A Proposal for Risk Identification Approach in Collaborative Networks Considering Susceptibility to Danger

Jiayao Li, Frederick Benaben, Juanqiong Gou, Wenxin Mu

A Proposal for Risk Identification Approach in Collaborative Networks Considering Susceptibility to Danger

Jiayao Li[1,1], Frédérick Bénaben[2], Juanqiong Gou[1], and Wenxin Mu[1]

[1] School of Economics and Management, Beijing Jiaotong University, Beijing, China
{jiayaol, jqgou, wxmu}@bjtu.edu.cn
[2] Mines Albi, University of Toulouse, Albi, France
frederick.benaben@mines-albi.fr

Abstract. The paper proposes a research framework for risk identification approach in collaborative networks dedicated to develop a formalizing, structured reference for risk identification and risk mitigation and explore an effective mechanism that can motivate diverse partners to manage risks collaboratively. The approach is based on a formalized vision of Danger/Risk/Consequence chain that is defined as the primary schema of the proposed methodology. The DRC chain indicates five risk-related concepts and their interrelationships, which is able to well describe risk-related collaborative contexts. Cascading effect in the concept chain are presented for further interpreting. Furthermore, a supply chain scenario of three use cases is given to illustrate the proposed framework.

Keywords: Risk identification, DRC chain, Susceptibility to danger, Cascading effect, Collaborative network.

1 Introduction

A collaborative network is an alliance constituted by a variety of entities (e.g. organizations and people) that are largely autonomous, geographically distributed, and heterogeneous in terms of their operating environment, culture, social capital and goals, but that collaborate to better achieve common or compatible goals, and whose interactions are supported by a computer network [1]. Collaborative networks such as virtual organizations, dynamic supply chains, professional virtual communities, collaborative virtual laboratories, etc. are complex systems associated with uncertainties in dynamic business environments [2]. It is noted that the collaboration increases the dependences among enterprises, which makes enterprises more susceptible to risks. It is critical for collaborative networks to take systematic approaches to identify risks as early as possible, and implement appropriate strategies to manage the risk propagation throughout the evolution of collaboration [3].

[1] Corresponding author.

While the above discussion shows the importance of risk identification, however, it is worthy to note that there appears to be no overarching typology to delineate exactly what constitutes risk and how to understand risk [4]. [5] argues that risk management consists of four key management aspects: (i) assessing the risk sources; (ii) defining the adverse consequences; (iii) identifying the risk drivers; and (iv) mitigating risks. [6] indicates that risk is at least made up of three essential components: (i) a driver or drivers which trigger the risk to happen; (ii) an event with probability that signifies the occurrence of the risk; and (iii) a consequence or consequences resulted from the risk. [7] presents a three-dimensional framework dedicated to structure the domain of crisis management based on the Danger/Risk/Consequence chain (DRC chain). In summary, the risk-related concepts could be concluded as *danger*, *stake*, *risk*, *event* and *consequence*.

Anyway, risk management is a very complex domain with a lot of constraints. Consequently, it is very difficult to get a global overview of such a domain. This article is mainly dedicated to present a proposal for risk identification approach to support collaborative networked organizations. The proposed approach is based on the DRC chain (as shown in Fig.1), which is not so far from FTA (Fault Tree Analysis) principles [8]. Furthermore, *danger*, *risk* and *consequence* may be considered as causal sources (in a waterfall structure) that must be formalized as models to help decision makers [7].

More specifically, the research methodology is proposed:

- A danger typology and a stake typology are developed for collaborative networked organizations based on the review of present related literatures.
- The interconnections rules between *dangers* and *stakes* and their impacts on *risks* could be summarized, which aims to build a risk typology as a static reference model of risk knowledge.
- In addition to *danger*, *stake* and *event*, *risk* and *consequence* can be also considered in a *cascading effect* structure [9]. Their interrelationships could be analyzed and summarized.
- A risk knowledge base with a risk typology and interrelationships is used for the deduction of risk identification rules based on previous research works.
- A metamodel connected with a risk knowledge base will be defined based on the research of collaborative situation metamodel [10,11].

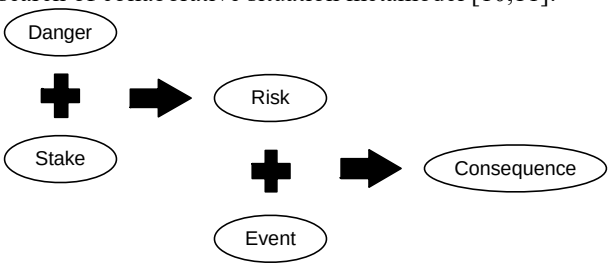

Fig. 1. A framework for risk identification approach

The research should contribute to a deeper and broader understanding risk based on the schema of DRC chain. Besides, the risk identification research based on such an understanding will contribute to better practices by suggesting collaborative responses

from multiple partners in collaborative networks.

This article is structured according to the following sections: Section 2 presents a literature review; section 3 describes the DRC chain considering susceptibility to danger and interrelationships of the five risk-related concepts; in section 4, a supply chain scenario is given to illustrate the part of proposed methodology; section 5 concludes this research work and gives some perspectives for future works.

2 Literature Review

According to [12], risk is the combination of the frequency, or probability, of occurrence and the consequence of special hazardous events.

Risk Management corresponds to a set of activities that organizations use to control the many risks, which may undermine their ability to achieve objectives. Considering international standards on entrepreneurial management process risk, [13] organizes a reference risk taxonomy, which shows that risk management includes two principal dimensions, namely, assessment and treatment. Risk assessment could be summarized as three phases: analysis, identification and evaluation. Risk identification can be defined as a process of identifying the dangers, events and consequences.

It is a common assumption that participation in a collaborative network has the potential of bringing benefits to the involved partners. However, the interconnections between partners of collaborative network cause numerous new risks, of which the impacting magnitude and scope are larger than ever before [6]. In recent years, there are few studies about the risk identification of collaborative networks by considering susceptibility to danger existing in the literature of collaborative networks and further research in this field is required.

Regarding the approach of risk identification in collaborative context, it focuses on literature review, semi-structured interviews and questionnaire. They can be called as the experienced-based methods. [14] directly takes advantage of the risks identified by project manager to determine the events with negative impacts. [15] identifies the stakeholder-associated risks through the previous risk identification literatures, and classified them into seven categories. [16] identifies the risks caused by customer collaboration in product development through relevant literatures by domain experts and questionnaire in the enterprises. [17] analyzes the research paradigms regarding risk and stakeholder analysis in green buildings through literature review. [18] undertakes a systematic literature review on risks sources and resilience factors in agri-food supply chains. [19] successively uses literature review, semi-structured interviews and questionnaires to identify a list of human safety risk factors and also the cause–effect relationships among those risks.

Regarding the application of risk identification results, most results of identified risks are used to further risk evaluation and propose risk response or risk mitigation strategies. In order to investigate those risk interactions, the focus of risk evaluation methods has gradually been shifting from individual risks to networks of risk [6], [19]. It considers nodes in the network and their relationships, focusing on the

structure and patterning of these relationships and seeking to identify both their causes and effects [20,21].

We conclude the following:

- A systematic approach to the identification and categorization of risks in collaborative context is lacking.
- The current risk identification methods mainly focus on review, expert interview and questionnaire.
- More future works are attentive to the identification of risk interconnections.
- The present research of the application of risk identification result also lacks of a sharing-based risk response mechanism considering capabilities and resources of partners to contribute to their collaboration.

3 Understanding Risk

Risk can be seen as combination of the probability of an *event* and its *consequence*. However, *danger* and *stake* are also closely related to *risk* with the exception of the concepts of *event* and *consequence*. DRC chain is a concepts schema that is able to describe risk-related contexts.

3.1 General Illustration of DRC Chain

In this schema, the five risk-related concepts could be defined as follows:

- *Danger* can be defined as any specific dangerous characteristic of the environment, which is a signal word used to indicate an imminently hazardous situation [22].
- *Stake* or *assets* can be seen as item, thing or entity that has potential or actual value to an organization [23] and potential susceptibility to dangers.
- *Risk* is a potential manifestation of the *danger* onto some concerned *stakes* [7].
- *Event* is defined as a change or outcome that triggers *risks*. If one *risk* might occur it would be due to some *events* [24].
- *Consequence* generally means a set of negative impacts of the risk occurrence.

The general illustration of DRC chain could be described as follows: Each of those negative facts is due to one (or several) *event*(s) that trigger(s) one (or several) *risk*(s); This (or these) *risk*(s) occur(s) because the considered area/system is concerned by one (or several) *danger*(s) that affect(s) one (or several) *stake*(s) [7].

Furthermore, the DRC chain could indicate the *susceptibility to danger*, which means the state of being very likely to be influenced or affected by danger. The following example in enterprise collaborative context illustrates *susceptibility to danger* (see Fig.2).

Company C is the only one able to produce *Product P* for the *core company CC*, which is a *danger* for the *stake CC* because its *Product PP* must be produced by using *P*. Consequently, the *risk* is that *PP* may not be produced. It would be triggered if C decides not to produce *P* anymore (an *event* occurs), then cause a *consequence* as

which *CC* cannot sell *PP* to its customers. For this general illustration of DRC chain, the demand side *CC* is susceptible to the danger of which there is no alternative provider regarding its required product. Different *stakes* have different degrees of susceptibility to danger while some *stakes* are not susceptible to danger.

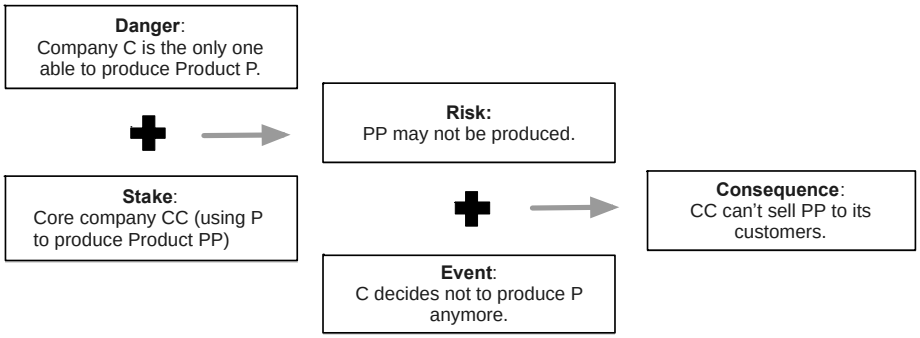

Fig. 2. An illustration of "susceptibility to danger" in DRC chain

3.2 Interconnections in DRC Chain

In the schema of the DRC chain, *risk* is created by *danger* and *stake* while *consequence* is created by *risk* and *event*. It can be seen that *risk* and *consequence* are the "generated" elements. Therefore, they are the ones which directly impact the considered system. Accordingly, it is worth to focus on what effects that they might create. One of perspective that can indicate it is *cascading effects* that could be described as multiple connections initiated by *risk* and *consequence* in the DRC chain.

A *cascading effect* is an inevitable and sometimes unforeseen chain of *events* due to an act affecting a system [25]. If there is a possibility that the *cascading effect* will have a negative impact on the system, it is probable to analyze the effects with a *risk* or *consequence* analysis. Fig.3 shows six connections initiated from *consequence* (see connections (1)(2)(3)) and *risk* (see connections (4)(5)(6)), in order to present the *cascading effect* as follows: *consequence* and *risk* are regarded as the causal sources that target at *danger*, *stake* and *event*.

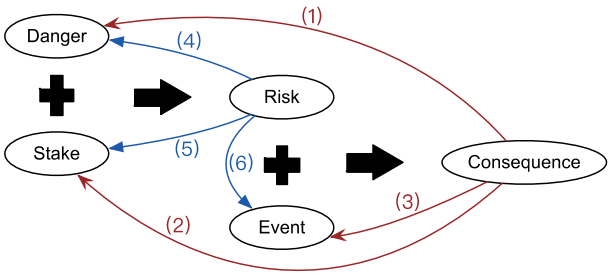

Fig. 3. Interconnections in DRC chain

To illustrate the *cascading effect* further, three use cases are presented in Fig.4, which are the real ones from a cosmetic French company. The interconnections between the first two use cases (see connections (1)(2)(3) of Fig.4) could indicate *consequence* as the causal source. The first use case is already described in previous section, the *consequence* of which is that *CC* cannot sell *PP*. It is worth mentioning that this *consequence* could bring about the next use case.

The second use case is described as follows: *CC* has to contract with another company *C'* that can produce *P*, however, which is a *danger* for the new provider *C'*. Concerning this *stake*, the *danger* could be manifested as a *risk* that its *Product P* may decline in quality. Under this circumstance, if there is a big demand for *P* from *CC*, the *risk* would be triggered and cause a *consequence* as which *C'* produces lower quality products and its image might be degraded.

In summary, it can be seen that one *consequence* in a scenario could create a new *danger* (*CC* contracts with *C'*), also a new *stake* (*company C'*) and even an *event* (big demand from *CC*), which lead to another risk-related scenario.

The third use case is described as follows: A huge workload of employees in *Company C'* is a *danger* for the *stake C'*, because it could create a *risk* that the employees may go on strike for salary increase. The *risk* would be triggered if *C'* requires them to work overtime (an *event*), then a *consequence* of employees' strike might be caused.

Regarding *risk* as the causal source, the creation of *danger*, *stake* and *event* is generally due to the actions of risk prevention and mitigation. The interconnections between these three use cases (see connections (4)(5)(6) of Fig.4) could indicate it as below:

- *Risk-danger*: *C'* is confronted with a *risk* that its products may decline in quality in the second use case. In order to prevent the *risk*, *C'* might increase the workload of its employees to ensure the products' quality, which is a new *danger* shown in the third use case.
- *Risk-stake*: *CC* needs to find the other company that can also produce its required *Product P* in order to prevent the *risk* in the first use case (*PP* may not be produced). As a result, the *risk* creates a new *stake Company C'* that is shown in the second use case.
- *Risk-event*: For the sake of qualified quality of *Product P*, *C'* might requires its employees to work overtime. Consequently, the *risk* in the second use case (*P* by *C'* may decline in quality) creates an *event* in the third use case.

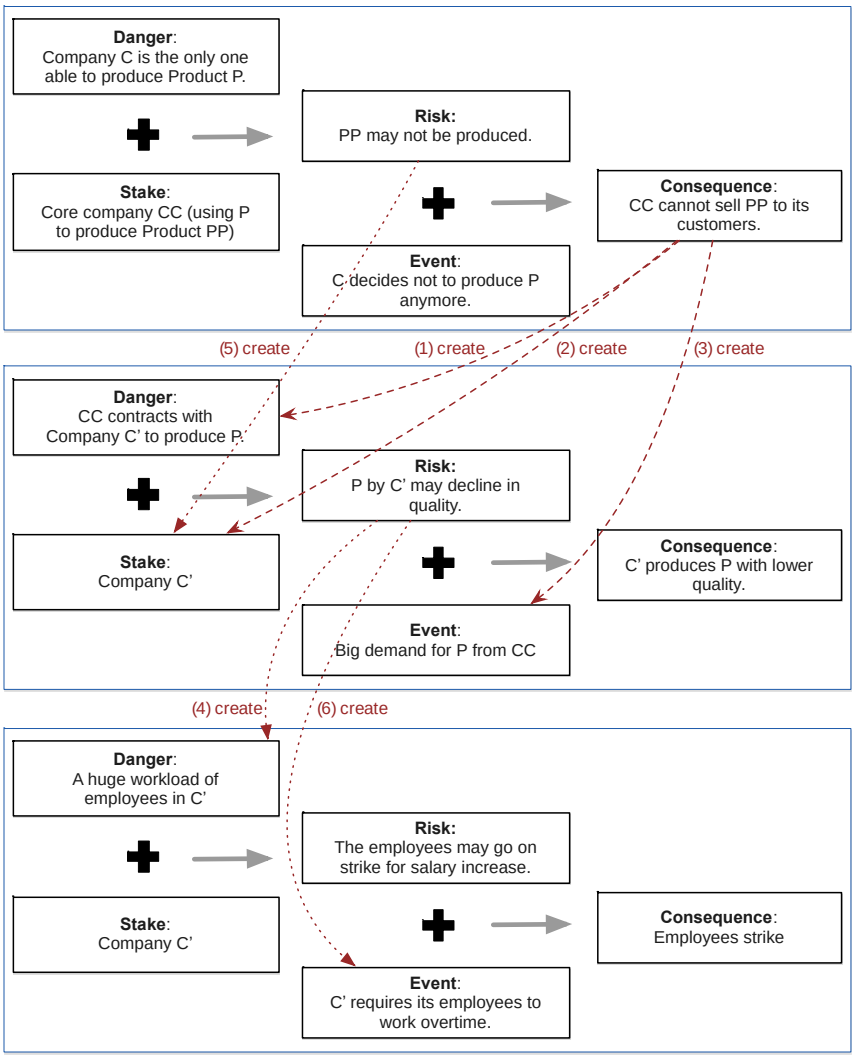

Fig. 4. An illustration of cascading effect in DRC chain

In addition to the interrelationship "*create*" between *consequence/risk* and *danger/stake/event*, there are some other interrelationships presented in Table 1. We define the interrelationships in DRC chain as follows:

- "*Create*": *Consequence/risk* makes new *danger/stake/event* happen.
- "*Update*": *Consequence/risk* makes *danger/stake/event* from one state or form into another.
- "*Delete*": *Consequence/risk* removes or makes *danger/stake/event* invisible.

"Yes" in Table 1 means that we have found the use cases to support this type of interconnection (it cannot be all shown in this article). Accordingly, "No" in Table 1

means that the interrelationship does not exist between the concepts. To conclude, we hold that in considered scenario *consequence or risk* could create new *danger, stake and event*, and update or delete the current state or form of *danger* and *stake*. Nevertheless, *event* could not be updated or deleted because we cannot change what has happened before.

Table 1. Interrelationships in DRC chain

	Danger			**Stake**			**Event**		
	Create	Update	Delete	Create	Update	Delete	Create	Update	Delete
Consequence	(1)Yes	(1)Yes	(1)Yes	(2)Yes	(2)Yes	(2)Yes	(3)Yes	(3)No	(3)No
Risk	(4)Yes	(4)Yes	(4)Yes	(5)Yes	(5)Yes	(5)Yes	(6)Yes	(6)No	(6)No

4 Supply Chain Scenario Illustration

Supply chain is considered as a specific form of collaborative network. It is a stable long-term network of enterprises each having clear roles in the value chain, covering all steps from initial product design and the procurement of raw materials, through production, shipping, distribution, and warehousing until a finished product is delivered to a customer [26].

In order to further illustrate the proposed DRC chain, three use cases of the supply chain scenario (presented in Fig. 5) would be given to be used to perform the progress of current work. Two partners are involved in this simple scenario: the ***core enterprise*** is the demand side, which submits orders to buy its required materials from the ***suppliers***. Furthermore, the three use cases are described as follows:

- The first use case: Labor strike of suppliers is a *danger* for the core enterprise (a *stake*), because it would create the *risk* of the shortage of its required products. If the production disruption (an *event*) happens, the *risk* could be triggered. Then the *consequence* of overdue delivery cannot be avoided.
- The second use case: Shortage of products required by the core enterprise is a *danger* for the supplier who provides them (a *stake*). The *risk* is that the core enterprise might give a negative feedback in the evaluation of this supplier, and the *risk* occurs if overdue delivery from the supplier (an *event*) happens for several times. The core enterprise might consider to change the supplier to ensure its normal operation of business (a *consequence*).
- The third use case: Overdue delivery of supplier for long time is a *danger* for the core enterprise (a *stake*). It would create a *risk* that the core enterprise has to change the supplier. If many negative comments from the evaluation of the supplier (an *event*) are given to the decision-maker, the *risk* could be triggered. Consequently, the core enterprise needs to reselect the other suppliers to replace the tasks of the original supplier as soon as possible (a *consequence*).

By comparing with the three use cases (presented in Fig. 5) and referring to the *cascading effect* in DRC chain (presented in Fig. 3), it can be seen that a target or outcome in one situation could be the causal source to connect another situation. Accordingly, several interconnections could be concluded:

- *Consequence-danger* and *Consequence-event*: The *consequence* of overdue delivery in the first use case could create a *danger* in the third use case (see connection (1)), and also create an *event* in the second use case (see connection (3)).
- *Risk-danger*: The *risk* of shortage of required products in the first use case could create a *danger* in the second use case (see connection (4)).
- *Risk-event*: The *risk* of negative evaluation in the second use case could create an *event* in the third use case (see connection (6)).

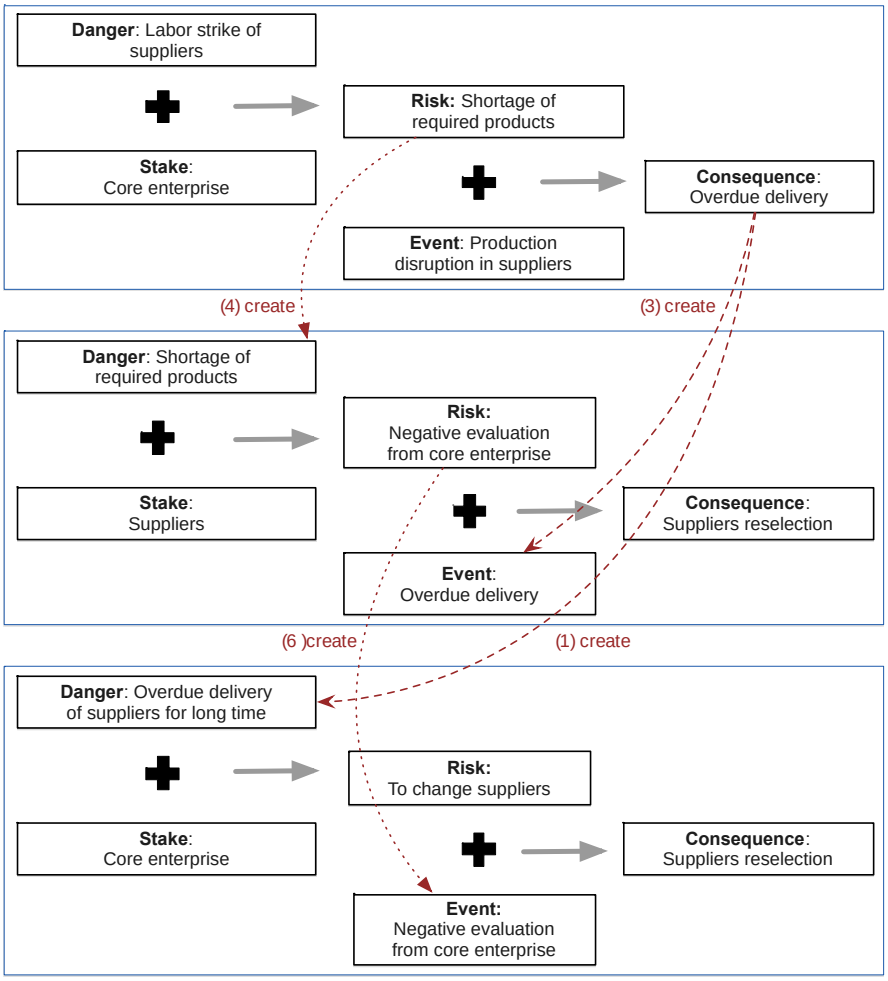

Fig. 5. Use cases illustration of supply chain scenario

5 Conclusion

The presented framework of risk identification approach might be considered as a formalizing reference dedicated to identify and mitigate risk in collaborative networks. The proposed approach is compliant with the schema of Danger/Risk/Consequence chain that helps to formalize the risk-related knowledge that includes five concepts (*danger*, *stake*, *risk*, *event* and *consequence*) and their interrelationships. Cascading effect could be indicated in DRC chain, which could contribute to a deeper understanding of risk-related collaborative contexts. Besides, the devised danger typology and stake typology can be further used to develop a risk knowledge base for risk identification of collaborative networks. Furthermore, the risk knowledge base combined with the current methodology of metamodeling could contribute to further explore the ways in which an effective mechanism that can motivate diverse partners in collaborative networks to manage risks collaboratively.

The future works would use System Dynamics [27] to develop the proposed approach, which focus on: (i) developing a danger typology and a stake typology by synthesizing the growing diverse literatures; (ii) the deduction of interconnection rules of dangers and stakes in order to build a risk knowledge base for collaborative networks; (iii) developing risk identification rules based on the risk knowledge base; (iv) metamodeling with risk knowledge base that can be dedicated to support collaboration of partners, and deduce the collaborative processes of risk mitigation.

Acknowledgments. The presented research works have been supported by "the Fundamental Research Funds for the Central Universities of China". The authors would like to thank the project partners for their advice and comments.

References

1. Camarinha-Matos, Luis M. and Afsarmanesh, H.: On reference models for collaborative networked organizations. *International Journal of Production Research*, 46, 9, 2453-2469 (2008).
2. Jamshidi A., Abbasgholizadeh Rahimi S., Ait-kadi D., Ruiz A.: A New Decision Support Tool for Dynamic Risks Analysis in Collaborative Networks. In: Camarinha-Matos L., Bénaben F., Picard W. (eds) Risks and Resilience of Collaborative Networks. IFIP Advances in Information and Communication Technology, vol. 463. Springer, Cham (2015).
3. Wulan, M. and Petrovic, D.: A fuzzy logic based system for risk analysis and evaluation within enterprise collaborations. Computers in Industry, 63, 8, 739-748 (2012).
4. Rao, S. and Goldsby, T. J.: Supply chain risks: a review and typology. International Journal of Logistics Management, 20, 1, 97-123 (2009).
5. Juttner, U., Peck, H. and Christopher, M.: Supply chain risk management – outlining an agenda for future research. International Journal of Logistics: Research and Applications, 6,4, 197-210 (2003).
6. Zeng, B. and Yen, P. C.: Rethinking the role of partnerships in global supply chains: a risk-based perspective. International Journal of Production Economics, 185, 52-62 (2017).

7. Bénaben, F., Barthe-Delanoë, A. M., Lauras, M. and Truptil, S.: Collaborative Systems in Crisis Management: A Proposal for a Conceptual Framework. Collaborative Systems for Smart Networked Environments, pp. 396-405. Springer Berlin Heidelberg (2016).
8. Vesely, W.E., Goldberg, F.F., Roberts, N.H., Haasl, D.F.: Fault Tree Handbook. Office of Nuclear Regulatory Research (1981).
9. Turoff, M., Bañuls, V. A., Plotnick, L., Hiltz, S. R. and Huerga, M.R.D.L.: A collaborative dynamic scenario model for the interaction of critical infrastructures. Futures, 84, 23-42 (2016).
10. Bénaben, F., Lauras, M., Truptil, S. and Salatge, N.: A Metamodel for Knowledge Management in Crisis Management. Hawaii International Conference on System Sciences, 126-135. IEEE Computer Society (2016).
11. Lauras, M., Bénaben, F., Truptil, S., Lamothe, J., Macé-Ramète, G. and Montarnal, A.: A meta-ontology for knowledge acquisition and exploitation of collaborative social systems. International Conference on Behavior, Economic and Social Computing (pp.1-7). IEEE (2015).
12. Edwards, P. J. and Bowen, P. A.: Risk management in project organisations. Elsevier, Oxford, UK (2005).
13. Rosas J., Urze P., Tenera A., Abreu A., Camarinha-Matos L.M.: Exploratory Study on Risk Management in Open Innovation. In: Camarinha-Matos L., Afsarmanesh H., Fornasiero R. (eds) Collaboration in a Data-Rich World. PRO-VE 2017. IFIP Advances in Information and Communication Technology, vol. 506, pp.527-540. Springer, Cham (2017).
14. Fang, C., Marle, F., Zio, E. and Bocquet, J. C.: Network theory-based analysis of risk interactions in large engineering projects. Reliability Engineering & System Safety, 106(2), 1-10 (2012).
15. Yang, R. J. and Zou, P.: Stakeholder-associated risks and their interactions in complex green building projects: a social network model. Building & Environment, 73, 1, 208-222 (2014).
16. Zhang, X., Yang, Y., and Su, J.: Risk identification and evaluation of customer collaboration in product development. Journal of Industrial Engineering and Management, 8, 3, 928-942 (2015).
17. Yang, R. J., Zou, P. X. W. and Wang, J.: Modelling stakeholder-associated risk networks in green building projects. International Journal of Project Management, 34, 1, 66-81 (2016).
18. Zhao, G., Liu, S., Lopez, C., Zhao, G., Liu, S. and Lopez, C., et al.: A Literature Review on Risk Sources and Resilience Factors in Agri-Food Supply Chains. In: Camarinha-Matos L., Afsarmanesh H., Fornasiero R. (eds) Collaboration in a Data-Rich World. PRO-VE 2017. IFIP Advances in Information and Communication Technology, vol. 506, pp.739-752. Springer, Cham (2017).
19. Wang, X., Xia, N., Zhang, Z., Wu, C. and Liu, B.: Human safety risks and their interactions in china's subways: stakeholder perspectives. Journal of Management in Engineering, 33, 5 (2017).
20. Scott, J.: Social network analysis: A handbook, Sage, Thousand Oaks, CA (2000).
21. Zhou, X. and Lu, M.: Risk evaluation of dynamic alliance based on fuzzy analytic network process and fuzzy TOPSIS. Journal of Service Science & Management, 05, 3, 230-240 (2012).
22. ISO 3864-2, Technical Committee, ISO/TC 145/SC 2, Graphical symbols - Safety colours and safety signs (2016).
23. ISO 41011, Technical Committee, ISO/TC 267, Facility management – Vocabulary (2017).

24. Lahmar, A., Galasso, F., Chabchoub, H. and Lamothe, J.: Towards an Integrated Model of Supply Chain Risks: An Alignment Between Supply Chain Characteristics and Risk Dimensions. In: Camarinha-Matos L., Bénaben F., Picard W. (eds) Risks and Resilience of Collaborative Networks. IFIP Advances in Information and Communication Technology, vol. 463, pp.3-16. Springer, Cham (2015).
25. Cascade effect. A Dictionary of Ecology. Encyclopedia.com.
26. Camarinha-Matos, L. M., Afsarmanesh, H., Galeano, N. and Molina A.: Collaborative Networked Organization -Concepts and Practice in Manufacturing Enterprises. *Computers & Industrial Engineering*, 57, 1, 46–60 (2009).
27. Forrester, J.: System dynamics, systems thinking, and soft OR. System dynamics review, 10(2-3), 245-256 (1994).