Proceedings of the Estonian Academy of Sciences,
2018, **67**, 1, 17–27
https://doi.org/10.3176/proc.2017.4.27
Available online at www.eap.ee/proceedings

INDUSTRIAL
ENGINEERING

Risk assessment approach for a virtual enterprise of small and medium-sized enterprises

Kashif Mahmood*, Eduard Shevtshenko, Tatjana Karaulova, and Tauno Otto

Department of Mechanical and Industrial Engineering, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia

Received 28 July 2017, accepted 18 October 2017, available online 14 December 2017

Abstract. A risk assessment methodology for a Virtual Enterprise (VE) was developed to facilitate analysis of the key factors of risks and assessment of the level of risks a VE faces during its complete functioning period. The paper provides a relatively simple and straightforward method to estimate risks and intends to give a concept for mitigating the risks related to the action phase of a VE. A model of the existence of a VE with hierarchical risk factors was developed, which can be helpful to a decision-maker of a collaborative network of small and medium-sized enterprises in formulating risk management strategies and tactics in order to mitigate overall risks of the VE. The proposed semi-quantitative risk assessment method uses for the estimation and evaluation of risks matrices based on probability and impact. This research proposes Fault Tree Analysis (FTA) for determining the overall risk factor of a VE. Also, the Internet of Things (IoT)-based smart concept is suggested for risk mitigation.

Key words: virtual enterprise, risk assessment, Fault Tree Analysis, IoT-based monitoring.

1. INTRODUCTION

In today's advance and competitive world, small and medium-sized enterprises (SMEs) are facing comprehensive competition in the global marketplace. To work efficiently within the global environment, they have to collaborate with other companies in the form of a virtual organization or partner network. However, as compared to the traditional enterprise a Virtual Enterprise (VE) is exposed to more complicated risk management issues. For the desired profit and particular goal, a VE has to avoid risks successfully.

The purpose of this paper is to provide a concept for analysing the key risk factors and to assess the level of risk a VE faces during its whole functioning period. Four phases of a VE are defined in this paper, and the possible risks that can occur in each phase are identified. Moreover, the paper proposes a risk assessment model to evaluate the project-based risk of a VE, followed by risk mitigation through the Internet of Things (IoT)-based concept. A hypothetical case is used to demonstrate how to calculate the risk factors and to verify the relevance of the proposed methodology.

Nowadays, the business environment is characterized by a high level of global competition, demanding customers and employees, shortened product life cycles, and fast response times. Therefore, many enterprises stretch outside of their permissible boundaries by forming a competitive network of enterprises, sometimes known as a partner network or a VE. This not only allows companies to become more flexible and sustainable in the marketplace but also helps to align a group of companies with a similar vision for the sake of quicker solution to their common problems.

* Corresponding author, kashif.mahmood@ttu.ee

According to Camarinha-Matos and Afsarmanesh, a VE 'represents a temporary alliance of enterprises that come together to share skills or core competencies and resources to respond more effectively to business opportunities, and whose cooperation is supported by computer networks' [1]. It comprises a coordinated network of enterprises that act together to deliver a product or service to the end-user [2].

However, a VE also involves various risk factors. As it is an alliance of enterprises, both internal (within a company) and external uncertainties can exist. The difficulties may consist in resource unavailability, information flow disruptions within a firm and between enterprises, reduced operational efficiencies, price fluctuations, changes in the political environment, etc., which may lead to potential risks. Risks and opportunities exist side by side in a VE. The success of risk management as well as quality management secures an efficient operation of not only in a VE but in any organization [3]. Hence, the risk management of the VE now becomes the core topic of attention among SMEs.

2. LITERATURE REVIEW

Before we continue with the assessment of risks in a VE, it is necessary to have a brief overview of the definitions of risk, uncertainty in networking, risk management approaches, and risk assessment methods. We will also discuss the concept of a VE in this section.

2.1. Definitions of risk

A risk is defined as a possibility of losses or harmful consequences. From this definition, it can be perceived that risk has two fundamental components: losses and uncertainty about their occurrence and quantity [4]. Researchers define risk as a possibility of danger, damage, loss, injury, or any other undesired consequences. It is the product of two factors: probability of an event that might occur and its severity (Risk = Probability × Severity) [5].

Sometimes risks are described in a negative context; for example, according to the Society for Risk Analysis (SRA), risk is the 'potential for realisation of unwanted, adverse consequences to human life, health, property, or the environment' [6]. However, risk does not always result in an adverse outcome since some risks are taken purely in hope of a positive outcome. For instance, the acquisition of a company means significant risk-taking, but the risk would most likely not be considered if there was no chance of a positive effect [7]. What most authors do agree upon is that a risk is always a state of uncertainty [7,8].

2.2. Networking risk

A network is defined as a specific relationship that links persons, entities, and events, and ultimately a set of enterprises [4]. A collaborative network is described as a synergy of companies where companies are seeking for collaborative innovation practices outside their boundaries [9]. Networking has several benefits such as, but not only, improved coordination of interrelated competencies; larger common knowledge pool; more strategic decision-making power of partners; possibility of sharing financial risks; reduction of costs of required resources, products or services; reduction of dependence on expertise [4,10]. On the other hand, a VE cannot be considered free of risk. When SMEs are functioning as a partner by means of a VE, they have been at the edge of significant changes. These involve mostly organizational changes such as changes of operating procedure, performance measurement, communication channels, and overall operational changes for effective management of the flow of physical goods and services in the whole value chain of the VE. Those changes may lead to risks and cause impairment of the functioning of the VE.

Thus, assessment of risks within the framework of a VE is vitally important, and enterprises should recognize all kinds of threats, not only direct risks to their operations but also the risks to all other events caused by the linkages between them [11]. The risk factors in a collaborative network can be divided into performance and network risks. Network risk is related to the interdependence in which lack of trust, inaccurate information sharing, etc. hinder effective collaboration. Performance risk is related to quality and capacity constraints of individual enterprises [12]. According to the study by Harland et al., factors such as globalization, product/service complexities, subcontracting, e-business, and demanding customers may lead to outsourcing and bring about new risks [5]. Chopra and Sodhi listed factors such as disruptions, delays, systems, forecasts, intellectual property, procurement, receivables, inventories, and capacity, and argued that each of these could have many variations and different sources and forms of impact and steer networking risks [13].

2.3. Risk management

An approach to managing risks can be defined as consisting of the following steps: mapping business processes, identification of risks, evaluation of the consequences and likelihood, risk level determination, and control strategy [14]. The primary aim of risk management is to understand the consequences of risks and to reduce their effect by paying attention to elements such as probability and impact. It is also significant to note

Fig. 1. Risk management process for a network of project-based enterprises [15−19].

that the phases in relation to the process of risk management may appear to be variable in terms of classification, risk identification, analysis (or estimate), risk assessment (or evaluation), and different strategies for risk management. Although classifications differ among authors, the steps are similar [15–19]. Risk management process is illustrated in Fig. 1.

2.4. Risk assessment methods

Risk assessment is a technique for identifying risks, which evaluates them as the opportunity for significant reduction in costs and lead-time. It is a formalized approach to determining and assessing the risks. Klüppelberg and co-authors start the initiation step with the definition of the environment in which the analysis takes place [20]. Researchers have used many methods for risk assessment, which can be categorized as follows:

- *Quantitative Assessment* – the final result is in the form of a numerical value. The probability of an event at time t is based on reliability theory as $P(t) = 1 - R(t)$, and its consequences can be re-presented as time lost, non-conformance per year, financial loss, etc.
- *Qualitative Assessment* – the final result is based on attributes such as controlled and uncontrolled, safe and unsafe, or high, medium, and low. The most common qualitative techniques are Strength, Weaknesses, Opportunities, and Threats (SWOT) analysis and Political, Economic, Sociological, Technological, Legal and Environmental (PESTLE).
- *Semi-quantitative Assessment* is based on risk matrices such as the probability and impact matrices.

Several well-known methods of risk assessment have been recognized in the literature [7,21]. Some of them are listed below:

- Hazard and Operability Studies (HAZOP Analysis)
- Fault Tree Analysis (FTA), Event Tree Analysis
- Management Oversight and Risk Tree (MORT)
- Action Error Method
- Process Hazard Analysis (PHA)
- Failure Mode and Effects Analysis (FMEA)
- Cause–Consequence Diagram
- Reaction Matrix
- Hierarchical Task Analysis
- Analytic Network Process (ANP) approach
- Supply Chain Operations Reference (SCOR) model
- Bayesian network approach.

In this article, a semi-quantitative method based on the risk matrix is proposed and hypothetically used to assess the risk of a VE within its phases of existence. The overall risk of a VE is determined through FTA.

2.5. Concept of virtual enterprise

Many researchers have introduced their descriptions of a VE that are slightly different from the basic meaning. Byrne was the first to give the definition of a VE in 1993 [22]. He defines a VE as ‘a temporary network of independent companies—suppliers, customers, even erstwhile rivals—linked by information technology to share skills, costs, and access to one another’s markets’ [22]. The idea of the formation of a VE from a collaborative network of enterprises having different expertise and similar goals can be depicted as in Fig. 2.

To sum up the definitions and characteristics of the different points of view introduced in the literature, a VE can be defined as a new, temporary entity that is created for the fulfilment of a goal and dissolved after the goal is achieved. The Value Added Chain (VAC) structure of a VE is similar to the structure of a physical enterprise. Furthermore, the VE members bring their vital core activities to the new organization. The ‘virtuality’ of the entity also means that the enterprise that established the VE, known also as the Focal Player (FP), does not have sufficient physical resources for project realization alone and it is using the partner network resources [24]. A VE can adjust its tactic in order to adapt to the market changes in time and can integrate all the advantages of the partner enterprises to reach a ‘win-win’ situation. Therefore, researchers have significantly extended the meaning of *Virtual Enterprise* since it was first introduced. The FP creates a VE when the market opportunities arise and dissolves it after it has fulfilled the goal. Moreover, Liu et al. recognize the existence of phases in the lifespan of a VE [25], which are described later in Section 4.1.

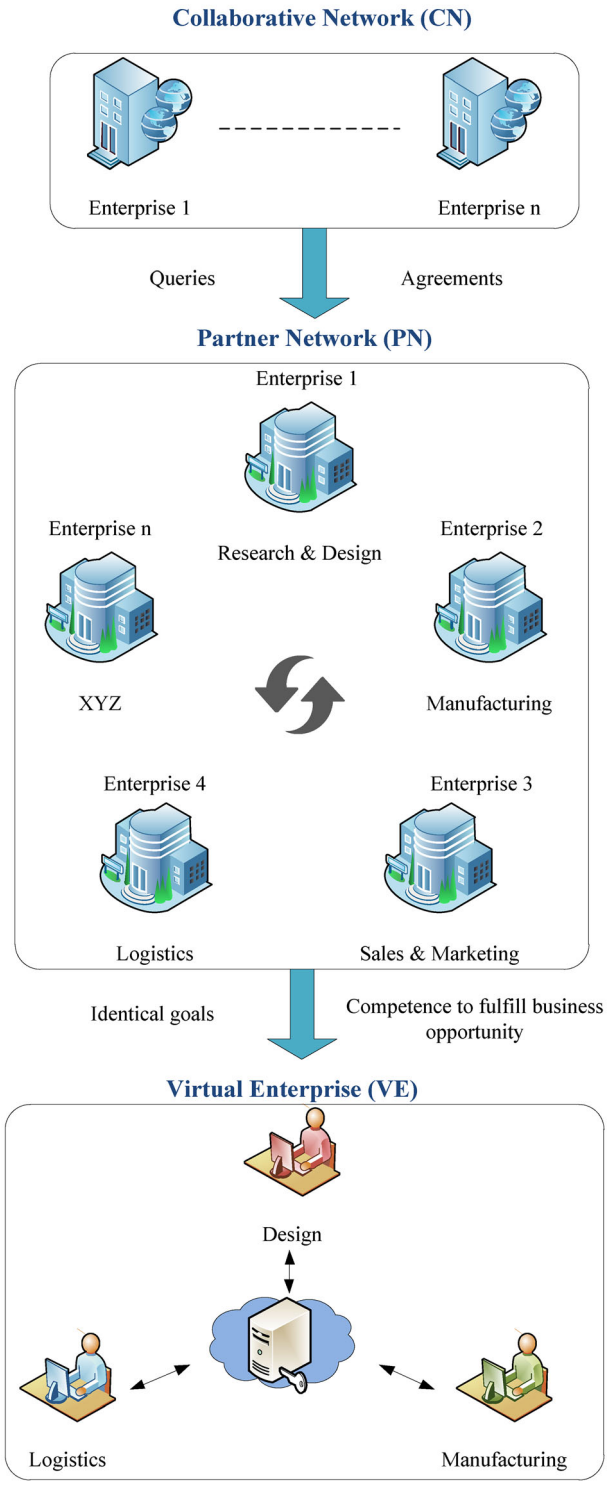

Fig. 2. Structure of collaborative networks, partner network (PN) and virtual enterprise [23]; XYZ stands for an arbitrary business process.

2.6. Concept of Internet of Things

Paavel et al. use IoT-based monitoring systems in manufacturing to facilitate access to information about the particular product in a production process to give real-time input to process analysis [26]. The IoT is an infrastructure of the global network, it links physical and virtual objects together through the utilization of data capturing and communication capabilities. The IoT offers particular object identification and sensor and connection competence as the foundation for the development of independent cooperative services and applications. Jia et al. categorize it by a high degree of autonomous data capturing, event transfer, network connectivity, and interoperability [27]. Shrouf et al. define the IoT as a system in which physical objects are booted up with embedded electronics such as radio-frequency identifiction (RFID) tags, sensors, etc. The system depends on smart objects and smart networks [28]. This paper gives an idea how IoT-based monitoring helps to set up a risk mitigation plan for the action phase risks of a VE.

3. METHODOLOGY

In order to define and understand the purpose of a VE and how risk assessment can be carried out during its working phases, we performed a literature study. Based on the collected knowledge, we built up a risk assessment approach for a VE to verify the corresponding methodology. We suggest a risk management approach for a VE that consists of modelling the VE, classification of possible faults (risks) within the VE, assessment of risks through a risk matrix, determination of the overall risk level through FTA, and risk mitigation and monitoring through the IoT as shown in Fig. 3.

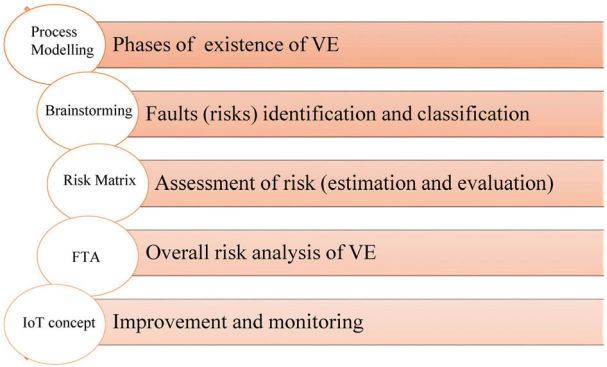

Fig. 3. Schematic of the risk assessment approach.

4. HYPOTHETICAL CASE STUDY

In the following sub-sections, we introduce a computational case study that enables to realize and perceive the relevance of the proposed approach.

4.1. Phases of the existence of a VE

The lifespan of a VE can be divided into the following four phases [29]:

- Realization phase
- Formation phase
- Action phase
- Closure phase.

We consider these four phases of the working of a VE to be appropriate. The phases of the existence of a VE are depicted in Fig. 4.

A VE starts its activity with the *realization phase*, where the essential tasks are the understanding, evaluation, and selection of the market opportunities. The second or the *formation phase* of a VE consists of the selection of partners and building an organizational working and VAC model of the VE, establishment of VE goals, and setting up the information systems. The main elements of the *action phase* include the circulation and co-ordination of tasks, cost control, performance monitoring, and credit management. The *closure phase*, which is the dissolution of the VE with the vanishing of opportunities, comprises of the termination of the contract and submitting the feedback report to the VE partner organizations.

4.2. Risk identification and description

In this paper, we identify the internal risks of a VE. The internal risks emerge from the enterprise's activities, and companies can control them by implementing appropriate strategies. There are also some external risk factors such as political risk, market risk, finance risk (global financial crises), etc., but enterprises can hardly manage and control them. The internal risks in a hierarchical model based on the VE's lifespan and the VE's internal risk assessment system are depicted in Fig. 5. The hierarchical system of internal risk assessment is split into four layers or phases: realization, formation, action, and closure. Each layer in turn has its sub-groups.

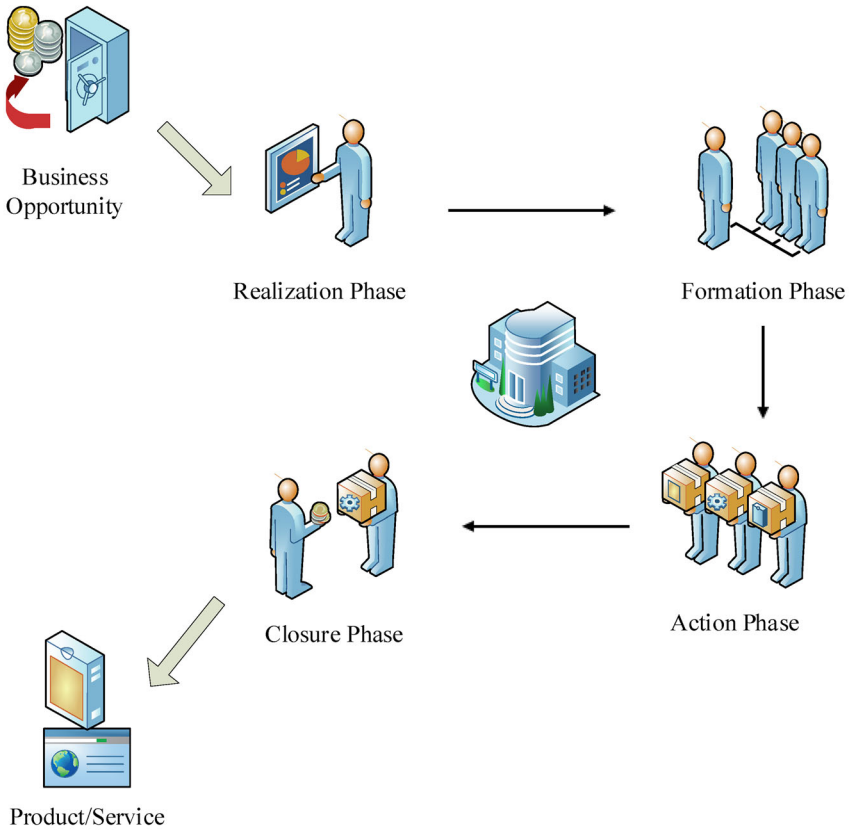

Fig. 4. Phases of a virtual enterprise.

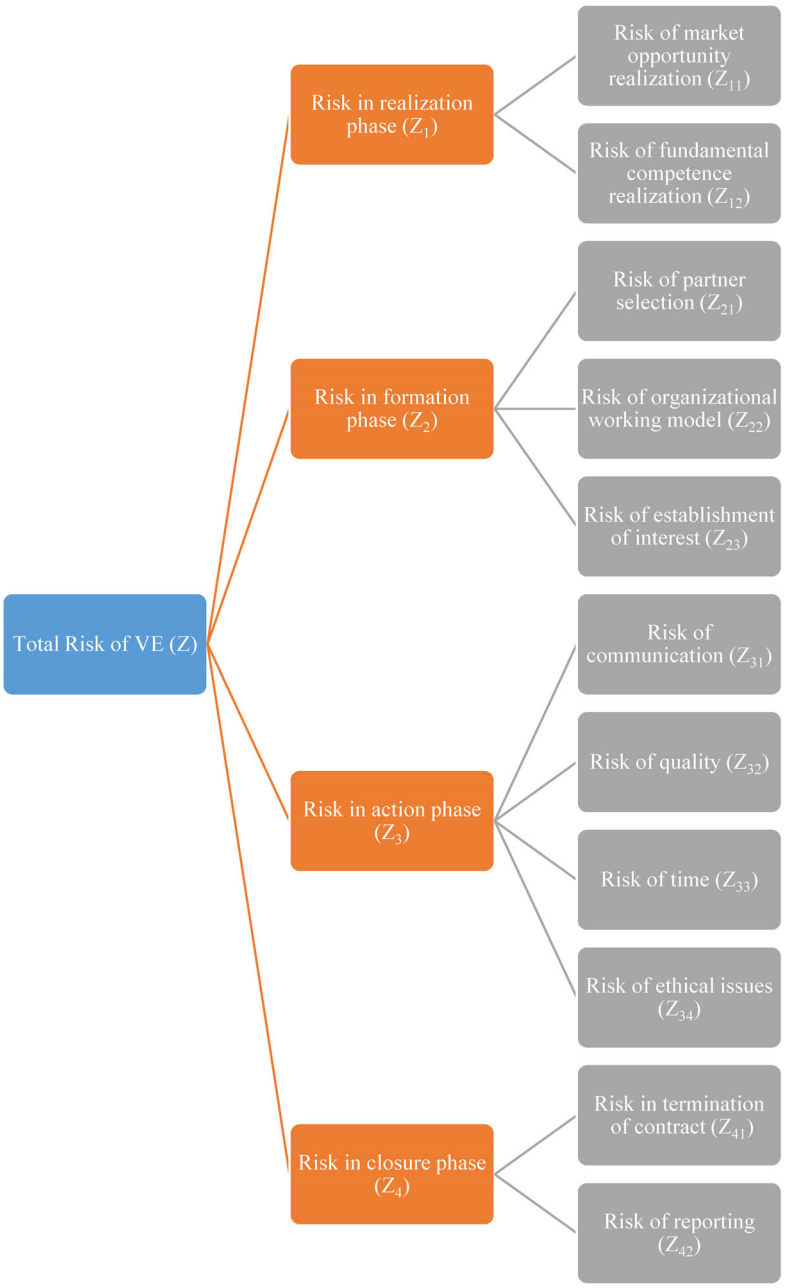

Fig. 5. Hierarchy of identified risk factors.

4.2.1. Realization phase risks

- The risk of market opportunity realization means that the core enterprises misinterpret the low-valued market opportunity as a favourable market opportunity due to collecting incorrect information or choosing wrong analytical tools.
- The risk of fundamental competence realization means that the core enterprise over- or underestimates its primary competencies, which leads to an incorrect choice with regard to the market opportunity.

4.2.2. Formation phase risks

- The risk of partner selection refers to the improper choice of a partner by the FP, which leads to a frequent change of partners or unplanned termination of the VE.

- The risk of an organizational working model is an inappropriate allocation of tasks and inadequate resource integration, which may cause high operational costs or time losses due to an inability of the partners to finish the work on time.
- The risk of the establishment of interest means that terms and conditions set by the core enterprise (FP) are unsuitable. It may lead to demotivation of partners and they might quit midway.

4.2.3. Action phase risks

- The risk of communication means that partners may have miscommunication either due to an inappropriate information system or due to lack of expertise in the selected area. This may disrupt the process of carrying out tasks.
- The risk of quality means that there are different quality policies and levels of quality among partners, which may cause problems when the quality of one partner affects the quality of the whole product.
- The risk of time means that some partners may not finish their tasks on time due to the lack of planning competence or inadequate information.
- The risk of ethical issues implies that each partner concentrates only on getting maximum self-benefits and advantages, and so one partner may influence benefits of other partners.

4.2.4. Closure phase risks

- The risk in the termination of the contract refers to unsettled financial obligations or other legal issues and may cause legal problems.
- The risk of reporting means that feedback and related results are not settled or are pending.

4.3. Risk estimation and evaluation

Risk assessment is the process that includes evaluation of the identified possible risks and losses due to these, which enables an enterprise to take effective measures to prevent and control risks. In the previous section, we built a hierarchical system for the identification, description, and assessment of VE risks; however, it is hard to obtain the exact numerical factors for the evaluation. Therefore, in this paper we adopted a semi-quantitative method based on the risk matrix to evaluate the project risk in a VE. The main idea is to estimate the four risk driven factors and then to integrate them to calculate the entire system factor.

According to its definition, risk (R) is the product of risk events probability (P) and the impact (I) or consequence of those particular events. Now it is easy to see that although some event has a high probability but a low impact, it is categorized as a low risk. On the other hand, if some event that occurs infrequently, but its consequences have high expenses, it is classified as highly risky. Thus, the function of risk can be defined as $R = \mathrm{f}(P, I)$. Let P_f be the probability that the event fails and I_f be the degree of the severity of the failed event, then the risk function will be

$$R_\mathrm{f} = P_\mathrm{f} \times I_\mathrm{f}. \quad (1)$$

In the hypothetical case we described the risk factor system in a hierarchical way with each subsystem having its risk factor (Z_{11}, Z_{12}); (Z_{21}, Z_{22}, Z_{23}); (Z_{31}, Z_{32}, Z_{33}, Z_{34}); (Z_{41}, Z_{42}), respectively. Those subsystem risk factors are estimated and evaluated by applying the risk matrix technique and the total Z is determined by FTA, which is described in the following sections.

4.3.1. Probability and impact estimation

For the matrix-based risk assessment, we suggest scaling the probability of an event and the impact of that event. The consequences of a risk event are its after-effects or the extents to which the risk event might influence product quality and process integrity or damage the whole process of the VE. We also recommend ranking each risk event to describe its level of severity.

The probability of a risk event illustrates the likelihood of failure or of a false event. It depends on whether the existing controls make the failure less likely to occur or increase the detectability of the failure. If the risk event is highly detectable, the likelihood of its occurrence may be reduced. This study ranked each failure to describe its probability of occurrence. The probabilities and consequences were evaluated and rated on a scale from one to five, where one is the lowest and five is the highest (Fig. 6).

Probability	1	< 20%
	2	
	3	50%
	4	
	5	> 80%
Impact	1	Low
	2	
	3	Medium
	4	
	5	High

Fig. 6. Scale for probability and impact ratings.

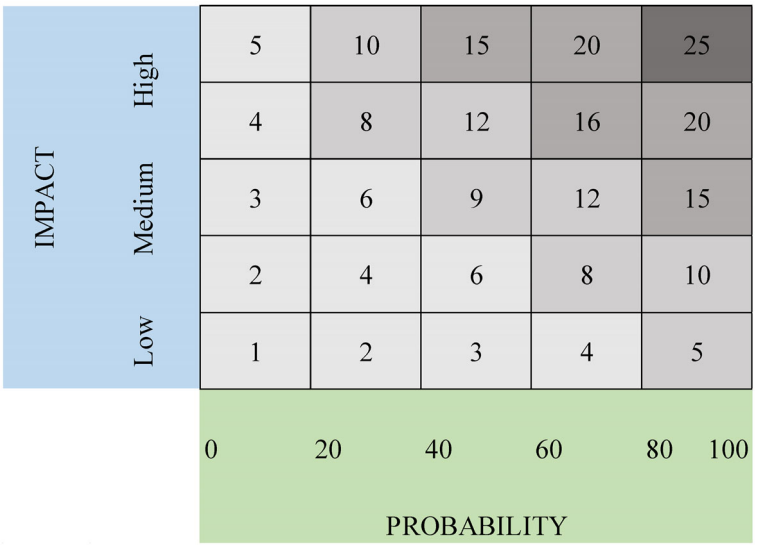

Fig. 7. Risk matrix for risk level evaluation.

4.3.2. Evaluation with a risk matrix

We used a risk matrix to evaluate the risk level of events. The levels of identified VE risks during its lifespan are determined by inserting the risks into an array where the axes represent probability and impact as depicted in Fig. 7. The risk level shows the overall risk associated with the failure based on the ranking of probability and consequence. The numbers represent the risk values ranging from 1 to 25. Risks located at the top right corner of the probability and impact matrix have to be handled first, and the same is true for all the risks with high impact values.

The subsystem risk factors and their corresponding values with likelihood, probability factor, and impact factor of each subsystem can be seen in Table 1. The impact factor of each risk event is assumed to be 3 (medium) for the whole hierarchical system as the analysis of the variation of likelihoods indicates.

Table 1. Subsystem risk estimation through risk matrix

Risk factor	Likelihood	Probability factor	Impact factor	Risk level
R_{Z11}	0.25	2	3	6
R_{Z12}	0.1	1	3	3
R_{Z21}	0.3	2	3	6
R_{Z22}	0.2	2	3	6
R_{Z23}	0.1	1	3	3
R_{Z31}	0.4	3	3	9
R_{Z32}	0.15	1	3	3
R_{Z33}	0.2	2	3	6
R_{Z34}	0.1	1	3	3
R_{Z41}	0.15	1	3	3
R_{Z42}	0.1	1	3	3

4.4. FTA of the overall risk of a VE

Considering that the classification of the risks in VEs is described in a hierarchical manner, FTA was used for the estimation of the overall reliability of a VE.

According to the axioms of FTA, the probability of the occurrence of a high risk level event can be defined as follows:

$$\text{AND events: } P(A \cap B) = P(A) \times P(B), \quad (2)$$

$$\text{OR events: } P(A \cup B) = P(A) + P(B), \quad (3)$$

where A and B stand for random events.

The probability of the top event (Z) for the VE can be represented by Eq. (4):

$$P_Z = P_{Z1}(\sum P_{Z1i}) \cap P_{Z2}(\sum P_{Z2i}) \cap P_{Z3}(\sum P_{Z3i}) \cap P_{Z4}(\sum P_{Z4i}). \quad (4)$$

Figure 8 illustrates FTA of a VE. It was observed that the risk weights of the action phase were higher than of the other stages. Therefore, a risk mitigation concept for the action phase was proposed. It is described through IoT-based monitoring in the next sub-section. Table 2 presents the risk factors of the remaining events that are known after the construction of FTA.

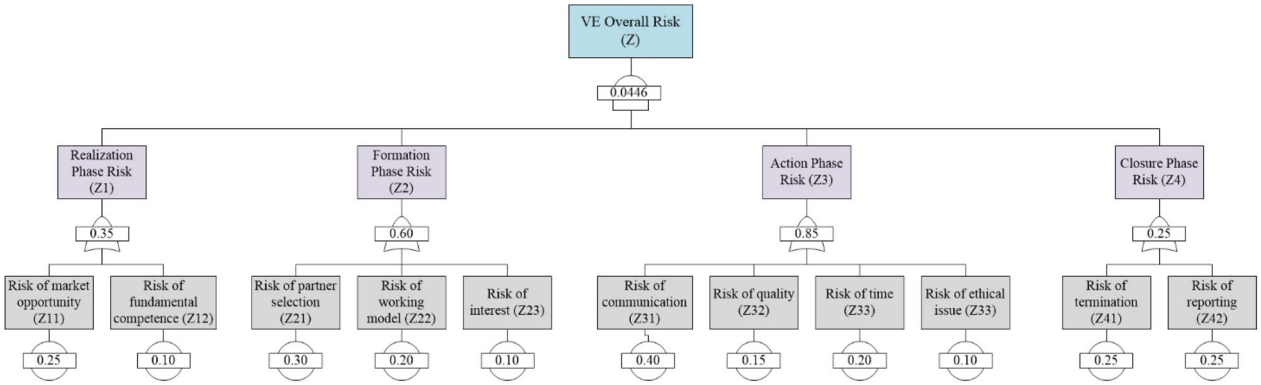

Fig. 8. Fault Tree Analysis of the lifespan of a VE.

Table 2. Overall risk estimation through FTA

Risk factor	Likelihood	Probability factor	Impact factor	Risk level
R_{Z1}	0.35	2	3	6
R_{Z2}	0.60	3	3	9
R_{Z3}	0.85	4	3	12
R_{Z4}	0.25	2	3	6
R_{Z}	0.04	1	3	3

4.5. IoT-based monitoring

IoT-based monitoring helps to mitigate action phase risks. In particular, risk of communication should be reduced as its level is the highest within a VE. The concept of the IoT-based monitoring of a VE is illustrated in Fig. 9.

This study suggests monitoring the business processes of each VE partner through embedded electronics such as sensor-enabled technologies and tools. These tools

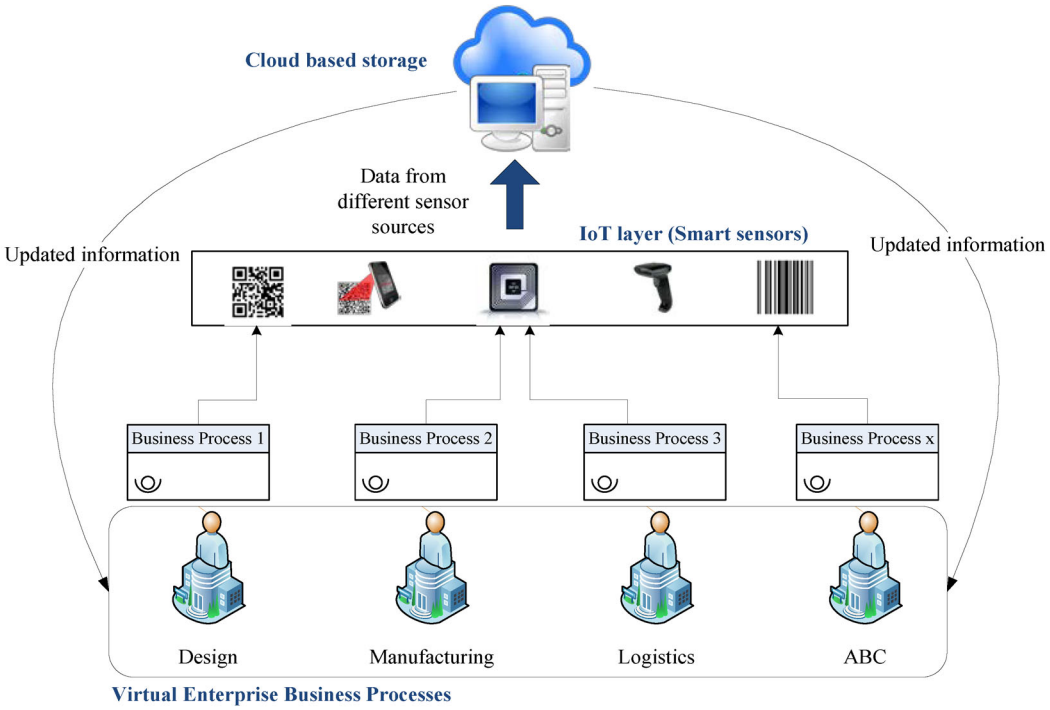

Fig. 9. Concept of IoT-based monitoring within a VE; ABC stands for an arbitrary process.

could be wireless technology, bar codes, RFID tags, Quick Response (QR) codes, etc., usually known as the IoT. Each business process has its own smart sensor that transfers real-time process information. The FP stores the process data collected from the sensor readers into the cloud-based data storage.

Since each VE partner can access the business process monitoring information, the individual enterprises receive valuable inputs related to business processes that require improvement. This way the monitoring system helps to keep an eye on and manage dynamically VE business processes, which ultimately reduces the action phase risks, i.e. communication, time, and quality risks. Moreover, it supports the improvement of the overall efficiency and effectiveness of the VE.

5. DISCUSSION AND CONCLUSIONS

This research is a contribution to the development of the risk assessment approach that enables to evaluate project reliability and facilitates the analysis of a system's vulnerability. Results of this research can also be applied as a preventive approach that helps decision-makers to improve their business model reliability. The proposed method for risk assessment of a VE's life cycle can be adopted by decision-makers of a collaborative network of SMEs to formulate and estimate the potential risks and to set up an action plan that facilitates mitigation of the overall VE risks. However, the suggested risk assessment method is mainly designed for the project-based management system and for the networking process.

The paper identifies possible risks that could occur during the functioning of a VE, and it provides a relatively simple method to estimate risks. We developed the model with hierarchical risk factors system for a functioning VE. Moreover, the FTA method was applied to determine the top-level event probability, which helps to assess the overall risk level of a VE. Also the concept of IoT-based risk monitoring and mitigation is proposed to improve the overall performance of a VE.

To implement the proposed concept, it is necessary that each player (partner) of a VE provide periodic information on the probability and occurrence of the risk events to the cloud-based storage. We suggest transforming this information into an evaluation matrix to create a new risk profile for each partner in the network. This would help to adjust the risk management strategies, policies, and tactics according to the new risk realities associated with the VE of SMEs. In this way, the method of risk assessment offers a proactive means for the risk management of the VE.

ACKNOWLEDGEMENTS

The work was supported by the European Regional Fund ERF, project No. 2014-2020.4.01.16-0183, Smart Industry Centre (SmartIC). The publication costs of this article were covered by Tallinn University of Technology and the Estonian Academy of Sciences.

REFERENCES

1. Camarinha-Matos, L. M. and Afsarmanesh, H. Collaborative networks: a new scientific discipline. *J. Intell. Manuf.*, 2005, **16**, 439–452.
2. Lockamy, A. III and McCormack, K. Modelling supplier risks using Bayesian networks. *Ind. Manage. Data Syst.*, 2012, **112**, 313–333.
3. Dudek-Burlikowska, M. The concept of Total Quality Management and the contemporary entrepreneurship in practice. *J. Achiev. Mater. Manuf. Eng.*, 2015, **73**(2), 229−236.
4. Hallikas, J., Tuominen, M., Karvonen, I., Pulkkinen, U., and Virolainen, V. M. Risk management processes in supplier networks. *Int. J. Prod. Econ.*, 2004, **90**, 47–58.
5. Harland, C., Walker, H., and Brenchley, R. Risk in supply networks. *J. Purch. Supply Manag.*, 2003, **9**, 51–62.
6. The Society for Risk Analysis (SRA). 2015, www.sra.org (accessed 2017–07–26.)
7. Hopkin, P. *Fundamentals of Risk Management*. 3rd edition. Kogan Page, 2014.
8. International Organization for Standardization. ISO 31000:2009: Risk management -- Principles and guidelines. Geneva, Switzerland, 2009.
9. Appio, F. P., Martini, A., Massa, S., and Testa, S. Collaborative network of firms: antecedents and state-of-the-art properties. *Int. J. Prod. Res.*, 2016, **55**, 2121–2134.
10. Rosas, J., Urze, P., Tenera, A., Abreu, A., and Camarinha-Matos, L. M. Exploratory study on risk management in open innovation. In *Collaboration in Data-Rich World. PRO-VE 2017* (Camarinha-Matos, L., Afsarmanesh, H., and Fornasiero, R., eds). IFIP Advances in Information and Communication Technology, 2017, Vol. 506, 527–540. Springer, Cham.
11. Jüttner, U. Supply chain risk management: understanding the business requirements from a practitioner perspective. *IJLM*, 2005, **16**, 120–141.
12. Ojala, M. and Hallikas, J. Investment decision-making in supplier networks: management of risk. *Int. J. Prod. Econ.*, 2006, **104**, 201–213.
13. Chopra, S. and Sodhi, M. S. Managing risk to avoid supply-chain breakdown. *MIT Sloan Manag. Rev.*, 2004, **46**, 53–61.
14. Mahmood, K. and Shevtshenko, E. Analysis of machine production processes by risk assessment approach. *Journal of Machine Engineering*, 2015, **15**, 112–124.
15. Norrman, A. and Jansson, U. Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *IJPDLM*, 2004, **34**, 434–456.

16. Karkoszka, T. Conformity assessment as a manner of risk optimisation in organisations. *J. Achiev. Mater. Manuf. Eng*., 2012, **55**(2), 881−888.
17. Project Management Institute. *A Guide to the Project Management Body of Knowledge (PMBOK ® Guide)*, 5th edition. Pennsylvania, USA, 2013.
18. Tonnquist, B. *Project Management: A Guide to the Theory and Practice of Project, Program and Portfolio Management and Business Change*. Bonnier Utbildning AB, Stockholm, 2008.
19. Kania, A., Spilka, M., and Wieczorek, K. Modification of selected occupational risk assessment method. *J. Achiev. Mater. Manuf. Eng*., 2015, **69**(1), 38−44.
20. Klüppelberg, C., Straub, D., and Welpe, I. M. (eds). *Risk – A Multidisciplinary Introduction*. Springer, 2014.
21. Kostina, M., Karaulova, T., Sahno, J., and Maleki, M. Reliability estimation for manufacturing processes. *J. Achiev. Mater. Manuf. Eng*., 2012, **51**(1), 7−13.
22. Byrne, J. The virtual corporation. *Business Week*, 1993, Feb. 8, 98–102.
23. Polyantchikov, I., Shevtshenko, E., Karaulova, T., Kangilaski, T., and Camarinha-Matos, L. M. Virtual enterprise formation in the context of a sustainable partner network. *Ind. Manage. Data Syst*., 2017, **117**(7), 1446–1468.
24. Shevtshenko, E., Poljantchikov, I., Mahmood, K., Kangilaski, T., and Norta, A. Collaborative project management framework for partner network initiation. *Procedia Engineering*, 2014, **100**, 159–168.
25. Liu, G., Zhang, J., Zhang, W., and Zhou, X. Risk assessment of virtual enterprise based on the fuzzy comprehensive evaluation method. In *Integration and Innovation Orient to E-Society* (Wang, W., Li, Y., Duan, Z., Yan, L., Li, H., and Yang, H., eds). IFIP – The International Federation for Information Processing book series, 2007, Vol. 251, 58–66. Springer, Boston, MA.
26. Paavel, M., Snatkin, A., and Karjust, K. PLM optimization with cooperation of PMS in production stage. *Arch. Mater. Sci. Eng*., 2013, **60**(1), 38−45.
27. Jia, X., Feng, Q., Fan, T., and Lei, Q. RFID technology and its applications in Internet of Things (IoT). In *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. IEEE, 2012, 1282–1285.
28. Shrouf, F., Ordieres, J., and Miragliotta, G. Smart factories in industry 4.0: a review of the concept and of energy management approached in production based on the Internet of Things paradigm. In *International Conference on Industrial Engineering and Engineering Management*. IEEE, 2014.
29. Camarinha-Matos, L. M. and Afsarmanesh, H. Classes of collaborative networks. *Encyclopedia of Networked and Virtual Organizations*. IGI Global, 2008.

Riskihindamise metoodika väikeste ja keskmise suurusega ettevõtete virtuaalettevõttele

Kashif Mahmood, Eduard Shevtshenko, Tatjana Karaulova ja Tauno Otto

Uurimistöö eesmärgiks oli arendada virtuaalettevõtte (VE) riskihindamise metoodikat, mis võimaldaks analüüsida riski võtmetegureid ja hinnata virtuaalettevõtte riskitaset kogu selle tegevusperioodi vältel. Uuringu tulemusel töötati välja funktsionaalne riskihindamise meetod ja kontseptsioon riskide vähendamiseks VE tegevuses. VE eksistentsiaalne mudel hõlmab hierarhilisi riskitegureid, mille abil on võimalik aidata väikeste ja keskmise suurusega ettevõtete (VKE) koostöövõrgustiku otsustaja(te)l koostada riskijuhtimise strateegiaid ning taktikaid, et leevendada VE üldisi riske. Poolkvantitatiivses riskihindamise meetodis kasutati riskide hindamiseks tõenäosuse ja mõju maatrikseid. Uuringus kasutati VE üldise riskiteguri määramiseks edukalt rikkepuuanalüüsi (FTA). Riskide leevendamiseks pakuti välja IoT (Internet of Things) seirepõhine nutikas kontseptsioon. Riskitegurite arvutamiseks ja kavandatud lähenemisviisi asjakohasuse hindamiseks kasutati esitatud hüpoteetilises VE näites arvutisimulatsioone.