: IF W is low (W_2) AND D is very low (D_1) AND R is very low (R_1) AND P is very low (P_1), THEN SE is very low with a belief degree of ($\delta_D + \delta_R + \delta_P$)%, low with a belief degree of (δ_W)%, medium with a belief degree of 0%, high with a belief degree of 0% and very high with a belief degree of 0%.
R_3: IF W is medium AND D is very low AND R is very low AND P is very low, THEN SE is very low with a belief degree of ($\delta_D + \delta_R + \delta_P$)%, low with a belief degree of 0%, medium with a belief degree of (δ_W)%, high with a belief degree of 0% and very high with a belief degree of 0%.

Such rules can be further expressed in the form of conditional probability as follows.
R_1: Given W_1, and D_1, and R_1, and P_1, the probability of SE_i (i = 1, …, 5) is (1, 0, 0, 0, 0).
R_2: Given W_2, and D_1, and R_1, and P_1, the probability of SE_i (i = 1, …, 5) is ($\delta_D + \delta_R + \delta_P$)%, ($\delta_W$)%, 0, 0, 0).
R_3: Given W_3, and D_1, and R_1, and P_1, the probability of SE_i (i = 1, …, 5) is ($\delta_D + \delta_R + \delta_P$)%, 0, ($\delta_W$)%, 0, 0).

Alternatively, they can be expressed as

$$p(SE|\, W_1, D_1, R_1, P_1) = (1, 0, 0, 0)$$
$$p(SE|\, W_2, D_1, R_1, P_1) = (\delta_D + \delta_R + \delta_P)\%, (\delta_W)\%, 0, 0, 0)$$
$$p(SE|\, W_3, D_1, R_1, P_1) = (\delta_D + \delta_R + \delta_P)\%, 0, (\delta_W)\%, 0, 0) \quad (3)$$

Using a BN technique, the above fuzzy rule base can be modelled and converted into a five-node converging connection. It includes four parent nodes, N_W, N_D, N_R, and N_P (Nodes W, D, R and P); and one child node N_{SE} (Node SE). Having transferred the rule base into a BN framework, the rule-based risk inference for the security risk analysis will be simplified as the calculation of the marginal probability of the node N_{SE}. To marginalize SE, the required conditional probability table of N_{SE}, $p(SE|W, D, R, P)$, can be obtained using (3). Consequently, the marginal probability of N_{SE} can be calculated in Eq. (4).

$$p(SE) = \sum_{k=1}^{5}\sum_{l=1}^{5}\sum_{m=1}^{5}\sum_{n=1}^{5} p(SE\,|\,W_k, D_l, R_m, P_n)\, p(W_k)\, p(D_l)\, p(R_m) p(P_n) \quad (4)$$

where $p(W_k)$, $p(D_l)$, $p(R_m)$ and $p(P_n)$ can be obtained by expert judgements based on the linguistic terms (very low, low, medium, high, very high) or by fuzzy mapping techniques to transfer raw data in different forms into the prior probabilities associated with the linguistic set (Yang et al., 2008).

To prioritize the pairs of threats and vulnerabilities, SE_i (i = 1, …, 5) requires the assignment of appropriate utility values U_{SE}. The utility values can be defined on the basis of the combination of specific fuzzy rules (Yang et al., 2005) and preference numbers through satisfying the following conditions.

1) IF *very low* (W_1), and *very low* (C_1), and *very low* (R_1), and *very low* (P_1), THEN {(*1*, *very low* (SE_1)), (*0*, *low* (SE_2)), (*0*, *medium* (SE_3)), (*0*, *high* (SE_4)), (*0*, *very high* (SE_5))}.
2) IF *low* (W_2), and *low* (C_2), and *low* (R_2), and *low* (P_2), THEN {(*0*, *very low* (SE_1)), (*1*, *low* (SE_2)), (*0*, *medium* (SE_3)), (*0*, *high* (SE_4)), (*0*, *very high* (SE_5))}.
3) IF *medium* (W_3), and *medium* (C_3), and *medium* (R_3), and *medium* (P_3), THEN {(*0*, *very low* (SE_1)), (*0*, *low* (SE_2)), (*1*, *medium* (SE_3)), (*0*, *high* (SE_4)), (*0*, *very high* (SE_5))}.
4) IF *high* (W_4), and *high* (C_4), and *high* (R_4), and *high* (P_4), THEN {(*0*, *very low* (SE_1)), (*0*, *low* (SE_2)), (*0*, *medium* (SE_3)), (*1*, *high* (SE_4)), (*0*, *very high* (SE_5))}.
5) IF *very high* (W_5), and *very high* (C_5), and *very high* (R_5), and *very high* (P_5), THEN {(0 *very low* (SE_1)), (*0*, *low* (SE_2)), (*0*, *medium* (SE_3)), (*0*, *high* (SE_4)), (*1*, *very high* (SE_5))}.
6) The preference degree *PN* of each linguistic term W_k, D_l, R_m or P_n (k, l, m or n = 1, …, 5) is described using a preference fuzzy number in the scale [1, 10], where 1 indicates "minimum risk contribution", and 10 means the "maximum risk contribution". For example, if the five linguistic terms (very low, low, medium, high, very high) are defined using evenly distributed triangular fuzzy membership functions as ((0, 0, 3), (1, 3, 5), (3, 5, 7), (5, 7, 9), (7, 10, 10)), then the crisp PNs of five the linguistic terms are obtained by the centroid defuzzification technique as (1, 3, 5, 7, 9) (Mizumoto, 1995).
7) As a result, the U_{SEi} values (i = 1, …, 5) can be calculated as
   $U_{SE1} = PN(W1) \times PN(D1) \times PN(R1) \times PN(P1) = 1 \times 1 \times 1 \times 1 = 1$
   $U_{SE2} = PN(W2) \times PN(D2) \times PN(R2) \times PN(P2) = 3 \times 3 \times 3 \times 3 = 81$
   $U_{SE3} = PN(W3) \times PN(D3) \times PN(R3) \times PN(P3) = 5 \times 5 \times 5 \times 5 = 625$
   $U_{SE4} = PN(W4) \times PN(D4) \times PN(R4) \times PN(P4) = 7 \times 7 \times 7 \times 7 = 2401$
   $U_{SE5} = PN(W5) \times PN(D5) \times PN(R5) \times PN(P5) = 9 \times 9 \times 9 \times 9 = 6561$

Then a new security risk ranking index for independent components can be developed as

$$RI_{component} = \sum_{i=1}^{5} p(SE_i) U_{SEi} \tag{5}$$

where the larger the value of $RI_{component}$is, the higher the security risk level of the analysed TV pair.

4.2 Synthesis of security risks of dependent components in maritime transport systems

Maritime transport systems (e.g. container supply chains) present a strong networking feature, which is indicated by many transport nodes (e.g. ports) and links (e.g. shipping routes). A system (global) security level therefore relies on both its individual components' (local) risks as well as the security criticality of the interdependent components in the system network. While Section 4.1 addresses the challenge of security risk estimates of individual components based on very little or no data, this section aims to produce new hybrid algorithms to synthesise the security estimates from components to a global system level by taking into account their independency.

Unlike the safety evaluations in quantitative risk analysis, which are precisely expressed by some numerical values (e.g. potential loss of life), the security estimates using fuzzy sets (in Eq. 4) are impossibly synthesized by using normal mathematic logical operations. It is therefore extraordinarily

important to introduce a new method to synthesise the security estimates of the components in a rational way, in which a) the estimated results expressed by linguistic variables can be aggregated without the loss of useful information; b) the estimated results from different experts[1] can be combined effectively; and c) the interdependency among the components can be incorporated logically. An ER approach is well suited to model subjective credibility induced by partial evidence. While ER can provide a powerful tool/solution to the above requirements a) and b), it fails to model the interdepency in c). Consequently, centrality measures (Freeman, 1977 and 1978) are introduced to combine with ER in a complementary manner, in which the former is used to calculate the relative weights/importance of interdependent components in terms of their security criticality (external security influence), while the latter is employed to synthesise the security estimates from local to global levels.

There are many methods for measuring centrality of components to represent their importance in a network system. "Degree centrality" and "betweenness centrality" are among the two most common centrality measures. In risk assessment studies, centrality measures including degree centrality, betweenness centrality and closeness centrality, have been adopted to highlight the critical nodes within a network (Cadini *et al*., 2009; Büttner *et al*., 2013), while betweenness centrality measures are particularly seen in the vulnerability analysis of the most critical links (edges) in the network (Zio *et al*. 2011). It is because of the fact that unlike other measures, betweenness offers a pragmatic way for highlighting the importance of a node in the network. If a node is located in a strategic position of being in the shortest paths connecting many other nodes in the network, the node tends to be in a powerful position for connecting or breaking between other nodes. Therefore betweenness centrality is hired in this study to calculate the security criticality in maritime transport systems.

The concept of betweenness centrality is based on identification of the shortest paths between pairs of components in a system. In a weighted network, the shortest path $[d^w(s,t)]$ is formularized when Newman's (2001) and Brandes (2001) implemented Dijkstra's (1959) algorithm to binary network analysis definition as follows:

$$d^w(s,t) = min\left(\frac{1}{w_{sr}} + \cdots + \frac{1}{w_{rt}}\right) \tag{6}$$

where r represents intermediary components on paths between components s and t when indirect connections are considered. The shortest path between s and t, $d^w(s,t)$ in a weighted network could be identified by minimizing the sums of the reciprocals of the weighted links w_{sr} between s and t through different in-between component r. The weighted links are determined by the associated throughputs passing through the links in the investigated maritime transport network.

Therefore, betweenness centrality within a weighted maritime transport network can be simplified with reference to Freeman (1978) as follows:

$$C_B^w(s) = \frac{g_{tu}^w(s)}{g_{tu}^w} \tag{7}$$

where g_{tu}^w is the number of the weighted shortest paths between components t and u, and $g_{tu}^w(s)$ is the number of those paths that pass through focal component s. Consequently, $C_B^w(s)$ can be used as the relative weight of component s when synthesising its security estimate with the ones from other components.

To capture the non-linear relationship between security estimates of components, the ER approach (Yang and Xu, 2002) is used to combine the security estimates from all components and generate a

[1] In complex security critical systems, risk based decisions are usually made by a group of decision makers and stakeholders.

final conclusion. The security estimate results in Eq. (4) are presented in probabilities, while ER is based on the belief theory. To minimise the possible conflicts between subjective probabilities and degrees of belief, the result from Eq. (4) can be transferred back and expressed by degrees of belief through an opposite operation of Eq. (3). It means that the security estimate of the s^{th} component $p^s(SE_i)$ can be expressed as β_i^s, $i = 1, 2, \ldots, 5$, $s = 1, 2, \ldots,$ or V, where V means the total number of the components in the transport system. Having represented belief degree distributions β_i^s, the *ER* approach can be implemented as follows.

First, it is required to transform the degrees of belief β_i^s for all $i = 1, 2, \ldots, 5$, $s = 1, 2, \ldots, V$ into basic probability masses using the following equations (Yang and Xu, 2002; Liu *et al.*, 2004):

$$m_i^s = \theta_s \beta_i^s,$$

$$m_{SE}^s = 1 - \sum_{i=1}^{5} m_i^s = 1 - \theta_s \sum_{i=1}^{5} \beta_i^s,$$

$$\overline{m}_{SE}^s = 1 - \theta_s,$$

$$\tilde{m}_{SE}^s = \theta_s \left(1 - \sum_{i=1}^{5} \beta_i^s\right), \text{ for all } i = 1, 2, \ldots\ldots, 5 \text{ and } s = 1, 2, \ldots, V.$$

where m_i^s are individual degrees to which the SE_i of each component s supports the final synthesised conclusion SE; θ_s represents the relevant importance of component s and thus, $\theta_s = \dfrac{C_B^w(s)}{\sum_{s=1}^{V} C_B^w(s)}$ (from Eq. (7); and $m_{SE}^s = \overline{m}_{SE}^s + \tilde{m}_{SE}^s$ for all $s = 1, 2, \ldots, V$. The probability mass of m_{SE}^s unassigned to the final synthesised conclusion SE, which is unassigned to any individual output variables, is split into two parts, one caused by the relative importance of the s^{th} component ($\overline{m}_{SE}^s$), and the other due to the incompleteness of the belief degree assessment β_i^s ($\tilde{m}_{SE}^s$).

Then, it is possible to aggregate all the output from s ($s = 1, 2, \ldots, V$) to generate the combined degree of belief (β_i) in each possible SE_i of SE. Suppose $m_i^{I(s)}$ is the combined belief degree in SE_i by aggregating all the output from the s components and $m_{SE}^{I(s)}$ is the remaining belief degree unassigned to any SE_i. Let $m_i^{I(1)} = m_i^1$ and $m_{SE}^{I(1)} = m_{SE}^1$. Then the overall combined belief degree in SE_i is generated as follows (Liu *et al.*, 2004).

$$\{SE_i\}: \; m_i^{I(s+1)} = K_{I(s+1)}[m_i^{I(s)} m_i^{s+1} + m_i^{I(s)} m_{SE}^{s+1} + m_{SE}^{I(s)} m_i^{s+1}]$$

$$m_{SE}^{I(s)} = \tilde{m}_{SE}^{I(s)} + \overline{m}_{SE}^{I(s)} \qquad s = 1, 2, \ldots\ldots, V-1$$

$$\{SE\}: \; \tilde{m}_{SE}^{I(s+1)} = K_{I(s+1)}[\tilde{m}_{SE}^{I(s)} \tilde{m}_{SE}^{s+1} + \tilde{m}_{SE}^{I(s)} \overline{m}_{SE}^{s+1} + \overline{m}_{SE}^{I(s)} \tilde{m}_{SE}^{s+1}]$$

$$\overline{m}_{SE}^{I(s+1)} = K_{I(s+1)}[\overline{m}_{SE}^{I(s)} \overline{m}_{SE}^{s+1}]$$

$$K_{I(s+1)} = \left[1 - \sum_{i=1}^{5} \sum_{\substack{y=1 \\ y \neq i}}^{5} m_i^{I(s)} m_y^{s+1}\right]^{-1}, \; s = 1, 2, \ldots, V-1$$

$$\{SE_i\}: \beta_i = \frac{m_i^{I(V)}}{1 - \overline{m}_{SE}^{I(V)}} \; (i = 1, 2, \ldots, 5)$$

$$\{D_j\}: \; \beta_D = \frac{\tilde{m}_D^{I(L)}}{1 - \overline{m}_D^{I(L)}}$$

where β_i indicates the normalised belief degree assigned to SE_i in the final synthesised conclusion SE and β_{SE} represents the normalised remaining belief degree unassigned to any SE_i. For a benchmarking purpose, a system security risk ranking index can be developed as

$$RI_{system} = \sum_{i=1}^{5} \beta_i U_{SEi}$$

where the larger the value of RI_{system} is, the higher the risk level of the investigated system.

5. A Vision to 2020 – future research challenges in QMSA

To further support the development and implementation of the six-step QMSA methodology (in Section 3), several challenging research questions apart from those mentioned in Section 4 need to be further investigated. First of all, the large number of potential attack scenarios and control options makes it difficult to evaluate portfolio effects of security measures. A new risk evolution model looks promising to address maritime security by designing different protective, detective and corrective (PDC) modes. Security critical systems will be initially identified and assessed in the protective mode. Such initial analysis as a basis can be extended to develop a scenario-based risk model which can produce an updated criticality result with newly available information from dynamic environments in the detective mode. The updated result will be used to select the best control measures in the corrective mode. All the relevant information in this analysis process, such as the one associated with risk scenario(s) and the corresponding mitigation measure(s), will be recorded in a "live" database. Relevant work should study maritime security management strategies in terms of operational practices, the characteristics of the operations, the availability of data for risk assessment and the cost benefit analysis. A survey should be conducted to investigate what management strategies in allocation of resources, inspection/maintenance strategies and response actions, etc. are currently being used, why they were chosen and the scope for further improvement. All the managerial and operational processes will be studied together with the characteristics of security operations, the type of equipment used, the procedure followed and the current strategies adopted. The requirement for an advanced quantitative risk-based framework will also be investigated in detail with an aim of improving the current maritime security practices. Piracy incidents in the records in the public domain should be analysed in terms of threat likelihood, consequences, attack modes and the ways of preventing them in the context of ship operations. Potential security failures involving terrorists' hijackings of vessels will be studied using the above analysis as a basis. A new attractiveness index should be developed with more relevant information/input (type of vessels, state of flag, location) to update such failure studies in a Bayesian way. The updating will entail extensive interaction with industrial stakeholders including questionnaire surveys, interview of marine masters and security officers, and analysis of historical accidents. The cost benefit will also be investigated in terms of maritime security managerial and operational strategies. In many situations, the quantification of this analysis may be difficult because the accurate costs and benefits of adopting a mitigation measure may not be well known unless it has been used for a period of time. Carefully designed questionnaires should be used to elicit security officers' and experts' opinions to obtain data needed for analysis.

Secondly, the framework should be practical (considering the limitations associated with maritime security operations) and effective. It should be capable of dealing with the risk associated with each operational strategy in terms of various criteria such as response time, operational cost and the level of risk and capable of accommodating a "live" database with which the models can be updated as more data is collected with time. The benchmarking and strategic quality control methodologies should be further investigated to enhance the proposed framework towards a self-assessed and self-motivated interactive security management regime. The key steps in the two methodologies, together with their significance and applicability to maritime security operations will be carefully investigated, including security vision, performance process analysis, threat identification and screening, risk estimation and criticality analysis, risk control, cost benefit analysis, decision making, monitoring

and verification. The updating of such a framework will depend on the success of the following research focuses:

1. Development of an "as high as reasonably practical (AHARP)" security performance measurement scheme where two boundaries, the highest and the lowest, will be set up using utility theory to model the status of the criticality parameters with reference to the implemented security regulations. Any performance better than the highest boundary is "desirable", which means that the risk is tolerable. Any performance worse than the lowest boundary is "unacceptable", which means that the risk has evolved to a corrective mode, requiring appropriate control measures to be selected and employed immediately. The performance between them requires to be AHARP, which means that the risk is kept in a protective mode and should be optimally minimised within a cost constraint.
2. Pairwise investigation of vulnerabilities and threats. The criticality of the vulnerabilities varies when facing different threats. Vulnerabilities will be identified from the multiple levels of asset and infrastructure, person, organisation and environment. For each vulnerability identified, the relevant threats will be analysed and its criticality will be prioritised with regard to these threats. In this process, new criticality parameters will be defined in a hierarchy using a top-down approach. Evaluations of the bottom level parameters will be synthesised to calculate criticality values, which can be benchmarked using the two boundaries in the AHARP scheme for selecting appropriate risk control models.
3. Design of a self-assessed and self-motivated security management tool. Given that anti-terrorism security management is a dynamic process, a slight change of the bottom level criticality parameter evaluation could lead to the selection of different countermeasures. Effective monitoring will therefore be necessary, enabling the construction of a "live" database, which can record and store a large amount of observable information associated with threats, vulnerabilities, the corresponding criticality analysis and countermeasures. By doing so, the stakeholders can continuously assess their system security performance against the boundaries in the AHARP scheme. A sound performance measurement loop in the security quality control process will be formed. The information in the database will be processed and regularly updated with more data obtained.

Thirdly, it is noteworthy that the success of the proposed framework is heavily influenced by the appropriate treatment of uncertainties. Therefore, particular attention will also be paid to the development of supporting models rationally dealing with fuzziness, incompleteness and randomness encountered in criticality analysis and decision making processes, In these circumstances a rational subjective model should be developed which is capable of incorporating expert judgements to compensate the incompleteness caused by the limited historical data. In this model, the advantages of the individual approaches involved will be explored and used in a hybrid manner to estimate the criticality of each vulnerability with respect to different threats under uncertainties. Belief fuzzy rule bases will be established to model the non-linear relationship between criticality parameters at a parent-children cluster in the hierarchy. The introduction of belief structures to fuzzy rule bases will assist in modelling not only fuzziness but also incompleteness when using expert knowledge. Bayesian reasoning will be used to conduct rule-based inference from the lower level parameters to the upper level ones in the cluster. The experience gained from the previous studies (Yang et al., 2008; 2009a; 2009b; 2009c) indicates the feasibility and potential of using fuzzy logic, Bayesian reasoning and their combination in security assessment and management. However, the original models developed have only been employed to analyse the security estimation of systems at a local component level subject to a static status. More importantly, degrees of belief assigned to each rule in the fuzzy rule bases require to be complete (equalling to 100%). More powerful tools by combining ER and Bayesian reasoning should be investigated to deal with the incompleteness of probabilities in BNs.

Fourthly, it will be a fresh challenge to develop a new comprehensive suite of mathematical models, which is capable of dealing with interdependences between multiple-level security parameters and between different vulnerabilities and capable of taking into account the security criticality of components from a global systematic perspective. In this investigation, the feasibility of adopting evidential reasoning based on Dempster-Shafer theory and centrality theory tackle the security criticality of different vulnerable parts in a system will be researched. The potential of using centrality measures to adjust the relative weights of security critical components subjectively assigned and to reduce the bias in measuring the importance of the components in an interactive environment will also be exploited.

Fifthly, many maritime security measures are not mandatory and this may leave maritime stakeholders to choose and define their "suitable" security strategies and polices which could be less strict than it should be for an economic purpose. Even though many companies are willing to implement some of the measures, it may be difficult to realise the optimal allocation of their limited available resources given that appropriate decision mechanisms may be required at different operational stages of the security practice. Having analysed the criticality of vulnerabilities, for those "unacceptable" risks, future work can produce security control measures relating to the fundamental type of risk reduction, the type of actions required and the confidence that can be placed in the measures. All risk reduction measures with the aim of reducing the likelihood of threats and/or mitigating their possible effects and consequences will be identified on the basis of the bottom level security parameters. In the first stage of implementing a risk-based regime, a set of finite operational options may be developed. The criteria used for selecting the most favourable ones may include response time, corrective cost and risk reduction, etc. In situations where the decision making process has to take place using incomplete information, a rational subjective risk-based approach capable of accommodating quantitative and qualitative data is more appropriate and thus will be developed to estimate the degree of preference associated with each operational option. The best options with the highest preference degree can then be chosen with respect to the particular requirements of the criteria (i.e. the reduction of the risk to the AHARP level).

As more and more security measures are implemented and security performance is improved, it reaches a stage where the criticality levels of all vulnerabilities are moving back to the AHARP region. In this situation, no specific vulnerability will be targeted to produce finite control measures. The practical anti-terrorism effort often requires the system security performance to be optimally maintained (i.e. the maximal risk reduction from a systematic viewpoint) using a limited available budget (within a cost constraint). Meanwhile, information produced in the best option selection process above is accumulated for carrying out risk-based multi-objective optimisation using the functions of describing the relationship between cost, time and risk associated with individual vulnerabilities. For instance, the frequency of security patrols to an asset or a piracy prone area will influence the presentation of the associated cost and risk. Influence differs from one asset/area to another. An optimisation modelling approach will be developed to deal with such a model of multiple objectives including risk, response time and cost. Risk, for example, can be minimised within the technical and economic constraints.

6. Conclusion

The security culture in the maritime industry has been changed over the last decades, moving from a reactive regime towards a proactive scheme. It is partially demonstrated by the implementation of the ISPS Code. Such a change gives more flexibility to maritime security analysts to employ the latest risk modelling techniques and decision making tools when they make security policies and strategies. It is therefore beneficial to explore, exploit and apply the advances that have been developed in general safety and reliability engineering in the context of maritime security assessment. This paper

proposes a novel QMSA framework capable of accommodating new security risk assessment and mitigation methods based on uncertainty modelling techniques. The QMSA framework, together with the associated methods, will pioneer a paradigm shift in maritime security assessment and management areas from the orientation of qualitative discussion to the focus of robust quantitative analysis. For instance, novel models are developed to conduct security estimate of the independent components in maritime security operation systems with little or no data and security synthesise of the interdependent components in a quantitative way. Nevertheless, any developed risk analysis approach should preferably be introduced into a commercially stable environment in order that the applications have the chance to become established and prove feasible. Therefore, future research opportunities are emphasised with respect to advancing the development of new techniques and methods to a point where applying them become feasible in the maritime environment.

Acknowledgements

This research was supported by an EU Marie Curie grant (ENRICH – 612546).

References

1. Al-Yami H., LEE P.T.W., Yang Z.L., Ramin R., Bonsall S. and Wang J. (2014), "An advanced risk analysis approach for container port safety evaluation", *Maritime Policy and Management*. Vol. 41, pp. 434-450.
2. Akyus, E., Karahalios, H. and Celik, M. (2015), "Assessment of the maritime labour convention compliance using balanced scorecard and analytic hierarchy process approach", *Maritime Policy and Management*, Vol. 42, No. 2, pp. 145-162.
3. Aven T. (2007), "A unified framework for risk and vulnerability analysis and management covering both safety and security", *Reliability Engineering & System Safety*, Vol. 92, pp. 745-754.
4. Aven T. (2009), "Identification of safety and security critical systems and activities", *Reliability Engineering & System Safety*, Vol. 94, pp. 404-411.
5. Balducelli C., Bologna S., Lavalle L. and Vicoli G. (2007), "Safeguarding information intensive critical infrastructures against novel types of emerging failures", *Reliability Engineering & System Safety*, Vol. 92, pp. 1218-1229.
6. Brandes, U. (2001), "A faster algorithm for betweenness centrality", *Journal of Mathematical Sociology*, Vol. 25, pp. 163–177.
7. Büttner, K., Krieter, J., Traulsen, A. and Traulsen, I. (2013), "Static network analysis of a pork supply chain in Northern Germany - Characterisation of the potential spread of infectious diseases via animal movements", *Preventive Veterinary Medicine*, Vol. 110, pp. 418-428.
8. Cadini, F., Zio, E. and Petrescu, C. A. (2009), "Using centrality measures to rank the importance of the components of a complex network infrastructure", *Critical Information Infrastructure Security*. Springer Berlin Heidelberg, 155-167.
9. Dabrowski, J.J. and de Villiers, J.P. (2015), "Maritime piracy situation modelling with dynamic Bayesian networks", *Information Fusion*, Vol. 23, pp. 116-130.
10. de Almeida A.T., Ferreira R.J.P. and Cavalcante C.A.V. (2015), "A review of the use of multicriteria and multi-objective models in maintenance and reliability", *IMA Journal of Management Mathematics*, Vol, 26, No. 3, pp. 249-271.
11. de Nevers, R. (2015), "Sovereignty at sea: States and security in the maritime domain", *Security Studies*, Vol. 24, No. 4, pp. 597-630.
12. Dijkstra, E. W. (1959), "A note on two problems in connexion with graphs", *Numerische Mathematik*, Vol. 1, pp. 269-271.
13. Dillon R.L., Liebe R.M. and Bestafka T. (2009), "Risk-based decision making for terrorism applications", *Risk Analysis*, Vol. 29, pp. 321-335.

14. Freeman, L. C. (1977), "A Set of Measures of Centrality Based on Betweenness", *Sociometry*, Vol. 40, pp. 35-41.
15. Freeman, L. C. (1978), "Centrality in social networks: conceptual clarification", *Social Networks*, Vol. 1, pp. 215–239.
16. Gerigk, M., (2007), "A model of performance-oriented risk-based assessment of safety of container ships", *Polish Maritime Research*, Vol. 1, pp. 53-57.
17. Gheorghe A.V., Masera M., Weijnen M. and Vries L.D. (2006), *Critical Infrastructures at Risk*, Springer, Dordrecht, Netherland.
18. Gorman S.P., Schintler L., Kulkarni R. and Stough R. (2004), "The revenge of distance: vulnerability analysis of critical information infrastructure", *Journal of Contingencies and Crisis Management*, Vol. 12, pp. 48-63.
19. Hastings, J.V. and Phillips, S.G. (2015), "Maritime piracy business networks and institutions in Africa", *African Affairs*, Vol. 114, No. 457, pp. 555-576.
20. IMO, 1997a. "Formal safety assessment: trial application to high speed passenger catamaran vessels." *Final Report, DE 41/INF.7,* submitted by International Maritime Organization (IMO) UK, IMO Sub-Committee on Ship Design and Equipment, 41st Session, Agenda Item 5, London, UK.
21. IMO, 1997b. *Interim Guidelines for the Application of Formal Safety Assessment to the IMO Rule-Making Process*, IMO/MSC Circular 829, London, 17th November.
22. IMO, 1998a. "Bulk carrier safety, proposal for a formal safety assessment of bulk carriers". *MSC70/4/Add1*, submitted to the IMO by the UK MCA.
23. IMO, 1998b. "Trial application of formal safety assessment to dangerous goods on passenger/ro-ro vessels." *MSC69/INF.24*, submitted by International Maritime Organization (IMO), Finland.
24. IMO, 2002a. "International collaborative FSA study on bulk carriers—step 2 of FSA (risk analysis) WP 11 — develop risk contribution tree components." *MSC 75/INF.22*, submitted by France to IMO, IMO, London, UK.
25. IMO, 2002b. "International collaborative FSA study—FSA step 3 (risk control options)". *MSC 76/INF.8*, submitted to the IMO by UK to IMO, London, UK.
26. Jenelius E., Petersen T. and Mattson L.G. (2006), "Importance and exposure in road network vulnerability analysis", *Transport Research A*, Vol. 40, pp. 537–560.
27. Johnson C.W. (2007), "Understanding the interaction between public policy, managerial decision-making and the engineering of critical infrastructures", *Reliability Engineering & System Safety*, Vol. 92, pp. 1141-1154.
28. Jonsson H., Johansson J. and Johansson H. (2007), "Identifying critical components of electric power systems: a network analytic approach", *Annual Conference of European Safety and RELiability (ESREL) 2007*, June 25-27, Stavanger, Norway.
29. Latora V. and Marchiori M. (2005), "Vulnerability and protection of infrastructure networks", *Physical Review E*, Vol. 71, pp. 1-4.
30. Lewis, J.S. (2016), "Maritime piracy confrontations across the globe: Can crew action shape the outcomes?", *Marine Policy*, Vol. 64, pp. 116-122.
31. Liu, J., Yang, J.B., Wang, J., Sii, H.S. and Wang, Y.M., (2004), "Fuzzy Rule-based Evidential Reasoning Approach for Safety Analysis", *International Journal of General Systems*, Vol. 23, No. 2-3, pp. 183-204.
32. Lois, P., 2004. "Cyprus and Mediterranean cruise market: A financial and economic appraisal." *PhD Thesis*, Liverpool John Moores University, UK.
33. Loughran, C., Pillay, A., Wang, J., Wall, A. and Ruxton, T., (2003), "A preliminary study of fishing vessel safety." *Journal of Risk Research*, Vol. 5, No. 1, pp. 3-21.
34. Marquez A.C., Gomez J.F. de Leon P.M. and Rosique A.S. (2013), "Modelling on-line reliability and risk to schedule the preventive maintenance of repairable assets in network utilities", *IMA Journal of Management Mathematics*, Vol, 24, No. 4, pp. 437-450.

35. Mizumoto, M. (1995), "Improvement of Fuzzy Control Methods", In: Fuzzy Logic and Intelligent Systems, Li, H. and Gupta, M. (Eds.) Kluwer Academic Publishers, pp. 1-16.
36. Montewka, J., Hinz, T., Kujala, P. and Matusiak, J. (2010), "Probability modelling of vessel collisions", *Reliability Engineering and System Safety*, Vol., 95, No. 5, pp. 573-589.
37. Newman, M. E. J. (2001), "Scientific collaboration networks. II. Shortest paths, weighted network, and centrality", *Physical Review E*, 64(1), 016132.
38. Papa, P. (2010), "US and EU strategies for maritime transport security: A comparative perspective", *Transport Policy*, Vol. 28, pp. 75-85.
39. Papamichail, K.N. and French, S. (2013), "25 Years of MCDA in nuclear emergency management", *IMA Journal of Management Mathematics*, Vol. 24, No. 4, pp. 481-503.
40. Patterson S.A. and Apostolakis G.E. (2007), "Identification of critical locations across multiple infrastructures for terrorist actions", *Reliability Engineering & System Safety*, Vol. 92, pp. 1183-1203.
41. Psaraftis, H.N., (2012), "Formal safety assessment: an updated review", *Journal of Maritime Science and Technology*, Vol. 17, pp. 390-402.
42. Qu Z., Laidlaw P., Fraser G., Jenkinson I., Wang J., and Yang Z.L. (2014), "Revised FMEA model to facilitate Six Sigma quality control in shipping management", *International Association of Maritime Economics Conference 2014 (IAME2014)*, July 15-18, Norfolk, USA.
43. Satty, T.L. (1980), *The Analytic Hierarchy Process*, University of Pittsburgh, USA.
44. Sii, H.S., (2001), "Marine and offshore safety assessment." *PhD Thesis, Staffordshire University/ Liverpool John Moores University*, UK.
45. Vanem, E., Antao, P., Ostvik, I. and de Comas, F.D., (2008), "Analysing the risk of LNG carrier operations", *Reliability Engineering & System Safety*, Vol. 83, pp. 1328-1344.
46. van der Borst M. and Schoonakker H. (2001), "An overview of PSA importance measures", *Reliability Engineering & System Safety*, Vol. 72, pp. 241-245.
47. Vu H.C. Do P. Barros A. and Berenguer C. (2015), "Maintenance planning and dynamic grouping for multi-component systems with positive and negative economic dependencies", *IMA Journal of Management Mathematics*, Vol, 26, No. 2, pp. 145-170.
48. Wang, J. and Foinikis, P., (2001), "Formal safety assessment of containerships", *Marine Policy*, Vol. 25, pp. 143-157.
49. Wang W.B. (2010), "Modelling in industrial maintenance and reliability", *IMA Journal of Management Mathematics*, Vol, 21, No. 4, pp. 317-318.
50. Willis H.H. (2007), "Guiding resource allocations based on terrorism risk", *Risk Analysis*, Vol. 27, pp. 597-606.
51. Yang J.B. and 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*, Vol. 32, pp. 289-304.
52. Yang Z.L. (2014c), "Formal security assessment - New approaches to maritime security risk quantification", *International Association of Maritime Economics Conference 2014 (IAME2014)*, July 15-18, Norfolk, USA.
53. Yang, Z.L., Bonsall, S., Wall, A. and Wang, J., (2005), "Reliable container line supply chains – a new risk assessment framework for improving safety performance", *Journal of World Maritime University*, Vol. 4, pp. 105-120.
54. Yang, Z.L., Bonsall, S. and Wang, J., (2008), "Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in FMEA." *IEEE Transactions on Reliability*, Vol. 57, pp. 517-528.
55. Yang, Z.L., Bonsall, S. and Wang, J., (2009a), "Use of hybrid multiple uncertain attribute decision making techniques in safety management", *Expert System with Applications*, Vol. 36, pp. 1569-1586.
56. Yang, Z.L., Bonsall, S. and Wang, J., (2009b), "Use of fuzzy evidential reasoning in maritime security assessment", *Risk Analysis*, Vol. 29, pp. 95-120.

57. Yang, Z.L., Bonsall, S. and Wang, J. (2010), "Facilitating uncertainty treatment in the risk assessment of container supply chains", *Journal of Marine Engineering and Technology*, Vol. A17, pp. 23-36.
58. Yang Z.L., Ng A. and Wang J. (2013a), "Prioritizing security vulnerabilities in ports", *International Journal of Shipping and Transport Logistics*, Vol. 5, pp. 622-636.
59. Yang Z.L., Ng A.K.Y. and Wang J. (2014), "Incorporating quantitative risk analysis in port facility security assessment", *Transportation Research Part A: Policy and Practice*, Vol. 59, pp. 72-90.
60. Yang, Z.L. and Wang, J., (2008), "Ship formal safety assessment". In: Talley, W.K. (Ed.), *Maritime Safety, Security and Piracy*, LLP, London, pp. 31-53.
61. Yang Z.L., Wang J. and Li K. (2013), "Maritime safety analysis in retrospect", *Maritime Policy and Management*, Vol. 40, No. 3, pp. 261-277.
62. Yeo, G.T., Pak J.Y. and Yang Z.L., (2013), "Analysis of dynamic effects on seaport adopting port security." *Transportation Research Part A: Policy and Practice*, Vol. 5, pp. 622-636.
63. Zhang D., Yan X.P., Zhang J.F., Yang Z. and Wang J. (2015), "Use of fuzzy rule-based evidential reasoning Approach in the navigational risk assessment of inland waterway transportation systems", *Safety Science*, Vol. 82, pp. 352-260.
64. Zio, E. Golea, L. R. and Rocco, C. M. (2011), "Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms", *Reliability Engineering & System Safety*, Vol. 99, pp. 172-177.