

THE SELECTED ISSUES OF THE CONCEPT OF RESILIENCE AND THE WAY OF ITS APPLICATION IN CRISIS MANAGEMENT OF THE COMPANY

Jozef Klučka²³⁹
Katarina Haviernikova²⁴⁰

<https://doi.org/10.31410/itema.2018.611>

Abstract: *Each enterprise can be taken as a system of social, economic and other relationships which are connected together and have a serious impact on each other's. An enterprise should have own capacity (resources, knowledge) to flexible reaction on incidents (disruptions, changes) with the impact on its strategy due to the conditions in which the company operates. The realization of business activities in dynamic conditions is not easy. The dynamics of changes is constantly growing; the business surroundings, market conditions, competition of activities, customer demands on the quality of services provided, and many other factors change so quickly that resilience of the company becomes important strategic ability. The paper deals with the concept of resilience, which is the framework for reaction on identified opportunities, threads and risks. In the paper, there are presented different definitions, aspects and approaches of organizational resilience and possibilities of its quantification. It is described also the application of the approach – quantification of organizational resilience. For achieving of main aim of the paper the qualitative (expert estimation) and quantitative methods (multi-criteria analysis) were used. The output of a qualitative assessment of the company's resilience is the design of measures to increase the company's resilience. The output of quantitative assessment of company's resilience is the determination of those areas in which an enterprise needs to increase its resilience.*

Keywords: *resilience, organizational resilience, resilience quantification*

1. INTRODUCTION

Complexity and the uncertainty of the environment in which today's organizations operate determine the search for new approaches to management. Business environment is characterized by growing dynamics, diversity and permanent changes. [1], [2], [3], [4] A system approach to organization (as a socio-economic system) is based on the anticipations of relations to internal and external environments. Nowadays internal and external environments are affected by many factors that cause the behavior of enterprises. An organization with its activities, changes internally, specifically influences external environments and it must have own capacity (resources, knowledge) for a flexible reaction on incidents (disruptions, changes) with the impact on its strategy. A reaction to threats and opportunities is therefore the part of the organizational resilient concept.

²³⁹ Crisis Management Department, Faculty of Security Engineering, University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovakia

²⁴⁰ Faculty of Social and economic relations, Alexander Dubček University of Trenčín, Študentská 3, 911 50 Trenčín, Slovakia

Resilience depends on a sector within an organization is active, on formulated strategy conditional external (economic, political, legislative) conditions as well as risk management strategy. Formulating organizational resilience is not a one-time activity, but a continuous and permanent managerial process.

Every organization is in equilibrium under normal conditions [5], [6] unless there is a disruption by an incident. Incident according to [7] is: “situation that might be, or could lead to, a business disruption, loss, emergency or crisis. Disruption is any expected or unexpected event, whose consequences can disrupt regular products provisions. Efficiency is defined by synergy of measures allocated to different phases. The solution is not the application of restricted measures but substantial is the system approach to security expressed with the term resilience”.

In relation with the explained there is possible to formulate some problems that create the content of this paper. Main aim of the paper is focused on evaluation of possibilities, ways and benefits of using the concept of resilience in crisis management of a company and to propose selected issues of its application. In the paper have been used scientific methods and approaches: analysis/synthesis, induction/deduction, quantification and discussion.

2. LITERATURE REVIEW

The fundamental idea of resilience is derived from Ch. Darwin who declares: „Not the strongest or the most intelligent will survive but a one who is the most adaptive“. The framework of resilience provides unique and relatively new approach to security.

We can find several definitions of resilience in literature. In [8] is the resilience defined as: „... ability of an organization (system) to hold or to achieve again dynamic stable state, that allow to continue in activity after an incident and/or permanent presence of stress“. The other resilience definition according [9] declares: “...ability of an organization to plan and adapt to changes or disruptions via anticipation, protection, reactive capacity and ability of recovery.” The author in [10] declares that resilient organization is: “capable to achieve entrepreneurial objectives and achieve opportunities, even in adverse circumstances”. According to [11] terminology is resilience ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. Resilience means the ability to “resile from” or “spring back from” a shock. The resilience of a community in respect to potential hazard events is determined by the degree to which the community has the necessary resources and is capable of organizing itself both prior to and during times of need. Individual resilience is demonstrated by individuals who adapt to extraordinary circumstances achieving positive and unexpected outcomes in the face of adversity [12]. Individual resilience could be understood as personal resistance on physical, emotional and stress factors which are directly connected to incident or disasters. Resilient individuals, however, are able to work through the emotions and effects of stress and painful events and rebuild their lives. The resilience can be seen from the aspect of society and therefore societal resilience is the timely capacity of individuals and groups—family, community, country, and enterprise—to be more generative during times of stability and to adapt, reorganize, and grow in response to any disruption [13]. The official version of American standard [14] declares: Resilience is organizational adaptive capacity in complex and ever changing environment. It is an ability to resist to adverse events or after such event to return to acceptable level of performance in a reasonable time. Resilience is also defined as the ability of a system

to hold its structure and functions in changing internal and external conditions or if necessary terminate its activity.

Organizational resilience is defined as the ability of an organization to absorb disturbance and perform changes in functioning in the way to be able to hold equal structures and functions as before violation [15]. Organizational resilience can be described e.g. as its ability to: effectively absorb impacts of incident, which potentially threatens its survival, develop specific reaction to an incident and exploit a new opportunity. Other authors are also dealing with organizational resilience generally or specifically – see [16], [17], [18].

The opposite of resilience is the fragility of an organization. The fragile organization is a system that is unable to adapt to unexpected changes and therefore system collapses due to impact of negative, destructive internal and external measures. [19]. Unexpected changes are conditions, events that lead to discontinuity of system behavior. There are a large number of resilience definitions. The spectrum is wide from psychology to crisis management.

From the definitions (see above) we can summarize:

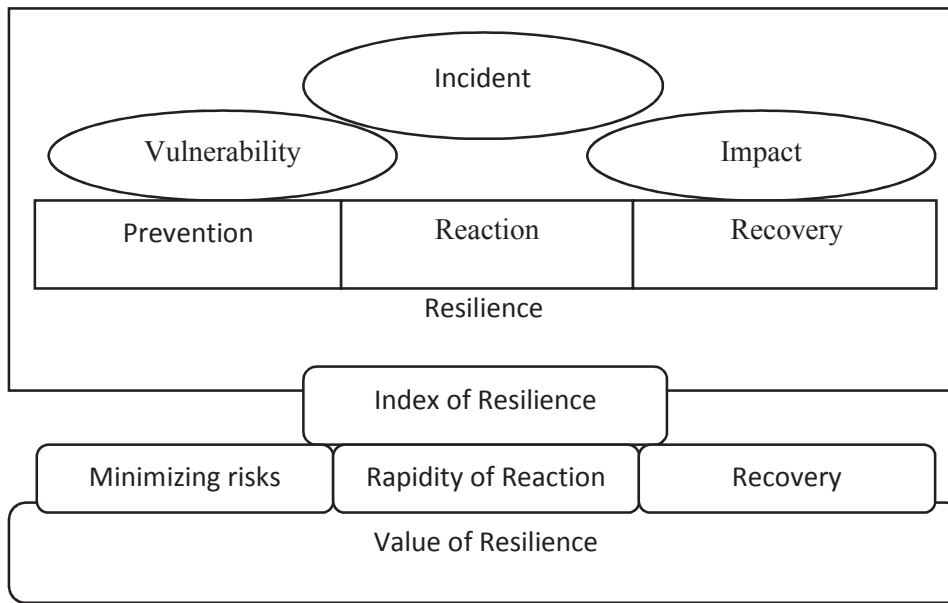
- the resilience concept is a complex approach to security,
- the concept has the ambition to quantify the achieved level of resilience (of an analyzed system),
- as an complex approach integrates all three phases (before, during and after incident) into unique, complex approach to security,
- its more theoretical rather than practical approach; it does not exclude any activities, measures constrained to only one phase; the system approach to security is applied via the presented concept of resilience,
- organizational resilience consists of different relevant aspects; relevancy is based on sectors, objectives.

Concept of resilience is surely a desirable approach. A lot of organizations are aware that sooner or later they will face unexpected events that can put them seriously into risk or failure. Nowadays just a few organizations have implemented the resilience concept into their strategy. Building resilience into the organization is therefore strategically suitable, but potentially it also could be high costly. For example, companies can protect themselves against supply chain disruptions by spreading their purchasing of inputs across multiple suppliers, but this usually entails higher costs. If we imagine organization as a system of components and their bounds, we can also abstract organizational resilience as part of components which is suitable to adopt in organizations. Also the authors or publications [19], [20], [21], [22], [23], [24], [25], [26] and [27] provide their approach to the resilience concept.

3. METHODOLOGICAL APPROCH

If the resilience concept is applied in different sectors, it does not mean that organization are resilient at equal level. There is a need to measure resilience. Based on stated facts and related to paper of [28] we present a possible ways for organizational resilience quantification (Figure 1).

Figure 1 The resilience concept and possibilities of quantification



The presented approach is based on the key assumption – to quantify resilience of an organization dealing with emergencies. The quantification is based on the incident phases and then via multiplication is calculated the final level of an organizational resilience. The value of resilience creates a complex indicator, whose level is determined by quantitative and qualitative features.

The concept of resilience is linked with a possibility (ambition) of its quantification. There are different systems, approaches of evaluation and quantification (see also ([29])). One of the approaches (declares that resilience consists of [30] :

- identification of a current situation (SA),
- management of key agents of vulnerability (KV),
- adaptive capacity (AC).

The value (weight) of specific agents reflects evaluation of current situation. The value of resilience is quantified:

$$VR = \sum SA_i * KV_i * AC_i \quad (1)$$

Where

VR is the value of organizational resilience.

4. RESULTS

In this part of paper we have presented the application of organizational resilience that is focused on an enterprise that description was provided by [9]. An enterprise is a shareholding company that was established in 2008 due to split of the enterprise with 40 years history. Its seat is in Žilina and has organizational branches in 5 towns within Slovakia. The activities cover provision of technical engineering services, business and consulting services. The scope of entrepreneurial activities is the spectrum of geodetic services for state, private organizations as well as private bodies. The enterprise has decreased number of employees. The market pressure

and the current state of building sector and its entrepreneurial culture have caused financial (problems with liquidity) and operational problems in a company.

For resilience quantification in enterprise, the simplified additive model of multi-criteria analysis was used to identify three characteristics/factors of resilience:

- adaptive abilities (AB) – eight indicators describing the organization, (see Table1),
- plans and strategies (PS) – five indicators, and
- level of risks – four indicators.

<i>Adaptive abilities</i>	<i>Plans and strategies</i>	<i>Risk rate</i>
<p>AB1 Internal and External Environment: level of knowledge and monitoring or relations with: suppliers, customers, owners, shareholders and public, state institutions.</p> <p>AB2 Engagement of employees: level of employees' identification with relation to their jobs, resilience and long term prosperity of the enterprise</p> <p>AB3 Communication among departments within the enterprise: level of cooperation and communication among them.</p> <p>AB4 Interior resources: level of economic, financial, technical and human resources to solve a crisis situation in the enterprise.</p> <p>AB5 Level of management: level of competencies and abilities of effective management of the enterprise before, during and after a crisis situation in the enterprise.</p> <p>AB6 Information and knowledge: level of employee information about procedures during a crisis situation (fire, accident at work, health problems), availability of documentation and crisis plans, data application, information and knowledge within the enterprise and between cooperating organizations.</p> <p>AB7 Innovations and creativity: level of support and rewards of innovative and creative solutions of existing or arising problems within the enterprise.</p> <p>AB8 Competencies: level of delegation of competencies to staff to solve problems at the beginning, level of employees qualification and their specific knowledge and qualification</p>	<p>PS1 Planning and Strategies: level of resilience strategy and planning activities.</p> <p>PS2 Practical Training: level of employee preparedness for emergency situations.</p> <p>PS3 External resources: level of external resources to handle crisis situations, their time and space availability</p> <p>PS4 Accuracy: level of perception of weak signals in the enterprise before escalation of problems, the ability of an effective response.</p> <p>PS5 Continuity: level of readiness to continue and run after crossing the crisis.</p>	<p>RR1 Risk rate of the company's technical and manufacturing processes: level of overall risk in the company's production processes, used technologies and plant facilities.</p> <p>RR2 Risk rate of enterprise information processes: level of overall risk associated with enterprise information systems - hardware, software, networks, data.</p> <p>RR3 Risk rate of economic and financial processes: level of overall risk associated with the enterprise's economic performance, financial management, internal corporate governance and internal and external financial resources.</p> <p>RR4 Risk level of management, organizational and social processes: level of overall risk associated with the strategy, management and human resources of the enterprise.</p>

Table1: Factors of resilience, processed according [9]

The procedure was as follows: each indicator was evaluated according to assigned level (expert evaluation). The scale was within 1 – as insufficient, critical resilience to 7 – as complex resilience. For each factor was identified relevant number of indicators. Then was assigned weight for each indicator and scale of this indicator was quantified the impact of each factor. Applying equation (1) – modified according to three factors written above, the value of organizational resilience was:

$$VR = 0,4 * 4,28 + 0,3 * 3,85 + 0,3 * 3,55 = 3,932$$

The total organizational resilience is 3,93 what can be interpreted as slightly under averaged resilience. The highest value was achieved adaptive abilities and the lowest level was factor level of risks.

The application of this concept will allow us to forecast the system behavior that is determined e.g. by level of investments, human and financial resources. This approach does allow monitoring trend of organizational resilience of an analyzed organization as well as comparing the achieved results to similar organizations (like benchmarking).

5. CONCLUSION

The concept of resilience can be applied after fulfillment of following conditions:

- to incorporate into the resilient model all relevant activities carried out at all departments at different organizational levels,
- to develop cooperation of private and public sectors,
- takes an applied system for resilience monitoring as a managerial tool,
- to develop theory and its application in practice; apply a model for strategic decisions.

Presented approach (its idea) is a tool that can be implemented in decision making process. The formal structure of composite indicator is determined by its objectives. There are possible (at least) two approaches:

- procedural; when structure of composite indicator is in relation to phases of core activities and its managerial support,
- structural; when composite indicator is based on evaluation of specific aspects.

The evaluation of resilience fulfills the following conditions:

- monitoring a development evaluation (trend),
- comparison of existing system to similar ones (competitors - benchmarking),
- create database for implementation of measures.

Resilient system is reliable and is able to recover with minimum impact after an incident in a relatively short time. From this point of view an application of the resilience concept is interesting and creates new challenges to security research or/and performance and its relations to security.

ACKNOWLEDGEMENTS

This publication was created in the frame of the project VEGA 1/0918/16 Risk management of SMEs in the context of clusters` involvement activities in the Slovak Republic as its partial output.

REFERENCES

- [1] Gorzen-Mitka, I., Okreglicka, M., 2015. Review of Complexity Drivers in Enterprise, Proceedings of the 12th International Conference: Liberec Economic Forum 2015, Liberec, Czech Republic, 16-17. 09.2015, 253-260.
- [2] Mura, L. 2017. Current situation in Family Businesses. *Managerial trends in the development of enterprises in globalization era*, pp. 178-185. ISBN 978-80-552-1739-0
- [3] Durkalić, D. (2016). Impact of trade openness on economic development: case from Serbia. *Acta Oeconomica Universitatis Selye* Vol. 5, No. 2, pp. 79 – 87.

- [4] Mura, L., Daňová, M., Vavrek, R., Dúbravská, M. (2017). Economic freedom – classification of its level and impact on the economic security. *AD ALTA-Journal of Interdisciplinary Research*, Vol. 7, No. 2, pp. 154 – 157.
- [5] Cseh Papp, I., Varga, E., Schwarczová L., Hajós, L. (2018). Public work in an international and Hungarian context. *Central European Journal of Labour Law and Personnel Management*, Vol. 1., No. 1., pp. 6 – 15.
- [6] Poliačiková, E. 2016. Category management as an effective instrument of relationship management. *Acta Oeconomica Universitatis Selye* Vo. 5, No. 1, pp. 119 – 127
- [7] Szabados, L., et al. (2008). Business Continuity Management. TATE International. Slovakia, ISBN 978-80-969747-2-6.
- [8] *Disaster Resilience: A National Imperative*. (2012). [online]. [cit. 2012-08-08]. Available at: http://www.nap.edu/catalog.php?record_id=13457.
- [9] Janurova, D. (2015). Koncept odolnosti a jeho aplikácia v krízovom manažmente podniku, FBI, ŽU v Žiline, diploma thesis.
- [10] Cockram, D. (2012). *Organizational resilience* [online]. [cit. 2015-02-18]. Available at: <http://www.bcifiles.com/OrganisationalResiliencePaper.pdf>.
- [11] UNISDR. (2009). UNISDR Terminology on Disaster Risk Reduction. Geneva : UNISDR. [online]. [cit. 2015-03-15]. Available at: http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf
- [12] Fraser, M. W., et al. (1999). Risk, protection, and resilience: Toward a conceptual framework for social work practice. *Social Work*, 23(3), 131-143p. ISSN 1545-6838.
- [13] Leetch, L., Sutton, L. (2016). *An Introduction to the Social Resilience Model*. [online]. Threshold Global Works, LLC. [cit. 2015-01-20]. Available at: <https://www.thresholdglobalworks.com/about/social-resilience/>
- [14] ASIS SPC.1-2009. (2009). American national standards. *Organizational resilience: Security, Preparedness and Continuity Management Systems - Requirements with guidance for use*. March 12. ISBN 978-1-887056-92-2.
- [15] Walker, B. et al. (2010). Resilience Thinking: Integrating Resilience, Adaptability and Transformability [on line]. In *Ecology and Society*, No 2010 15(4): 20, [cit. 2015-04-18]. Available at: http://www.fs.fed.us/pnw/pubs/journals/pnw_2010_folke.pdf.
- [16] Brunner, E., Girroux, J. (2009). *Examining Resilience: A concept to improve societal security and technical safety* [online]. CRN Report. Center for Security Studies (CSS), ETH Zürich. June, 2009. [cit. 2015-03-15]. Available at: http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/dokumente/Unterlagen_Risiken.parsys.000130.downloadList.68565.DownloadFile.tmp/crnreportfactsheetresilience.pdf.
- [17] Dobeles, L. et al. (2015). Sustainable economic development: scenarios for promotion of social innovation in Latvia, *Journal of Security and Sustainability Issues* 5(2). pp. 149–158.
- [18] Míka, V. T., et al. (2009). *Manažment a krízový manažment. Úvod do krízového manažmentu*. Žilina : EDIS, ŽU.
- [19] Kantur, D., Iseri Say, A. (2012). Organizational resilience: A conceptual integrative framework. [online]. *Journal of Management and Organization*, No 18(6) [cit. 2015-01-20]. p. 762-773. Available at: <http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9230152&fileId=S1833367200000420>.
- [20] Rakauskiene, O. G., Strunz, H. (2016), Approach to Reduction of Socioeconomic Inequality: Decrease of Vulnerability and Strengthening Resilience, *Economics and Sociology*, Vol. 9, No 4, pp. 243-258.

- [21] Brae, B., Brooks, D. (2010). Organizational Resilience: A Propositional Study to Understand and Identify the Essential Concepts [online]. In *Proceedings of the 3rd Australian Security and Intelligence Conference, Perth*. [cit. 23. 1. 2015] p. 14-23. Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001&context=asi>.
- [22] *BS 65000 Guidance on Organizational Resilience*. (2014). [online]. [cit. 2015-04-06]. Available at: <http://www.bsigroup.com/en-GB/our-services/events/2014/Launch-of-BS-65000-Guidance-on-Organizational-Resilience/>.
- [23] Gibson, C., Tarrant, M. (2010). A Conceptual Models approach to organizational resilience. *The Australian Journal of Emergency Management* 25(02) [cit. 2015-03-10]. Available at: http://www.Researchgate.net/publication/235981328_A_conceptual_models_approach_to_organizational_resilience.
- [24] McManus, S. (2008). *Organizational Resilience in New Zealand*. PhD. thesis. Canterbury: University of Canterbury. 229 p. [online]. [cit. 2015-04-25]. Available at: http://ir.canterbury.ac.nz/bitstream/10092/1574/1/thesis_fulltext.pdf
- [25] Mitchell, T., Harris K. (2012). Resilience: A risk management approach. *ODI Background Note*. [online]. [cit.2015-03-15]. Available at: <http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7552.pdf>.
- [26] Stephenson, A. (2010). *Benchmarking the resilience of organizations*. PhD. thesis. Canterbury: University of Canterbury. 370 p. [online]. [cit. 2015-04-25]. Available at: <http://www.resorgs.org.nz/News/benchmarking-the-resilience-of-organisations.html>.
- [27] Whitehorn, G. (2010). *Building organizational resilience in the Public Sector*. [cit. 2013-23-08] Available at: <http://www.finance.gov.au/comcover/conferences/docs/July-2010-Grant-Whitehorn-Presentation.pdf>
- [28] Klučka, J. (2015). Resilience organizácie – teória a dôsledky [Organizational resilience – theory and consequences]. *Zborník z 20. vedeckej konferencie FBI, EDIS, Žilina*, pp. 265-272.
- [29] Tierney, K. (2003). *Conceptualizing and Measuring Organizational and Community Resilience: Lessons from the Emergency Response Following the September 11, 2001 Attack on the World Trade Center* [online]. Delaware: University of Delaware, Disaster Research Center, 2003. 14 p. [cit. 2015-04-06]. Available at: <http://www.drs.dpri.kyoto-u.ac.jp/us-japan/cd-3/KathleenTierney.pdf>.
- [30] Bruneau, M. (2003). *A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities*. [cit. 2013-23-08] Available at: <http://civil.eng.buffalo.edu/~reinhorn/PUBLICATIONS/Bruneau%20et%20al%20%282003%29%20EERI%20Spectra%20Resilience%20%20Paper%20Body%2019%284%29%20733-752.pdf>