John, A, Yang, Z, Riahi, R and Wang, J

A risk assessment approach to improve the resilience of a seaport system using Bayesian networks

http://researchonline.ljmu.ac.uk/id/eprint/3250/

Article

A proposed decision support system to improve the resilience of a seaport system using Bayesian networks

Dr. Andrew John is a former Researcher at Liverpool John Moores University (e-mail: j.andii44@yahoo.co.uk).

Dr Zaili Yang is Reader in Maritime Transport at Liverpool John Moores University (e-mail: z.yang@ljmu.ac.uk)

Dr Ramin Riahi is a Senior Lecturer in Marine Engineering at Liverpool John Moores University, James Parsons Building, Byrom Street, Liverpool, L3 3AF, UK (phone: 44-151-2312477; fax: 44-151-2073460; e-mail: r.riahi@ljmu.ac.uk).

Professor Jin Wang is the Director of Liverpool LOgistics, Offshore and Marine (LOOM) Research Institute at Liverpool John Moores University (e-mail: j.wang@ljmu.ac.uk).

Abstract

Over the years, many efforts have been focused on developing methods to design seaport systems, yet disruption still occur because of various human, technical and random natural events. Much of the available data to design these systems are highly uncertain and difficult to obtain due to the number of events with vague and imprecise parameters that need to be modelled. A systematic approach that handles both quantitative and qualitative data, as well as means of updating existing information when new knowledge becomes available is required. Resilience, which is the ability of complex systems to recover quickly after severe disruptions, has been recognised as an important characteristic of maritime operations. This paper presents a modelling approach that employs Bayesian belief networks to model various influencing variables in a seaport system. The use of Bayesian belief networks allows the influencing variables to be represented in a hierarchical structure for collaborative design and modelling of the system. Fuzzy Analytical Hierarchy Process (*FAHP*) is utilised to evaluate the relative influence of each influencing variable. It is envisaged that the proposed methodology could provide safety analysts with a flexible tool to implement strategies that would contribute to the resilience of maritime systems.

Keywords: Seaport systems, decision support model, Bayesian belief network, fuzzy set theory, resilience, sensitivity analysis.

1 Introduction

Over the last few years, many critical maritime infrastructure (CMI) systems have been ageing and deteriorating at a fast rate due to their challenging field of operations. However, given the importance of these systems in advancing global economy, decision makers have the challenging task of maintaining a balance between safety, security, sustainability and resilience of their systems to diverse operational uncertainties leading to disruption of the systems (John et al., 2014).

High-profile accidents, such as the 9/11 terrorist attacks in 2001, the lock-out of the American West Coast Port in 2002, and the Fukushima nuclear disaster in 2011, which forced some shipping firms to avoid key ports and sea lanes in Japan, are clear examples of systemic failures and disruptions in these complex socio-technical domain.

When critical maritime systems do not have the robustness to recover in the face of disruption, they present themselves as attractive targets to terrorism-related attacks. Because a large proportion of the world's trade is transported by sea, the global economy is heavily dependent on the effective operation of these systems, resulting in a high level of systemic complexity; disruptions at any point within their operation could potentially result in catastrophic and disastrous consequences.

Modelling of these systems can provide useful insights regarding how failures might propagate and lead to their disruption, and also the basis for the development of robust frameworks and approaches that can be used for the analysis of the systems (Codette-raiterri, et al., 2012). Building resilience in CMI requires creating capabilities and a sustained engagement with the stakeholders involved in their operations. Additionally, academics and industrialists acknowledge that safety and security efforts that are aimed at mitigating risks will always reach a point of diminishing returns. A more realistic way of optimising the system's defence capability is to incorporate resilience into its operations to adapt, cope and recover to a desired level of functionality.

An emphasis on resilience operation of the systems provides a flexible and collaborative modelling of the systems to address the diverse risks of disruption proactively, particularly as new hazards and threats are constantly evolving. Additionally, insufficiency of resilience-related literature in the maritime domain together with the vision to establish secure and resilient maritime operations (Mansouri et al., 2010 and Mostashari et al., 2011) has resulted in an urgent need to develop a modelling approach using an intelligent decision tool that can provide insight to decision makers on how to optimise the performance effectiveness of seaport operations.

As graphs have proven to be a natural language for analysts to represent dependence and independence relations among variables, and thus provide an excellent language for communication and discussing relations among variables, a Bayesian belief network (BBN) is used to assess the influencing factors leading to disruption of operations. Unlike rule-based approaches for risk analysis (e.g. approximate reasoning approaches), BBN has the ability to model randomness and capture non-linear causal relationships in complex socio-technical systems (Ren et al., 2005 and Yang et al., 2008).

However, both the fuzzy logic-based approach and BBN have limitations in safety analysis of complex systems. A common criticism of fuzzy reasoning approaches is their inability to conduct inference inversely; it is a feed-forward approximate reasoning approach, i.e. when a model is given a set of inputs, it can predict the output, but not vice versa; while the BBN approach is criticised due to the fact that it requires too much information in the form of prior probabilities, which is usually difficult to obtain in risk assessment. Research by Eleye-Datubo et al. (2008), Huang et al. (2006), Halliwell et al. (2003) and Bott and Eisenhawer (2002) has revealed that merging fuzzy logic and BBNs for safety and reliability studies of complex systems can be beneficial in compensating for their individual shortcomings. It is important to emphasize that the concept of the Fuzzy Bayesian Network (*FBN)* can be expressed in different ways to address various research needs and interests.

The main objective of this paper is to propose a modelling approach based on the Fuzzy Bayesian Network (*FBN*) to optimize the performance effectiveness of seaport operations. This has been organised as follows. Section 2 reviews the existing literature on resilience of CMI systems, presents and discusses the diverse risks factors associated with the systems, and analyses schemes to enhance the resilience of the systems. Section 3 discusses the modelling approach using a BBN. Section 4 explains the methodology of the study. Section 5 provides a case study to demonstrate the implementation of the proposed methodology. Section 6 presents the analysis of the experiment/discussion of result, and section 7 presents the conclusions of the study.

2 Literature review

The literature review examines resilience engineering literature, schemes to enhance the resilience of critical maritime infrastructure systems, and the analysis of the diverse risks and operational features of these systems.

2.1 Resilience of Critical Maritime Infrastructure Systems

Over the last decade, safety analysts have acknowledged the limitations in the existing approaches to the assessment of complex systems and resilience engineering (RE) has been suggested to overcome such limitations (Hallnagel et al., 2007)). RE focuses on theories and tools to create foresight about the changing patterns of risk scenarios before disruption occur. Subsequently, significant effort has been made in trying to highlight the basic features of resilient systems and the development of robust, flexible and acceptable concepts, principles and methods that can serve as the basis for developing approaches to enriching the field of resilience in order to optimize critical systems operations (Hallnagel et al., 2008; Nameth et al., 2009 and Woods, 2000).

The term resilience has various definitions due to different perspectives. It is considered as the capacity of a system or organisation to bounce back after a mishap (Widalsky, 1988). The research characterises resilience as the capacity to cope with unanticipated dangers after they have emerged. Reason and Hobbs [18] defined resilience as the properties of an organisation to make it more resistant to its operational hazards, while Rosness et al. (2004) defined resilience as the capacity of an organisation to accommodate failures and disturbances without producing serious accidents. However, Hollnagel et al., (2007) defined resilience as the inherent capacity of a system to adjust its functioning prior to or following changes and disturbances so that it can sustain operations even after a major mishap or in the face of continuous disruption or stress. Thus, the implication of these definitions from the literature is that, for a system or an organisation to be resilient, it must have the following capabilities:

- Anticipate future threats and opportunities.
- Respond to regular and irregular threats in a robust yet flexible manner.
- Monitor on-going developments.
- Learns from past failures and success alike.

Since complex systems operations involve uncertainty, security incidents may be characterized by the exploitation of vulnerabilities in the system to achieve a certain degree of disruption. Hence, resilience can be used as an innovative management strategy to achieve a high level of security in an uncertain and dynamic environment. Benefits derived from strategic implementation of resilience in complex systems operations can be in the form of (Johnsen and Veen, 2013; Weick and Robert, 1993):

- Increased focus on proactivity, i.e. mindful of anticipating unexpected and uncertain events that may disrupt system processes in a systematic fashion.
- Ability of the system to adjust operation in the face of adverse operational scenarios in order to maintain its functionality.
- Ability to prepare for the unexpected in a pragmatic environment.

The Committee on Marine Transportation Systems (CMTS) lists resilience as one of the five most pressing and current challenges to CMI systems and has outlined a framework for increasing the resilience of the system that is consistent with the national response framework (Omer et al., 2012). However, the literature makes little effort to analyse and quantify how the resilience of these systems can be assessed using robust yet flexible modelling tools.

Omer *et al.* (2012) proposed a framework for assessing the resiliency of maritime transportation systems (MTS) based on the methodology of a network infrastructure resiliency assessment framework. The framework consists of three stages in which a network model is extracted from the physical network and its resiliency metrics are identified and modelled using the network optimisation technique. Although showing some attractiveness, the method has still been criticised for not addressing uncertainties in measuring resilience and not providing clarity and insight on the Vensim software used for the assessment in a precise and succinct manner that can be understood by analysts who are not well versed with advanced computational algorithm.

Mansouri et al. (2010) proposed a risk management approach based on a decision analysis framework which was also based on common fundamental elements that defined the resiliency of port infrastructure systems. The framework develops a systemic approach to the decision making process in regard to assessing the vulnerabilities of the system and devising and valuing resiliency strategies. Nair et al. (2010) presented an approach to measure the resilience of a port system using the measure of intermodal (IM) resiliency. IM resiliency is measured as the ratio between the satisfied demand and the total demand between the origin and destinations of cargo shipments taking into account the disruptive scenarios.

The purpose of analysing the system is to enhance its resilience to operational uncertainties, promote security and reduce the susceptibility of the infrastructure to man-made and natural disruptions. Since the occurrence of natural disasters and the disruptions caused by man-made attacks on CMI systems are imprecise, it is therefore challenging to protect the systems from such perceived threats; thus the need for the resilience of their operations.

2.2 Schemes to Enhance the Resilience of Critical Maritime Infrastructure Systems

The current complexities of maritime operations emphasise that the functioning of the system cannot merely be explained by the aggregation of factors, but it has to be understood as an emergent phenomenon, where the system's vulnerability and its adaptive capacity are respectively analysed. When the seaport system's vulnerability is reduced, its susceptibility to disruption is reduced and when its adaptive capacity is increased, it reconfigures, reorganises and responds to shocks, thereby making it anticipate and recognize risks and critical situations (John et al., 2014 and Omer et al., 2012).

The focus of resilience in today's seaport operations is to create foresight about the diverse risk scenarios before failures and harm occur (Woods, 2000). This perspective relates to the seaports coping ability to handle expected and unexpected situations to continue functioning in a systematic manner. In light of the above, based on the literature review, the following schemes or strategies are identified to enhance the adaptive capacity of maritime systems and reduce their vulnerability to disruptions. These schemes or strategies are summarised as follows (John et al., 2014; Omer et al., 2012; Mostashari et al., 2011; Zio et al., 2011; Mansouri et al., 2010; Dalziell and Mcmanus, 2004):

- Proper allocation of resources to the various components of the system to enhance its operations.
- Hardening infrastructure systems: this can be achieved during the design and construction phase to promote structural integrity and enhance the resilience of the system to man-made and natural hazards.
- Increasing staffing in safety-critical areas and prioritise training in order to increase knowledge, experience, flexibility and redundancy. This requires management actions to increase budgets and staffing to accommodate high-capacity tolerance of the system.
- Creating modularity in systems: this can be achieved by building systems that can easily be separable and recombined. Based on the above analysis, since disruption events may impact on only certain parts of the system, modularity reduces the susceptibility of the system by the ease with which these parts can be separated for repairs and replacement.
- Enhancing the use of the Vessel Traffic Management System (VTMS)
- Implementing policies that manage the consequences of threats and facilitate the recovery procedures through a collaborative effort by the multiplicity of stakeholders in the system for an efficient information flow.
- Making the infrastructure system more cognitive (i.e. able to perceive changes that occur in it, select a course of action to deal with the current situation and, finally, track the system's behaviour for an enhanced and improved operation).

Some of the suggested strategies relate to the physical infrastructure, while others relate to the operational and socio-technical aspects of the system aimed at increasing its resilience in a pragmatic and scientific environment.

Due to the complex nature of seaport operations, a logical approach to facilitate the investment of the suggested resilience strategies is to break down the system into functional entities comprising sub-systems and components. Safety modelling of these functional entities can be carried out to fit such a logical structure, then the interrelationships can be examined and a system safety model can be formulated for risk-based decision making in all phases of the system in order to enhance the resilience of its operations. This is evidenced in the fact that different risk categories discussed in literature affect the multiplicity of stakeholders involved in their operations. Complexities in the systems may further arise when they interrelate with other risk characteristics such as uncertainty and dependence, as explained through the classification of risk in Table 1 (Nair et al., 2010; Hardley-Schacher and Navare, 2010; Mokhtari et al., 2011 and Fritelli, 2005). Each risk event as presented in Table 1 can be investigated based on its associated causes. These causes are chosen because they are regarded as the most significant ones associated with major disruption of seaport processes. The selection of such disruption risks and causes is conducted based on extensive discussions with experts and a robust literature review.

<Figure 1: Sea-land interface of maritime transportation systems>

<Table 1: Causes of seaport disruption>

2.3 Operational Risk Factors

CMI systems cannot afford disruptions caused by unexpected risks. Due to their complex operations, disruption and damage may well be inflicted not only on property but also on human life and the environment once an accident occurs during a system's operations. The operational risk factors that cause disruption of maritime activities are due to port equipment/machinery failures, ship/vessel accident/grounding, and cargo spillage (John et al., 2014). These are attributed to movement of oil tankers, large and small boats, loading and unloading of oil and other cargoes, ferry services, cargo forwarding operations, human errors and management (Berle et al., 2011 and Vanem et al., 2008).

2.4 Security Risk Factors

Since the 9/11 attacks, security experts have shown serious concerns over the efficiency and robustness of the CMI system security, with regard to its possible exploitation by terrorists to wreak havoc on the system either through sinking of a large vessel in a port channel or attacking a port's physical infrastructure facilities (Bichou, 2008 and Vanem et al., 2008).

Over the years, decision makers have invested significant resources on sophisticated security measures in order to ensure smooth flows of trade, yet face a severe challenge in the effectiveness of these security measures (Christopher, 2010). It is worth mentioning that the effective performance of security systems or measures can be built based on the evaluation and aggregation of the security risks associated with CMI systems, such as sabotage, terrorism attacks, surveillance system failure and arson (McGill et al., 2007).

2.5 Technical Risk Factors

While technical solutions will continue to play an important role in facilitating smooth operations of maritime systems, the need for a systemic understanding and analysis of CMI systems has led to the categorisation of the seaport system as marine constructions, port maintenance, port operations and logistics. Because ports are open facilities with multiple means of access by both land and sea routes, they involve multiple modes and each is managed by a different entity within the system. Due to the importance of maritime operations in global trade and logistics, lack of equipment, navigation, IT and dredging maintenance have been identified as significant issues in causing severe disruption of operations with long-term financial consequences (Mokhtari et al., 2011).

2.6 Organisational Risk Factors

Organisational aspects of CMI systems are often at the root of disruptions to maritime operations yet, when searching for risk management strategies, analysts tend to focus on technical issues. Events such as labour unrest, dispute with regulatory bodies, breakdown in organisational communications leading to berth congestion, incompatible management goals leading to gate congestion and poor management procedures leading to storage area congestions are major factors mentioned in literature which lead to the disruption of CMI systems (John et al., 2014; Mansouri et al., 2010). There is a widespread agreement among safety researchers that the key means of tackling the human element contribution to disruptions will be via the incorporation of resilience into the operations of the system (John et al., 2014).

2.7 Natural Risk Factors

The dynamics of the natural environment affect the entirety of CMI systems. Its influences are capable of disrupting maritime business and therefore make such business vulnerable to hazards. The most important hazards due to natural factors are hydrological, atmospheric and geologic (Kroger, 2008). The impacts of these hazards have consistently added more cost to the management of CMI systems in the form of annual maintenance, reconstruction and preparedness. Heavy rainfall, flooding and snow are important examples of hydrologic hazards; tsunamis and earthquake are categorised as geological or seismic hazards; hurricanes and cyclones are classed as atmospheric hazards.

3 Modelling Using a Bayesian Network Approach

Bayesian Belief Networks (BBNs) are referred to as the theory of reasoning from uncertain evidence to uncertain conclusion. Ultimately, the network provides a framework for graphical representation of the causal relations between variables and captures the uncertain dependencies between them using conditional probabilities. A BBN model normally consists of a set of variables making up the nodes in the network, a set of directed links (with arrows) connecting the nodes representing dependencies, and a list of probability distributions associated with each node describing the probabilistic influence of its parents on the node.

The dependence structure is thus represented by a set of conditional probability distributions. A variable, which is dependent on other variables, is often referred to as a ‘child node’. Likewise, directly preceding variables are called ‘parents’. Nodes that have no parents are called ‘root nodes’ and nodes without children are called ‘leaf nodes’. Quantitative probability information is specified in the form of conditional probability tables (CPTs). For each node, the table specifies the probability of each possible state of the node, given each possible combination of the states of its parents. The table for a root node contains unconditional probabilities. The structure of a BBN is referred to as a Directed Acyclic Graph (DAG), meaning that the arrows originating from a node should not return to it by any path. The network consists of nodes and arcs; the nodes represent random variables and the arcs represent causal relations between variables. The arcs are directed from the “parent” or cause node to the “child” or effect node. Nodes that have no parents are called “root nodes” and nodes without children are called “leaf nodes”.

3.1 Obtaining the Conditional Probabilities for System Modelling

The categorisation of the model as shown in Figure 3 was based on information presented in section 2. The model has 26 nodes of which 20 are input nodes, five are intermediate nodes and one is a decision node. In addition to the BBNs’ ability to represent causal relationships, they have been used to represent joint probability distributions (JPDs) efficiently. This ability comes from local JPDs that are linked to each variable in the network, whose purpose is to quantify the strength of the causal relationships depicted in the BBN through its structure. The JPDs can be obtained using the combination of qualitative and quantitative relationship. More importantly, given the structure and the local JPD of a BBN, the JPD of the domain of n variables can be calculated as follows:

$$P(Y_1, Y_2, \dots., Y_n) = \prod_{i=1}^{n} P(Y_i|Z_i) \qquad (1)$$

where Z_i denotes the set of direct parents of variable Y_i.

Modelling using a BBN requires much information in the form of prior probability. In principle, most values could be acquired through finding failure frequencies in database or conducting experiments. However, experiments may be difficult to design and conduct correctly, and historical data do not often satisfy the requirements of the Bayesian approach. In practice, it is often necessary and important to rely on subjective probabilities provided by experts as a rational expression of an individual’s degree of belief (Zimmer, 1986).

In constructing a BN, the converging connections between nodes are always a problem for both Bayesian statisticians and experienced analysts. To reveal the mentioned difficulties, assume Y_1 and Y_2 are the two children listing all the effects of the single parent Y_3. Based on equation (1), the JPD for the diverging connections can be calculated as follows:

$P(Y_1, Y_2, Y_3) = P(Y_1/Y_3)P(Y_2/Y_3)P(Y_3)$

Alternatively, assume Y_1 and Y_2 are the two parent nodes of the their single child Y_3; based on Equation 1 the JPD of the converging connections can be computed as follows:

$P(Y_1, Y_2, Y_3) = P(Y_1)P(Y_2)P(Y_3/Y_1, Y_2)$

Because $P(Y_3/Y_1, Y_2)$ cannot be further decomposed, it is too difficult for humans to understand and may be too specific for any expert. Many research analysts associated with BNs have generated some novel and effective methods to deal with this problem from both quantitative and qualitative viewpoints, such as ‘Noisy-Or’ approaches (Pearl, 1986). This paper used a symmetric model as described in Riahi et al. (2013) for the modelling process.

3.2 Symmetric Model Utilisation

The utilisation of the model is based on the fact that an expert’s opinion is distributed by relative importance of each parent node to the associated child node. The relative importance (weights) can be assigned to each parent node by using the fuzzy analytical hierarchy process (FAHP) method (An et al., 2007). It is important to emphasize that the strength of direct dependence of each child node to its associated parents is indicated by their normalised weights $(w_1, w_2, \dots . w_n)$. Based on the influence of each parent node and in the normalised space, the conditional probability of a child node Z given by each parent node Y_r, where $r = 1, 2, 3 \dots . . n$, can be expressed as follows (Riahi et al., 2013):

$$\begin{gathered} P(Z = Present|Y_1 = Present) = w_1 \\ P(Z = Present|Y_2 = Present) = w_2 \\ \vdots \\ P(Z = Present|Y_r = Present) = w_r \end{gathered}$$

$$\sum_{r=1}^{n} w_r = 1 \qquad (2)$$

Based on Equation 2, and considering the situation of the symmetry approach (i.e. normalised space), the probability of the child node Z being conditional upon parent node Z_r, where $r = 1, 2, \dots . n$ can be estimated as follows:

$$P(Z|Y_1, Y_2, Y_3 \dots . Y_n) = \sum_{r=1}^{n} \widetilde{w_r} \qquad (3)$$

where,

$\widetilde{w_r} = w_r$: If the state of the rth parent node is identical to the state of its child

$\widetilde{w_r} = 0$: If the state of the rth parent node is different from the state of its child

By utilising the symmetric model and based on Equation 3, a CPT for each child node can be computed.

3.3 Determining the Unconditional Probabilities

For quantifying the relationships in the model, the unconditional probabilities of the starting nodes or input nodes need to be provided. The starting nodes in the proposed BBN model for the port under investigated can be valuated via audit reports of the seaport operations provided by the operations and maintenance department. Decision makers have to deal with two types of data when evaluating the unconditional probabilities of the starting nodes; these data are qualitative and quantitative in nature. Qualitative data can be presented by linguistic variables (i.e. linguistic terms and their corresponding belief degrees). The number of linguistic terms can be selected by Miller's method (Miller, 1956). Miller showed a number of remarkable coincidences between the channel capacity of a number of human cognitive and perceptual tasks. In each case, the effective channel capacity is between five and nine equally weighted errorless choices. Normally, too few levels are not adequate to represent the real knowledge of analysts, while too many levels will bring extra difficulties in the following assessment (Miller, 1956). As a result, linguistic variables in this article are presented with five linguistic terms based on the experts' assessment.

For instance, there are 16 qualitative datasets obtained through a set of questionnaires and interview sessions with the selected experts in the domain of seaport operations and optimisation. Based on the questionnaires, each expert is expected to tick a probability rate based on the situation discussed and the goal of the research. The probability rates given by the experts are in the scale of [1, 10], which will then be transformed into a probability value ranging from [0, 1], as shown in Table 3. It is important to note that the probability value of each node given by the experts must sum up to 1.

<Table 2: Probability scale distribution>

Moreover, any quantitative data such as those presented in Table 3 can be transformed into a qualitative estimate for use in the BBN by using a rule-based reasoning approach or a set of membership functions (MFs). In general, the degree of membership or degree of belief is often indicated on a vertical axis and with possible values ranging over the real interval [0, 1]. Whether a particular shape is suitable or not can be determined only in the application context. If any quantitative number (e.g. h_i) is found in the range of $h_{n+1,i}$ (with a grade of H_{n+1}) and $h_{n,i}$ (with a grade of H_n), if $h_{n,i} < h_i < h_{n+1,i}$, its belief degrees can be assessed as follows (Riahi et al., 2012).

$$\beta_{n,i} = \frac{h_{n+1,i} - h_i}{h_{n+1,i} - h_{n,i}}, \beta_{n+1,i} = 1 - \beta_{n,i} \tag{4}$$

where $\beta_{n,i}$ stands for the degree of belief of the concerned quantitative number with the grade H_n and $\beta_{n+1,i}$ stands for the degree of belief of the concerned quantitative number with the grade H_{n+1}.

4 Methodology

The proposed model for decision support involves the use of BBNs to assess the influence of each variable on the disruption of a seaport, which is a critical maritime infrastructure system. The development of the model consists of two major steps which include the identification of influencing factors (variables) and their relations, and the quantification of the strength of the relationships among the influencing factors. The strength of the relationships among the influencing factors is established by defining the CPT of each node with its associated parent. The methodology is presented in Figure 2 and represented in a stepwise order as follows:

Step 1: Customise the BBN.

Step 2: Specify variable states to all starting nodes in the model.

Step 3: Establish relationship quantification (CPTs).

Step 4: Obtain the estimates of disruption risk.

Step 5: Evaluate the crisp value of the obtained estimate in step 4 above.

Step 6: Validate the result using appropriate techniques including sensitivity analysis.

<Figure 2: Flow diagram for implementing the proposed model>

<Table 3: Representation of influencing factors>

4.1 Customize the Bayesian network (Step 1)

The first step is to customise the generic model with respect to the specific goal of the study under consideration. CMI systems involve different stakeholders and systems that interrelate to ensure efficient smooth operation of the system. The main influencing factors have been identified and presented in Table 1. These factors are divided into five major groups or criteria and the nodes associated with the root causes at the first stage are defined as starting nodes. All the starting nodes are identified and the nodes associated with them are defined as intermediate nodes. This hierarchical process continues until all the variables have a place in the graph and all parent-child links are accounted for at the edge of the graph. Based on the modelling approach presented in (Bayraktar and Hastak, 2009), states are assigned to all the nodes in the graph, as shown in Table 3. Consequently, in order to demonstrate the implementation of the methodology, a dependency model is constructed for the system as shown in Figure 3. This model is produced due to available information for this research and to ease the computational process involved in the analysis. Also, using the concept of d-separation to check and modify the model in Figure 3, it is necessary to investigate one node after another, starting from the root nodes. Such analysis is carried out smoothly for the complete network and the effectiveness of the model is acknowledged. The notation for d-separation originates from Pearl (1988), it is a well-known approach yet it is rarely mentioned in reliability analysis of complex systems despite its effectiveness within the Bayesian domain in speeding-up inferences.

4.2 Specification of Variable States (Step 2)

In order to perform the analysis, states of each node or variable have to be defined in order to quantify the relationships between the influencing variables. Moreover, if the states of the variables are defined quantitatively, it is easier to transform the quantitative data into qualitative data for smooth modelling of the system.

4.3 Quantifying the Relationship of Variables (Conditional probability table) (Step 3)

The relationship between a child node and all its parents is described by a conditional probability table (CPT). The strength of direct dependence of each child node to its parents is quantified by assigning each child node a CPT using the symmetric model described in section 3. As a consequence, the relative influence of a parent node to its associated child node is assessed using the fuzzy analytical hierarchy process (FAHP) to obtain the weights. By using the symmetric model and based on Equation 3, a CPT can be formulated for each child node. The number of data that need to be inserted in a CPT can be calculated using Equation 5.

$$N^{y+1} \tag{5}$$

where N and y stand for number of linguistic terms and number of parents respectively.

4.4 Obtaining the Estimates of Disruption Risk (Step 4)

The estimates of *BBN* probabilities for the decision node can be obtained by feeding the input data or the starting nodes' data into the model. Consequently, the estimate of disruption to the system can be obtained as follows:

$$Target\ node = Very\ Low, \beta_1), (Low, \beta_2), (Medium, \beta_3)(High,\ \beta_4), (Very\ High,\ \beta_5)$$

where β_1, β_2, β_3, β_4, β_5 are the probability values or the belief degrees associated with the five linguistic terms.

4.5 Evaluating the Crisp Value for Disruption Estimate (Step 5)

The concept of expected utility is utilised to generate numerical values equivalent to the distributed assessment of the top-level criterion or goal of each alternative for ranking in order to obtain the probable risk level of disruption for decision making.

In light of the above, let the utility value of an evaluation grade H_n be denoted as $u(H_n)$ and $u(H_{n+1}) > u(H_n)$ if H_{n+1} is preferred to H_n (Yang, 2001). It is worth mentioning that $u(H_n)$ represents the utility values of each linguistic term and can be determined using the decision makers' preference. If there is no preference information available, it could be presumed that the utilities of the evaluation grades are equidistantly distributed in a normalised utility space. The utilities of evaluation grades that are equidistantly distributed in a normalised utility space are calculated as follows:

$$u(H_{n)} = \frac{V_n - V_{\min}}{V_{\max} - V_{\min}} \quad (6)$$

where V_n is the ranking value of the linguistic term that has been considered *(H_n)*, V_{max} is the ranking value of the most preferred linguistic term *(H_N)*, and V_{min} is the ranking value of the least preferred linguistic term (H_1).

Therefore, the utility value of the target node is denoted by *u(S(E))* and can be calculated as follows:

$$u(S(E)) = \sum_{n=1}^{N} \beta_n u(H_n) \quad (7)$$

where β_n stands for the belief degree of an evaluation grade H_n.

4.6 Validation of the Model (Step 6)

Model validation is an important aspect of this experiment as it provides a reasonable level of confidence in the result produced. In this research, sensitivity analysis as a means of validating the model is utilised. The analysis allows the studying of uncertainties in the output of a model and how they can be apportioned to different sources of variations in the input variables of that model. The objective of the sensitivity analysis within this section is to test the logicality and sensitivity of the output result to a slight variation in the input data. If the model reflects the realistic situation, then an increment/decrement in the rate or probability at which any of the input variables may occur would certainly result in a relative increment/decrement in the rate or probability of occurrence of the output node. If the methodology is sound and its inference reasoning is logical and robust, then the sensitivity analysis must at least reflect any of the following three axioms:

Axiom 1: A slight increase or decrease in the degree of belief associated with any linguistic variables of an input variable should certainly result in a relative increase or decrease of utility value of the model output.

Axiom 2: If the degrees of belief associated with the highest preference linguistic variable of a lowest level criterion are decreased by p and q (i.e. simultaneously, the degrees of belief associated with its lowest preference linguistic variable are increased by p and q *(1 > q > p)*), and accordingly the utility value of the model's output is assessed as U_p and U_q respectively, then U_p should be greater than U_q.

Axiom 3: If K input variables from N input variables ($K < N$) are selected and the degree of belief associated with the highest preference linguistic terms of each of such N and K input variables is decreased by the same amount (i.e. simultaneously the degree of belief associated with the lowest preference linguistic terms of each of such N and K criteria is increased by the same amount) and the utility value of the model output is evaluated as $U_K$and U_N respectively, then U_K should be greater than U_N.

5 Test case

The test case is used to show how the methodology (decision support model) can be implemented in a seaport, which is a critical maritime infrastructure system for resilience improvement of its operations.

5.1 BN Customisation (Step 1)

The customisation of the BN includes the calibration of the model's variables with respect to the goal of the research as obtained from the port under investigation. Given that the data regarding these influencing variables differ for each port, it is necessary to employ a modelling technique that will help integrate both the qualitative and quantitative data for a smooth modelling of the system. In order to establish a relation among the influence variables of the system, a model showing the dependency of the variables is constructed for a seaport and presented in Figure 3. It consists of nodes that represent variables that are connected with directional arrows that represent conditional dependence relationships between those nodes.

<Figure 3: Dependency model for the disruption risk of a seaport>

5.2 Specification of the Variable States (Step 3)

Having customized the model in Figure 3, it is important to identify the states of the nodes which defined the different influencing variables leading to the disruption of a seaport operation. As a consequence, states were assigned to all the variables of the model by the experts and are presented in Tables 5. Based on the data provided by the experts, 4 of the 20 starting nodes have quantitative data (Table 4) while 16 are qualitative in nature. It is important to mention that all the qualitative data are represented by five linguistic terms. Decision makers have to assign probability value or belief degrees based on their understanding of the situation discussed and the linguistic term presented to them for the analysis. As an example, during the interview session and by using the questionnaire presented, the experts have assigned the following states to port equipment failure based on Table 2 as follows:

$Port\ equipment\ failure = \{(Slight, 0), (Minor, 1), (Significant, 0)(Serious, 0), (Worst, 0)\}$

From the above assessment, the experts have 100% belief that the disruption to port operation is minor due to port equipment failure. Also, based on the given information, there are four quantitative data as presented in Table 3; each quantitative data is transformed to qualitative data as follows:

<Table 4: List of quantitative data>

<Figure 4: Membership functions (MFs) for quantitative criterion (lack of equipment maintenance)>

Based on Figure 4 and Equation 4, the belief degrees for lack of equipment maintenance (based on Table 4, average period of disruption is 30 days) can be calculated as follows:

- H_{n+1} represents the Very High grade for MF for lack of equipment maintenance.
- H_n represents the High grade for MF for lack of equipment maintenance.
- $h_i = 30$, $h_{n,i} = 28$ and $h_{n+1,i} = 32$.

Thus, $\beta_{n,i} = \frac{32-30}{32-28} = 0.5$, with the High grade and $\beta_{n+1,i} = 1 - 0.5 = 0.5$ with the Very High grade. Therefore, lack of equipment maintenance is assessed as follows:

$\text{Equipment maintenance} = \{(Very\ Low, 0), (Low, 0), (Medium, 0), (High, 0.5), (Very\ High, 0.5)\}$

In a similar manner, the remaining quantitative data (lack of navigational aid maintenance, lack of IT system maintenance and lack of dredging maintenance) are transformed accordingly.

<Table 5: Linguistic assessment for nodes>

5.3 Quantify the Relationship among Variables (CPTs)

Quantification of the relationships among the variables implies the specification of the *CPTs* for the child nodes to their associated parents with respect to their direct dependence. By using the symmetric model, and based on Equation 3, a CPT for each child node can be formulated and quantified. The relative influence (importance) of each parent node to its associated child node can be obtained using the fuzzy analytical hierarchy process (FAHP) and the obtained results (normalised weights) are presented in Table 6. Based on

Equation 3, a CPT for each child node can be quantified. The number of data that need to be inserted in CPT for operational risk factors (R1), security risk factors (R2), technical risk factors (R3), organisational risk factors (R4), natural risk factors (R5) and the decision node (goal) are respectively computed based on Equation 4 as $5^5, 5^5, 5^5, 5^6, 5^4$ *and* 5^6 (i.e. 41250 data).

<Figure 5 Aggregation result for disruption estimate>

<Table 6: Nodes' normalised weights>

5.4 Obtaining the Estimates of Disruption Risk

Based on the data provided by the experts, the input data are fed into the BBN software and the result of the experiment is presented in Figure 5. The estimate of disruption obtained at the decision node or goal is evaluated as:

$$\text{Goal} = \{(Very\ Low, 0), (Low, 0.4245), (Medium, 0.1033), (High, 0.2582), (Very\ High, 0.2140)\}$$

5.5 Evaluating the Crisp Values of the Obtained Estimate of Disruption Risk

The obtained result from the experiment as presented in section 5.4 is characterised by five linguistic terms. In order to evaluate the crisp value of the assessment, the highest preference of the estimate is given to the "Very High" linguistic term and the lowest preference is given to the "Very Low" linguistic term and the ranking value is obtained from five (i.e. highest preference) to one (i.e. lowest preference). Accordingly, by using Equations 6 and 7, the crisp value for the risk of disruption for the port under investigation is obtained as 0.5655 or 57%, as shown in Table 7. Based on the obtained result, it is important to mention that assessment based on a single value is much easier and a more realistic tool for a decision maker to rank the risk variables in order to analyse and design the system for resilience.

<Table 7: Crisp value evaluation for disruption risk>

6 Model Validation

Sensitivity analysis was undertaken to identify the relative influence of different nodes on the output categories of the decision node. Essentially, the analysis was conducted by varying the values of input data based on the axioms discussed in section 4.5. With reference to the axioms discussed in section 4.5, input data or the belief degrees of all the 20 variables or root nodes are decreased by 10%, 20% and 30% respectively and, simultaneously, the input data or belief degrees associated with the lowest preference linguistic terms of the variables are increased by the same amount of 10%, 20% and 30% respectively and the results are recorded. It is worth mentioning that when decreasing the belief degree of the highest preference linguistic term β_γ of a root node by z, simultaneously the belief degree of its lowest preference linguistic term has to be increased by z. However, if β_γ is less than z, then the remaining belief degree (ie $z - \beta_\gamma$) can be taken from the belief degree of the next linguistic term. This process continues until z is consumed. The obtained results are presented in Figure 6 and Table 8, and are in harmony with axioms 1 and 2.

Moreover, if the belief degree associated with the highest linguistic term of the 20 variables is decreased by 25%, the obtained result at the decision node or the utility value is evaluated as 0.5286. However, by selecting 15 input variables out of 20 (i.e. R11, R12, R13, R14, R21, R22, R23, R24, R31, R32, R33, R34, R41, R42 and R43) and by decreasing the input data by 25%, the utility value of the model is assessed as 0.5591 or 55.91%. Due to the fact that 0.55911 is greater than 0.5286, the output result is in harmony with axiom 3, as discussed in section 4.5.

<Table 8: Changes in root nodes due to some variation of unconditional prior probabilities>

<Figure 6: Sensitivity analysis result due to variation of input data>

From the experiment conducted, the probability of occurrence of each individual root node is decreased by 10%, 20% and 30% and the obtained results are presented in Table 8 and Figure 6 respectively. Figure 6 depicts the sensitivity of the model input variables. Having performed the experiment under varying conditions, it is evident that the model is more sensitive to R22 (i.e. terrorism attacks). Experience has shown that the influence magnitude of R21 (i.e. if the surveillance system of a port is very bad then, due to flaws in the security systems/measures, terrorists and saboteurs could exploit the situation and commit sabotage or stage an attack on the port's infrastructure systems thereby wreaking severe havoc on operation) on maritime operations can be very devastating with long-term consequence.

7 Analysis of Experiment and Discussion of Results

A sensitivity analysis was undertaken to identify the relative influence of each starting node on the output categories of the decision node. The analysis was conducted by varying the input data or belief degree values of the individual starting nodes, as discussed in section 4.5. As a consequence, the disruption risk value at the decision node was evaluated as 0.7204 This value is used as the frame of reference in order to analyse the influence magnitude of the most sensitive parameter of the model given a slight change in input data.

Based on Table 8, the accuracy of the input data and the result of the output data show the variations and influence magnitude of each node on the system. Figure 6 exhibits the behaviours of several inferences of disruptions in the port under study, with R22 as the most sensitive node that influenced the operations of the system. The curve reveals the impact conditions of the nodes and highlights the degree of disruptions to the system. More importantly, it can be seen that R22 (terrorism attacks) seems more sensitive in the analysis, and R41 (labour unrest) seems less sensitive based on the analysis result. By examining the effect of different variables with respect to their contribution to the disruption of seaport operations, decision makers can devise necessary schemes to optimise the operations of their systems.

The implementation of the proposed methodology shows that the model development requires careful consideration of relevant organisational issues, technical, operational, security and natural contextual factors in group collaborative modelling, and the synthesis of a combination of both qualitative and quantitative data into a single model framework. Evidently, the evaluation process further highlight the significance of security in port operations and how it affects the many stakeholders involved in the system. Such an analysis can help to measure the performance effectiveness of seaports. Thus, by improving the resilience and reliability of the system, not only can the occurrence of accidents be reduced, but also the grade of port security can be enhanced. Evaluation of the disruption risk of the system provides a platform for implementation of necessary schemes to improve the resilience of the system in a dynamic environment.

8 Conclusion

This paper has highlights the modelling approach using a BBN to understand the operation of a seaport system and improve its performance. The framework allows port authorities to employ a sound and coherent approach to exploit the BBN in modelling various influencing factors through a flexible tools that can address the diverse risk of disruption proactively, particularly when the need to take into account operational, security, technical, organisational and natural factors is crucial to facilitating resilient port operations.

Representation of uncertainty in results is a concept that is becoming increasingly important for modelling in support of decision making. The methodology presented in this paper is based on utilising a BBN as an intelligent tool for analysing different variables and ranking them according to their influence. The modelling approach includes the identification of relevant factors that influenced the performance of a seaport system for resilience improvement with regard to safety, security and efficiency under high uncertainty.

Potentially, the procedure highlights how both quantitative and qualitative datasets can be integrated in a flexible manner. It further helps to modify and check the accuracy of the model using the concept of d-separation and results in a simpler aggregation of the assessment. The proposed approach also ensures that important factors are not unintentionally omitted during the computational analysis and improves the basis for understanding and design of the system.

The routine monitoring of seaport processes, often carried out by terminal operators and other stakeholders involved in maritime operations, generates vast sets of data that are often analysed periodically and rarely disseminated. The BBN model provides a platform to integrate these diverse monitoring sets and extend their use in a realistic manner, thereby leading to quantifiable improvement in understanding a seaport's processes for resilience improvement. It is envisaged that the proposed model can assist scientists and decision makers to understand the complex operational processes in order to develop necessary strategies aimed at improving the resilience of their systems in a dynamic environment.

Acknowledgements

This research was supported by an EU-funded project WEASTFLOWS (2011-2015).

References

Abdul Rahman, N. S. F., 2013, An assessment of global factors towards the financial performance of a containership using a Bayesian network method. European Journal of Business and Management, Vol.5, No.7, pp. 2222-2839.

An, M., Huang, S. and Baker, C., 2007, Railway risk assessment-the fuzzy reasoning approach and fuzzy analytic hierarchy process approaches: A case study of shunting at Waterloo depot. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 221, 365-383.

Bayraktar, M. E. and Hastak, M., 2009, A decision support system for selecting the optimal contracting strategy in highway work zone projects. Automation in Construction, 18, 834-843.

Berle, Ø., Asbjørnslett, B.E, and Rice, J.B., 2011, Formal vulnerability assessment of a maritime transportation system. Reliability Engineering & System Safety 96 (6):696-705.

Bichou, K.., 2008, Security and risk-based models in shipping and ports: review and critical analysis. OECD/ITF Joint Transport Research Centre Discussion Paper.

Bott, T. F. and Eisenhawer S. W., 2002, Risk analysis using a hybrid Bayesian-approximation methodology, Proceedings of Annual Reliability and Maintenance Symposium, Seattle, USA, Jan 28–31, pp. 127-133.

Christopher, K.., 2010, Port security management: Auerbach Publications. Taylor and Francis group, Florida.

Codetta-raiteri, D., Bobbio, A., Montani, S. and Portinale, L., 2012, A dynamic Bayesian network based framework to evaluate cascading effects in a power grid. Engineering Applications of Artificial Intelligence, 25, 683-697.

Dalziell, E. & Mcmanus, S., 2004, Resilience, vulnerability, and adaptive capacity: implications for system performance.

Eleye-Datubo A., Wall, A. and Wang, J., 2008, Marine and Offshore Safety Assessment by Incorporative Risk Modeling in a Fuzzy-Bayesian Network of an Induced Mass Assignment Paradigm. Risk Analysis, 28, 95-112.

Fritelli, J., 2005, Port and maritime security: background issues for congress. CRS report for congress. Congressional Research Service, Order code RL31733.

Halliwell, J., Keppens, J. and Shen, Q., 2003, Linguistic bayesian networks for reasoning with subjective probabilities in forensic statistics. Proceedings of the 9th international conference on artificial intelligence and law, ACM, 42-50.

Handley-Schachler, M, and Navare, J., 2010, Port risk management and public private partnerships: factors relating to risk allocation and risk sustainability. World Review of Intermodal Transportation Research, 3(1):150-166.

Hollnagel, E., Woods, D. D. and Leveson, N., 2007, Resilience engineering: Concepts and precepts, Ashgate, Aldershot, USA..

Hollnagel, E., Nemeth, C. P. and Dekker, S., 2008, Resilience engineering perspectives: remaining sensitive to the possibility of failure, Ashgate Publishing, Ltd.

Huang, H.-Z., Zuo, M. J. and Sun, Z.-Q., 2006, Bayesian reliability analysis for fuzzy lifetime data. Fuzzy Sets and Systems, 157, 1674-1686.

John, A., Paraskevadakis, D., Bury, A., Yang, Z., Riahi, R. and Wang, J., 2014, An integrated fuzzy risk assessment for seaport operations. Journal of Safety Science, Vol. 68, pp. 180-194.

Johnsen, S. O. and Veen, M., 2013, Risk assessment and resilience of critical communication infrastructure in railways. Cognition, Technology & Work, 15, 95-107.

Kröger, W., 2008, Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. Reliability Engineering & System Safety 93 (12):1781-1787.

Mansouri, M., Nilchiani, R. and Mostashari, A., 2010. A policy making framework for resilient port infrastructure systems, Marine Policy 34 (6):1125-1134.

McGill, W.L, Ayyub, B.M. and Kaminskiy, M., 2007. Risk analysis for critical asset protection. Risk Analysis 27(5):1265-1281.

Miller, G. A., 1956. The magical number seven plus or minus two: some limits on our capacity for processing information. Psychology Rev 63(1): 81–97.

Mokhtari, K.., Ren, J., Roberts, C. and Wang, J., 2011, Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. Journal of hazardous materials 192(2): 465-475.

Mostashari, A., Nilchiani, R., Omer, M., Andalibi, N. and Heydari, B., 2011. A cognitive process architecture framework for secure and resilient seaport operations. Marine Technology Society Journal, 45**,** 120-127.

Nair R., Avetisyan, H. and Miller-hooks, E., 2010. Resilience framework for ports and other intermodal components. Transportation Research Record: Journal of the Transportation Research Board, 2166**,** 54-65.

Nemeth, C. P., Hollnagel, E. and Dekker, S., 2009. Resilience Engineering Perspectives: Preparation and Restoration in Human Systems, Ashgate Publishing, Ltd.

Omer, M., Mostashari, A., Nilchiani, R. and Mansouri, M., 2012. A framework for assessing resiliency of maritime transportation systems. Maritime Policy & Management, 39**,** 685-703.

Pearl, J., 1988. Probabilistic Reasoning in Intelligent Systems: Networks of Plausble Inference, Morgan Kaufmann Pub.

Ren, J., Jenkinson, I., Sii, H., Wang, J., Xu, L. and Yang, J., 2005. An offshore safety assessment framework using fuzzy reasoning and evidential synthesis approaches. Proceedings of IMarEST-Part A-Journal of Marine Engineering and Technology, 2005**,** 3-16.

Reason, J.T. and Hobbs, A., 2003. Managing maintenance error. Aldershot , UK: Ashgate.

Riahi, R., Bonsall, S., Jenkinson, I., and Wang, J., 2012 A seafarer’s reliability assessment incorporating subjective judgements. In: Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment 226(4):313-334.

Riahi, R., Bonsall, S., Jenkinson, I., Wang, J., 2013. A proposed methodology for assessing the reduction of a seafarer’s performance with insufficient recuperative rest, Journal of Marine Engineering and Technology, Vol. 12, no. 2.

Riana, S. and Terje, A. 2011. A risk perspective suitable for resilience engineering, Safety science, Vol. 49, Issue 2, pp. 292–297.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R. K. and Herrera, I. A. 2004. Organisational accidents and resilient organisations: five perspectives. Trondheim, SINTEF Industrial Management, Safety and Reliability. SINTEF report no. STF38 A0440.

Vanem, E., Antao, P., Ostvik, I. and Decomas, F.D.C., 2008. Analysing the risk of LNG carrier operations. Reliability Engineering & System Safety 93(9):1328-1344.

Weick, K. E. and Roberts, K. H., 1993. Collective mind in organizations: Heedful interrelating on flight decks. Administrative science quarterly, 357-381.

Widalsky, A., 1988. Searching for Safety. New Brunswick. CT: Transaction Books.

Woods, D. D., 2000. Lessons from beyond human error: Designing for resilience in the face of change and surprise. Design for Safety Workshop, NASA Ames Research Center,. 8-10.

Yang, J. B., 2001. Rule and utility based evidential reasoning approach for multi attribute decision analysis under uncertainties. European Journal of Operational Research 131(1):31-61.

Yang, Z., Bonsall, S. and Wang, J., 2008. Fuzzy rule-based Bayesian reasoning approach for Prioritization of failures in FMEA. Reliability, IEEE Transactions on, 57, 517-528.

Zimmer, A. C. 1986. What uncertainty judgments can tell about the underlying subjective probabilities? In: Kanal LN and Lemmer JF (eds) Uncertainty in artificial intelligence. Amsterdam, Elsevier Science, 249–258.

Zio, E., Piccinelli, R. and Sansavini, G., 2011. An all-hazard approach for the vulnerability analysis of critical infrastructures. Proceedings of the European Safety and Reliability Conference 2011, 2451-2458.

References

Abdul Rahman, N. S. F., 2013, An assessment of global factors towards the financial performance of a containership using a Bayesian network method. European Journal of Business and Management, Vol.5, No.7, pp. 2222-2839.

An, M., Huang, S. and Baker, C., 2007, Railway risk assessment-the fuzzy reasoning approach and fuzzy analytic hierarchy process approaches: A case study of shunting at Waterloo depot. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 221**,** 365-383.

Bayraktar, M. E. and Hastak, M., 2009, A decision support system for selecting the optimal contracting strategy in highway work zone projects. Automation in Construction, 18**,** 834-843.

Berle, Ø., Asbjørnslett, B.E, and Rice, J.B., 2011, Formal vulnerability assessment of a maritime transportation system. Reliability Engineering & System Safety 96 (6):696-705.

Bichou, K.., 2008, Security and risk-based models in shipping and ports: review and critical analysis. OECD/ITF Joint Transport Research Centre Discussion Paper.

Bott, T. F. and Eisenhawer S. W., 2002, Risk analysis using a hybrid Bayesian-approximation methodology, Proceedings of Annual Reliability and Maintenance Symposium, Seattle, USA, Jan 28–31, pp. 127-133.

Christopher, K.., 2010, Port security management: Auerbach Publications. Taylor and Francis group, Florida.

Codetta-raiteri, D., Bobbio, A., Montani, S. and Portinale, L., 2012, A dynamic Bayesian network based framework to evaluate cascading effects in a power grid. Engineering Applications of Artificial Intelligence, 25**,** 683-697.

Dalziell, E. & Mcmanus, S., 2004, Resilience, vulnerability, and adaptive capacity: implications for system performance.

Eleye-Datubo A., Wall, A. and Wang, J., 2008, Marine and Offshore Safety Assessment by Incorporative Risk Modeling in a Fuzzy-Bayesian Network of an Induced Mass Assignment Paradigm. Risk Analysis, 28**,** 95-112.

Fritelli, J., 2005, Port and maritime security: background issues for congress. CRS report for congress. Congressional Research Service, Order code RL31733.

Halliwell, J., Keppens, J. and Shen, Q., 2003, Linguistic bayesian networks for reasoning with subjective probabilities in forensic statistics. Proceedings of the 9th international conference on artificial intelligence and law, ACM, 42-50.

Handley-Schachler, M, and Navare, J., 2010, Port risk management and public private partnerships: factors relating to risk allocation and risk sustainability. World Review of Intermodal Transportation Research, 3(1):150-166.

Hollnagel, E., Woods, D. D. and Leveson, N., 2007, Resilience engineering: Concepts and precepts, Ashgate, Aldershot, USA..

Hollnagel, E., Nemeth, C. P. and Dekker, S., 2008, Resilience engineering perspectives: remaining sensitive to the possibility of failure, Ashgate Publishing, Ltd.

Huang, H.-Z., Zuo, M. J. and Sun, Z.-Q., 2006, Bayesian reliability analysis for fuzzy lifetime data. Fuzzy Sets and Systems, 157**,** 1674-1686.

John, A., Paraskevadakis, D., Bury, A., Yang, Z., Riahi, R. and Wang, J., 2014, An integrated fuzzy risk assessment for seaport operations. Journal of Safety Science, Vol. 68, pp. 180-194.

Johnsen, S. O. and Veen, M., 2013, Risk assessment and resilience of critical communication infrastructure in railways. Cognition, Technology & Work, 15**,** 95-107.

Kröger, W., 2008, Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. Reliability Engineering & System Safety 93 (12):1781-1787.

Mansouri, M., Nilchiani, R. and Mostashari, A., 2010. A policy making framework for resilient port infrastructure systems, Marine Policy 34 (6):1125-1134.

McGill, W.L, Ayyub, B.M. and Kaminskiy, M., 2007. Risk analysis for critical asset protection. Risk Analysis 27(5):1265-1281.

Miller, G. A., 1956. The magical number seven plus or minus two: some limits on our capacity for processing information. Psychology Rev 63(1): 81–97.

Mokhtari, K.., Ren, J., Roberts, C. and Wang, J., 2011, Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals. Journal of hazardous materials 192(2): 465-475.

Mostashari, A., Nilchiani, R., Omer, M., Andalibi, N. and Heydari, B., 2011. A cognitive process architecture framework for secure and resilient seaport operations. Marine Technology Society Journal, 45**,** 120-127.

Nair R., Avetisyan, H. and Miller-hooks, E., 2010. Resilience framework for ports and other intermodal components. Transportation Research Record: Journal of the Transportation Research Board, 2166**,** 54-65.

Nemeth, C. P., Hollnagel, E. and Dekker, S., 2009. Resilience Engineering Perspectives: Preparation and Restoration in Human Systems, Ashgate Publishing, Ltd.

Omer, M., Mostashari, A., Nilchiani, R. and Mansouri, M., 2012. A framework for assessing resiliency of maritime transportation systems. Maritime Policy & Management, 39**,** 685-703.

Pearl, J., 1988. Probabilistic Reasoning in Intelligent Systems: Networks of Plausble Inference, Morgan Kaufmann Pub.

Ren, J., Jenkinson, I., Sii, H., Wang, J., Xu, L. and Yang, J., 2005. An offshore safety assessment framework using fuzzy reasoning and evidential synthesis approaches. Proceedings of IMarEST-Part A-Journal of Marine Engineering and Technology, 2005**,** 3-16.

Reason, J.T. and Hobbs, A., 2003. Managing maintenance error. Aldershot , UK: Ashgate.

Riahi, R., Bonsall, S., Jenkinson, I., and Wang, J., 2012 A seafarer's reliability assessment incorporating subjective judgements. In: Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment 226(4):313-334.

Riahi, R., Bonsall, S., Jenkinson, I., Wang, J., 2013. A proposed methodology for assessing the reduction of a seafarer's performance with insufficient recuperative rest, Journal of Marine Engineering and Technology, Vol. 12, no. 2.

Riana, S. and Terje, A. 2011. A risk perspective suitable for resilience engineering, Safety science, Vol. 49, Issue 2, pp. 292–297.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R. K. and Herrera, I. A. 2004. Organisational accidents and resilient organisations: five perspectives. Trondheim, SINTEF Industrial Management, Safety and Reliability. SINTEF report no. STF38 A0440.

Weick, K. E. and Roberts, K. H., 1993. Collective mind in organizations: Heedful interrelating on flight decks. Administrative science quarterly**,** 357-381.

Widalsky, A., 1988. Searching for Safety. New Brunswick. CT: Transaction Books.

Woods, D. D., 2000. Lessons from beyond human error: Designing for resilience in the face of change and surprise. Design for Safety Workshop, NASA Ames Research Center,. 8-10.

Yang, J. B., 2001. Rule and utility based evidential reasoning approach for multi attribute decision analysis under uncertainties. European Journal of Operational Research 131(1):31-61.

Vanem, E., Antao, P., Ostvik, I. and Decomas, F.D.C., 2008. Analysing the risk of LNG carrier operations. Reliability Engineering & System Safety 93(9):1328-1344.

Yang, Z., Bonsall, S. and Wang, J., 2008. Fuzzy rule-based Bayesian reasoning approach for Prioritization of failures in FMEA. Reliability, IEEE Transactions on, 57**,** 517-528.

Zimmer, A. C. 1986. What uncertainty judgments can tell about the underlying subjective probabilities? In: Kanal LN and Lemmer JF (eds) Uncertainty in artificial intelligence. Amsterdam, Elsevier Science, 249–258.

Zio, E., Piccinelli, R. and Sansavini, G., 2011. An all-hazard approach for the vulnerability analysis of critical infrastructures. Proceedings of the European Safety and Reliability Conference 2011, 2451-2458.

Figure Captions:

Figure 1: Sea-Land Interface of Maritime Transportation Systems

Figure 2: Flow Diagram for Implementing the Proposed Methodology

Figure 3: Dependency Model for the Disruption Risk of a Seaport

Figure 4: Membership Functions (MFs) for Quantitative Criterion (Lack of Equipment Maintenance)

Figure 5: Aggregation Result for Disruption Estimate

Figure 6: Sensitivity Analysis Result due to Variation of Input Data

FIGURE 1

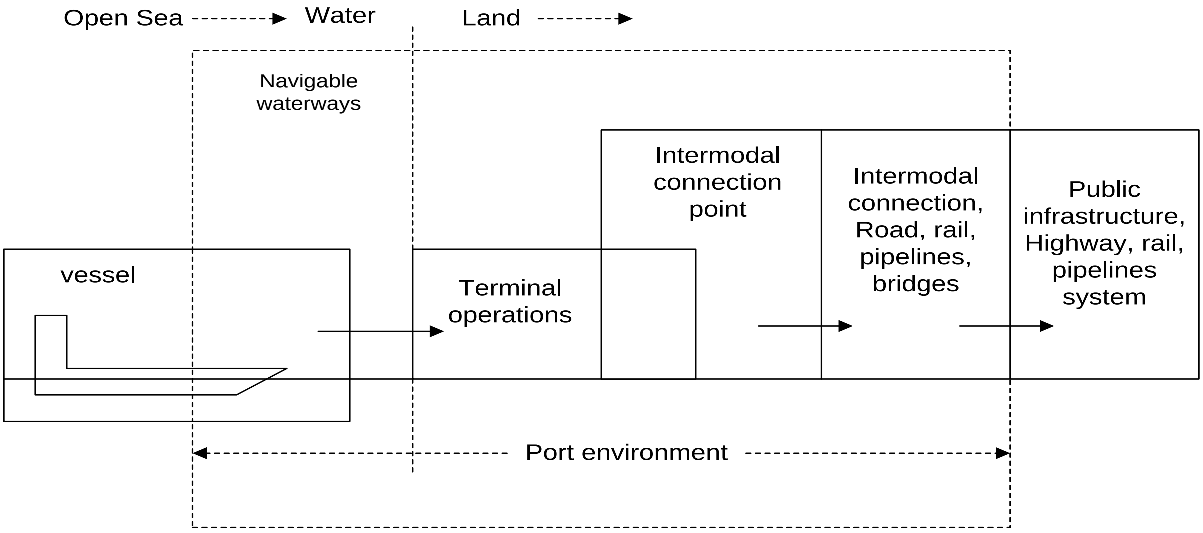
Open Sea
Water
Land
Navigable waterways
vessel
Terminal operations
Intermodal connection point
Intermodal connection, Road, rail, pipelines, bridges
Public infrastructure, Highway, rail, pipelines system
Port environment

FIGURE 2

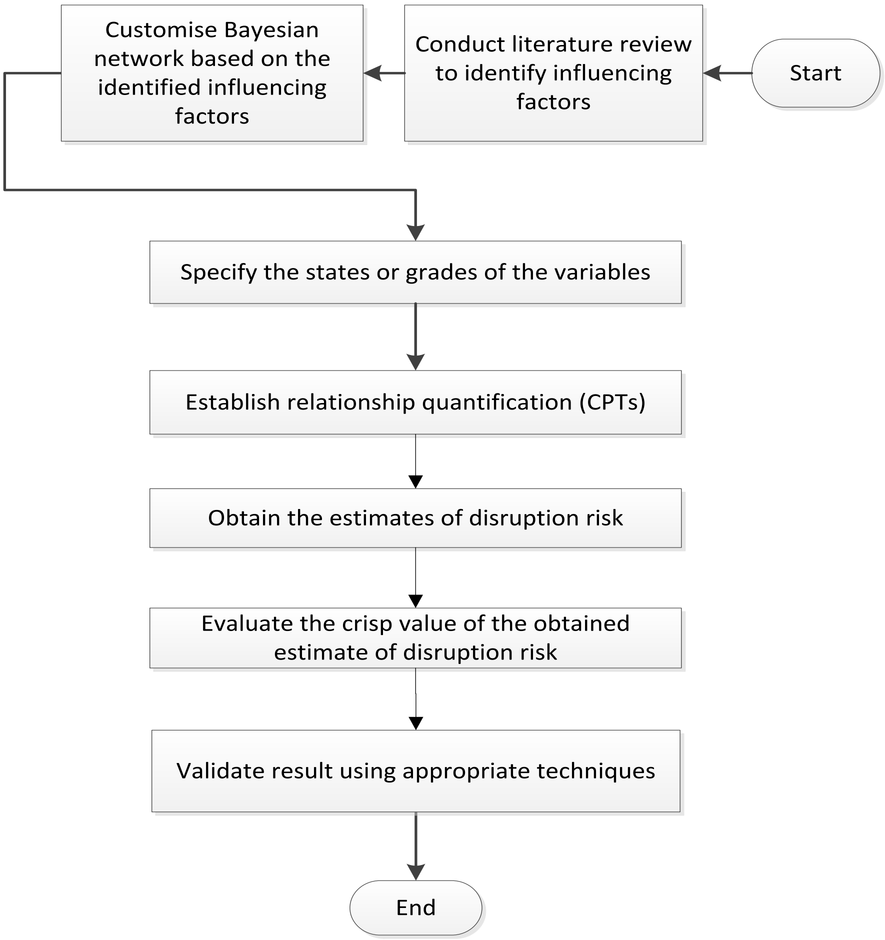
Start
Conduct literature review to identify influencing factors
Customise Bayesian network based on the identified influencing factors
Specify the states or grades of the variables
Establish relationship quantification (CPTs)
Obtain the estimates of disruption risk
Evaluate the crisp value of the obtained estimate of disruption risk
Validate result using appropriate techniques
End

FIGURE 3

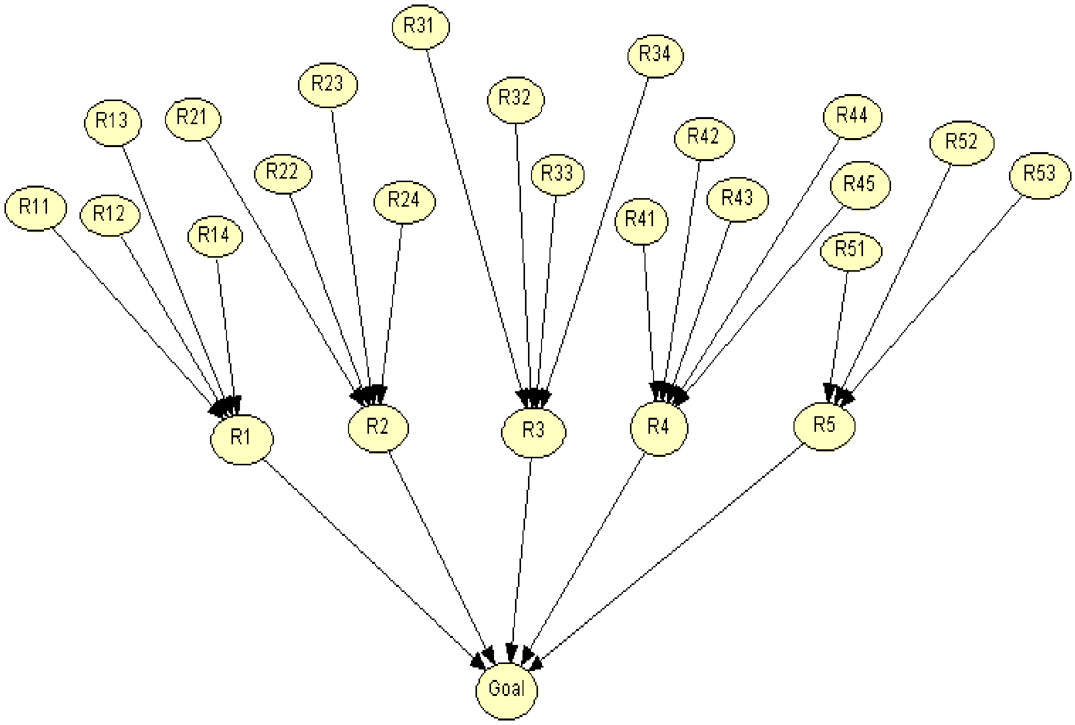

FIGURE 4

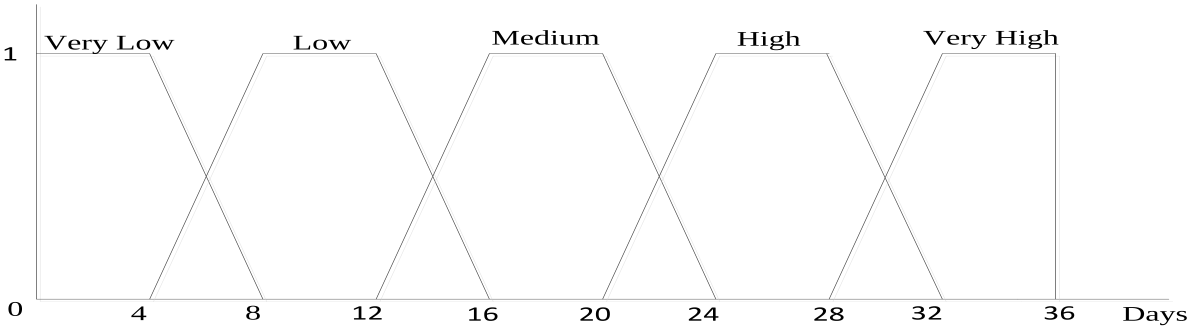

FIGURE 5

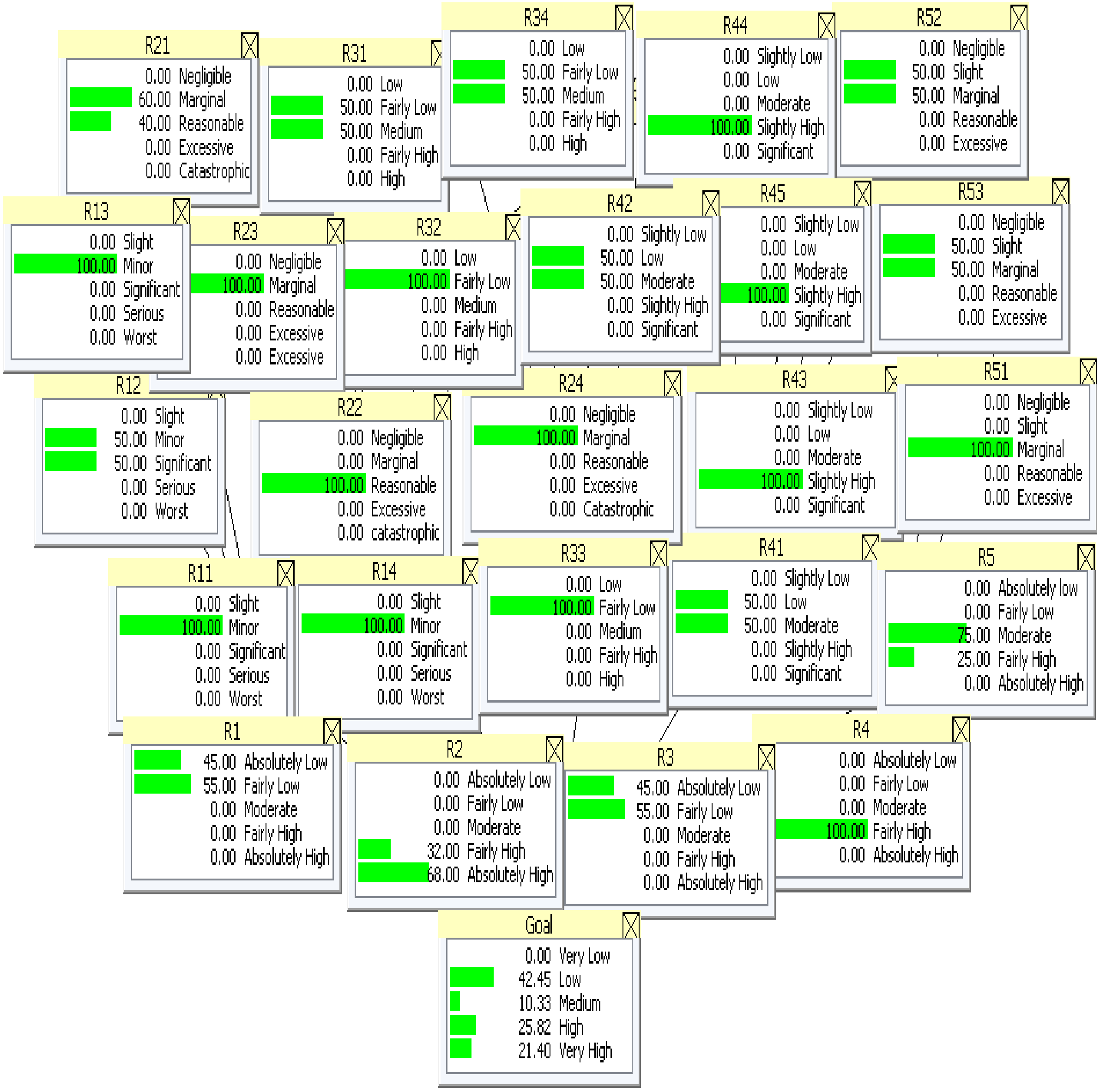
R21
0.00 Negligible
60.00 Marginal
40.00 Reasonable
0.00 Excessive
0.00 Catastrophic
R31
0.00 Low
50.00 Fairly Low
50.00 Medium
0.00 Fairly High
0.00 High
R34
0.00 Low
50.00 Fairly Low
50.00 Medium
0.00 Fairly High
0.00 High
R44
0.00 Slightly Low
0.00 Low
0.00 Moderate
100.00 Slightly High
0.00 Significant
R52
0.00 Negligible
50.00 Slight
50.00 Marginal
0.00 Reasonable
0.00 Excessive
R13
0.00 Slight
100.00 Minor
0.00 Significant
0.00 Serious
0.00 Worst
R23
0.00 Negligible
100.00 Marginal
0.00 Reasonable
0.00 Excessive
0.00 Excessive
R32
0.00 Low
100.00 Fairly Low
0.00 Medium
0.00 Fairly High
0.00 High
R42
0.00 Slightly Low
50.00 Low
50.00 Moderate
0.00 Slightly High
0.00 Significant
R45
0.00 Slightly Low
0.00 Low
0.00 Moderate
100.00 Slightly High
0.00 Significant
R53
0.00 Negligible
50.00 Slight
50.00 Marginal
0.00 Reasonable
0.00 Excessive
R12
0.00 Slight
50.00 Minor
50.00 Significant
0.00 Serious
0.00 Worst
R22
0.00 Negligible
0.00 Marginal
100.00 Reasonable
0.00 Excessive
0.00 catastrophic
R24
0.00 Negligible
100.00 Marginal
0.00 Reasonable
0.00 Excessive
0.00 Catastrophic
R43
0.00 Slightly Low
0.00 Low
0.00 Moderate
100.00 Slightly High
0.00 Significant
R51
0.00 Negligible
0.00 Slight
100.00 Marginal
0.00 Reasonable
0.00 Excessive
R11
0.00 Slight
100.00 Minor
0.00 Significant
0.00 Serious
0.00 Worst
R14
0.00 Slight
100.00 Minor
0.00 Significant
0.00 Serious
0.00 Worst
R33
0.00 Low
100.00 Fairly Low
0.00 Medium
0.00 Fairly High
0.00 High
R41
0.00 Slightly Low
50.00 Low
50.00 Moderate
0.00 Slightly High
0.00 Significant
R5
0.00 Absolutely low
0.00 Fairly Low
75.00 Moderate
25.00 Fairly High
0.00 Absolutely High
R1
45.00 Absolutely Low
55.00 Fairly Low
0.00 Moderate
0.00 Fairly High
0.00 Absolutely High
R2
0.00 Absolutely Low
0.00 Fairly Low
0.00 Moderate
32.00 Fairly High
68.00 Absolutely High
R3
45.00 Absolutely Low
55.00 Fairly Low
0.00 Moderate
0.00 Fairly High
0.00 Absolutely High
R4
0.00 Absolutely Low
0.00 Fairly Low
0.00 Moderate
100.00 Fairly High
0.00 Absolutely High
Goal
0.00 Very Low
42.45 Low
10.33 Medium
25.82 High
21.40 Very High

FIGURE 6

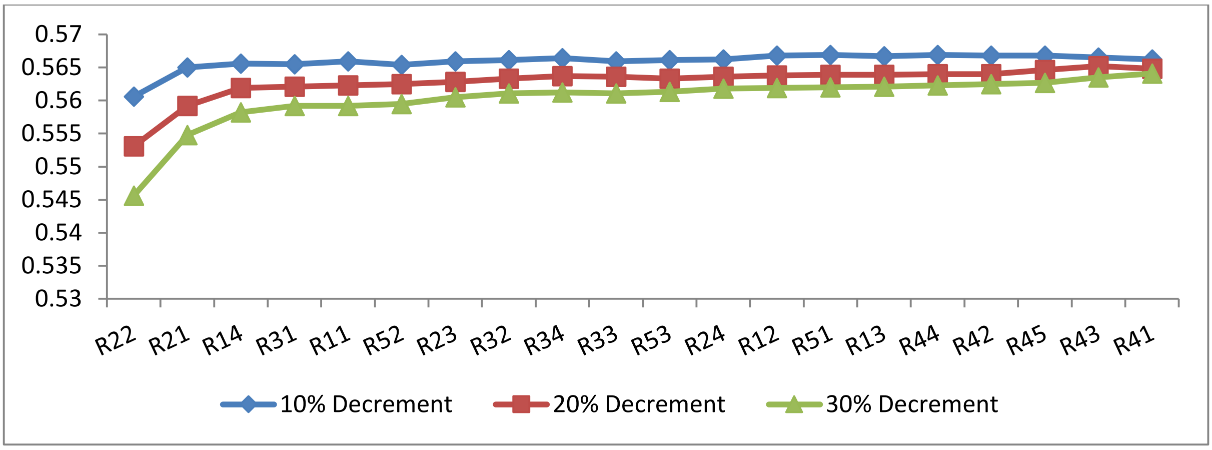
0.57
0.565
0.56
0.555
0.55
0.545
0.54
0.535
0.53
R22
R21
R14
R31
R11
R52
R23
R32
R34
R33
R53
R24
R12
R51
R13
R44
R42
R45
R43
R41
10% Decrement
20% Decrement
30% Decrement

Table Captions

Table 1

Risk Type	Cause
Operational Risk Factors	Port equipment failures
	Vessel accident/grounding
	Cargo spillage
	Human errors
Security Risk Factors	Sabotage
	Terrorism attacks
	Surveillance system failures
	Arson
Technical Risk Factors	Lack of equipment maintenance
	Lack of navigational aid maintenance
	Lack of IT system maintenance
	Lack of dredging maintenance
Organisational Risk Factors	Labour unrest
	Dispute with regulatory bodies
	Berth congestion
	Gate congestion
	Storage area congestion
Natural Risk Factors	Geologic/Seismic
	Hydrologic
	Atmospheric
Goal	Operational Risk Factors
	Security Risk Factors
	Technical Risk Factors
	Organisational Risk Factors
	Natural Risk Factors

Table 2 (Adapted and modified from (Abdul Rahman, 2013))

Probability Rate	0	1	2	3	4	5	6	7	8	9	10
Probability Value	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0

Table 3

Node Type	Abbreviation	Node Description
Decision node	DR	Disruption Risk of a Seaport
Target node	R1	Operational Risk Factors
Starting node	R11	Port Equipment Failures
Starting node	R 12	Vessel Collision/Grounding
Starting node	R 13	Cargo Spillages
Starting node	R 14	Human Related Failures
Target node	R 2	Security Risk Factors
Starting node	R 21	Sabotage
Starting node	R 22	Terrorism Attacks
Starting node	R 23	Surveillance System Failure
Starting node	R 24	Arson
Target node	R 3	Technical Risk Factors
Starting node	R 31	Lack of Equipment Maintenance
Starting node	R 32	Lack of Navigational Maintenance
Starting node	R 33	Lack of IT System Maintenance
Starting node	R 34	Lack of Dredging Maintenance
Starting node	R 4	Organisational Risk Factors
Target node	R 41	Labour Unrest
Starting node	R 42	Dispute with Regulatory Bodies
Starting node	R 43	Berth Congestion
Starting node	R 44	Gate Congestion
Starting node	R 45	Storage Area Congestion
Starting node	R 5	Natural Risk Factors
Target node	R 51	Geologic
Starting node	R 52	Hydrologic
Starting node	R 53	Atmospheric
Starting node		

Table 4

Quantitative Criteria	Period of Disruption
Lack of equipment maintenance	28-32 days
Lack of navigational aid maintenance	20-24 days
Lack of dredging maintenance	20-24 days
Lack of IT system maintenance	12-16 days

Table 5

Nodes	**Linguistic assessment**				
Goal	Very Low	Low	Medium	High	Very High
Operational risk factors	Absolutely Low	Fairly Low	Moderate	Fairly High	Absolutely High
Security risk factors	Absolutely Low	Fairly Low	Moderate	Fairly High	Absolutely High
Technical risk factors	Absolutely Low	Fairly Low	Moderate	Fairly High	Absolutely High
Organisational risk factors	Absolutely Low	Fairly Low	Moderate	Fairly High	Absolutely High
Natural risk factors	Absolutely Low	Fairly Low	Moderate	Fairly High	Absolutely High
Port equipment failures	Slight	Minor	Significant	Serious	Worst
Vessels accident	Slight	Minor	Significant	Serious	Worst
Cargo spillage	Slight	Minor	Significant	Serious	Worst
Human related error	Slight	Minor	Significant	Serious	Worst
Sabotage	Negligible	Marginal	Reasonable	Excessive	Catastrophic
Terrorism attacks	Negligible	Marginal	Reasonable	Excessive	Catastrophic
Surveillance system failure	Negligible	Marginal	Reasonable	Excessive	Catastrophic
Arson	Negligible	Marginal	Reasonable	Excessive	Catastrophic
Lack of equipment maintenance	Low	Fairly Low	Medium	Fairly High	High
Lack of navigational aid maintenance	Low	Fairly Low	Medium	Fairly High	High
Lack of IT system maintenance	Low	Fairly Low	Medium	Fairly High	High
Lack of dredging maintenance	Low	Fairly Low	Medium	Fairly High	High
Labour unrest	Slightly Low	Low	Moderate	Slightly High	High
Dispute with regulatory body	Slightly Low	Low	Moderate	Slightly High	High
Berth congestion	Slightly Low	Low	Moderate	Slightly High	High
Gate congestion	Slightly Low	Low	Moderate	Slightly High	High
Storage area congestion	Slightly Low	Low	Moderate	Slightly High	High
Geologic/Seismic	Negligible	Slight	Marginal	Reasonable	Excessive
Hydrologic	Negligible	Slight	Marginal	Reasonable	Excessive
Atmospheric	Negligible	Slight	Marginal	Reasonable	Excessive

Table 6

Child node	Root nodes	Weights
Operational Risk Factors	R11	0.310
	R12	0.183
	R13	0.258
	R14	0.249
Security Risks Factors	R21	0.281
	R22	0.406
	R23	0.124
	R24	0.189
Technical Risk Factors	R31	0.390
	R32	0.176
	R33	0.283
	R34	0.150
Organisational Risk Factors	R41	0.275
	R42	0.154
	R43	0.181
	R44	0.214
	R45	0.176
Natural Risk Factors	R51	0.388
	R52	0.357
	R53	0.255
Goal	R1	0.246
	R2	0.291
	R3	0.188
	R4	0.153
	R5	0.122

Table 7

H_n	Very Low	Low	Medium	High	Very High
V_n	1	2	3	4	5
$u(H_n)$	$\frac{1-1}{5-1}=0$	$\frac{2-1}{5-1}=0.25$	$\frac{3-1}{5-1}=0.5$	$\frac{4-1}{5-1}=0.75$	$\frac{5-1}{5-1}=1$
β_n	0	0.4245	0.1033	0.2582	0.2140
$\sum_{n=1}^{N}\beta_n = 0 + 0.4245 + 0.1033 + 0.2582 + 0.2140 = 1 \rightarrow \beta_H = 0$					
$\beta_n \times u(H_n)$	0	0.1061	0.0517	0.1937	0.2140
$D_{DR} = \sum_{n=1}^{N}\beta_n \times u(H_n) = 0.5655 \approx 0.57$					

Table 8

Child Nodes	Root Nodes	10%	20%	30%
R1	R 11	0.5606	0.5531	0.5456
	R 12	0.565	0.5592	0.5548
	R 13	0.5656	0.5619	0.5582
	R 14	0.5655	0.5621	0.5592
R2	R 21	0.5659	0.5623	0.5592
	R 22	0.5654	0.5625	0.5595
	R 23	0.5659	0.5628	0.5605
	R 24	0.5661	0.5633	0.5611
R3	R 31	0.5664	0.5637	0.5612
	R 32	0.5659	0.5636	0.5611
	R 33	0.5661	0.5633	0.5613
	R 34	0.5662	0.5636	0.5618
R4	R41	0.5668	0.5638	0.5619
	R42	0.5669	0.5639	0.562
	R43	0.5667	0.5639	0.5621
	R44	0.5669	0.564	0.5623
	R45	0.5668	0.564	0.5625
R5	R51	0.5668	0.5646	0.5627
	R52	0.5665	0.5652	0.5635
	R53	0.5662	0.5648	0.5641