MANAGING SUPPLY CHAIN RISKS: A FUZZY-FAILURE MODE AND EVALUATION APPROACH FOR RANKING THREATS

AYODELE OLUWASEGUN OLUWOLE¹, BABATUNDE OMONIYI ODEDAIRO¹*, VICTOR OLUWASINA OLADOKUN¹

¹Department of Industrial and Production Engineering, University of Ibadan, 200284, Nigeria

Abstract: On the backdrop of lower transportation cost, outsourcing paved the way for borderless production activities and ushered in the era of Supply Chain Management (SCM). For many organizations, achieving the goals of their Supply Chain (SC) is constantly threatened by increased competition and disruption. In this study, the aim is to identify, and rank, SC threats in a developing country using Failure Mode and Effects Analysis (FMEA) with Fuzzy Logic (FL). FMEA parameters were derived for 44 supply chain threats (SCT1 – SCT44) and their Risk Priority Number (RPN) determined. Subsequently, the Mamdani Fuzzy Inference system was utilized to arrive at a Fuzzy-RPN with 125 rules using severity as a determining factor. The rules were ranked to prioritize SC threats. From the conventional FMEA, demand variation (SCT42) and long-distance sourcing (SCT27) had the highest and lowest RPN, respectively. After fuzzification and defuzzification, Fuzzy-RPN identified raw material delay (SCT1), government policy (SCT11), poor transport infrastructure (SCT18) and political instability (SCT19) as threats with the highest Fuzzy-RPN (210) and product recalls (SCT28) with the lowest Fuzzy-RPN (99). Based on these results, it is concluded that a Fuzzy-FMEA approach can identify and rank SC threats with the use of an RPN devoid of sentiments and inaccuracies.

Keywords: supply chain, fuzzy-logic, threats, risk priority number, disruption

1. INTRODUCTION

Before the 1990s, the approach of many organizations to customer fulfilment was vertical integration with little or no emphasis on core competencies. On the backdrop of lower transportation cost, outsourcing paved the way for borderless production activities and ushered in the era of Supply Chain Management (SCM). SCM coordinates decisions on production, inventory, location and transportation among the firms in a Supply Chain (SC) to reduce operating and inventory costs [1].

SC as a network of relationships aligns firms and the required chain drivers to deliver products and services [2–4]. From a system view, SC drivers include production facilities, material suppliers, distribution and retailing services, location, transporters, and customers connected to exchange materials and share information [1]. While one of the goals of an SC is to ensure virtual integration among participating companies, a robust SC system should possess the ability to maintain a balance between responsiveness and efficiency. Such a system can increase the efficiency of different business process through integration and proper coordination. On responsiveness, an excellent decision-making structure will enable an organisation respond to disruptions from increased competition, globalisation, global pandemic, and technological advancement. Invariably, failure events characterized by the

* Corresponding author, email: bo.odedairo@ui.edu.ng
© 2021 Alma Mater Publishing House
termination of the ability to exchange resources and information in the chain will occur if disruptions and risks are poorly managed.

Supply chain risks are events (or conditions) at macro and micro levels with the potential to negatively influence core drivers in the chain leading to failures [5]. Micro-risk considers recurrent events which have their root cause from components within the network. Macro-risk includes external and man-made events. Harington [6] commented that 90% of firms do not formally measure risk and about 47% do not possess any backup plan in the event of unexpected disruptions. Based on the multiplicity and diverse risky events among chain drivers, Supply Chain Risk Management (SCRM) should be a collaboration effort. SCRM should consider environmental, social, and economic risks at macro and micro levels, and propose a contingency approach to increase SC resilience. The resilience of an SC describes the internal and external capability of the system elements to manage inevitable disruptions and revert to pre-disruption status. This ability will mitigate (or ameliorate) against the ripple effect of disruptions; for example, Peck [7] sighted SC disruptions of two Finnish phone makers Nokia and Ericsson in 2000. The disruption caused Ericsson about $400 million loss in new product sales. In addition, UPF-Thompson, a major supply of chassis to Land Rover became insolvent in 2001. These events and others opened a new era in SCRM research as interests in creating a resilient supply chain increased.

Singhal et al. [8] reviewed research articles on SCRM and concluded that a large proportion of the methods appeared disjointed despite growing diverse techniques and applications. Similarly, lack of understanding of SCRM and an all-inclusive SCRM technique are barriers to effectively manage SC risks [5, 9]. Tang and Musa [10] commented that quantitative models in SCRM are lacking despite a significant rise in intellectual understanding of SCRM. Ghadge et al. [11] used Failure Mode and Effects Analysis (FMEA) to identify and access SC risks. Cankabis et al. [12] utilized FMEA with Analytic Hierarchy Process (AHP) to model risk assessment for SC system. Their study indicated that a prioritized sub-risks in SC can be obtained using FMEA despite its limitations. However, the limitations of the conventional FMEA [13-15] can be enhanced when integrated with other techniques e.g. Analytic Hierarchy Process (AHP), Fuzzy Logic (FL), Value Analysis, etc. [16]. In this study, the aim is to develop a quantitative knowledge repository to rank, prioritize and manage supply chain threats in a developing country using Failure Mode and Effects Analysis (FMEA) with Fuzzy Logic (FL).

1.1. Supply chain risk management

The quest to identify, manage and minimize the vulnerability of the elements of a supply chain via a structured approach is the goal of SCRM [8]. As a background for this research work, previous methods used in SCRM are presented in Table 1.

| S/N | Author(s) | Year | Keywords | Approach/Method |
|-----|-----------|------|----------|----------------|
| 1.  | Juttner et al. [17] | 2003 | Risk management. Supply chain risk management | Qualitative |
| 2.  | Juttner [18] | 2005 | Supply chain risk management, supply chain | Qualitative focus group and quantitative survey and |
| 3.  | Tang [19] | 2006 | Supply chain, risk management | Qualitative literature review |
| 4.  | Peck [7] | 2006 | Supply chain, vulnerability, supply chain management | Qualitative |
| 5.  | Manuj and Mentzer [20] | 2008 | Supply chain risk management | Integrated literature review |
| 6.  | Tang and Musa [10] | 2011 | SCRM, risk management | Literature survey and citation analysis |
| 7.  | Singhal et al. [8] | 2011 | SCRM, risk, uncertainty, literature review | Multi-layered top town taxonomy for classifying literature |
| 8.  | Sodhi et al. [21] | 2012 | Supply chain, SCRM | Qualitative |
| 9.  | Sakli et al. [22] | 2014 | Manufacturing systems, SC, performance analysis, Time series analysis risk, Performance indices | Stochastic model of product flows |
| 10. | Ho et al. [5] | 2015 | SCRM, risk types, risk factors literature review, risk management methods | Literature review |
11. Ghadge et al. [11] 2017  Supply chain risk management, Product safety and security, Fuzzy, FMEA  Fuzzy, FMEA
12. Canbakis et al. [12] 2018  Risk management, Supply Chain, AHP, FMEA, WP  FMEA, AHP, WP
13. Bier et al. [23] 2019  Supply chain, Disruptions, Risk management  Systematic literature review
14. Hudin et al. [9] 2019  SCM, Risk management, Supply chain risk management, Barrier automotive  Qualitative case study method

1.2. Failure mode and evaluation analysis and Fuzzy logic
FMEA is a subjective human thinking used to identify and analyse failure modes and their causes in components and systems [24, 25]. As a bottom-up framework, each potential failure mode in FMEA; severity (S), occurrence (O) and detectability (D) are identified and assigned values between 1 and 10. Thereafter, a risk priority number (RPN) between 1 and 1000 will be obtained for each failure mode.

FL possess a high tolerance for inaccurate data and allows the modelling of intricate non-linear situations within little time [26]. An FL system has the following components: fuzzifier rules, inference engine, and defuzzifier. The FL process combines a set of crisp input, transformed into a fuzzy set through fuzzy linguistic variables, fuzzy linguistic terms and membership functions. Fuzzification allows an inference to be made based on set of rules. Using membership functions, the result can be presented as a crisp output in what is known as defuzzification [27, 28].

1.3. Fuzzy-FMEA
In Fuzzy-FMEA, the failure modes in FMEA are fuzzified with their respective membership function to obtain a degree of importance for each parameter. The technique of Fuzzy-FMEA as described by Balaraju et al. [28] is described in Figure 1.

![Figure 1. Fuzzy-FMEA technique.](image)

2. METHODOLOGY

2.1. Primary and secondary data collection
Primary data obtained through interviews and questionnaire distributed among 7 organisations are presented in Table 2.
Table 2. Summary of sources of data collected.

| S/N | Organisation   | Experts                     | Sector          | Data Collection Type        |
|-----|----------------|-----------------------------|-----------------|-----------------------------|
| 1   | Company A      | Field Service Engineer      | Telecommunication | Questionnaire/Interview     |
| 2   | Company B      | Supply chain personnel      | Construction    | Questionnaire               |
| 3   | Company C      | Project Administrator       | Real Estate     | Questionnaire/Interview     |
| 4   | Company D      | Account officer             | Construction    | Questionnaire/Interview     |
| 5   | Company E      | Architect                   | Construction    | Questionnaire               |
| 6   | Company F      | Project Engineer            | Maintenance     | Questionnaire/Interview     |
| 7   | Company G      | Business Development officer| Oil and gas     | Questionnaire               |

From Rwakira [29], 44 SC threats were adopted to capture relevant aspects threats within the context of developing countries. The threats with their representative codes are shown in Table 3.

Table 3. Supply chain threats.

| Code  | Threat Description               | Code  | Threat Description               |
|-------|----------------------------------|-------|----------------------------------|
| SCT1  | Raw materials delay              | SCT23 | Outsourcing                      |
| SCT2  | Financial difficulties           | SCT24 | Communication barriers           |
| SCT3  | Poor customer delivery performance | SCT25 | In-transit material theft        |
| SCT4  | Poor quality products            | SCT26 | Natural disasters e.g. flood, drought etc. |
| SCT5  | Product counterfeiting            | SCT27 | Long-distance sourcing           |
| SCT6  | Machine breakdowns               | SCT28 | Product recalls                  |
| SCT7  | Customer dynamism                | SCT29 | Demand forecasting               |
| SCT8  | Unfair competition               | SCT30 | Exchange rate fluctuations       |
| SCT9  | Payment threat                   | SCT31 | Unstable taxation                |
| SCT10 | Risk communication               | SCT32 | Geographic location              |
| SCT11 | Government policy                | SCT33 | Weak legal system                |
| SCT12 | Corruption                       | SCT34 | National politics                |
| SCT13 | Effective contracting            | SCT35 | Economic policies                |
| SCT14 | Limited local supply market      | SCT36 | Market dynamics                  |
| SCT15 | Order cancellation               | SCT37 | Stock theft                      |
| SCT16 | Supplier delivery failure        | SCT38 | Manufacturing flexibility         |
| SCT17 | Dishonest suppliers              | SCT39 | Exclusive sourcing               |
| SCT18 | Poor transport infrastructure     | SCT40 | Distributor complacency          |
| SCT19 | Political instability            | SCT41 | Raw materials shortages          |
| SCT20 | Procurement risks                | SCT42 | Demand variations                |
| SCT21 | Power shortage                   | SCT43 | Reputational risk                |
| SCT22 | Insufficient skilled manpower    | SCT44 | Poor internal coordination       |

2.2. Fuzzy-FMEA method

In this study, the Mamdani Fuzzy Inference System (MFIS) will be adopted. MFIS considers the Fuzzify input variables (i.e. S, O and D), the Fuzzy operator (AND / OR), Implication method (IF-THEN rule), Aggregation method (Max Function), and Defuzzification. The MFIS used in this research is presented in Figure 2. In Table 4, the linguistic variables, term sets and membership functions required to convert FMEA into equivalent FIS are highlighted. Membership functions map non-fuzzy inputs to fuzzy linguistic variable and vice-versa in the Fuzzification and Defuzzification process. In essence membership functions are used to quantify linguistic terms. A total of 125 rules combination were obtained from the membership functions.
In Figure 3, a sample screenshot of the developed FIS based fuzzy rules is presented. Using the Fuzzy Logic toolbox in MATLAB software, Fuzzy RPN (FRPN) value was obtained for each threat.

| Linguistic Variables | Term sets       | Membership functions |
|----------------------|-----------------|----------------------|
| INPUT 1: SEVERITY    | None            | trapmf               |
|                      | Low             | trimf                |
|                      | Moderate        | trimf                |
|                      | High            | trimf                |
|                      | Hazardous       | trimf                |
|                      | Unlikely        | trapmf               |
| INPUT 2: OCCURRENCE  | Low             | trimf                |
|                      | Moderate        | trimf                |
|                      | High            | trimf                |
|                      | Very-high       | trimf                |
|                      | Excellent       | trapmf               |
|                      | High            | trimf                |
| INPUT 3: DETECTABILITY | Moderate       | trimf                |
|                      | Low             | trimf                |
|                      | Remote          | trimf                |
|                      | Very-low        | trapmf               |
|                      | Low             | trimf                |
| OUTPUT: FRPN         | Moderate        | trimf                |
|                      | High            | trimf                |
|                      | Very-high       | trimf                |
3. RESULTS

From the conventional FMEA, RPN value for each threat is presented in Table 5. Demand variation (SCT42) and long-distance sourcing (SCT27) had the highest and lowest RPN, respectively.

Table 5. RPN for SC Threats and ranking using FMEA.

| SC Threats | Severity | Occurrence | Detectability | FMEA RPN | Ranking |
|------------|----------|------------|---------------|----------|---------|
| SCT1       | 8        | 8          | 3             | 192      | 6       |
| SCT2       | 8        | 7          | 4             | 224      | 2       |
| SCT3       | 7        | 7          | 3             | 147      | 12      |
| SCT4       | 8        | 6          | 3             | 144      | 13      |
| SCT5       | 7        | 6          | 3             | 126      | 19      |
| SCT6       | 8        | 8          | 1             | 64       | 38      |
| SCT7       | 5        | 3          | 6             | 90       | 29      |
| SCT8       | 6        | 8          | 3             | 144      | 13      |
| SCT9       | 5        | 3          | 8             | 120      | 23      |
| SCT10      | 6        | 4          | 8             | 192      | 6       |
| SCT11      | 8        | 7          | 2             | 112      | 27      |
| SCT12      | 8        | 5          | 5             | 200      | 5       |
| SCT13      | 6        | 3          | 7             | 126      | 19      |
| SCT14      | 5        | 4          | 8             | 160      | 10      |
| SCT15      | 4        | 3          | 6             | 72       | 36      |
| SCT16      | 4        | 3          | 7             | 84       | 31      |
| SCT17      | 6        | 3          | 7             | 126      | 19      |
| SCT18      | 8        | 8          | 2             | 128      | 17      |
| SCT19      | 8        | 8          | 2             | 128      | 17      |
| SCT20      | 7        | 8          | 4             | 224      | 2       |
| SCT21      | 7        | 8          | 3             | 168      | 8       |
| SCT22      | 3        | 2          | 8             | 48       | 42      |
| SCT23      | 3        | 3          | 7             | 63       | 39      |
| SCT24      | 4        | 3          | 7             | 84       | 31      |
| SCT25      | 5        | 4          | 7             | 140      | 16      |
| SCT26      | 8        | 7          | 1             | 56       | 41      |
| SCT27      | 6        | 5          | 1             | 30       | 44      |
| SCT28      | 7        | 2          | 3             | 42       | 43      |
| SCT29      | 5        | 5          | 6             | 150      | 11      |
| SCT30      | 6        | 4          | 5             | 120      | 23      |
| SCT31      | 5        | 5          | 5             | 125      | 22      |
| SCT32      | 4        | 4          | 5             | 80       | 35      |
| SCT33      | 5        | 3          | 7             | 105      | 28      |
| SCT34      | 5        | 3          | 6             | 90       | 29      |
| SCT35      | 6        | 5          | 7             | 210      | 4       |
| SCT36      | 6        | 4          | 6             | 144      | 13      |
| SCT37      | 4        | 3          | 5             | 60       | 40      |
| SCT38      | 4        | 3          | 7             | 84       | 31      |
| SCT39      | 5        | 3          | 8             | 120      | 23      |
| SCT40      | 4        | 3          | 7             | 84       | 31      |
| SCT41      | 8        | 5          | 3             | 120      | 23      |
| SCT42      | 8        | 6          | 5             | 240      | 1       |
| SCT43      | 3        | 3          | 8             | 72       | 36      |
| SCT44      | 6        | 4          | 7             | 168      | 8       |

The membership function editor, the Fuzzy-FMEA viewer, and the Fuzzy-FMEA editor from the Fuzzy Logic toolbox in MATLAB are presented in Figure 4, Figure 5 and Figure 6, respectively.
After fuzzification and defuzzification, the Fuzzy RPN for each threat is presented in Table 6. Fuzzy-RPN identified raw material delay (SCT1), government policy (SCT11), poor transport infrastructure (SCT18) and political instability(SCT19) as threats with the highest Fuzzy-RPN (210) and product recalls (SCT28) with the lowest Fuzzy-RPN (99).
Table 6. RPN for SC threats and ranking using Fuzzy- FMEA.

| SC Threats | S | O | D | FMEA RPN | Ranking | FRPN | FRPN Ranking |
|------------|---|---|---|----------|---------|------|-------------|
| SCT1       | 8 | 8 | 3 | 192      | 6       | 210  | 1           |
| SCT2       | 8 | 7 | 4 | 224      | 2       | 207  | 5           |
| SCT3       | 7 | 7 | 3 | 147      | 12      | 185  | 19          |
| SCT4       | 8 | 6 | 3 | 144      | 13      | 193  | 6           |
| SCT5       | 7 | 6 | 3 | 126      | 19      | 176  | 22          |
| SCT6       | 8 | 8 | 1 | 64       | 38      | 193  | 6           |
| SCT7       | 5 | 3 | 6 | 90       | 29      | 151  | 31          |
| SCT8       | 6 | 8 | 3 | 144      | 13      | 152  | 30          |
| SCT9       | 5 | 3 | 8 | 120      | 23      | 189  | 10          |
| SCT10      | 6 | 4 | 8 | 192      | 6       | 189  | 10          |
| SCT11      | 8 | 7 | 2 | 112      | 27      | 210  | 1           |
| SCT12      | 8 | 5 | 5 | 200      | 5       | 189  | 10          |
| SCT13      | 6 | 3 | 7 | 126      | 19      | 171  | 24          |
| SCT14      | 5 | 4 | 8 | 160      | 10      | 189  | 10          |
| SCT15      | 4 | 3 | 6 | 72       | 36      | 125  | 41          |
| SCT16      | 4 | 3 | 7 | 84       | 31      | 144  | 34          |
| SCT17      | 6 | 3 | 7 | 126      | 19      | 171  | 24          |
| SCT18      | 8 | 8 | 2 | 128      | 17      | 210  | 1           |
| SCT19      | 8 | 8 | 2 | 128      | 17      | 210  | 1           |
| SCT20      | 7 | 8 | 4 | 224      | 2       | 181  | 21          |
| SCT21      | 7 | 8 | 3 | 168      | 8       | 185  | 19          |
| SCT22      | 3 | 2 | 8 | 48       | 42      | 140  | 39          |
| SCT23      | 3 | 3 | 7 | 63       | 39      | 125  | 41          |
| SCT24      | 4 | 3 | 7 | 84       | 31      | 144  | 34          |
| SCT25      | 5 | 4 | 7 | 140      | 16      | 171  | 24          |
| SCT26      | 8 | 7 | 1 | 56       | 41      | 193  | 6           |
| SCT27      | 6 | 5 | 1 | 30       | 44      | 149  | 33          |
| SCT28      | 7 | 2 | 3 | 42       | 43      | 99   | 44          |
| SCT29      | 5 | 5 | 6 | 150      | 11      | 187  | 18          |
| SCT30      | 6 | 4 | 5 | 120      | 23      | 161  | 28          |
| SCT31      | 5 | 5 | 5 | 125      | 22      | 188  | 16          |
| SCT32      | 4 | 4 | 5 | 80       | 35      | 133  | 40          |
| SCT33      | 5 | 3 | 7 | 105      | 28      | 172  | 23          |
| SCT34      | 5 | 3 | 6 | 90       | 29      | 151  | 31          |
| SCT35      | 6 | 5 | 7 | 210      | 4       | 188  | 16          |
| SCT36      | 6 | 4 | 6 | 144      | 13      | 161  | 28          |
| SCT37      | 4 | 3 | 5 | 60       | 40      | 115  | 43          |
| SCT38      | 4 | 3 | 7 | 84       | 31      | 144  | 34          |
| SCT39      | 5 | 3 | 8 | 120      | 23      | 189  | 10          |
| SCT40      | 4 | 3 | 7 | 84       | 31      | 144  | 34          |
| SCT41      | 8 | 5 | 3 | 120      | 23      | 189  | 10          |
| SCT42      | 8 | 6 | 5 | 240      | 1       | 193  | 6           |
| SCT43      | 3 | 3 | 8 | 72       | 36      | 142  | 38          |
| SCT44      | 6 | 4 | 7 | 168      | 8       | 171  | 24          |

4. CONCLUSIONS

In this study, the integration of FMEA with Fuzzy Logic was utilized to rank supply chain threats. A Mamdani-FIS was developed with 3 inputs of severity, occurrence, and detectability. The output was a FuzzyRPN with a total of 125 rules. These rules were formed with severity as the most important factor to adequately rank the threats. With the use of fuzzy logic, subjectivity, vagueness, and incompleteness associated with the supply chain threats...
were made clearer. Based on these results, it is concluded that a Fuzzy-FMEA approach can identify and rank SC threats with the use of an RPN devoid of sentiments and inaccuracies.

REFERENCES

[1] Hugos, M.H., Essentials of supply chain management, 3rd Edition, USA, John Wiley and Sons, Hoboken (NJ), 2011.
[2] http://fcm.csa.iisc.ernet.in/scm/supply_chain_intro.html (28.04.2021).
[3] Lu, D., Fundamentals of supply chain management, Venust Publishing ApS, Frederiksberg, 2011.
[4] Chopra, S., Meindl, P., Supply chain management: strategy, planning and operation, 5th Edition, USA, Pearson Hall, New Jersey, 2013.
[5] Ho, W., Zheng, T., Yildiz, H., Talluri, S., Supply chain risk management: A literature review, International Journal of Production Research, vol. 53, no. 16, 2015, p. 5031-5069.
[6] Harrington, L., Supply chain security and risk management: New thinking, PSM Workshop, June 6-7, 2017, Maryland.
[7] Peck, H., Drivers of supply chain vulnerability: An integrated framework, International Journal of Physical Distribution and Logistics Management, vol. 35, no. 4, 2005, p. 210-232.
[8] Singhal, P., Agarwal, G., Lal Maittal, M., Supply chain risk management: Review, classification and future research directions, International Journal of Business Science and Applied Management, vol. 6, no. 3, 2011, p. 15-42.
[9] Hudin, N.S., Hamid, B.A., Habidin, N.F., Mustafa, S.W., Barrier analysis of supply chain risk management adoption in automotive companies, International Journal of Academic Research in Accounting, Finance and Management Sciences, vol. 9, no. 3, 2019, p. 295-299.
[10] Tang, O., Musa, S.N., Identifying risk issue and research advancements in supply chain risk management, International Journal of Production Economics, vol. 133, no. 1, 2011, p. 25-34.
[11] Ghadge, A., Fang, X., Dani, S., Antony, J., Supply chain risk assessment approach for process quality risk, International Journal of Quality and Reliability Management, vol. 34, no. 7, 2017, p. 940-954.
[12] Canbakis, S.K., Karabas, M.K., Kilic, H., Koseoglu, S., Unal, E., A risk assessment model for supply chains, Press Academia Procedia, vol. 7, no. 1, 2018, p. 122-125.
[13] Xu, K., Tang, L.C., Xie, M., Ho, S.L., Zhu, M.L., Fuzzy assessment of FMEA for engine systems, Reliability Engineering and System Safety, vol. 75, no. 1, 2002, p. 17-29.
[14] Xiao, N.C., Huang, H.Z., Li, Y.F., He, L., Jin, T., Multiple failure modes analysis and weighted risk priority number evaluation in FMEA, Engineering Failure Analysis, vol. 18, no. 4, 2011, p. 1162-1170.
[15] Song, W., Ming, X., Wu, Z., Zhu, B., Failure modes and effects analysis using integrated weight-based fuzzy TOPSIS, International Journal of Computer Integrated Manufacturing, vol. 26, no. 12, 2013, p. 1172-1186.
[16] Odedairo, B.O., Bell, D., Framework for introducing and implementing value methods: A novel toolkit for small and medium scale industries in developing nations, International Journal of Basic and Applied Sciences, vol. 9, no. 10, 2009, p. 87-95.
[17] Jüttner, U., Peck, H., Christopher, M., Supply chain risk management: Outlining an agenda for future research, International Journal of Logistics Research and Applications, vol. 6, no. 4, 2003, p. 197-210.
[18] Jüttner, U., Supply chain risk management: Understanding the business requirements from a practitioner perspective, The International Journal of Logistics Management, vol. 16, no. 1, 2005, p. 120-141.
[19] Tang, C.S., Perspectives in supply chain risk management, International Journal of Production Economics, vol. 103, no. 2, 2006, p. 451-488.
[20] Manuj, I., Mentzer, J.T., Global supply chain risk mangement strategies, International Journal of Physical distribution and logistics management, vol. 38, no. 3, 2008, p. 192-223.
[21] Sodhi, M.S., Son, B.-G., Tang, C.S., Researchers’ perspectives on supply chain risk management, Production and Operations Management, vol. 21, no. 1, 2012, p. 1-13.
[22] Sakli, L., Hennet, J.-C., Mercantini, J.-M., An analysis of risks and vulnerabilities in supply networks, IFAC Proceedings Volumes, vol. 47, no. 3, 2014, p. 8933-8938.
[23] Bier, T., Lange, A., Glock, C.H., Methods for mitigating disruptions in complex supply chain structures: A systematic literature review, International Journal of Production, vol. 58, no. 6, 2020, p. 1835-1856.
[24] Carlson, C.S., Understanding the fundamental definitions and concepts of FMEAs, John Wiley and Sons, Hoboken (NJ), 2012, p. 21-55.
[25] Hayati, M., Abroshan, M.R., Risk assessment using Fuzzy FMEA (Case Study: Tehran Subway Tunneling Operations), Indian Journal of Science and Technology, vol. 10, no. 9, 2017, p. 1-9.
[26] Oladokun, V.O., Proverbs, D.G., Lamond, J., Measuring flood resilience: A fuzzy logic approach, International Journal of Building Pathology and Adaptation, vol. 35, no. 5, 2017, p. 470-487.
[27] Sharma, R.K., Kumar, D., Kumar, P., Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling, International Journal of Quality and Reliability Management, vol. 22, no. 9, 2005, p. 986-1004.
[28] Balaraju, J., Raj, M.G., Murthy, C.S., Fuzzy-FMEA risk evaluation approach for LHD machine - A case study, Journal of Sustainable Mining, vol. 18, no. 4, 2019, p. 257-268.
[29] Tukumuhabwa Rwakira, B., Supply chain resilience: a case study analysis of a supply network in a developing country context, PhD Thesis, Lancaster University Management School (UK), 2015.