Use of Fuzzy Systems for Vulnerability Evaluation: An Example of a Container Terminal

Stefanie Gote
Institute for the Protection of Maritime Infrastructures
German Aerospace Center (DLR)
Bremerhaven, Germany
Stefanie.Gote@dlr.de

Chathura Wanigasekara
Institute for the Protection of Maritime Infrastructures
German Aerospace Center (DLR)
Bremerhaven, Germany
Chathura.Wanigasekara@dlr.de

Frank Sill Torres
Institute for the Protection of Maritime Infrastructures
German Aerospace Center (DLR)
Bremerhaven, Germany
Frank.SillTorres@dlr.de

***Abstract*—This paper investigates the use of a fuzzy system to evaluate vulnerability with performance indicators. First, the use of fuzzy logic and performance indicators for vulnerability assessment are shown, then the fuzzy systems used in this study are described, using different examples. This is followed by a comprehensive comparison carried out to investigate how different vulnerability values change depending on the examples. Results indicates that the shape and the number of the membership functions have a strong influence on the resulting vulnerability. Hence, the shape and the number of the membership functions should be considered carefully. Further, the use of various inference methods has no impact on the vulnerability.**

***Index Terms*—Fuzzy Logic, Vulnerability Evaluation, Container Terminal**

I. Introduction

Maritime transportation has become the most dominant mode of transportation in international trade nowadays, covering around 80% of international trade and playing a vital role in the world economy [1]. Maritime container terminals play a vital role in this system. This raises a concern about how vulnerable these terminals are and how they behave under disturbances [2], [3]. Such assessment can be executed, for example, by analysing the vulnerability of a shipping network when exposed to disruptions [4].

Vulnerability is defined as the susceptibility of a critical infrastructure to disruptions in functionality in relation to a specific hazardous event [5]. For vulnerability evaluation, indicators are commonly used. Such indicators are for example used to describe characteristics which impact the vulnerability of humans, institutions, or organisations [6]. The researchers in [7] investigated the vulnerability of a hospital considering the performance of patients, stations etc.. Authors in [8] and [9] show that performance evaluation can also be carried out considering vulnerability as the measure [8], [9].

Vulnerability is always associated with uncertainties, which also results from the fuzziness of the indicator values employed for vulnerability assessment. One way to deal with such uncertainties is fuzzy logic, which provides the use of qualitative statements, like "high" or "medium" vulnerability [10]. With further advancements, it was also used as a means of incorporating expert knowledge into a system [11]. There exists different application examples for the use of fuzzy-logic in vulnerability or risk assessment such as use of fuzzy logic for the assessment of groundwater vulnerability [12], [13], risk assessment of underground power distribution network cables [13] and vulnerability of marine fishes [14]. For the risk assessment, the risk is calculated as a combination of fault vulnerability and fault consequences using fuzzy logic [13]. The researchers in these examples see the advantage in using fuzzy logic to handle uncertainties when describing vulnerability in linguistic terms.

However, there is a lack of methods based on fuzzy logic for the vulnerability assessment of maritime container terminals, which motivates the present study. The main contributions of this investigation can be summarised as follows:

1) Choosing an appropriate performance indicator for the vulnerability evaluation of maritime container terminals.
2) Definition of the fuzzy system for the vulnerability evaluation of maritime container terminals.
3) Detailed description and analysis on the influence of different variations of fuzzy systems on the vulnerability.

This paper is organised as follows. Section II briefly describes the fuzzy system and calculation of the vulnerability. Section III shows the obtained results and in Section IV results are discussed, limitations of the present study and future directions are given, with concluding remarks in Section V.

II. Fuzzy System and Estimation of the Vulnerability

The following section introduces the performance indicator and fuzzy systems.

A. Performance

Vulnerability is closely related with *performance*, which indicates the likeliness for the disruption of functionality. The term *functionality* is used to describe a fulfillment of a process or task where the term *performance* describes the resource utilisation to carry out such a process task. In this study, productivity is chosen as the performance indicator.

Let us look at an example of a container terminal in an import-export terminal, with ships, trains and trucks. The main processes of the terminal could be summed up as transportation, loading, unloading and storage of the containers. In order to move the containers, container handling equipment (CHE), like quay cranes (QCs), straddle carriers (SCs), etc., are used. The *productivity* of the CHE is calculated as follows:

$$\text{Productivity}_{\text{CHE}} = \frac{\text{Number of Cycles}_{\text{CHE}}}{\text{Work Time}_{\text{CHE}}} \tag{1}$$

Where a *cycle* is defined as the CHE handling process of a container which starts with picking up a container and ends with delivery of the container [15]. For the vulnerability evaluation, the productivity is associated with cycle times found in literature [16], [17]. Normal productivity and Normalised productivity for a CHE are defined as:

$$\text{NormalProductivity}_{\text{CHE}} = \frac{1}{\text{Cycle Time}_{\text{CHE}}} \tag{2}$$

$$\text{NormalisedProductivity}_{\text{CHE}} = \frac{\text{Productivity}_{\text{CHE}}}{\text{NormalProductivity}_{\text{CHE}}} \times 100\% \tag{3}$$

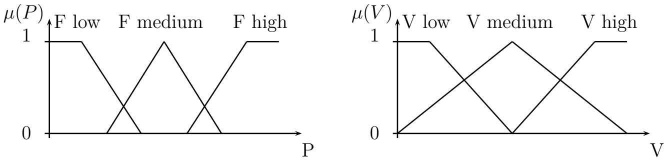
B. Fuzzy System

This subsection briefly describe the fuzzy system used for the vulnerability assessment for the sake of completeness. A fuzzy system consists of following basic elements:

1) A fuzzyfier, which transfers a numerical input (e.g. Productivity $P = \alpha$), into a fuzzy value (e.g. Functionality(F)) using membership functions (e.g. Functionality (F)=$\mu(P = \alpha) = \beta$);
2) A knowledge base, which defines IF-THEN rules;
3) A fuzzy inference engine, where the rules of the knowledge base are used to approximate reasoning to derive an output fuzzy set;
4) A defuzzyfier, which transfers a fuzzy output into a numerical value.

The interested reader can find more details in [11].

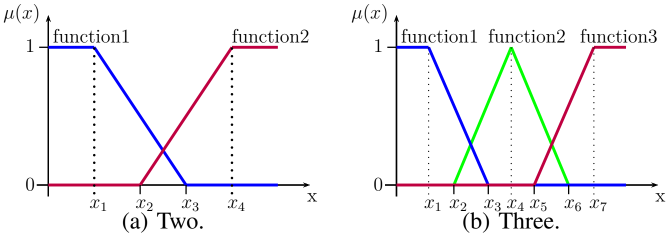
In the fuzzy system for vulnerability evaluation proposed in this paper, the numerical input is the normalised productivity (P) and the output is the vulnerability (V). The functionality (F) is calculated using the productivity (see equation 3). For the functionality a linear relationship with the productivity is assumed, so the productivity degree could directly be assigned to the linguistic values of the functionality. This is a fair assumption given that only working times are used to calculate productivity, which is normalised with an average value that is free from delays. For example the time when a CHE waits for the supply of a container is not considered in this study.



(a) Input.

(b) Output.

Figure 1: Membership Functions of the Fuzzy System.



(a) Two.

(b) Three.

Figure 2: Points in Membership Functions for the Shape Description for Different Linguistic Values.

Vulnerability is obtained using the following steps. First, the productivity degree is fuzzificated into linguistic values of functionality. Secondly, the fuzzy inference engine is applied to the fuzzified values. Finally a vulnerability value is the result of the defuzzification. In this study, the linguistic values for functionality (F) and vulnerability (V) are low and high or low, medium and high. The membership functions for three values are described in Figure 1a, as there is only one input variable and the number of the input and output values are varied together, the rules show a direct connection of the functionality to the vulnerability. Fuzzy rules are defined as:

1) IF F is low THEN V is high
2) IF F is medium THEN V is medium
3) and IF F is high THEN V is low

For the transfer of the rules in the fuzzy system, two different inference methods are used namely Mamdani-Assilan method which is also referred to as max-min-inference [11] and the max-prod-inference method [18]. The former uses minimum-function for the evaluation of the IF-THEN rule and the maximum-function to summarise all applied rules. For the latter, IF-THEN rules are the product of the IF part value with the membership function of the output value.

C. Calculation of Vulnerability and Examples

For the calculation of vulnerability values, four spreadsheet maps are created using Microsoft Excel. The first map is for two linguistic values with max-prod-inference, the second for three linguistic values with max-prod-inference, the third for two values with max-min-inference and the fourth for three values with max-min-inference. All these maps provide a value for the vulnerability when a normalised productivity is given as a input.

The examples defined for membership functions are the same for functionality and vulnerability where the range for the values is from 0 to 100. For two linguistic values, there are

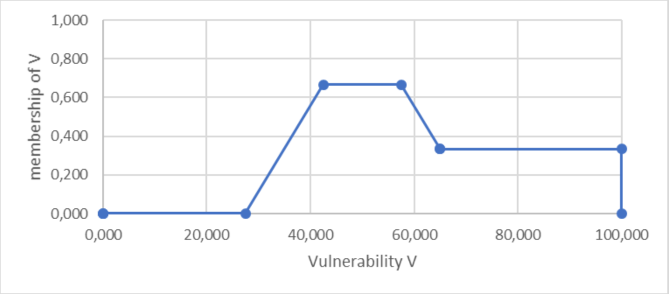


Figure 3: Output Set for the Described Example.

two trapeze shaped membership functions, which are described using x_1, x_2, x_3, x_4 shown in Figure 2a. For three linguistic values, a triangular function is included in the middle between the two trapezoids, where the functions are described using $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ (see Figure 2b). The membership functions are varied in terms of the size of the overlap and plateau and in the orientation of the plateaus and overlap. Note that, *plateau* in this context describes the part of the trapezoid shaped function which is constant. Refer to Table I for a selection of examples used in this study, for different variations.

To calculate the vulnerability for the variations of the functionality membership functions, fixed values for the form of the vulnerability membership functions are required. Therefore, medium values have been chosen. For the fixed values of the functionality membership functions, while the vulnerability membership functions are varied, the results from the variation of the functionality membership function are used to find a variation where the functionality does not have a big influence on the vulnerability. Out of these combinations, variation with medium overlap, small plateau and orientation in the middle is chosen as they form linear relationships.

Let us consider an example of a QC in a container terminal that has a cycle time of 2 minutes. During the last two hours QC finished 25 cycles (completed 25 tasks) within 100 minutes. Normalised productivity for this QC is calculated as:

$$\text{NormalisedProductivity}_{\text{QC}} = \frac{\frac{25}{100}}{\frac{1}{2}} * 100 = 50\%$$

Then this normalised productivity is inserted into the Excel sheet for calculation of vulnerability. Example 12 from Table I is used for the functionality membership function and for vulnerability function fixed values are used. For a productivity of 50% the membership of F *low* is 0.333, of F *medium* 0.667 and of F *high* 0. Then, max-min-inference is applied to calculate the vulnerability output set as shown in Figure 3. Then this fuzzy output is defuzzified to get a numerical output for the vulnerability. For this example with a productivity of 50% the vulnerability of the loading and unloading QC process is 61.75.

III. Results

This section discusses the results using the examples of variation described in Subsection II-C and listed in Table I. First, the vulnerability is calculated for the normalised productivity from 5 to 100 in steps of 5 for different examples of the membership functions. This means that there are 20 vulnerability values for every variation, which are compared visually by plotting them in diagrams. The diagrams are created using the max-min-inference and membership functions of the functionality are varied. In the resulting diagrams, if there is a "v" behind the example number, the membership function of the vulnerability is varied and if there is a "Prod" behind the example number in the graph name, the max-prod-inference is used.

Comparison of the linguistic values are conducted for all membership variations and considering both inference methods. The membership functions could be varied in terms of the size of the overlap, size of the plateau and the orientation of the plateau and overlap such as the overlap size is varied while all the other factors are fixed.

First, the comparisons for having two or three options for linguistic values are carried out and results are shown in Figure 4. From the figure, it can be seen that for variations with a small overlap, linguistic number influences the number of sectors where the values are concentrated. For all variations of functionality, membership functions with a medium overlap and a large plateau, the shape for both variations is the same, only with a small value difference between two and three values. For all other variations there is a shape in between the two cases described above which could not be categorised.

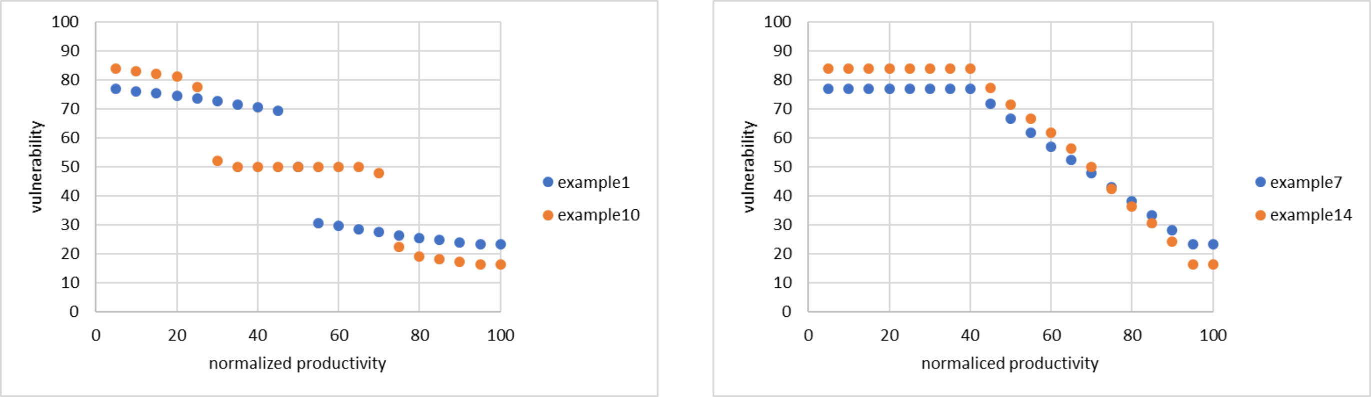
A comparison of different membership functions influence on the course of the vulnerability is done in the next step. The overlap size is varied for different examples and results are shown in Figure 5. Figure 5a, indicates that a small overlap with a small plateau leads to two sectors where values are concentrated for two linguistic values and the medium and large overlap leads to a approximate uniform decrease of progression. For three linguistic values, small overlap leads to three sectors where the values are concentrated, in contrast to medium and large overlap where the values are spread over a large range. Further, in Figure 5b, for variations with a large plateau, sectors where the values are concentrated can be observed for the small and medium overlap.

Then, the plateau size is varied for different examples and results are shown in Figure 6. From Figure 6a, it can be seen that, for two value variations with small or large overlap, plateau size does not have an impact. However, for three value variations with small overlap, a sector where the values are concentrated is visible for large and small plateau, as shown in Figure 6b. For a medium overlap, there is a large sector where the values are concentrated in the output for big plateau and for small plateau, there is only a very small value concentration (see Figure 6c).

The variation in orientation is most visible for the variations that lead to a large sector where the values are concentrated and results are shown in Figure 7. In Figure 7a, the value concentration is stronger to the sides or to the center depending on whether the alignment is right, left or centre. For variations with two linguistic values and large or small overlap with

Table I: Selection of Analysed Examples.

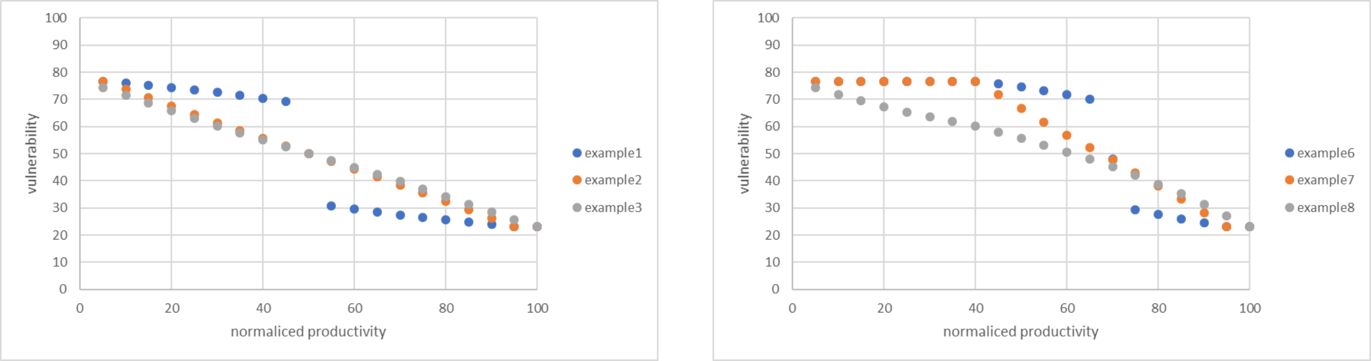
No.	Overlap	Plateau	Orientation	x_1	x_2	x_3	x_4	x_5	x_6	x_7
1.	Small	Small	Middle	5	47	53	95	-	-	-
2.	Medium	Small	Middle	5	5	95	95	-	-	-
3.	Large	Small	Middle	5	0	100	95	-	-	-
4.	Large	Large	Middle	30	0	100	70	-	-	-
5.	Medium	Small	Right	10	10	95	95	-	-	-
6.	Small	Large	Right	40	67	73	95	-	-	-
7.	Medium	Large	Right	40	40	95	95	-	-	-
8.	Large	Large	Right	40	0	100	95	-	-	-
9.	Medium	Small	Left	5	5	90	90	-	-	-
10.	Small	Small	Middle	5	24.5	30.5	50	69.5	75.5	95
11.	Small	Large	Middle	30	37	43	50	57	73	70
12.	Medium	Small	Right	10	10	70	70	70	95	95
13.	Small	Large	Right	40	52	58	70	79.5	85.5	95
14.	Medium	Large	Right	40	40	70	70	70	95	95
15.	Small	Large	Left	5	14.5	20.5	30	42	48	60



(a) Example 1 & 10.

(b) Example 7 & 14

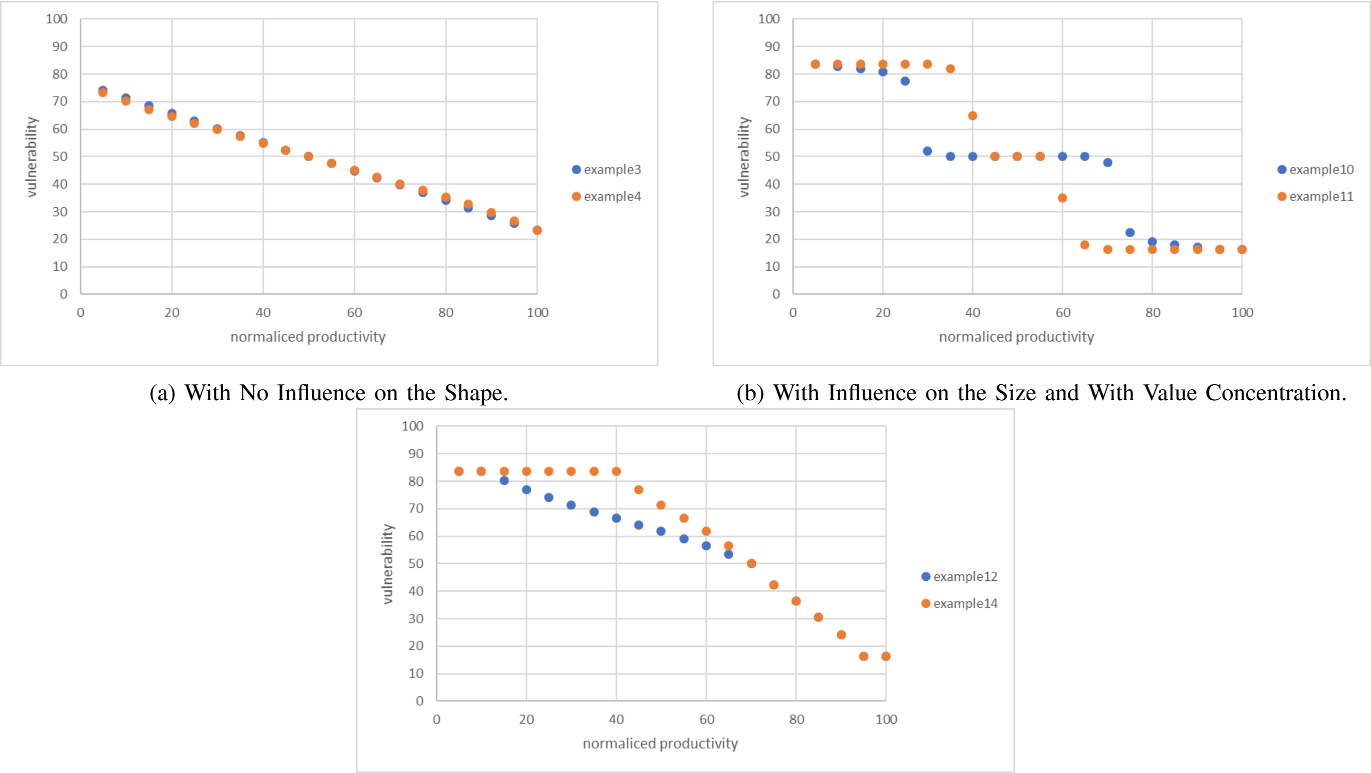
Figure 4: Examples for Variation of Linguistic Values.



(a) Small Plateau.

(b) Large Plateau.

Figure 5: Examples for Variation of Overlap.



(a) With No Influence on the Shape.

(b) With Influence on the Size and With Value Concentration.

(c) With Medium Overlap.

Figure 6: Examples for Variation of Plateau.

small plateau, the orientation does not have an influence on vulnerability (see Figure 7b).

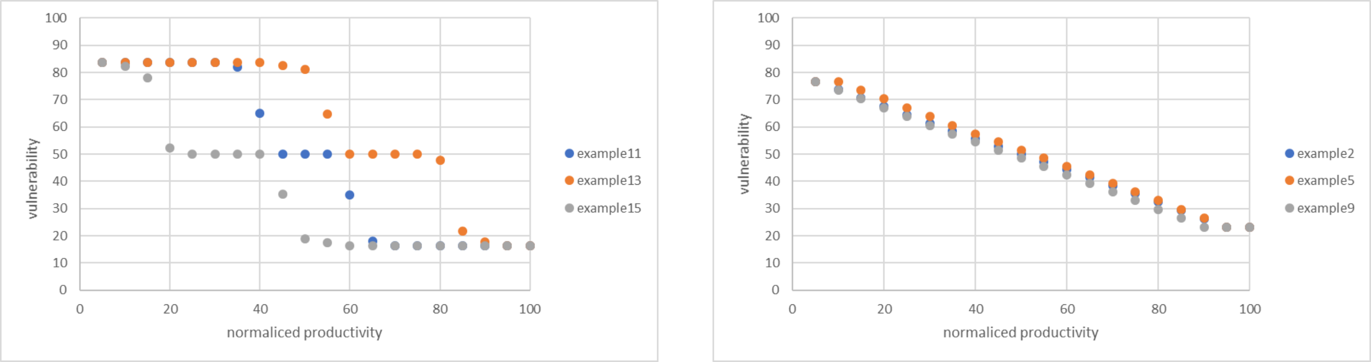
Finally, the vulnerability membership functions and the inference methods are varied and results are shown in Figure 8. From Figure 8a, it can be seen that variation of the membership functions of the vulnerability shows more variation in the value range and not in the form of the curve. The value range difference is the strongest in the peripheral areas for the most variations, so it can be used to reach specific limits of vulnerability. Overall, it could be concluded that the number of linguistic values influences the course of the vulnerability strongly, depending on the used membership functions. As there is a connection between the number of linguistic values and the form of membership functions, especially for the input, they must be considered together to find a fitting description for the vulnerability. As it is seen in Figure 8b, inference method has no influence on vulnerability. However, a distinction can be made here about the implementation effort. For the max-min-inference with three values there are three more cases for the output function to take into account for the calculation, thus it is numerically expensive.

IV. Discussion

In this study, there are only two and three linguistic variables used. However, as fuzzy sets allow to make a partially assignment to the sets, there are more sets of resulting vulnerabilities than three. The range of values of vulnerabilities depends on the variation of functionalities. This is a common practice in the literature (see [19] and [20]), where authors have only used three input variables, but for the output four to five values were extracted. As explained in [19] and [20], fuzzy system are used to combine multiple inputs in order to have different input combinations to investigate diverse output values. In other cases, the number of values for the input and output variables can also be defined using the systems different stakeholders. For example, there can be four different classes of categorisation risk for the security management because security management classifies its measures in four classes.

One of the limitations of the present study is that the proposed fuzzy system can only be used if the productivity consist of working time without other times, like waiting time for another process. Otherwise the functionality has to be calculated through another fuzzy system where the productivity and the functionality are the input and output, respectively, then functionality has to be used as an input for a second fuzzy system where vulnerability is the output. Further, the information about how the shape of the membership functions influences the output set of the fuzzy system can also be used in this extended system, as it contains two systems of the same type, similar to the system considered in this study. This could be subjected to future study.

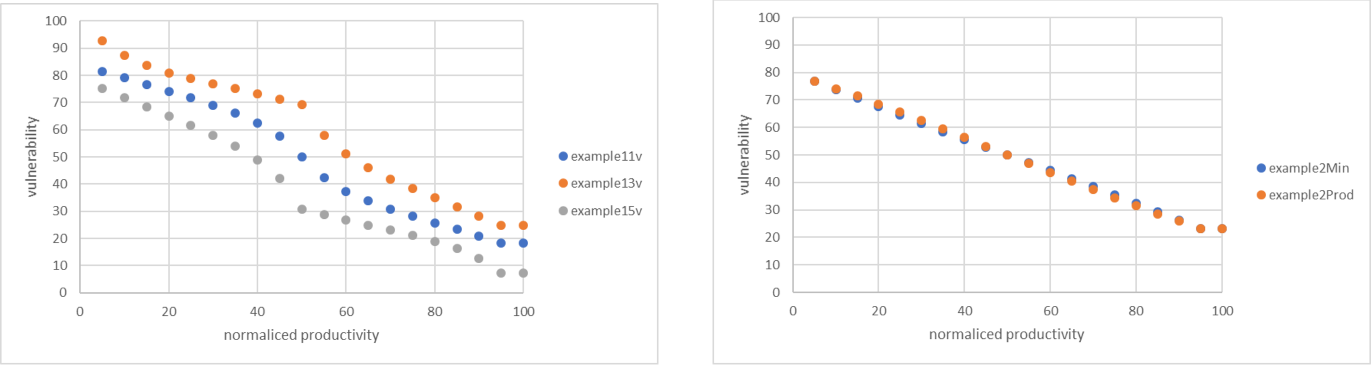
Fuzzy systems are not the only way to estimate vulnerability. There are other alternative procedures to calculate the vulnerability from the productivity, like the use of classes with



(a) With Strong Influence on the Orientation.

(b) Without Influence on the Shape.

Figure 7: Examples for Variation of Orientation.



(a) Vulnerability Membership Functions.

(b) Inference Method.

Figure 8: Examples for Variation of Membership Functions and Inference Method.

sharp borders. For example a productivity degree from 0 to 0.3 corresponds to a *low* class functionality and that corresponds to a *high* vulnerability. One of the other ways is to represent the relationship between productivity and functionality and the functionality and vulnerability using mathematical functions. For the fuzzy system used in this study, there is a linear relation between the productivity and functionality, so representing it mathematically is straightforward. By comparing these two alternative methods with the fuzzy system method, it can be clearly seen that, in terms of the accuracy and the complexity, use of functions is preferred, but at the cost of higher expenditure. However, use of classes with sharp borders leads to less accuracy and only results in very general statements about the vulnerability. By weighing these pros and cons, it can be concluded that fuzzy systems are lower in accuracy compared to mathematical functions, but more accurate than classes with sharp borders. Also the expenditure is higher compared to classes with sharp borders. In practical applications, a final decision must be made after carefully considering all the information and the use case. One of the common examples is that the effort for the creation of a fuzzy system is high compared to accuracy gain of when there are only between five to ten varying values, so that sharp borders are preferred.

V. Conclusion

This paper investigated the use of fuzzy systems to evaluate vulnerability with performance indicators. First, the use of fuzzy logic and performance indicators in vulnerability assessment where shown, then the fuzzy systems used in this study were described, using different examples. Afterwards a comprehensive comparison was carried out to investigate how different vulnerability values change depending on the examples. Results show that the shape and the number of the membership functions have a strong influence on the resulting vulnerability. Hence, the shape and the number of the membership functions should be considered carefully. Further, the use of various inference methods had no impact on the vulnerability. The described fuzzy system is to be implemented in a disruption simulation in order to investigate the suitability of vulnerability evaluation for a container terminal which is subjected to future research.

References

[1] A. Alessandri, C. Cervellera, M. Cuneo, M. Gaggero, and G. Soncin, "Modeling and Feedback Control for Resource Allocation and Performance Analysis in Container Terminals," *IEEE Transactions on Intelligent Transportation Systems*, vol. 9, no. 4, pp. 601–614, 2008.

[2] D. Steenken, S. Voß, and R. Stahlbock, "Container terminal operation and operations research-a classification and literature review," *OR spectrum*, vol. 26, pp. 3–49, 2004.

[3] R. Stahlbock and S. Voß, "Operations research at container terminals: a literature update," *OR spectrum*, vol. 30, pp. 1–52, 2008.

[4] X. Liu, J. Li, Y. Yang, and B. Xu, "Vulnerability change of container shipping network on Maritime Silk Road under simulation disruption," in *2022 International Symposium on Sensing and Instrumentation in 5G and IoT Era (ISSI)*. IEEE, nov 2022.

[5] S. Lenz, *Vulnerabilität Kritischer Infrastrukturen*. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2009.

[6] M. Kappes, M. Papathoma-Köhle, and M. Keiler, "Assessing physical vulnerability for multi-hazards using an indicator-based methodology," *Applied Geography*, vol. 32, no. 2, p. 577–590, 2012.

[7] F. Brauner, T. Münzberg, M. Wiens, F. Fiedrich, A. Lechleuthner, and F. Schultmann, "Critical infrastructure resilience: A framework for considering micro and macro observation levels," in *ISCRAM 2015 Conference Proceedings - 12th International Conference on Information Systems for Crisis Response and Management*, 2015.

[8] I. El-Baroudy and S. P. Simonovic, "Application of the fuzzy performance measures to the city of london water supply system," *Canadian Journal of Civil Engineering*, vol. 33, no. 3, p. 255–265, 2006.

[9] B. A. Beker and M. Lal Kansal, "Fuzzy logic-based integrated performance evaluation of a water distribution network," *Aqua Water Infrastructure, Ecosystems and Society*, vol. 71, no. 4, p. 490–506, 2022.

[10] L. Zadeh, "Fuzzy Sets," *Information and Control*, vol. 8, pp. 338–353, 1965.

[11] R. Czabanski, M. Jezewski, and J. Leski, *Introduction to Fuzzy Systems*. Springer International Publishing, 2017, pp. 23–43.

[12] B. Agoubi, R. Dabbaghi, and A. Kharroubi, "A mamdani adaptive neural fuzzy inference system for improvement of groundwater vulnerability," *Groundwater*, vol. 56, no. 6, pp. 978–985, 2018.

[13] F. Rezaei, H. R. Safavi, and A. Ahmadi, "Groundwater vulnerability assessment using fuzzy logic: A case study in the zayandehrood aquifers, iran," *Environmental Management*, vol. 51, no. 1, pp. 267–277, 2012.

[14] W. W. Cheung, T. J. Pitcher, and D. Pauly, "A fuzzy logic expert system to estimate intrinsic extinction vulnerabilities of marine fishes to fishing," *Biological Conservation*, vol. 124, no. 1, pp. 97–111, 2005.

[15] Terminal Industry Committee 4.0, "Cycle 2021.002," 2021.

[16] U. Speer, *Optimierung von automatischen Lagerkransystemen auf Containerterminals*. Springer Fachmedien Wiesbaden, 2017.

[17] S. Voß, R. Stahlbock, and D. Steenken, "Container terminal operation and operations research - a classification and literature review," *OR Spectrum*, vol. 26, no. 1, pp. 3–49, 2004.

[18] J. Blieberger, B. Burgstaller, and G.-H. Schildt, *Informatik : Grundlagen*. Springer, 2002.

[19] M. S. Guettouche, "Modeling and risk assessment of landslides using fuzzy logic. application on the slopes of the algerian tell (algeria)," *Arabian Journal of Geosciences*, vol. 6, no. 9, pp. 3163–3173, 2012.

[20] M. D. Wardhana, A. Sofwan, and I. Setiawan, "Fuzzy logic method design for landslide vulnerability," *E3S Web of Conferences*, vol. 125, p. 03004, 2019.