Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 54-1 (2021) 1029–1034

Knowledge Registration Module Design for Enterprise Resilience Enhancement

Raquel Sanchis*, Giulio Marcucci, Faustino Alarcón*, Raul Poler***

**Research Centre on Production Management and Engineering (CIGIP). Universitat Politècnica de València. Calle Alarcón, nº1, Alcoy, 03801 Alicante, Spain (e-mail: rsanchis@cigip.upv.es, faualva@cigip.upv.es, rpoler@cigip.upv.es)*

***Department of Industrial Engineering and Mathematical Science, Università Politecnica Delle Marche, Via Brecce Bianche, Ancona, 60131, Ancona, Italy; (e-mail: g.marcucci@staff.univpm.it).*

Abstract: The present situation characterized by the coronavirus pandemic has made businesses to be aware about the importance of being resilient to face undesirable impacts like the one caused by this pandemic. One of the constituent capacities of enterprise resilience is the recovery ability to bounce back and restore the operations after disruptions' occurrence. This paper is focused on the recovery perspective of enterprise resilience and its enhancement through knowledge registration. This research proposes the design of the Knowledge Registration Module addressed to the register of valuable information at different knowledge level with the main aim to reuse this piece of information to facilitate the recovery process when the same or an unexpected similar disruptive event occurs. Future research lines will be based on applying the knowledge approach to real cases to study the influence of knowledge management in the enhancement of enterprise resilience.

Keywords: Knowledge, Registration, Enterprise Resilience, Protocol, Recovery.

1. INTRODUCTION

The coronavirus pandemic has affected the world community from both health and economic point of view. Companies have been very negatively impacted by this disruptive event. They have had to take adaptive measures to adjust to the new circumstances as well as recovery measures to try to guarantee their long-term survival (Sanchis and Poler, 2020). Multitude of investigations have been developed motivated by coronavirus outbreak to guarantee enterprises long-term survivability highlighting the one performed by Ivanov and Dolgui, (2020).

However, companies do not only have to face this new situation, but in the last decade they have had to face numerous events that have altered their normal level of operation. The ability of companies to cope with, adapt and recover from these events has been defined as enterprise resilience (Antomarioni et al., 2017; Bevilacqua et al., 2019; Sanchis and Poler, 2019).

Therefore, it is necessary to build resilient enterprises to recover, once that a disruptive event has occurred, in an efficient way. For this reason, it is advisable to work on building theory in this area with the development of novel proposals designed for enhancing the recovery perspective in the event of a threat occurrence (Bevilacqua et al. 2020).

The concept of resilience was firstly coined ecological field by Holling (1973) from an ecological perfective. He defines it as a system that persists in a state of equilibrium and how dynamic systems behave when they are stressed and move from this stability. Ponomarov and Holcomb (2009) performed a review on the concept of supply chain resilience from the social, psychological, and economic perspectives. From the business perspectives, Hosseini, Ivanov and Dolgui (2019) define resilience as the capacity to withstand, adapt, and recover from disruptions to meet customer demand and ensure performance which is line with the present research.

Sanchis, Canetta and Poler (2020) define the Conceptual Reference Framework for Enterprise Resilience Enhancement in which they identify three constituent capacities to reach resilient enterprises. These authors affirm that a resilient company is prepared in advance in the event of a potential disruptive event (proactive perspective). The second constituent capacity is related to the adaptive ability as the degree of the enterprise to modify its circumstances and move towards a condition of stability (Luers et al., 2003). The last capacity is the recovery one, to respond and restore operations after disruptions occurrence.

This research is focused on the third constituent capacity of enterprise resilience, the recovery capacity. Ivanov et al., (2017) perform a literature review on disruption recovery in the supply chain. Significant investments to obtain a resilient enterprise have been therefore enabled to meaningfully improve company's ability to react after destructive phenomena (Bevilacqua, Ciarapica and Marcucci, 2018). One of the most important means to recover as quickly and efficiently as possible is through knowledge, considered in this research as the awareness and understanding of events under uncertainty to take decisions about which actions and which other means (like stock level, redundant equipment, multiple suppliers, among others) will be needed to enhance the recovery process and consequently the resilient capacity of enterprises. For this reason, it is crucial that companies encourage constant learning and continuous innovation. This will facilitate the recovery process since the available knowledge will enable the return to the steady state of operation before that the disruptive event occurred.

10.1016/j.ifacol.2021.08.122

Mafabi, Munene and Ntavi (2012) state that organisational resilience can be built based on knowledge management. Knowledge management requires the acquisition, creation and use of information to adapt to changes (Nonaka, 2007) and, ultimately, for the enhancement of enterprise resilience. For this reason, resilient organisations should be able to create, register and distribute the knowledge rapidly and efficiently for recovering from a disruption in the shortest possible time and cost. At this point, it is important to highlight that knowledge is a strategic asset that contribute to expand the cognitive capacities of individuals what in turn, improve the enterprise resilience capacity, particularly to recover from complex situations (Sanchis, Sanchis-Gisbert and Poler, 2020). This is also supported by Hora and Klassen (2013) who suggest that senior managers need to develop organizational systems and training to expand the screening by risk managers to enhance knowledge acquisition.

Nonaka and Takeuchi (1995), promoters of knowledge management, develop a model by which the creation of knowledge is obtained through the relationship of tacit and explicit knowledge. The stage of the model of Nonaka et al. (1995) that most interests companies from a resilient point of view, is the combination stage. In this stage, on the one hand, all relevant knowledge obtained by the occurrence of past disruptive events and how the company acted is registered, that is, what recovery actions were carried out. But it is also vitally important to register action protocols that specify how to act, in order to improve the "how the company acted" and thus act efficiently in the case that the same or similar unexpected disruptive events occur again. The most resilient companies will be those that explicitly register knowledge.

Based on this, the objective of this research is to design a knowledge registration module, focused on the enhancement of the recovery capacity when an enterprise has been impacted by a disruption, to provide the foundations for improving the recovery capacity of resilient companies. This design will support enterprises to come back to a steady state while the actions performed from a preparedness and adaptive perspective will support to reach a new and more desirable state. However, this research is only focused on the third capacity of enterprise resilience, the recovery one.

2. KNOWLEDGE REGISTRATION MODULE DESIGN (KRM)

This section provides an overview of the knowledge registration design module (KRM). The KRM has been designed and developed in a spreadsheet as a prototype version. This design is ready to be used by any company. However, companies can also use the design and structure of the KRM through:

- Web applications, such as the corporate intranet. To do that, it will be necessary to adjust and prepare the KRM to make it compatible with web applications and with the database where the information is stored.
- Desktop applications. ICT departments of companies may also develop applications in Windows, Linux or Mac OS environments, based on the design and structure of the KRM prototype.
- File hosting service. The KRM prototype can be available in a hosting service such as Google Drive, which offers the possibility of being able to edit information online and share information collaboratively. between different users of the company.

The design of the KRM offers companies the configuration and structure to register relevant information about the description of disruptive events, in order to create a knowledge basis that facilitates the process of retrieving the necessary relevant information, in the event of a new occurrence of the same or similar unexpected disruptive events. Figure 1 offers an overview of the KRM scheme.

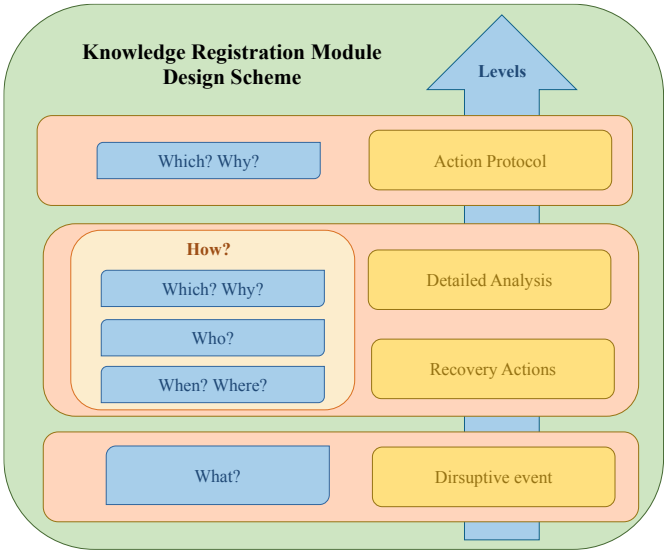

Fig. 1. Knowledge Registration Module Design Scheme.

2.1 What has happened?

This knowledge registration level is related to what has happened? In this case, the objective is to register information about the adverse situation that has had a negative impact on the company. This level contains fields characterized by different degree of detail to be filled in. Some of them cover general information about the disruptive event and other are more specific fields to offer more detailed information as a supporting source for the development of the following knowledge levels.

This level is divided into two main sections. One of general information in which the following fields have been defined: identifier of the disruptive event, name, date and time in which the disruptive event occurred, its description, the functional areas, departments or personnel involved, the causes identified (if any has been already determined), legislative / regulatory aspects, and the short-term and long-term consequences. In this section, the date and the user who registers the information is also required in order to monitor the registration activities through the different users involved in the registration process.

Figure 2 offers the design of the general section of the disruptive event registration level with an example the disruptive event: 'Computer crime (hacking, viruses, malicious codes)' of a textile company that has participated

in this research. The specificity of the example is due the fact that it is a real registration case. Other examples that are currently being defined are related to the coronavirus pandemic. One of them is related to the lack of employees. due to COVID-19. The protocol, that is being developed in a multinational company, will be applied to all the companies when necessary in the event of similar expected or unexpected circumstances. In this case, the ill employee was from the administration department. Therefore, as all the employees work in the same office, all the administration employees had to be confined at home and they teleworked while the administration department in the headquarters was empty. The protocol will contemplate the creation of stable work groups that work on alternate days to increase the probability that at least one employee will always be present on the premises.

Register

General Information	
Disruptive Event (DisEvent) Identifier	23
DisEvent Name	Computer crime (hacking, viruses, malicious codes)
DisEvent Date	11-10-20
DisEvent Time	15:30
Registration date	11-10-20
User who registers	jsmith
DisEvent Description	One of the computers from Administration has been infected with a virus and the computer is not working properly. Half an hour later, another computer from the same department also stops working.
Functional areas or departments involved	Administration and Direction
Involved personnel	Administrative and manager
Identified causes (if any)	It seems that the cause was to click on a link in an email
Legislative / regulatory aspects	-
Short-term consequences	Two computers of the administrative office are inoperative, so it is not possible to work
Long-term consequences	We do not know if we will recover the equipment and if we will lose information
Details	The information about the email that seems to be the cause of the computer malfunction is located on the server C:\Resilience\Events\23\email_virus.msg The subject of the email has been searched online and several web pages show that it is a virus
Historical Registration	
Protocol number (if any)	It does not exist
Number of times the DisEvent has already occurred	It is the second time, but the first only affected a computer and it was solved by running the antivirus and quarantining some files. In that occasion, no event was registered
Preventive actions that have already been implemented (if any)	Kaspersky Antivirus 2021
Previous experiences in the recovery	In that occasion, the antivirus was used w and the computer worked properly again. No external services were required

Fig. 2. Fields for the registration of information about the disruptive event

The more particular section of the disruptive event level has been designed to register historical data related to the occurrence of the different events. Some of the fields defined in this section are the protocol number (if it exists), the number of times that the disruptive event has already occurred, to obtain statistical data about the frequency of the event and to be able to analyse its causes, the preventive actions that were implemented (if any), and the previous experiences in the recovery process of such disruptive event.

2.2 Which actions, Who, When, and Why was it done? Recovery actions.

In this level, the objective is to register information about the recovery actions that were carried out in the past when a specific disruptive event occurred in order to return to the steady state of operation. In this level the fields are defined to collect information about:

- What was it done? Description of the actions that were carried out to deal with the disruptive event.
- Who did it? Description of who carried out the action with twofold objectives. Firstly, the goal is, to register who carried out the action to analyse whether the registering person was the most proper one and secondly, to know who carried out the action, in case it is necessary to collect more information.
- When was it done? Description of the actions' chronology, i.e. registration about when each action was carried out to study if they were implemented at the right time period.
- Why was it done? Justification by who performed the action about why such an action was performed at that specific moment. The mail goal of this section is to provide the motivations about executing such actions, since the decision-making process is associated with the decision maker's tacit knowledge. This tacit knowledge should be made explicit in order to know the reasoning that has led the decision maker to make such decision.
- Appropriateness of the action. In this section, the correctness of the executed actions is analysed. This will serve as a starting point for the definition of the action protocol. The analysis of the recovery actions carried out (either by the decision-maker or from another member/s of the company), will provide an evaluation about whether the actions carried out are as efficient as expected. In the case of identifying actions with low or medium appropriateness, this piece of information will be very valuable to redefine the steps to be followed in the protocol with actions that improve the recovery from the disruptive event. The colours red, orange and green (traffic light colours) warn the company about the appropriateness of the different actions carried out (Figure 3).

Continuing with the example of the textile company's registration about the disruptive event of "Computer crime (hacking, viruses, malicious codes)", Figure 3 shows the actions that were carried out and their degree of appropriateness.

2.3 Summary.

The summary section presents a repository where the information available in the previous two sections is shown as a synopsis. In this way, the most relevant information is available and easily accessible for its extraction and reuse in case that the company requires it. In each of the previous sections, there is a registration option (up on the left) to save the information in a database.

	Register			When it was					
	What was done?	Who did it?	Day	Time	Duration	Why it was done?	Actions' Appropriateness		Comments
Action 1	Restart your computer	Administrative	11-10-20	16:00	10 min	To try to make applications to work properly again	Medium		Perhaps restarting the infected cimpouter makes virus spreads and infects other computers on the network. Perhaps, it would have been more convenient to restart the computer in test mode
Action 2	Ask if the manager's computer works well	Administrative	11-10-20	16:10	5 min	To know the magnitude and scope of the problem (to know if it is a specific problem of the administration computer or if, on the contrary, it affects more computers)	High		Several checks were carried out and it was found that the only affected computer was the Administration one
Action 3	Inform the manager of the problem and the probable cause of the problem.	Administrative	11-10-20	16:15	5 min	To inform manager and make appropriate decisions	High		-
Action 4	The manager searches online for the "email subject" that he has also received and the search validate that it is a virus	Manager	11-10-20	16:20	15 min	To try to install the antivirus on the infected computer and try to fix the problem	Medium		-
Action 5	Download a free online antivirus and install it on the administration computer using a pendrive	Manager	11-10-20	16:35	15 min	To try to install the antivirus on the infected computer and try to fix the problem	Low		Once there is an infected computer, special attention should be paid with the company's network. The administration computer is not working and it is not possible to apply the antivirus. Moreover, after searching for the antivirus online, the management computer also stops working properly.
Action 6	Contact external IT services	Manager	11-10-20	16:50	10 min	To try to explain the problem and identify a possible solution by phone	High		Name Surname (phone number) was contacted. The problem could not be resolved by phone. A visit from the IT technician was scheduled on 13/10/20 at 10:00 as 12/10/20 is a national festivity. In the meantime, it was agreed to not turn on the two infected computers and disconnect them from the network.
Action 7	Format both computers' hard drives and restore backups	External IT services	13-10-20	10:00	30 hours	To remove viruses and restore company backups	High		The restored backups were from 07/10/20 (at 8:00 PM), so some work was lost for several days (10 and 11/10/2020). Cost 200 euros + VAT (external computer services) + loss of information + non-availability of the equipment until 4:00 p.m. on 14/10/2020

Fig. 3. Fields for the registration of information about Which actions, Who, When, and Why was it done? Recovery actions.

2.4 Action Protocol.

The KRM has been defined to also provide the structure and main fields for registering the information of an action protocol. The action protocol differs from the: What, Who, When and Why was it done? Section, as this such a section registers the information on recovery actions carried out by the company in the past but the company does not know if such actions were the most suitable ones. A post-analysis is required to verify the correctness of the actions taken:

- If the post-analysis of the recovery actions carried out offers better alternatives, the protocol should describe in detail the new alternatives. It is important to have both perspectives: (i) the actions implemented to know exactly what was executed, but also (ii) what is planned to be done if the same or a similar unexpected disruptive event occurs again.
- In the case of verifying that the actions carried out were the optimal ones, in the action protocol, such actions should be described in a greater level of detail so that it is registered clearly and concisely an as understandable.

The design of the action protocol consists of two main divisions (Figure 4). A first general information section in which the user should register the information about the following fields:

- Definition date: It is important to register the exact date when the protocol is defined, since over time, the protocol is likely to become obsolete.
- Review date: Registration of the date when the protocol has been examined and modified.
- Update date: Registration of the protocol updating date.
- Authors: Sánchez, González, Molina and Guil (2009) affirm that a protocol should be generated through consensus among experts. In this case, the protocol should be defined by common consent among the personnel who have been involved in the recovery process of the disruptive event because they are the ones who have extensive knowledge of what actions have been taken, where they have been wrong and what-how should it be done.
- Reviewers: Although, it seems that the personnel who have been involved in the recovery process of a specific disruptive event are the most appropriate for defining the protocol due to their experience, it is recommended that the protocol is defined and reviewed by different members of the company to have a multidisciplinary view. For example, one of the reviewers does not understand what is described in one of the steps of the protocol. In this case, the step should be redefined in a more clear and concise way, since if the reviewer is the person in charge of implementing that recovery actions, it would be very difficult for him/her to do it as such a step has not been defined in an understandable way.
- Updaters: With the passage of time, the high dynamism of the environment and of the company, causes circumstances to change, so it is advisable that the different protocols are periodically reviewed and updated.

General Information		
Protocol Number	23.1	Register
Protocol definition date	7-11-20	
Protocol review date	-	
Protocol update date	-	
Authors	jmperez, rcortes	
Reviewers	-	
Updaters	-	
Objectives	Protocol 23.1 is an action guide in the event that the computer system of company XXX are again infected by a virus	
Scope of the protocol	Protocol 23.1 applies to all computer systems of the company	
Terms and definitions	CPU: Central Processing Unit	

Action Protocol Registration

	Definition	Description	Person in charge	Contact information		Duration	Resources	Techniques	Comments
Step 1	Disconnect the network cable	The network cable is connected to the computer through the CPU and is a blue cable	User of the infected computer	Email	user@company.com	Until verifying that it is really infected	-	-	-
				Phone	99 999 99 99				
Step 2	Restart the computer in test mode	This step consists of checking if the computer equipment has really stopped working due to a virus or for another possible reason	User of the infected computer	Email	user@company.com	Until verifying that it is really infected	-	The instructions for restarting the computer in test mode are in the following folder on the server: C:\Resilience\Protocols\23.1\Restart test mode.pdf	-
				Phone	99 999 99 99				
Step 3	Scan the computer with the antivirus	The company's current antivirus is Panda Gold Protection	User of the infected computer	Email	user@company.com	Aprox. 1 hr	Panda Gold Protection	The manual to perform the computer scanning with Panda Gold Protection antivirus can be found in the following folder on the server: C:\Resilience\Protocols\23.1\Panda Analysis Manual.pdf	-
				Phone	99 999 99 99				
Step 4	Inform management	If it is not possible to inform the manager as soon as possible, the user of the infected computer will be the one who performs Step 5 (through the computer resources available in the company)	User of the infected computer	Email	user@company.com	-	-	-	-
				Phone	99 999 99 99				
Step 5	Inform the company	All the company must be informed about the possible cause of infection, to try to safeguard the rest of the company's equipment from infection (Training)	Manager	Email	manager@company.com	-	-	Email, Phone, face-to-face	-
				Phone	96 999 99 99				
Step 6	Contact IT services	The IT services, through the information generated in Steps 1, 2 and 3, will connect (if appropriate) the network cable to take remote control of the company's IT equipment. If they cannot solve it, contract No. XXX (found in the server folder C:\Resilience\Protocols\23.1\ Contract services informatics.pdf), through clause XXX, guarantees the visit of the technical service in less than 24 hrs.	User of the infected computer	Email	user@company.com	-	External IT services	-	The backups have been automated since 25/10/20 and managed by the external IT services company. Backups are programmed periodically (every day at 11:00 p.m.).
				Phone	99 999 99 99				

Fig. 4. Fields of the action protocol.

- Objectives: The definition of objectives seeks to describe the purpose to be achieved with the protocol. It is quite usual to define two types of objectives: (i) Global: they define, in a general way, which the situation will be after the implementation of the protocol and (ii) Particular: they describe in detail the purpose of the protocol.
- Scope: This defines to whom it is addressed. It answers the question of: is the protocol addressed to all the company or to a specific functional unit?
- Terms and definitions: This section defines those particular concepts or acronyms included in the protocol to facilitate users, a complete understanding.

The second division for registering the information of the action protocol is based on the procedures and steps to follow to recover from a specific disruptive event. The required information fields defined are described below:

- Definition: Statement of each of the steps to be executed in the face of the disruptive event occurrence. The definition should be very clear, direct and with an adequate length. The definition is usually short, as the details of the definition are already specified in the description.
- Description: The description should allow third parties to understand in a clear, precise and simple way the steps to be followed when a specific event occurs. It differs from the definition, in the level of detail of the registered information.
- Person in charge: For each action to be carried out, the persons in charge of the different tasks should be described, to guarantee that the different steps are being carried out appropriately. Moreover, the contact information regarding the person in charge should be also specified in the protocol.
- Start: This registration field has been defined to determine the start (for example the time) at which the actions should be executed. This field will be used in the definition of very specific protocols. The example illustrated in Figure 4 does not represent this field since it is not a relevant field in this specific case to carry out the actions.
- Duration: It is important to register an estimate of the duration of each of the actions to be carried out, in order to be able to plan the complete sequence of the protocol.
- Resources (tools, software ...): It is also crucial to register the necessary means that are necessary to carry out each of the constituent steps of the protocol. The resources include tools software and human resources, among others. The person/s in charge of carrying out and controlling each of the steps have been defined

previously, but the executors of the different steps should also be registered, so that at the time of the action (if necessary), all personnel are aware of what should be done and who should do it and there are no conflicts with the definition of responsibilities and assignment of tasks.

- Techniques: There is a field to register information about whether there is any technique that should be used for a specific step in the recovery actions.
- Comments: Finally, the KRM also has a comments section, where the company can add additional useful information to clarify the implementation of the action protocol for the avoidance of any doubt.

4. CONCLUSIONS

The importance of companies being resilient in these difficult times has been demonstrated through the multitude of current investigations that are being developed. The COVID pandemic has generated a watershed in the history of mankind. From a business perspective, companies wonder if this or a similar unexpected event happens, how they should act. Recent studies point to the creation and registration of knowledge as an adequate mean to facilitate the recovery process, and therefore improve the resilient capacity of companies. In light of this, this paper describes a knowledge registration module that has been particularly designed with the purpose of recording relevant information that facilitate the recovery process. The KRM is composed by different knowledge levels. The first one is related to the 'What?' in which it is vital to characterize the disruptive event that has impacted the enterprise. The second knowledge level involves 'How?' and it is related to the definitions of the past actions performed in order to bounce back after a disruption. Finally, the third knowledge level is related to the definition of an action protocol which will be the guidelines for acting in case that the same or a potential similar disruptive event occurs. Further research lines will be focused on analysing the performance and the degree of recovery that enterprises experiment in the long term by applying the KRM.

ACKNOWLEDGEMENTS

This research was supported by the Programme to support the academic career of the faculty of the Universitat Politècnica de València 2019/2020 as part of Project 'Enterprise and Supply Chain Resilience Enhancement' granted to Dr. Raquel Sanchis, who wishes to thank Università Politecnica delle Marche, particularly the Department of Industrial Engineering and Mathematical Science, for its support, during her stay, to conduct the present research.

REFERENCES

Antomarioni, S., Bevilacqua, M., Ciarapica, F. E., & Marcucci, G. (2017, April). Resilience in the Fashion Industry Supply Chain: SoA Literature Review. In Workshop on Business Models and ICT Technologies for the Fashion Supply Chain (95-108). Springer, Cham.

Bevilacqua, M., Ciarapica, F. E., & Marcucci, G. (2018). A modular analysis for the supply chain resilience triangle. *IFAC-PapersOnLine*, 51(11), 1528-1535.

Bevilacqua, M., Ciarapica, F. E., & Marcucci, G. (2019). Supply Chain Resilience research trends: a literature overview. *IFAC-PapersOnLine*, 52(13), 2821-2826.

Bevilacqua, M., Ciarapica, F. E., Marcucci, G., & Mazzuto, G. (2020). Fuzzy cognitive maps approach for analysing the domino effect of factors affecting supply chain resilience: A fashion industry case study. *International Journal of Production Research*, 58(20), 6370-6398.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual review of ecology and systematics*, 4(1), 1-23.

Hora, M. and Klassen, R. D. (2013). Learning from others' misfortune: Factors influencing knowledge acquisition to reduce operational risk. Journal of Operations Management, 31(1-2), 52-61.

Hosseini, S., Ivanov, D. and Dolgui, A. (2019). Review of quantitative methods for supply chain resilience analysis. Transportation Research Part E: Logistics and Transportation Review, 125, 285-307.

Ivanov, D., Dolgui, A., Sokolov, B., & Ivanova, M. (2017). Literature review on disruption recovery in the supply chain. International *Journal of Production Research*, 55(20), 6158-6174.

Ivanov, D. and Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research*, 58(10), 2904-2915.

Luers, L., Lobell, D.B., Sklar, L.S., Addams, C.L. and Matson, P.A. (2003). A method for quantifying vulnerability, applied to the agricultural system of the Yaqui Valley, Mexico. *Global Environment Change*, 13, 255–267.

Mafabi, S., Munene, J., and Ntayi, J. (2012). Knowledge management and organisational resilience. *Journal of Strategy and Management*, 5(1), 57-80.

Nonaka, I. (2007). Knowledge management: theoretical and methodological foundations. In Smith, K.G. and Hitt, M.A. (ed.), *Great Minds in Management: The Process of Theory Development*, 373-393. Oxford University Press, New York, NY.

Nonaka, I. and Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation.* Oxford University Press.

Ponomarov, S. Y., and Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The international Journal of Logistics Management*, 20(1), 124-143

Sanchis, R., and Poler, R. (2019). Mitigation proposal for the enhancement of enterprise resilience against supply disruptions. *IFAC-PapersOnLine*, 52(13), 2833-2838.

Sanchis, R. and Poler, R. (2020). Enterprise Resilience in Times of Pandemic. *Boletín de Estudios Económicos*, 75(231). 501 - 520.

Sanchis, R., Canetta, L., and Poler, R. (2020). A Conceptual Reference Framework for Enterprise Resilience Enhancement. *Sustainability*, 12(4), 1464.

Sanchis, R., Sanchis-Gisbert, M. R., and Poler, R. (2020). Conceptualisation of the three-dimensional matrix of collaborative knowledge barriers. *Sustainability*, 12(3).