Port vulnerability assessment from a supply chain perspective

Abstract: Rapid development of maritime transportation networks meets international trade demands while rendering them in high risk and disruption concerns particularly at ports being the bottlenecks of the whole flows. Port operations call for an effective approach to assess port vulnerability and to ensure the resilience of its associated maritime supply chains (MSCs). However, traditional quantitative risk analysis reveals challenges due to data incompleteness and ambiguity, and operational and environmental uncertainty when being applied in port vulnerability analysis. This paper aims to develop a novel port vulnerability assessment (PVA) framework, which can guide and realise a standardised vulnerability analysis process for the ports from different geographies involving in the same MSC and hence the resources can be better managed from a global network level for optimal resilience of the chain. It is especially important for the shipping and port industries which are in nature international and desire strong international uniform standardization. The fuzzy theory, evidential reasoning (ER) approach, and expected utility theory are combined in a holistic way to form the proposed PVA framework. The new framework is validated and demonstrated by using a case study in which five key ports along an established MSC in China are investigated. The findings can be used as a stand along method to compare the vulnerability levels of the ports in an MSC and/or integrated with decision optimisation methods for rational safety resource distribution from a supply chain perspective.

Keywords: Port vulnerability; transport resilience; vulnerability analysis, port risk; evidential reasoning; maritime supply chain

1. Introduction

Maritime supply chain (MSC) is a network chain structure formed by a series of upstream and downstream enterprises or departments that provide maritime services to the end users. In other words, an MSC is a supply chain that is composed of maritime stakeholders providing shipping services and aims at customer satisfaction to jointly complete the transportation function of goods from the place of shipment to the destination (Vanelslander and Sys, 2020). During the past decades, MSCs have been

one of the largest complex transportation networks in the world on account of the rapid development of economic globalisation, trade liberalisation, and green transportation (Blonigen and Wilson, 2013). Maritime transportation as the most crucial transport mode for global trade, accounts for over 80% of intercontinental trade volume (UNCTAD, 2019). The safe operations of the nodes (i.e. ports) and links (i.e. shipping routes) play a significant role to ensure the resilience of an MSC (Calatayud et al., 2017). Ports, as lifelines in coastal cities while the bottlenecks of MSCs, are vulnerable to a variety of threats including both natural disasters and deliberate attacks due to their natural geographical advantages and important economic functions (Cao and Lam, 2019). The failures of ports tend to disrupt the efficient and smooth flow of products along the MSCs thus affects global trade. Djankov et al. (2011) and Hummels and Schaur (2013) have argued that if a product is delayed for one day, its likelihood of being traded decreases by 1% (6% for time-sensitive products) and it is devalued by 0.8%. Different with the traditional risk analysis of ports at which each port is treated in isolation, the recent literature (Calatayud et al., 2017; Liu et al., 2018) reveals that the resilience of the ports along an integrated MSC should be analysed from a systematic network point of view, where port vulnerability assessment (PVA) from an MSC perspective becomes necessary. In the meantime, the standardization of container ports grows given the increased containerised cargo volume globally. This paper aims to develop a new PVA framework that can help standardise the vulnerability assessment of all the ports along the same MSC, and hence facilitate the competition and cooperation of operational resources for resilient maritime transportation holistically.

Some previous accidents concerning port safety include the 9/11terrorist attacks in 2001, the lock-out of the American West Coast Port in 2002, the Port of Busan in the 2003 Typhoon Maemi, the Fukushima nuclear disaster in 2011, and the recent major explosion of Tianjin Port in 2015, etc. They arise high attention on risk assessment and management of ports in MSCs. As the core content of risk-based resilience analysis of a complex transport network, vulnerability assessment is critical to decision-makers (Hsieh, 2014). Measures such as efficiency, resilience, and robustness can well reflect and show a high association with port vulnerability (Cao and Lam, 2019). As a result, the connotations of risk, safety, vulnerability, and vulnerability measures overlap to some extent, but are not identical (Wan et

al., 2018). Among numerous existing papers, risk is described as a combination of the hazardous event, consequence and uncertainty. It can be quantified by risk parameters derived from different transportation systems that risk analysts studied (Nguyen et al., 2019). The definition of safety by Merriam Webster is the condition of being safe from undergoing or causing hurt, injury, or loss. The research effort on transportation safety has been extensive, ranging from traditional safety risk to vulnerability and resilience (Wan et al. 2018). Vulnerability is defined as the degree to which a transportation system is susceptible to that may limit its ability to endure, handle and survive hazardous events, inspired by McIntosh and Becker (2019). The concept of resilience, often used in a more positive context than vulnerability, is considered as the ability of systems to recover quickly from hazardous event or trend or disruptions.

A careful literature review on port vulnerability in MSCs reveals three major challenges which urge some relevant theoretical implications to be addressed from a supply chain/transport network perspective. First, in tradition, port risk in general and vulnerability in specific has received relatively less attention compared to other managerial studies such as port efficiency, competition, and cooperation (e.g. Xie et al., 2021; Xu et al., 2021a; Xu et al., 2021b; Xu et al., 2021c; Song et al., 2018; Ishii et al., 2013; Serebrisky et al., 2016; Suárez-Alemán et al., 2016). Secondly, most port risk analysis is conducted from the perspective of a single port safety in isolation without the consideration of its impact on the upstream/downstream ports in the same MSC (e.g. Alyami et al., 2014, 2019; Yeo et al., 2013; Yang et al., 2014). Furthermore, despite much effort, the definitions of port vulnerability vary and are still at large context dependent (Liu et al., 2018). Therefore, there lacks of a generic methodology that is capable of using a quantitative method to describe port vulnerability scientifically. Thirdly, the vulnerability measures are described by data in diverse formations. It is critical to fuse these diverse data formations (Liu et al., 2004) and to cope with the high uncertainty in data (Yang et al., 2009), in order to gain an acceptable and robust measure to represent the vulnerability uniformly for all the involved ports in an MSC. Given such challenges, it is necessary and beneficial to develop a new PVA method with urgency.

In light of the above, this paper starts with the analysis of the different terms relating to vulnerability. In this process, the measures used to describe port vulnerability are identified and then further verified by the incorporation of domain experts. A PVA framework is developed with the supporting methods of fuzzy theory and an ER approach (Yang et al., 2001; Zhang et al., 2020) within the context of MSCs. In the framework, network modelling is first used to obtain the importance of ports by degree centrality. Here, we defined the degree centrality of a node *i* (i.e. port) as the number of links a node *i* incoming or outgoing connections to and from nodes *j* in the same MSC (Calatayud wt al., 2017; Laxe et al., 2012). It symbolizes the importance of the node in the MSC. The result from the port centrality is used to define the port importance in an MSC (e.g. Liu et al., 2018) and to present its external impact on upstream/downstream bodies in the MSC. The weights of all the involved ports are then integrated as a measure to calculate each port's vulnerability level using a hybrid fuzzy ER approach (Yang et al., 2009; 2013). The vulnerability measures of a port consist of several aspects based on their characteristic functions. The importance of a port in an MSC refers to the influential degree that a port is affected when facing disruptions (Liu et al., 2018). The importance of a port plays a critical role in PVA. Thus, its importance among the MSC is taken into consideration as a vulnerability measure. By doing this, the paper is for the first time to integrate the port importance in an MSC into their vulnerability analysis in a quantitative manner.

Since the risk data relating to ports are often presented in diverse formations, the fuzzy theory is used for its superiority in dealing with both objective and subjective data (Wan et al., 2019). Linguistic terms are used to describe vulnerability measures. The ER approach is selected to assess the vulnerability of ports because of its suitability in fusing diverse data formations and its capability of minimizing the loss of important information in the fusion process (John et al., 2014). The fuzzy IF-THEN rules with degrees are used for its advantage in the inference between the premises and the conclusions (Yang et al., 2014; Yang et al., 2009). In addition, the rules do not require numerical numbers as input data to assess the vulnerability measures (Wang et al., 1995). Furthermore, the network modelling method based on the centrality theory is applied to assess the importance of a port along an MSC for its easiness and visibility, which is appreciated by maritime stakeholders in practice

(Calatayud et al., 2017). The novelty of this work lies in 1) the application of a network modelling method that enriches the measures of vulnerability by taking into account the interactive impact of the ports in an MSC; 2) the use of a hybrid method of fuzzy rule base and the ER that can properly deal with the uncertainties and fuse various forms of data without losing important information; 3) the presentation of a common framework that can, from both theoretical and practical viewpoints, facilitate the assessment of various port vulnerabilities of different natures in the same framework and provide decision-makers with a standardised process of vulnerability assessment for the ports from different geographies in MSCs.

The remainder of this study is organized as follows. The next section reviews the relevant literature on the vulnerability studies in MSCs. Section 3 describes a new PVA framework and the integrated supporting methods in detail. In Section 4 the proposed framework is applied in a real case by analysing the five key ports of an MSC. The research implications and main conclusions are drawn in Sections 5 and 6, respectively.

2. Literature review

Previous port studies mainly focus on competitiveness, cooperation, economic growth, and port efficiency. However, with the rapid development of complex maritime transportation networks and occurrence of the hazard events of low frequency but high consequence, port vulnerability has been receiving increasing attention in recent years (Elleuch et al., 2016). The concept of vulnerability was first used in disaster reduction literature in 1970s, and then it was quickly referred to other disciplines (Gaillard, 2010). Until now, the definition of vulnerability varies and there is no universally accepted definition due to its multidimensional characteristics (Laxe et al., 2012; Mattsson and Jenelius, 2015; Li et al., 2019). The UN/ISDR (2009) defined the vulnerability associated with systems or elements that make them susceptible to the damaging influence of a hazard and divided vulnerability into different aspects containing social science, natural science, and engineering science. Thus, vulnerability is a negative indicator during the process of system performance assessment. In other words, systems (e.g. ports) with higher vulnerability are those which are less robust to hazard events. In addition, the

importance of elements or systems is related to their vulnerability. A careful research review on vulnerability argued that more important elements or systems are more vulnerable in a transportation network (Liu et al., 2018; Calatayud et al., 2017; Laxe et al., 2012). Brooks (2003) proposed a definition of vulnerability that is considered as the amount of damages a hazard event causes to the affected systems or elements. The definition turns the qualitative characteristic of vulnerability into quantifiable ones that can be calculated by a proper method. Hsieh et al. (2014) analysed the port vulnerability with the concept of the efficiency to provide sufficient operational service as a port and the resilience of a port against these hazard events. Elleuch et al. (2016) provided an overview of the literature to understand the concepts of vulnerability and resilience within the context of MSCs. Wang et al. (2020) added a new risk parameter (i.e. resilience) in the design of a risk analysis of the UK nationwide rail systems to climate change. The resilience is considered as a part of measures for determining how vulnerable a system is. Contrary to the concept of vulnerability, resilience has a positive connotation. Many measures can well reflect and show a high association with vulnerability within the port context, including but not limited to robustness (e.g. Liu et al., 2018; Wan et al., 2018), importance (e.g. Liu et al., 2018; Calatayud et al., 2017; Laxe et al., 2012), efficiency (e.g. Yuen et al., 2012; Cao and Lam, 2019), and resilience (e.g. Elleuch et al., 2016; Wan et al., 2018; Mcintosh and Becker, 2019). It is noteworthy that the same term can sometimes be interpreted from various perspectives to meet the different needs in a variety of applications. The most commonly used terms that can well reflect and describe the characteristics and connotations of vulnerability are summarized in Table 1.

Table 1 Interpretation of terms related to vulnerability

Measures	Interpretation/description	Reference
Robustness	It is generally defined as the capability to resist or absorb hazardous events or disruptions. It is the quality of strength, health, and endurance.	Liu et al., 2018; Wan et al., 2018
Importance	It is defined as the role that the presence and location of a specific element play with respect to the average global and local connection properties of the whole network. The importance of a port among an MSC refers to the influential degree that a port is affected when facing disruptions.	Liu et al., 2018; Calatayud et al., 2017; Laxe et al., 2012
Efficiency	It is defined as the capability of providing normal operational functions after hazardous events or disruptions.	Yuen et al., 2012; Cao and Lam, 2019; Gaillard, 2010
Resilience	It is defined as the ability of an entity or system to return to a normal condition after its original state being affected by hazardous events or disruptions.	Elleuch et al., 2016; Wan et al., 2018;

	Mcintosh and Becker, 2019; Wan et al., 2020

In this paper, the concepts of vulnerability used in the previous studies are investigated, and robustness (R), importance (I), efficiency (E), and resilience (S) are selected as the port vulnerability measures (Cao and Lam, 2019; Earnest et al., 2012; Liu et al., 2018). By doing so, the port vulnerability is for the first time evaluated from both internal (local port level) and external (global MSC impact) perspectives. Robustness concerns the ability of a port system to maintain its desired state within a narrow range of performance (Mumby et al., 2014). Specifically, port robustness describes the ability of a port to adapt and innovate in responding to hazard events. A robust port needs feedback controls to resist hazard events, and its throughput does not decline significantly despite the disturbances. Port importance describes the role that a port affects the others within the MSC it involves from the perspective of the whole network (Liu et al., 2018). It as a bridge connects the port local vulnerability in isolation with the associated MSC via the network centrality and coordination. In this case, more important a port, more vulnerable it could be in the MSC. The importance of a port is measured in a direct way by using the degree centrality (Laxe et al., 2012; Calatayud et al., 2017; Liu et al., 2018). Port efficiency is used to measure the capabilities of a port providing resources and assets it possesses to resist, cope with, and recover after a disruption (Gaillard, 2010). The efficiency of a port can be quantified by the percentage of its actual throughput of cargoes to its total capacity after a disruption. Obviously, in this manner, the loss of port efficiency after a disturbance can be used to measure the vulnerability of the port. Port resilience defines the ability (in terms of speed/recovery period) of a port to return to a stable state after a major disturbance (Elleuch et al., 2016). It associates with the period prior to a hazard event, and temporal period during and after the disturbance (Mcintosh and Becker, 2019). A vulnerable port needs longer time than robust ones to return to its original state or a new acceptable equilibrium after a disruption.

3. A novel port vulnerability assessment framework

This section outlines the steps of developing the proposed PVA framework. As shown in Fig.1, after an investigated port in an MSC is selected, a vulnerability assessment hierarchy structure is first established, where the unique vulnerability measures and their hierarchical structure characterising the MSC are identified. The fuzzy theory and ER approach are used to fuse different types of vulnerability measures to obtain comprehensive vulnerability estimates. The estimates of each expert regarding the defined four measures in Table 1 are combined to generate the final results and the crisp numbers for vulnerability prioritization. They are obtained and used as a benchmarking index for expressing the overall port vulnerability in a quantitative manner. Finally, a sensitivity analysis is performed to verify the proposed framework.

Detailed steps are illustrated in the following sub-sections. Section 3.1 describes the research framework visually presented in Fig.1, providing a basic foundation for the layout and integrity of all the supporting methods. Section 3.2 introduces a detailed application of the fuzzy theory in information acquisition and representation in the preparatory step. Section 3.3 shows the inference mechanism and synthesis procedure of the ER approach within the PVA context.

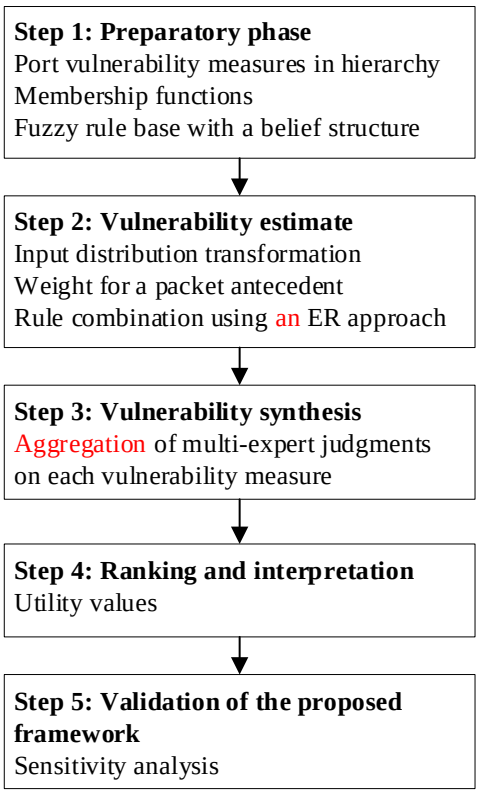

Fig.1 Research framework for vulnerability analysis

3.1 Research framework

As shown in Fig. 1, the preparatory step focuses on the identification and process of port vulnerability measures. In this step, the vulnerability-related measures are represented using fuzzy linguistic terms and the fuzzy membership functions of the linguistics terms are defined and explained. A fuzzy rule base with a belief structure is applied to capture the non-linear causal relationships between these measures and the port vulnerability levels. The next step aims at estimating the vulnerability measure levels of any investigated port from each expert, if and when they are qualitative in nature. Based on the results of the preparatory phase, the actual input can be transformed into the defined distributed linguistics representations. Then the rule base is used to enable the ER approach to combine the activated rules after the activation of the weight for a packet antecedent using the degree centrality calculation. Step 3 is to aggregate the judgements and objective data on the vulnerability measure levels from multi-experts using the ER approach. Finally, the ranking of vulnerable levels is determined by using utility values before the model validation test using sensitivity analysis.

3.2 The fuzzy theory approach

3.2.1 Identification of vulnerability measures

As discussed in Section 2, robustness (R), importance (I), efficiency (E), and resilience (S) are selected as the measures to evaluate the port vulnerability in an MSC. The interpretations of these selected measures are detailed explained in Section 2 (e.g. Table 1).

3.2.2 Description of the fuzzy input and output variables

This section describes the determination of linguistic terms and its granularities, and the definitions of fuzzy membership functions. Firstly, the input variables are defined as robustness (R), importance (I), efficiency (E), and resilience (S), and the granularity for the associated linguistic terms of each measure are determined. Then the types of fuzzy membership functions are selected to delineate input variables.

Regarding the granularity for the linguistic terms, the previous studies reveal that the granularity from four to seven linguistics terms is used to model risk parameters in safety evaluation (Bowles and Peláez, 1995). Based on the definitions of the four vulnerability measures (i.e. Table 1), the linguistic terms for R are determined as 'very low (VL)', 'low (L)', 'medium (M)', 'high (H)', and 'very high (VH)'. The ones for I are displayed as 'not important (NI)', 'slightly important (SI)', 'important (I)', and 'very important (VI)'. The terms used to evaluate E include 'very low (VL)', 'low (L)', 'high (H)', and 'very high (VH)'. S is determined by the terms of 'very strong (VS)', 'strong (S)', 'average (A)' 'weak (W)', and 'very weak (VW)'. The linguistics terms used to describe each measure refer to the previous studies in maritime risk analysis using fuzzy logic (e.g. Wang et al., 1995; 1996; Yang et al., 2009; 2013). Detailed interpretations of the above linguistic variables of vulnerability measures are shown in Appendix A-D.

It is worth noting that it is difficult to construct curved fuzzy membership functions that fit the real situation perfectly due to lack of information. Yang et al. (2009) provided some straightline membership functions, such as the triangular and trapezoidal membership functions when taking into account the good balance between accuracy and computation easiness with reference to the fuzzy logic previous

use in transport risk studies. Figs. 2-5 show the definitions of the fuzzy sets for R, I, E, and S. They are widely used in risk analysis because of their advantage of simplicity (Yang, 2001). The vulnerability estimate, as shown in Fig. 6, is the only output fuzzy variable, which is expressed by such linguistic terms as 'Very vulnerable (VV)', 'Vulnerable (V)', 'Slightly vulnerable (SV)', and 'Not vulnerable (NV)'.

It should be noteworthy that the input variables of "important" is collected by objective data using the centrality theory. The degree centrality of a node i $C_d(i)$ is measured by the number of links a node i incoming or outgoing connections to and from nodes j in the MSC ($C_d(i) = \sum_{j=1}^{n} a_{ij} + a_{ji}$). Liu et al. (2018) had collected the information of degree centrality of ports using the data from Maersk shipping line, which shows the maximum and minimum degree centrality are 15 and 1, respectively. Consequently, 15 and 0 are defined as "very important" and "not important" for I. Moreover, the interval between 15 and 0 is divided into four grades as shown in Fig. 3.

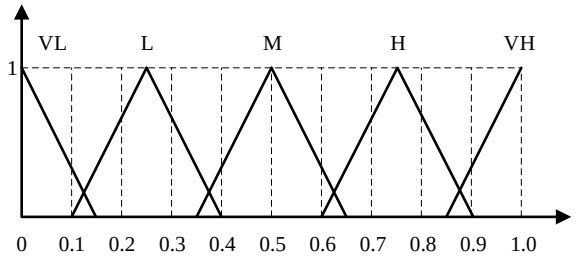

Fig.2 Membership function of fuzzy ***R*** set

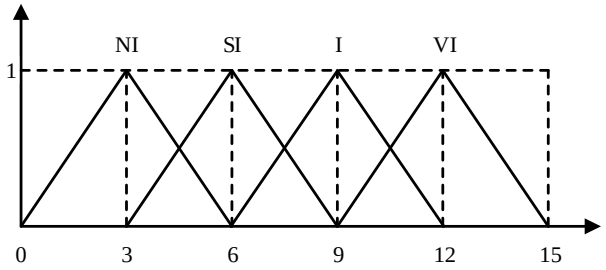

Fig. 3 Membership function of fuzzy ***I*** set

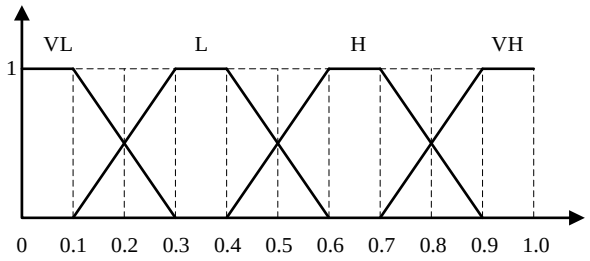

Fig. 4 Membership function of fuzzy ***E*** set

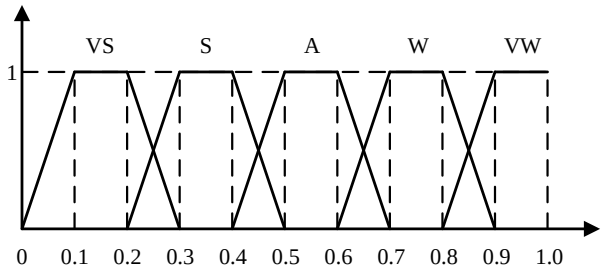

Fig. 5 Membership function of fuzzy ***S*** set

Although it is possible to modify the defined fuzzy membership functions (verified by the port experts in this study) to fit different investigated port context, it still requires careful justification on such modifications by the domain experts of good knowledge on the studied ports.

3.2.3 Construction of a fuzzy rule base with belief structures

After identifying the vulnerability measures and defining their linguistic terms, a fuzzy rule with belief degrees is developed to transform input knowledge into output variables. A generic fuzzy IF-THEN rule with a belief degree is defined as Eq. (1) (Yang et al., 2009), which concludes the premise and the conclusion. Within the PVA context, they are presented as follows.

$$R_k: IF\ A_{1,k} and\ A_{2,k}\ and \dots and\ A_{M,k}, THEN\ \{(D_1, \beta_{1,k}), (D_2, \beta_{2,k}), \dots, (D_N, \beta_{N,k})\} \quad (1)$$

R_k – the kth rule in a rule base, $\forall k \in \{1, \dots, L\}$, L is the number of rules;

$A_{i,k}$– the linguistic term corresponding to the ith attribute in R_k, $\forall i \in \{1, \dots, M\}$;

D_j– the jth output linguistic term;

$\beta_{j,k}$– the belief degree assigned to D_j, $\forall j \in \{1, \dots, N\}, \sum_{j=1}^{N} \beta_{j,k} \leq 1$;

M – the number of input vulnerability measures, hence equalling to 4 in this study;

N – the number of output linguistic terms, associated with the 4 linguistic terms used to describe port vulnerability levels.

3.3 The ER approach

3.3.1 Transformation of the input

The procedure for input transformation is to transform the actual input into the distributed representation by using belief structures. Within the context of PVA, the input for an antecedent attribute $U_i \in \{R, I, E, S\}$ can be expressed by a distributed representation as Eq. (2).

$$S(U_i) = \{(A_{ij}, \alpha_{ij}); j = 1, \dots, J_i\}, i = 1, 2, 3, 4 \quad (2)$$

where A_{ij} represents the jth linguistic term of the ith attribute, α_{ij} is the belief degree to which A_{ij} belongs to the linguistic terms with $\alpha_{ij} \geq 0, \sum_j^{J_i} \alpha_{ij} \leq 1$ ($i = 1, 2, 3, 4$; j $= 1, \dots, J_i$ with $J_1 = J_4 = 5$, and $J_2 = J_3 = 4$).

Note that α_{ij} in Eq. (2) can be derived in various ways based on the nature of actual input and available data. The matching function method is one of the ways suitable for both quantitative and qualitative data while the actual input is in numerical forms and the fuzzy membership functions are applied to characterize the linguistic value. In this paper, the max-min operation matching function (Zimmermann, 1991) is selected to capture the relationship between actual input and the corresponding fuzzy linguistic term. For the purpose of vulnerability assessment, every actual input in different forms based on objective data (i.e. importance) and expert judgement meets the requirement of the proposed model. In other words, the process of input transformation can be used for both of objective data and subjective data. The actual input forms can be a numerical value (i.e. importance), a closed interval, and a triangular distribution.

Based on Eq. (1), the general input form in the kth rule is shown as Eq. (3), the antecedent in this paper contains four attributes:

$$(A_1^*, \varepsilon_1) AND (A_2^*, \varepsilon_2) AND (A_3^*, \varepsilon_3) AND (A_4^*, \varepsilon_4) \quad (3)$$

where ε_i is the degree of belief of A_i^* $(i = 1, \dots, 4)$ assigned by experts which reveals the uncertainty. Then, α_{ij} can be calculated by Eqs. (4) - (5).

$$\alpha_{ij} = \frac{\tau(A_i^*, A_{ij}) \cdot \varepsilon_i}{\sum_{j=1}^{J_i} [\tau(A_i^*, A_{ij})]}, \quad i = 1, \dots, 4; j = 1, \dots, J_i \quad (4)$$

$$\tau(A_i^*, A_{ij}) = max[\min(A_i^*(x), A_{ij}(x))] \quad (5)$$

where (A_i^*, ε_i) defines the actual input of the ith antecedent, τ represents the selected marching function, $\tau(A_i^*, A_{ij})$ means the matching degree to which A_i^* assigns to A_{ij}.

3.3.2 Activation weight

If an actual input is given based on Eq. (3), the corresponding to the kth rule defined as in Eq. (1) is described as follows:

$$R \text{ is } (A_{1,k}, \alpha_{1,k}) \text{ AND } I \text{ is } (A_{2,k}, \alpha_{2,k}) \text{ AND } E \text{ is } (A_{3,k}, \alpha_{3,k}) \text{AND } S \text{ is } (A_{4,k}, \alpha_{4,k}) \quad (6)$$

where $\alpha_{i,k} \in \{\alpha_{ij},\ j = 1, \dots, J_i\}$ is the individual belief degree in the kth rule, $A_{i,k} \in \{A_{ij},\ j = 1, \dots, J_i\}$ is the linguistic term in the kth rule. The "AND" conjunction presents all the antecedents in a rule, which means the consequent of a rule cannot be considered to be true until all the antecedents of the rule are activated.

Thus, the activation weight ω_k for the packet antecedent A_k in R_k can be aggregated as Eqs. (7) – (9).

$$\omega_k = (\theta_k . \alpha_k) / \sum_{i=1}^{L} \theta_i . \alpha_i \quad (7)$$

$$\alpha_k = \prod_{i=1}^{4} (\alpha_{i,k})^{\bar{\delta}_i} \quad (8)$$

$$\bar{\delta}_i = \delta_i / \max_{i=1,2,3,4} \{\delta_i\} \quad (9)$$

where α_k represents the total degree of to which the actual input matches to the A_k in R_k, it is calculated by combining the $\alpha_{i,k}$. δ_i and θ_k represent the weight of the *i*th antecedent attribute and the relative

weight of the kth rule respectively. In this paper, the attribute weight δ_i (i =1,2,3,4) is set equally and the relative weight of kth rule is set θ_k =1 for the four attributes and all rules contribute equally to vulnerability. Here the attribute values are set equally, mainly based on the state of the art literature where the risk/vulnerability related attribute are given the same weight in the safety studies of the relevant fields including maritime/port (e.g. Yang et al., 2009; Al Yami et al., 2019, 2020), transport (e.g. Wang et al., 2019; 2020) and supply chains (e.g. Wan et al., 2020). It also reflects the limited knowledge of the domain experts in the exploration of this vulnerability measurement involving multiple new elements. In the meantime, the model (i.e. Eqs (7) – (9)) is the flexibility and can accommodate different weights of the variables whenever the relevant supporting evidence becomes available.

3.3.3 Rule combination and multi-expert aggregation

In this section, the ER approach (Yang et al., 2009; Liu et al., 2004) is further introduced to synthesize rules and calculate the final conclusions after obtaining the fuzzy rule base expressed by a matrix based on the above process. Firstly, the belief degree $\beta_{j,k}$ is transformed into basic probability masses $m_{D,k}$, which consists of two parts, as shown in Eqs. (10) – (13). The first part is unassigned probability mass derived from the relative importance of the kth rule ($\bar{m}_{D,k}$), and the other part is unassigned probability mass generated by the incompleteness of the belief degree ($\tilde{m}_{D,k}$).

$$m_{j,k} = \omega_k \beta_{j,k} \;\; j = 1, \dots, N \tag{10}$$

$$m_{D,k} = 1 - \sum_{j=1}^{N} m_{j,k} = 1 - \omega_k \sum_{j=1}^{N} \beta_{j,k} \tag{11}$$

$$\bar{m}_{D,k} = 1 - \omega_k \tag{12}$$

$$\tilde{m}_{D,k} = \omega_k (1 - \sum_{j=1}^{N} \beta_{j,k}) \tag{13}$$

$$m_{D,k} = \bar{m}_{D,k} + \tilde{m}_{D,k} \tag{14}$$

where $m_{j,k}$ represents individual belief degree of R_k belongs to the consequent D, ω_k is activation weight for the packet antecedent A_k in R_k.

Then, generate the combined degree of belief of each possible $D_j$in D by synthesizing all the rules. Define that $m_{j,I(k)}$ is the combined belief degree in D_j by synthesizing all the kth rules, and $m_{D,I(k)}$ is the rest belief degree unassigned to any D_j. Let $m_{j,I(1)} = m_{j,1}$ and $m_{D,I(1)} = m_{D,1}$. The overall combined belief degree β_j of D_j is generated by Eqs. (15) – (21).

$$\{D_j\}: m_{j,I(k+1)} = K_{I(k+1)} \times \left(m_{j,I(k)}m_{j,(k+1)} + m_{j,I(k)}m_{D,(k+1)} + m_{D,I(k)}m_{j,(k+1)}\right) \quad (15)$$

$$m_{D,I(k)} = \overline{m}_{D,I(k)} + \widetilde{m}_{D,I(k)} \quad k = 1, \dots, L \quad (16)$$

$$\{D\}: \widetilde{m}_{D,I(k+1)} = K_{I(k+1)} \times \left(\widetilde{m}_{D,I(k)}\widetilde{m}_{D,(k+1)} + \widetilde{m}_{D,I(k)}\overline{m}_{D,(k+1)} + \overline{m}_{D,I(k)}\widetilde{m}_{D,(k+1)}\right) \quad (17)$$

$$\overline{m}_{D,I(k+1)} = K_{I(k+1)} \times \left(\overline{m}_{D,I(k)}\overline{m}_{D,(k+1)}\right) \quad (18)$$

$$K_{I(k+1)} = \left[1 - \sum_{j=1}^{N}\sum_{\substack{r=1 \\ r\neq j}}^{N} m_{j,I(k)}m_{r,(k+1)}\right]^{-1}, k = 1, \dots, L-1 \quad (19)$$

$$\{D_j\}: \beta_j = m_{j,I(L)}/1 - \overline{m}_{D,I(L)}, j = 1, \dots, N \quad (20)$$

$$\{D_j\}: \beta_D = \widetilde{m}_{D,I(L)}/1 - \overline{m}_{D,I(L)} \quad (21)$$

where β_D describes the remaining unassigned belief degrees to any D_j. The final output calculated by synthesizing the L rules is displayed as Eq. (22).

$$S(A^*) = \{(D_j, \beta_j), j = 1, \dots, N\} \quad (22)$$

Until this step, the result of vulnerability estimate has been obtained by an expert, the overall result by a panel of experts can be obtained by synthesizing their individual vulnerability estimates by using the ER approach.

Six experts $e_i (i = 1, \dots, 6)$ meet the selection criteria and give the fuzzy ratings for vulnerability estimate. Their expertise and background information are introduced in the case study in Section 4. Assume that w_{ei} $(i = 1, \dots, K)$ is the weight of different experts, and $A_{ei,j} (j = 1,2,3,4)$ is an input matrix obtained from e_i for an antecedent attribute. For every input, there is a corresponding vulnerability estimate D_{ei} by using the above proposed ER approach. Finally, the overall result of

vulnerability estimate can be obtained by synthesizing multi-expert's evaluation using the ER algorithm above again.

3.3.4 Ranking

The final result shown in Eq. (22) presents the vulnerability in a distributed way, which can provide stakeholders a whole view about the vulnerable level of an investigated port. They can clearly know what belief degree is assigned to the associated linguistic terms. However, it may not straightforward for them to understand the ranking of the port in an MSC by using the distributed representation. Thus, the utility value associated with each linguistic term is introduced to facilitate decision making. Define $u(D_i)$ $(i = 1, \dots, N)$ is the utility of a vulnerability expression D_i. Then the vulnerability ranking index value V_p $(p = 1, \dots, P)$ can be calculated as follows:

$$V_p = \sum_{i=1}^{N} \beta_j^p \times u(D_i) \tag{23}$$

where P is the number of the ports in an MSC. Note that $\sum_{p=1}^{P} \beta_j^p = 1$ for the pth port. Thus, the ranking of ports in the MSC can be determined by the index value.

Finally, a sensitivity analysis approach by slightly adjusting the change in input is employed in this study to verify the robustness and reliability of the PVA framework. The minor changes can be variations of the parameters of the model or changes of belief degrees assigned to the linguistic terms to represent the parameters of the model. In order to validate the approach and its inference reasoning, the following axioms (Yang et al., 2009) must be met.

Axiom 1. Slight decline of belief degrees associated with linguistic terms of risk parameters should result in a decrease of the risk estimates of the model output correspondingly.

Axiom 2. Slight increment of belief degrees associated with linguistic terms of risk parameters should result in an increase of the risk estimates of the model output correspondingly.

4. Case study

According to the throughput and the number of ship calls, we selected the top five key ports in a well-established MSC in China to participate in this vulnerability assessment. They have well connected routes among them, taking account of approximate 80% volume across the MSC annually in the past ten years. In terms of qualitative measures, evaluation data are collected from the selected six experts to assess the vulnerability of the ports using the PVA methodology in Section 3. The quantitative measure (i.e. importance) of each port is calculated by their centrality.

4.1 Vulnerability estimate by each expert

It is challenging to be holistically estimate vulnerability considering the associated uncertainties by expert knowledge. This type of uncertainty is defined as epistemic uncertainty, which comes from the weakness of the knowledge base and expert capabilities, including the evidence collected and the reasoning tool to the output results (Nguyen et al., 2019). Epistemic uncertainty lies in the lack of knowledge base and the irreducible subjectivity in the process of vulnerabilities quantification. Therefore, epistemic uncertainty can be well minimized through a stronger knowledge base, including more professional and experienced experts, available evidence and model quality. The experts below are carefully selected in the process of vulnerability estimate.

The selected experts involved in this case study would need to have a combination of the knowledge about the operations of the chain and the safety management. In particular, the concepts of vulnerability used in the previous studies are further developed to newly include robustness (R), importance (I), efficiency (E), and resilience (S) as the port vulnerability measures. The selected experts are required to have a professional cognition and evaluation ability of all measures in the survey process. In the initial contact, experts from all the stakeholder groups were contacted and after the screening, only the selected six ones are qualified for providing useful meaning input data. the profile of the selected experts are described below.

In this section, the assessments made by expert #1 of Port 1 are detailed discussed to illustrate the process of the PVA framework. For other experts' assessments, only the calculated results are provided.

The linguistic terms and corresponding membership functions are proposed in Section 3.2 as shown in Figs. 2-5 and Appendix A-D. Six experts have a wealth of expertise balance in port safety and operation participates in vulnerability evaluation. The profile of experts includes 2 academic researchers intensively engaged in port research projects of the investigated MSC in the past 10 years, 2 senior managers from safety and operation departments, and 2 captains serving on the routes connecting the five ports. Each expert has over more than10 years' experience working at/with the selected ports, and their expertise and background information are found in Table 2. The evaluation conducted by the six experts in terms of R, I, E, and S is depicted in Appendix E, in which it is observed that there is no significant inconsistency among the judgements from the multiple experts. It in part gains the credibility of the data.

Table 2 Expert profile for ratings

Expert no.	Title and department	Professional background	Working experience
1	Academic researcher, transportation planning and management departments	Engaged in port analysis of the MSC, in charge of many major projects related to the port	20 years
2	Academic researcher, water transport Department	Engaged in maritime network safety and shipping planning, involved in or led a variety of projects on maritime network and shipping planning	22 years
3	senior manager, Department of port safety and security	Involved in crucial safety and security measures develop and system upgrade	15 years
4	senior manager, Department of port operation	Involved in port safety related training and supervising operative personnel	16 years
5	Captain, Department of shipping	Engaged in the transport along the MSC calling at the selected ports as a captain	18 years
6	Captain, Department of pilot	Engaged in the pilotage work of the selected ports	12 years

A fuzzy rule base containing a number of 400 rules (4*4*5*5 linguistic variables of the four measures) with a belief structure is constructed in the case study. A part of the established fuzzy rule base is listed in Appendix F. The fuzzy ratings of vulnerability indictors of Port 1 by experts #1 is in the triangular distribution representation. The R is described as (0.7, 0.8, 0.9), the I of the port is evaluated using degree centrality as a value of 10, the E as (0.5, 0.7, 0.9), and the S as (0.3, 0.4, 0.5). The actual input values are transformed into the distributed representation in terms of linguistic terms by using Eqs. (4) - (5) and membership functions in Figs. 2-5. The calculated result is listed in Table 3, where ε_i in Eq. (4) is defined to be 1. Further, the process of input transformation is applied for the other five experts for Port 1 and for the other four ports, which are listed in Appendix G.

Table 3 Transformation of actual input for Port 1 by expert #1 into the distributed representation of linguistic terms

Input indicator	Linguistic term	τ	α_{ij}
R	High	0.8	0.8
	Very high	0.2	0.2
I	Important	0.67	0.67
	Very important	0.33	0.33
E	Low	0.25	0.143
	High	1	0.571
	Very high	0.5	0.286
S	Easy	1	0.667
	Medium	0.5	0.333

In the fuzzy rule base, 400 rules have been developed, of which only 24 rules are activated for Port 1 by expert #1, including Rules #287-288, #292-293, #297-298, #307-308, #312-313, #317-318, #367-368, #372-373, #377-378, #387-388, #392-393, #397-398. These activated rules are established in Appendix F.

The activation weight ω_k $(k = 1, \dots, 24)$ of each rule in the activated sub-rule base is computed by using Eq. (7) based on the individual matching belief degrees. The fuzzy rule with activated weight for activated rules is represented in Appendix F. Taking rule #287 for example, the result can be calculated as follows with the activation weight $\omega_{287} = 0.013$.

$S(A^{287}) =$

$\{(very\ vulnerable, 0), (vulnerable, 0.5), (slightly\ vulnerable, 0.5), (not\ vulnerable, 0)\}$

Then, the ER algorithm is used to combine the activated 24 rules and generate vulnerability estimates. The process is implemented by the Intelligent Decision System (IDS). The final results for Port 1 by expert #1 are calculated as follows and is shown in Fig.6.

Results: {(very vulnerable, 0.0367), (vulnerable, 0.1853), (Slightly vulnerable, 0.3917), (Not vulnerable, 0.3863)}

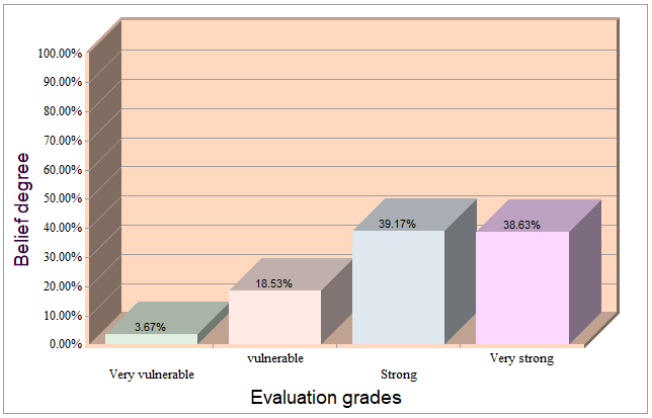

Fig. 6 The vulnerability estimate of Port 1 by expert #1

The result means the vulnerability estimate of Port 1 is 'very vulnerable' with a belief degree of 0.0367, 'vulnerable' with a belief degree of 0.1853, 'slightly vulnerable' with a belief degree of 0.3917, and 'not vulnerable' with a belief degree of 0.3863. The assessment of the other five experts and the other four ports are calculated in a similar process. The vulnerability estimates calculated for the other four ports by six experts are listed in Table 4.

Table 4 Vulnerability estimates by each expert for all the selected ports

Expert	Vulnerability estimate			
	Very vulnerable	Vulnerable	Slightly vulnerable	Not vulnerable
(1) Port 1				
E#1	0.0367	0.1853	0.3917	0.3863
E#2	0.0179	0.2169	0.5507	0.2145
E#3	0.0271	0.3052	0.4730	0.1946
E#4	0.0277	0.2725	0.3996	0.3002
E#5	0	0.1072	0.6071	0.2857
E#6	0.0564	0.1693	0.3103	0.4639
(2) Port 2				
E#1	0.0179	0.1256	0.3356	0.5208
E#2	0	0.0764	0.6182	0.3054
E#3	0.0175	0.1741	0.4768	0.3316
E#4	0.0275	0.1375	0.3827	04523
E#5	0.0571	0.1712	0.3851	0.3867
E#6	0.0278	0.1389	0.537	0.2963
(3) Port 3				
E#1	0.0084	0.1575	0.6579	0.1762
E#2	0	0.2452	0.5995	0.1552
E#3	0.0174	0.3091	0.5282	0.1452
E#4	0.0105	0.2906	0.5096	0.1893
E#5	0	0.1578	0.7134	0.1287
E#6	0	0.1024	0.6799	0.2176
(4) Port 4				
E#1	0.0185	0.2247	0.4753	0.2815
E#2	0	0.1361	0.6485	0.2154
E#3	0	0.1015	0.7431	0.1554
E#4	0.0175	0.2116	0.5489	0.222
E#5	0	0.2345	0.4678	0.2977

E#6	0	0.1048	0.5304	0.3648
(5) Port 5				
E#1	0	0.1248	0.6982	0.177
E#2	0	0.2125	0.6533	0.1342
E#3	0	0.3481	0.5057	0.1462
E#4	0.0214	0.1923	0.5186	0.2678
E#5	0	0.0941	0.8078	0.0981
E#6	0	0.2722	0.7278	0

4.2 Multi-expert vulnerability assessment systhesise

The ER approach is used not only to synthesize the activated fuzzy rules but also to aggregate the vulnerability estimate from each expert. Based on the results of the assessment shown in Table 4, the vulnerability aggregation results of multi-experts are shown in Table 5 for Ports 1-5, respectively. The employed six experts all have their professional knowledge in port analysis of the MSC, including professional field and practical field. In the process of port analysis, both practical experience and theoretical knowledge play the same important role. Thus, the relative weight of each expert is considered equal in this paper.

Table 5 Multi-expert's vulnerability synthesize with equal expert weights

Ports	Vulnerability synthesis			
	Very vulnerable	Vulnerable	Slightly vulnerable	Not vulnerable
Port 1	0.0235	0.1952	0.4803	0.3009
Port 2	0.0207	0.1218	0.4743	0.3832
Port 3	0.0048	0.1851	0.6643	0.1457
Port 4	0.0049	0.1484	0.6116	0.2351
Port 5	0.0028	0.1788	0.7044	0.114

4.3 Ranking results

The distribution assessment shown in Table 5 provides a panoramic view of the vulnerability, from which we can understand which grades the port is assessed to, what degrees of belief are assigned to the grades. However, it is difficult if not possible, for decision-makers to rank and compare the vulnerability levels among the ports directly. The utility values are therefore assigned to the linguistic terms of vulnerability levels. Assume the utility value to each linguistic term is [0, 0.33, 0.67, 1]. The linear distribution of the utility values indicates that the higher the index value, the lower level the vulnerability. The vulnerability ranking index value V_p for Port 1 is calculated based on the multi-expert vulnerability synthesize shown in Table 5 and Eq. (23) as follows:

$V_{port\ 1} = \sum_{i=1}^{4} \beta_j^{port\ 1} \times u(D_i) = 0.0235 \times 0 + 0.1952 \times 0.33 + 0.4803 \times 0.67 + 0.3009 \times 1 = 0.6871$

The ranking index values for the other ports are calculated and presented in Table 6. As shown in Table 6, Port 2 has the highest vulnerability ranking index value with 0.7412, which means Port 2 is the strongest to cope with risk events. The performance of Port 2 is better than other ports in terms of efficiency and robustness. Port 4 ranks second with a value of 0.6939, followed by Port 1 (0.6871), Port 3 (0.6519), and Port 5 (0.6450). The ranking results can provide decision-makers with an insight into the different vulnerable levels of the investigated ports. It provides scientific guide for rationalising safety resources.

Table 6 Vulnerability ranking

Port	Port 1	Port 2	Port 3	Port 4	Port 5
Index value	0.6871	0.7412	0.6519	0.6939	0.6450
Ordering	3	1	4	2	5

In order to further verify the robustness and reliability of the proposed framework, a sensitivity analysis is conducted by following the two Axioms in Section 3.3.4. The minor changes are either variations of the parameters of the model or changes of belief degrees assigned to the linguistic terms to represent the parameters of the model. In this sensitivity analysis, the IDS software is used to synthesize the information. The results of sensitivity analysis on Axiom1 and Axiom 2 for each port are shown in Fig. 7. The vulnerability distributions are steady and consistent for each port and found no abrupt change evident, which partially validates the robustness and reliability of the proposed framework.

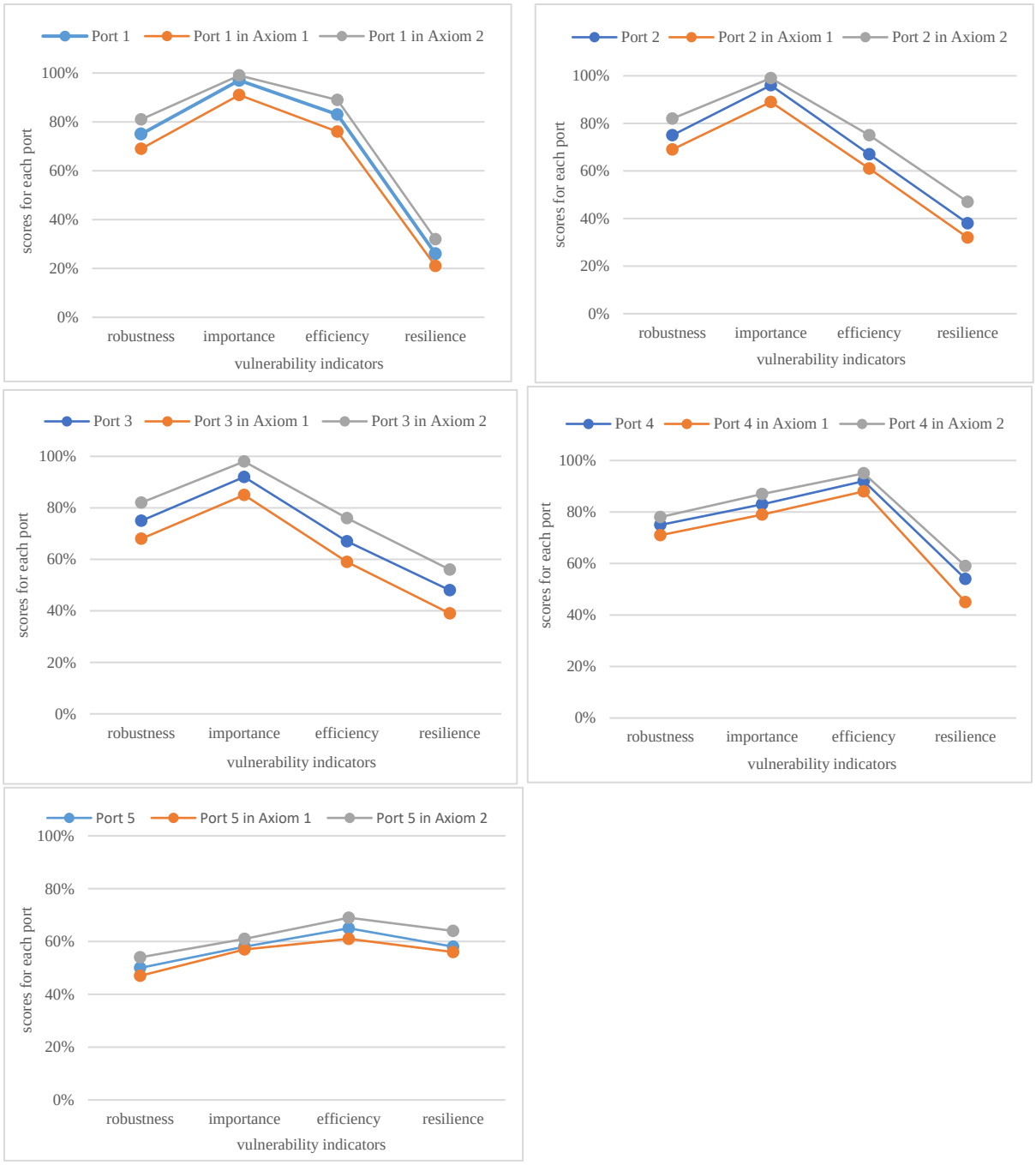

Fig 7 The results of sensitivity analysis

5. Research implications

This paper proposed a new PVA framework to provide MSC stakeholders such as shipping companies, ports, and shippers with more insightful analysis. Several research implications to research and practice are drawn as follows.

Initially, as the first attempt in the literature to evaluate the vulnerability of ports along an MSC in the same framework at a global level, this study enriches the literature on the basis of multi-perspective definitions of port vulnerability. At present, there is no universally accepted definition of vulnerability in port. It is crucial to make a specific definition of vulnerability when it comes to the certain domains, such as port vulnerability. The vulnerability of a port is defined from an MSC perspective including the measures used in a quantitative way. The findings provide useful insights for researchers to stimulate the development of vulnerability-related theories and development of the best-fit measures to improve the measurement of vulnerability as a whole.

Secondly, this paper fills the research gap by developing a new PVA framework to allow the port vulnerability assessment on the same plate. The methodology incorporates the features of port vulnerability, involves MSCs, considers multi-dimensional vulnerability measures, and has the capability of dealing with both qualitative and quantitative inputs. Since the rapid development of maritime transportation will greatly stimulate the development of standard analysis patterns of ports along an MSC, more attention needs to be paid on the application of the generic framework of port vulnerability. For instance, the currently occurring COVID-19 significantly affects port operations. Although the data collection occurred before the COVID-19 pandemic, the PVA framework and the supporting FER algorithms can perfectly be adapted to evaluate port vulnerability facing COVID-19 given the recent successful use of fuzzy ER on the outbreak risk analysis of epidemics (e.g. Shi et al., 2021). Within the port vulnerability study, the model should take into account different attribute weight assignments to reflect the feature of low-frequency-high-consequence events such as COVID-19.

Thirdly, this paper embedded the fuzzy rule base and ER method into port vulnerability assessment to tackle the high uncertainty in data. Port centric MSC is complex and massive with various elements, influential factors, and characteristics. In addition, the conditions of safety, operational, environment and management vary among the ports along an MSC, it will increase the difficulty to deal with the collected data or judgement in various formations with uncertainties. Therefore, this paper incorporates a fuzzy ‘IF-THEN’ rule base with belief structures and ER approach to deal with different formations

of data with uncertainties and synthesize the vulnerability estimate, where traditional vulnerability assessment approaches meet more challenges.

Furthermore, this work provides managerial insights to maritime stakeholders in a rational, reliable and transparent way. For instance, this work provides a standard and effective tool to make full use of information based on a comparative analysis of other relative ports along an MSC to make rational decisions for vulnerability improvement of port safety. It can increase the transparency and understanding of port operations and management in the upstream and downstream ports in the chain with respect to various vulnerabilities and hence port managers can improve the robustness and efficiency of the ports by the lessons from the ports of best performance. It is envisaged that the proposed approach could provide safety managers and risk analysts with a tool for use in understanding the importance of making safety protective measures in order to increase the robustness of MSC in a rational and transparent manner.

6. Conclusion

A new PVA framework that can guide to assess different types of vulnerabilities on the basis of a fuzzy rule-based multi-expert vulnerability analysis and synthesis framework is developed and applied to assess the vulnerability of ports in an established MSC in practice. It main contributions include that 1) PVA provides a powerful tool to deal with qualitative (e.g. importance measure data) and quantitative data under uncertainties simultaneously; 2) it for the first time incorporates centrality estimate of the ports to present their interactive influence in an MSC; 3) it defines vulnerability measures that are capable of evaluate port vulnerability taking into account the internal risk and external safety impact in one setting; and 4) from applied research perspectives, fuzzy evidential reasoning and the associated calculation software IDS are presented in a generic way, which could guide users to conduct their own assessment to eventually improve the port resilience in the world. More experiments will in return further validate the PVA and emphasize its value in future.

Further research can be orientated towards some directions. Methodologically, it can be twofold. One is to incorporate more centrality measures to define the node importance. Degree centrality is used

to determine the interval of "importance". The higher degree of a node, the higher degree centrality of the node, and the more "important" the node is in the network. However based on the different network features of the supply chains, betweenness centrality and degree centrality could be incorporated and combined together to jointly determine the port importance. Because of this importance measure, the PVA framework is not applicable for the ports that are not actively engaged in an MSC. The other is to assign different attribute weights to make the PVA model adaptive to low-frequency-high consequence events (e.g. COVID-19). The weight assignments can be dynamic with reference to different hazards/threats that a port could face. The power of FER in dealing with high uncertainty in data provides a promising solution to this methodological challenge. From the applied research perspective, one of future studies is the necessary data collecting of a broader period of time, for example, the ports' position as well as maritime transport network change over time. Another direction of further research could focus on applying the novel framework to other types of ports (e.g. dry ports and airports) regions or country groups. In this process, the attributes should be further validated by the domain experts and their fuzzy definitions should also be verified to reflect the applied context. This will facilitate the comparison of vulnerability levels among different regions, or country groups, and provide insight for decision making concerning maritime stakeholders within broader groups of countries. Further research could focus on identifying rules and regulations that can mitigate vulnerability from port disruptions.

Appendix A. ***R*** interpretation

Fuzzy number	*R*	Interpretation
(0, 0, 0.15)	Very low	0-15% of the port is operated normally after disturbance
(0.1, 0.25, 0.4)	Low	10-40% of the port is operated normally after disturbance
(0.35, 0.5, 0.65)	Medium	35-65% of the port is operated normally after disturbance
(0.6, 0.75, 0.9)	High	60-90% of the port is operated normally after disturbance
(0.85, 1, 1)	Very high	85-100% of the port is operated normally after disturbance

Appendix B. ***I*** interpretation

Fuzzy number	*I*	Interpretation
(0, 3, 6)	Not important	The degree centrality of the port is less than 6
(3, 6, 9)	Slightly important	The degree centrality of the port is between 3 and 9
(6, 9, 12)	Important	The degree centrality of the port is between 6 and 12
(9, 12, 15)	Very important	The degree centrality of the port is greater than 9

Appendix C. ***E*** interpretation

Fuzzy number	*E*	Interpretation
(0, 0, 0.1, 0.3)	Very low	The throughput of cargoes accounts for 0-30% of the total capacity after disturbance
(0.1, 0.3, 0.4, 0.6)	Low	The throughput of cargoes accounts for 10-60% of the total capacity after disturbance
(0.4, 0.6, 0.7, 0.9)	High	The throughput of cargoes accounts for 40-90% of the total capacity after disturbance
(0.7, 0.9, 1, 1)	Very high	The throughput of cargoes accounts for 70-100% of the total capacity after disturbance

Appendix D. ***S*** interpretation

Fuzzy number	*S*	Interpretation
(0, 0.1, 0.2, 0.3)	very strong	The time required for the port to return full capacity is approximately a few hours
(0.2, 0.3, 0.4, 0.5)	strong	The time required for the port to return full capacity is approximately a day
(0.4, 0.5, 0.6, 0.7)	average	The time required for the port to return full capacity is approximately one week
(0.6, 0.7, 0.8, 0.9)	weak	The time required for the port to return full capacity is approximately one month
(0.8, 0.9,1, 1)	very weak	The time required for the port to return full capacity is approximately three month

Appendix E. Experts assessment of four vulnerability measures using different forms to represent uncertainty for different ports. (1) Port 1, (2) Port 2, (3) Port 3, (4) Port 4, and (5) Port 5

Experts	***R***	***I***	***E***	***S***
(1) Port 1				
E#1	(0.7, 0.8, 0.9)	10	(0.5, 0.7, 0.9)	(0.3, 0.4, 0.5)
E#2	(0.6, 0.7, 0.8)	10	(0.5, 0.6, 0.7)	(0.4, 0.5, 0.6)
E#3	[0.6, 0.8]	10	[0.4, 0.7]	[0.3, 0.6]
E#4	[0.7, 0.9]	10	[0.4, 0.6]	[0.4, 0.6]
E#5	0.85	10	0.7	0.5
E#6	0.8	10	0.75	0.4
(2) Port 2				
E#1	(0.7, 0.8, 1)	11	(0.6, 0.8, 0.9)	(0.4, 0.5, 0.6)
E#2	(0.6, 0.7, 0.9)	11	(0.6, 0.7, 0.8)	(0.5, 0.65, 0.7)
E#3	[0.6, 0.9]	11	[0.5, 0.8]	[0.4, 0.7]
E#4	[0.7, 0.8]	11	[0.6, 0.9]	[0.3, 0.6]
E#5	0.8	11	0.75	0.4
E#6	0.85	11	0.7	0.45
(3) Port 3				
E#1	(0.6, 0.7, 0.8)	7	(0.5, 0.6, 0.7)	(0.4, 0.6, 0.8)
E#2	(0.5, 0.7, 0.8)	7	(0.4, 0.5, 0.7)	(0.5, 0.7, 0.9)
E#3	[0.5, 0.8]	7	[0.4, 0.7]	[0.4, 0.8]
E#4	[0.5, 0.7]	7	[0.5, 0.9]	[0.45, 0.75]
E#5	0.6	7	0.65	0.65
E#6	0.65	7	0.7	0.6
(4) Port 4				
E#1	(0.6, 0.7, 0.8)	12	(0.5, 0.6, 0.7)	(0.4, 0.5, 0.6)
E#2	(0.5, 0.7, 0.8)	12	(0.5, 0.6, 0.7)	(0.5, 0.7, 0.8)
E#3	[0.5, 0.8]	12	[0.6, 0.7]	[0.5, 0.8]
E#4	[0.5, 0.7]	12	[0.5, 0.8]	[0.4, 0.7]
E#5	0.6	12	0.8	0.6
E#6	0.65	12	0.85	0.55
(5) Port 5				
E#1	(0.5, 0.7, 0.8)	6	(0.5, 0.6, 0.7)	(0.6, 0.7, 0.8)
E#2	(0.4, 0.6, 0.8)	6	(0.4, 0.6, 0.8)	(0.6, 0.7, 0.9)
E#3	[0.4, 0.6]	6	[0.4, 0.7]	[0.6, 0.9]
E#4	[0.3, 0.5]	6	[0.5, 0.8]	[0.6, 0.8]
E#5	0.5	6	0.7	0.7
E#6	0.6	6	0.65	0.6

Appendix F. Activated rules with belief degrees and activation weight

Rule	Antecedent attribute	Vulnerability estimate

	activation weight		D_1(VV)	D_2(V)	D_3(S)	D_4(VS)
Rules #287	0.0130	(high, important, low, easy)		0.5	0.5	
Rules #288	0.0065	(high, important, low, medium)		0.6	0.4	
Rules #292	0.0518	(high, important, high, easy)		0.4	0.6	
Rules #293	0.0259	(high, important, high, medium)	0.1	0.3	0.6	
Rules #297	0.0259	(high, important, very high, easy)		0.3	0.6	0.1
Rules #298	0.0130	(high, important, very high, medium)		0.6	0.3	0.1
Rules #307	0.0633	(high, very important, low, easy)		0.6	0.4	
Rules #308	0.0316	(high, very important, low, medium)	0.2	0.4	0.4	
Rules #312	0.2529	(high, very important, high, easy)	0.1	0.3	0.6	
Rules #313	0.1263	(high, very important, high, medium)	0.1	0.4	0.5	
Rules #317	0.1267	(high, very important, very high, easy)		0.3	0.7	
Rules #318	0.0632	(high, very important, very high, medium)	0.1	0.5	0.4	
Rules #367	0.0032	(very high, important, low, easy)		0.5	0.4	0.1
Rules #368	0.0016	(very high, important, low, medium)		0.5	0.5	
Rules #372	0.0129	(very high, important, high, easy)		0.4	0.5	0.1
Rules #373	0.0065	(very high, important, high, medium)		0.4	0.6	
Rules #377	0.0065	(very high, important, very high, easy)		0.2	0.8	
Rules #378	0.0032	(very high, important, very high, medium)		0.5	0.4	0.1
Rules #387	0.0158	(very high, very important, low, easy)		0.5	0.5	
Rules #388	0.0079	(very high, very important, low, medium)	0.1	0.5	0.4	
Rules #392	0.0632	(very high, very important, high, easy)		0.4	0.6	
Rules #393	0.0316	(very high, very important, high, medium)	0.1	0.3	0.6	
Rules #397	0.0317	(very high, very important, very high, easy)		0.3	0.6	0.1
Rules #398	0.0158	(very high, very important, very high, medium)		0.5	0.4	0.1

Appendix G. Transformation of actual input for five ports assessed by six experts into the distributed representation of linguistic terms

Expert	***R***	***I***	***E***	***S***
(1) Port 1				
E#1	H 0.8, VH 0.2	I 0.67, VI 0.33	L 0.143, H 0.571, VH 0.286	E 0.667, M 0.333
E#2	M 0.2, H 0.8	I 0.67, VI 0.33	L 0.25, H 0.75	E 0.333, M 0.667
E#3	M 0.25, H 0.75	I 0.67, VI 0.33	L 0.5, H 0.5	E 0.5, M 0.5
E#4	H 0.75, VH 0.25	I 0.67, VI 0.33	L 0.5, H 0.5	E 0.5, M 0.5
E#5	H 1	I 0.67, VI 0.33	H 1	M 1
E#6	H 1	I 0.67, VI 0.33	H 0.5, VH 0.5	E 1
(2) Port 2				
E#1	H 0.65, VH 0.35	I 0.33, VI 0.67	H 0.529, VH 0.471	E 0.333 M 0.667
E#2	M 0.189, H 0.811	I 0.33, VI 0.67	H 0.75, VH 0.25	M 0.545 D 0.455
E#3	M 0.2, H 0.6, VH 0.2	I 0.33, VI 0.67	L 0.25, H 0.5, VH 0.25	E 0.33, M 0.33, D 0.33
E#4	H 1	I 0.33, VI 0.67	H 0.5, VH 0.5	E 0.5, M 0.5
E#5	H 1	I 0.33, VI 0.67	H 0.75, VH 0.25	E 1
E#6	H 1	I 0.33, VI 0.67	H 1	E 0.5, M 0.5
(3) Port 3				
E#1	M 0.2, H 0.8	SI 0.67, I 0.33	L 0.25, H 0.75	E 0.165, M 0.5, D 0.335
E#2	M 0.35, H 0.65	SI 0.67, I 0.33	L 0.471, H 0.529	M 0.333, D 0.5, VD 0.167
E#3	M 0.5, H 0.5	SI 0.67, I 0.33	L 0.5, H 0.5	E 0.33, M 0.33, D 0.33
E#4	M 0.5, H 0.5	SI 0.67, I 0.33	L 0.2, H 0.4, VH 0.4	E 0.2, M 0.4, D 0.4
E#5	M 1	SI 0.67, I 0.33	H 1	M 0.5, D 0.5
E#6	H 1	SI 0.67, I 0.33	H 1	M 1
(4) Port 4				
E#1	M 0.2, H 0.8	VI 1	L 0.25, H 0.75	E 0.333 M 0.667
E#2	M 0.35, H 0.65	VI 1	L 0.25, H 0.75	M 0.4, D 0.6
E#3	M 0.5, H 0.5	VI 1	H 1	M 0.5, D 0.5
E#4	M 0.5, H 0.5	VI 1	L 0.25, H 0.5, VH 0.25	E 0.33, M 0.33, D 0.33
E#5	M 1	VI 1	H 0.5, VH 0.5	M 1
E#6	H 1	VI 1	H 0.25, VH 0.75	M 1
(5) Port 5				
E#1	M 0.35, H 0.65	SI 1	L 0.25, H 0.75	M 0.333, D 0.667
E#2	M 0.555, H 0.445	SI 1	L 0.333, H 0.667	M 0.273, D 0.546, VD 0.181
E#3	M 1	SI 1	L 0.5, H 0.5	M 0.33, D 0.33, VD 0.33
E#4	L 0.4, M 0.6	SI 1	H 0.5, VH 0.5	M 0.5, D 0.5
E#5	M 1	SI 1	H 1	D 1

E#6	M 1	SI 1	H 1	M 1

References

Alyami, H., Lee, P.T.W.L., Yang, Z., Riahi, R., Bonsall, S., Wang, J., 2014. An advanced risk analysis approach for container port safety evaluation. Maritime Policy and Management. 41(7), 634-650.

Alyami, H., Yang, Z., Riahi, R., Bonsall, S., Wang, J., 2019. Advanced uncertainty modelling for container port risk analysis. Accident Analysis and Prevention. 123, 41-421.

Blonigen, B.A., Wilson, W.W., 2013. The growth and patterns of international trade. Maritime Policy and Management. 40 (7), 618–635.

Bowles, J.B., Peláez, C.E., 1995. Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis. Reliabilty Engineering and System Safety. 50 (2), 203–213.

Brooks, N., 2003. Vulnerability, risk and adaptation: a conceptual framework. Tyndall Centre Climate Change Research Working Paper. 38, 1–16.

Calatayud, A., Mangan, J., Palacin, R., 2017. Vulnerability of international freight flows to shipping network disruptions: A multiplex network perspective. Transportation Research Part E. 108, 195-208.

Cao, X., Lam, J.S.L., 2019. A fast reaction-based port vulnerability assessment: Case of Tianjin Port explosion. Transportation Research Part A. 128, 11-33.

Djankov, S., Freund, C., Pham, C.S., 2010. Trading on time. The Review of Economics and Statistics. 92 (1), 166–173.

Earnest, D.C., Yetiv, S., Carmel, S.M., 2012. Contagion in the Transpacific Shipping Network: International Networks and Vulnerability Interdependence. International Interaction. 38(5), 571-596.

Elleuch, H., Dafaoui, E., Elmhamedi, A., Chabchoub, H., 2016. Resilience and Vulnerability in Supply Chain: Literature review. IFAC-PapersOnLine. 49(12), 1448-1453.

Fuchs, S., Birkmann, J., Glade, T., 2012. Vulnerability assessment in natural hazard and risk analysis: current approaches and future challenges. Natural Hazards. 64, 1969–1975.

Gaillard, J.C., 2010. Vulnerability, capacity and resilience: perspectives for climate and development policy. J. Int. Dev. 22 (2), 218–232.

Hsieh, C.H., 2014. Disaster risk assessment of ports based on the perspective of vulnerability. Natural Hazards. 74 (2), 851–864.

Hsieh, C.H., Tai, H.H., Lee, Y.N., 2014. Port vulnerability assessment from the perspective of critical infrastructure interdependency. Maritime Policy and Management. 41(6), 589-606.

Hummels, D., Schaur, G., 2013. Trime as trade barrier. American Economic Review. 103(7), 2935–2959.

Ishii, M., Lee P.T., Tezuka, K., Chang, Y., 2013. A game theoretical analysis of port competition. Transportation Research Part E. 49, 92-106.

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

Laxe, F.G., Seoane, M.J.F., Montes, C.P., 2012. Maritime degree, centrality and vulnerability: port hierarchies and emerging areas in containerized transport (2008–2010). Journal of Transport Geography. 24, 33-44.

Li, T., Rong, L., Yan, K., 2019. Vulnerability analysis and critical area identification of public transport system: A case of high-speed rail and air transport coupling system in China. Transport. Res. Part A: Policy Pract. 127, 55-70.

Liu, H., Tian, Z., Huang, A., Yang, Z., 2018. Analysis of vulnerabilities in maritime supply chains. Reliability Engineering and System Safety. 169, 475-484.

Liu, J., Yang, J.B., Wang, J., Sii, H.S., Wang, Y.M., 2004. Fuzzy rule-based evidential reasoning approach for safety analysis. International Journal of General Systems. 33 (2–3), 183-204.

Mattsson, L.G., Jenelius, E., 2015. Vulnerability and resilience of transport systems – a discussion of recent research. Transport. Res. Part A: Policy Pract. 81, 16-34.

Mcintosh, R.D., Becker, A., 2019. Expert evaluation of open-data indicators of seaport vulnerability to climate and extreme weather impacts for U.S. North Atlantic ports. Ocean and Coastal Management. 180, 104911.

Mumby, P.J., Chollett, I., Bozec, Y.M., Wolff, N.H., 2014. Ecological resilience, robustness and vulnerability: how do these concepts benefit ecosystem management? Curr. Opin. Environ. Sustain. 7, 22–27.

Nguyen, S., Chen, P. S., Du, Y., Shi W., 2019. A quantitative risk analysis model with integrated deliberative Delphi platform for container shipping operational risks. Transportation Research Part E. 129, 203-227.

Serebrisky, T., Sarriera, J.M., Suárez-Alemán, A., Araya, G., Briceño-Garmendía, C., Schwartz, J., 2016. Exploring the drivers of port efficiency in Latin America and the Caribbean. Transport Policy. 45, 31-45.

Shi, X., Li, J., Huang, A., Song, S., Yang, Z., 2021. Assessing the outbreak risk of epidemics using fuzzy evidential reasoning. Risk Analysis, https://doi.org/10.1111/risa.13730.

Song, Z., Tang, W., Zhao, R., 2018. Cooperation mode for a liner company with heterogeneous ports: Business cooperation vs. port investment. Transportation Research Part E. 118, 513-533.

Suárez-Alemán, A., Sarriera, J.M., Serebrisky, T., Trujillo, L., 2016. When it comes to container port efficiency, are all developing regions equal? Transportation Research Part A. 86, 56-77.

UNCTAD, 2019. Review of Maritime Transport 2019. United Nations Conference on Trade and Development. UNCTAD.

UN/ISDR, 2009. 2009 UNISDR Terminology on Disaster Risk Reduction. United Nations International Strategy for Disaster Reduction. Geneva: United Nations.

Vanelslander, T. and Sys, C., 2020. Maritime Supply Chains. Elsevier. https://doi.org/10.1016/C2018-0-03190-4.

Wan, C., Yang, Z., Zhang, D., Yan, X., Fan S., 2018. Resilience in transportation systems: a systematic review and future directions. Transports Reviews, 38(4), 479-498.

Wan, C., Yan, X., Zhang, D., Qu, Z., Yang, Z., 2019. An advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks. Transportation Research Part E. 125, 222-240.

Wang, J., Yang, J.B., Sen, P., 1995. Safety analysis and synthesis using fuzzy sets and evidential reasoning. Reliability Engineering and System Safety. 47 (2), 103–118.

Wang, T., Qu, Z, Nichol, T., Yang, Z., Dimitriu, D., Clarke, G., Bowden, D., 2019. How can the UK road system be adapted to the impacts posed by climate change? By creating a climate adaptation framework. Transportation Research Part D: Transport Environment. 77: 403-424.

Wang, T., Qu, Z., Yang, Z., Nichol, T., Dimitriu, D., Clarke, G., Bowden, D., Lee, P. T., 2020. Impact analysis of climate change on rail systems for adaptation planning: A UK case. Transportation Research Part D: Transportation Environment. 83: 102324.

Xie, F., Wang, C., Xu, L., 2021. Whether to invest in terminal efficiency: A perspective considering customer preference and capital constraint in competitive environment? Ocean & Coastal Management. 205(1):105563.

Xu, L., Di, Z., Chen, J., Shi, J., Yang, C., 2021a. Evolutionary game analysis on behavior strategies of multiple stakeholders in maritime shore power system. Ocean & Coastal Management.202:105508.

Xu, L., Shi, J., Chen, J., 2021b. Platform encroachment with price matching: Introducing a self-constructing online platform into the sea-cargo market. Computers & Industrial Engineering. 156:107266.

Xu, L., Yang, S., Chen, J., Shi, J., 2021c. The effect of COVID-19 pandemic on port performance: Evidence from China. Ocean & Coastal Management. 209:105660.

Yang, J. 2001. Rule and Utility-Based Evidential Reasoning Approach for Multi Attribute Decision Analysis under Uncertainties. European Journal of Operational Research 131, 31 – 61.

Yang, Z., Ng, A.K.Y., Wang, J., 2014. A new risk quantification approach in port facility security assessment. Transportation Research Part A. 59, 72-90.

Yang, Z., Wang, J., Bonsall, S., Fang, Q.G., 2009. Use of fuzzy evidential reasoning in maritime security assessment. Risk Analysis. 29 (1), 95–120.

Yang, Z.L., Wang, J., Li, K.X., 2013. Maritime safety analysis in retrospect. Maritime Policy & Management. 40(3). 261-277.

Yeo, G.T., Pak, J.Y., Yang, Z., 2013. Analysis of dynamic effects on seaports adopting port security policy. Transportation Research Part A. 49, 285-301.

Yuen, C.L.A., Zhang, A., Cheung, W., 2012. Port competitiveness from the users' perspective: an analysis of major container ports in China and its neighbouring countries. Research in Transportation Economics. 35 (1), 34 – 40.

Zhang, D.H., Qu, Z.H., Wang, W.X., Yu, J.G., Yang Z. 2020. New uncertainty modelling for cargo stowage plans of general cargo ships. Transportation Research Part E: Logistics and Transportation Review. 144, 102151.

Zimmermann, H.J., 1991. Fuzzy Set Theory and its Application. Kluwer, Norwell, MA.