Interdisciplinary Description of Complex Systems 19(3), 366-374, 2021

COMPARING RISK AND RESILIENCE APPROACHES

Leon Runje[1], Amalija Horvatić Novak[2], Biserka Runje[2,*], Andrej Razumić[2] and Veljko Kondić[3]

[1]Ministry of Defence of the Republic of Croatia
Zagreb, Croatia

[2]University of Zagreb, Faculty of Mechanical Engineering and Naval Architecture
Zagreb, Croatia

[3]University North
Varaždin, Croatia

DOI: 10.7906/indecs.19.3.2
Regular article

Received: 9 March 2021.
Accepted: 27 September 2021.

ABSTRACT

Ever increasing challenges in the areas of risk management have led to a need for a risk management approach which deals not only with threat prevention but also adaption, absorption and recovery from adverse events. This has led to the rise of the concept of resilience analysis and management, which, unlike risk assessment and management focuses on the overall system under analysis rather than its individual components. Therefore, both the civilian and military sector have, over the past decade, emphasized the need to clarify the concept of resilience management as well as to differentiate it from related terms such as risk management. This article aims to build upon the existing literature and provide a comparison of the risk and resilience approaches which offer ways to analyse and manage these concepts.

KEY WORDS

risk assessment, risk management, resilience analysis, resilience management

CLASSIFICATION

JEL: D80, D84

*Corresponding author, η: biserka.runje@fsb.hr; +385 1 6168 222;
University of Zagreb, Faculty of Mechanical Engineering and Naval Architecture, Ivana Lučića 5,
HR -10 000 Zagreb, Croatia

INTRODUCTION

As referenced in Linkov and Palma-Oliveira [1; p7] the National Academy of Sciences (NAS) defines resilience as "the ability to plan and prepare for, absorb, recover from, and adapt to adverse events". Teoh and Seif [2] offer a different definition, focusing on resilience more as "a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationship between populations and state variables" and therefore a "fundamental quality of individuals, groups, organizations, and systems as a whole [which allows them] to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behavior". They further build upon this definition of resilience as "a function of an organization's overall situational awareness, keystone vulnerability and adaptive capacity in a complex, dynamic and interdependent system" [2]. In the last several years a significant number of norms which define key terms in the area of security and resilience from the point of view of emergency management, business continuity management systems and organizational resilience have been codified [3-8]. For example, the norm ISO 22300:2021 Security and resilience – Vocabulary defines the terms used in security and resilience standards. It defines resilience as the ability to absorb and adapt in a changing environment. A large number of norms which have yet to be codified will be dealing with authenticity, integrity and trust for products and documents, security management systems, crisis management and protective security. Such a large number of both already published and upcoming norms speaks to the need for standardization in the area of resilience management.

The process of risk analysis, risk evaluation and risk management is also codified via several international norms. The risk management vocabulary [9] defines risk as the effect of uncertainty on objectives which represents a deviation from the expected, that can be both positive and/or negative. Furthermore, risk is defined in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence [9] The importance of risk assessment was confirmed in the revision of the ISO 9001:2015 [10] norm, where a special emphasis was placed on introducing risk based considerations and thinking. The norms ISO 31000:2018 Risk management – Guidelines [11] and IEC 31010:2019 Risk management – Risk assessment techniques [12] are being applied in an ever increasing number of companies because the risk management process is applicable regardless of the size and type of the company. These are norms which are non-binding and describe generic methods of risk management and evaluation.

Ever increasing challenges in the areas of risk assessment & management have led to a need for a risk assessment & management approach which deals not only with threat prevention but also adaption, absorption and recovery from adverse events. Connelly et al. [13] identified features of resilience that are common across conceptualizations of resilience in various fields including (i) critical functions (services), (ii) thresholds, (iii) recovery through cross-scale (both space and time) interactions, and (iv) memory and adaptive management. These features are related to the National Academy of Science definition of resilience through the temporal phases of resilience [13]. The concept of critical functionality is important to understanding and planning for resilience to some shock or disturbance. Thresholds play a role in whether a system is able to absorb a shock, and whether recovery time or alternative stable states are most salient. Recovery time is essential in assessing system resilience after a disturbance where a threshold is not exceeded. Finally, the concepts of memory describe the degree of self-organization in the system, and adaptive management

provides an approach to managing and learning about a system's resilience opportunities and limits, in a safe-to-fail manner [13]. This has led to the rise of the concept of resilience analysis & management, which, unlike risk assessment & management, focuses on the overall system under study rather than its individual components.

This article aims to build upon the existing literature and provide a comparison of the two analytical and management approaches as well as to elaborate on the suitability of existing methodologies for measuring resilience in complex systems.

COMPARING RESILIENCE ANALYSIS AND RISK ASSESSMENT

Risk assessment which falls under the broader concept of risk management is defined as an overall process of risk identification, risk analysis, and risk evaluation by the risk management vocabulary [9]. As Linkov and Trump [14]. have noted, there exist the issue "of the definition of resilience analysis; where the various agencies interested in utilizing resilience analysis also make use of differing definitions of the term (…) agencies in the United States and research centers in Europe have begun to grapple with the issue of what resilience analysis definitely entails, yet no single definition has emerged as a standard for researchers to follow" [14]. Therefore, the working definition of resilience analysis in this article will be its characteristics as defined by the authors below.

While exploring the differences between the two approaches several authors have pointed out that the they contrast on two key aspects: how they assess and understand uncertainty and how they judge outcomes of hazardous events [15]. This is due to the fact that resilience analysis focuses on exploring threats to system stability and vulnerabilities at the level of an individual system (or systems) while risk assessment focuses on individual aspects of said system. Furthermore, resilience analysis focuses on a longer timescale than risk assessment. It seeks to foresee threats, prevent longstanding losses by ensuring the system can quickly and efficiently recover from external shocks. Risk assessment focuses on a relatively short time period with the aim of protecting a specific system component from defined threats and gives little attention to post-attack recovery of a component or system. Therefore, differences between the two are elucidated by the timeframe considered by resilience analysis being far greater in scope that risk assessment. Risk assessment tends to focus on both the likelihood and consequences of a given threat to an individual system component, such as a piece of infrastructure or institution with the aim of ensuring protection, response capability for the individual system components. Given its long term perspective, resilience analysis also focuses on less probable but high consequence threats, especially with the aim of avoiding cascading potential system failure. Furthermore, risk assessment focuses on preventing failure of a specific system component, while resilience analysis focuses on preventing but also on recovering entire systems from low probability adverse events which have the potential to cause cascading effects on an entire system as well as between several inter-connected systems [16]. Both approaches are specialized for different domains. While resilience analysis deals with broader more complex threats and concepts as well as a longer timeframe, risk management gives individual system elements the necessary level of detailed focus and places emphasis on better known, more probable and less harmful events which can be evaluated in greater certainty both in terms of impact and cost. Despite all of this, resilience analysis and risk assessment are compatible considering the fact they both seek to prevent negative outcomes and remove weaknesses from systems/components while focusing on differing levels of analysis and time scales. Both employ quantitative, semi-quantitative and qualitative methods to track and evaluate risk.

For Linkov and Palma-Oliveira [1], the relationship between risk assessment and resilience analysis can be seen as complimentary due to two factors: Firstly, they start from opposite starting points. Risk Assessment, as a bottom-up approach starts from data. The risk assessment process starts with data collection and progresses through modelling to characterization and visualization of risk for the purpose of risk management. Resilience takes a top-down approach starting with assessing the values of stakeholders as well as their critical functionality criteria, then through decision models it progresses towards the generation of metrics and data that ultimately can inform risk assessments. Secondly, one can consider risk assessment to be the preliminary phase to resilience analysis. It provides the first elements needed to trigger, or not, the need for resilience analysis. This is particularly true in the case of low-probability, high consequence risks of the distante future, such as those associated with climate change, large-scale cybersecurity threats, or severe weather events on the coasts [1; pp14-18]. Even though resilience analysis is typically used on a system wide level it is necessary to state that resilience analysis can be applied to lower level system areas and can therefore function in the areas typically considered the domain of risk assessment and in conjunction with it.

COMPARING RESILIENCE MANAGEMENT AND RISK MANAGEMENT

Risk management is defined by, the risk management vocabulary [9], as the coordination of all activities intended to direct and control an organization with regard to risk. The risk management process is defined as a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing risk [9].

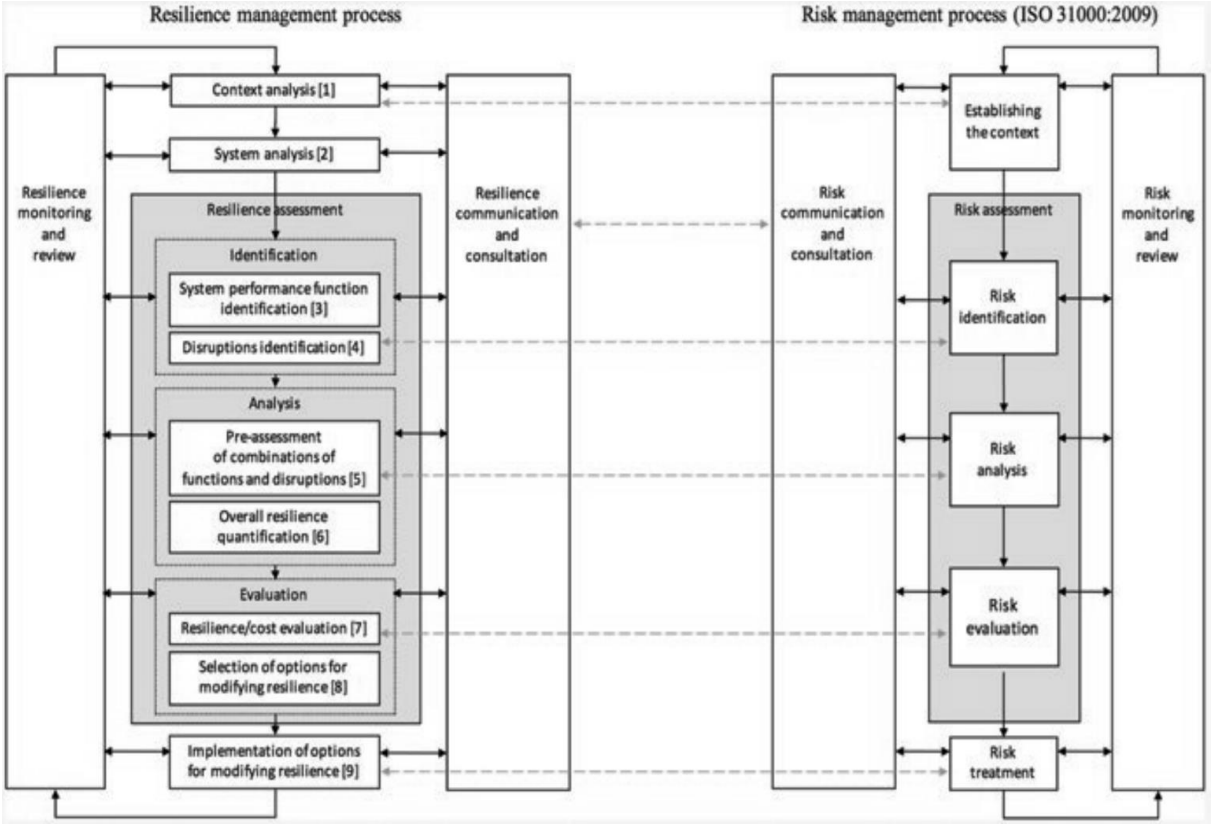

Figure 1. Comparison of the resilience management process and the risk management process [17].

Due to the relative novelty of the field a comprehensive definition of resilience management has yet to be generated. This issue is illustrated by an example of an existing definition provided by Teoh and Zadeh [2]. The definition states that resilience management is – "the ability of an organization to survive an unscheduled disruption or major crisis through its adaptability using proven and integrated risk management, crisis management, and business continuity management processes". The definition merely subsumes other concepts of risk and crisis management within itself. They further build on this however, by defining resilience management to be the act of developing overall situation awareness, demystifying inherent threats, and reducing risk and improving organizational efficacy with restoration plans. Furthermore, Häring et all. [17] define resilience management as an "iterative process that can be decomposed into sequential steps". They go on to specify nine steps for the resilience management process which they place within a resilience management cycle. Therefore, the working definition of resilience analysis in this article will be its characteristics as defined by Häring et all [17] in the resilience management cycle as outlined below.

Figure 1, developed by Haring [17], allows for a comparison of the 8-step resilience management process as described above with the risk management process as determined by the ISO 31000 standard.

A step by step comparison of the resilience and risk management procedure reveals several key factors. One key distinction between risk management and resilience management is the fact that the latter analyses potential disruption events with the aim of maintaining the functioning of a given system during and after a disturbance, with the goal of having it recover to a lower, same or even better state of equilibrium. Risk management, on the other hand, seeks to prevent the failure of the individual system component by shielding it from identified risk factors. When reviewing characteristic 1 and 2 of the resilience management process, given the fact that resilience management is more system focused than risk management, it distinguishes between defining the context and understanding the system under study, this is necessary due to the fact that threats can have impacts felt through one or many systems due to their inter-connected nature and due to the fact that the threat level of an individual disturbance event depends on the characteristics of the system itself. Risk management is focused more narrowly on individual system components and seeks to, above all else, determine the context so as to be able to carry out its tasks and identify specific knowable risks to a system component. When reviewing step 5 of the resilience management process it is evident that resilience management differs from risk management in that the latter seeks to analyze potential risks and neglects the interplay between system section characteristics and the risks themselves while resilience management seeks to assess critical combinations of both system functions and disruptions as well as an overall resilience assessment of critical combinations.

COMPARING AND CONTRASTING EXISTING METHODOLOGIES FOR MEASURING RISK AND RESILIENCE

As has been stated above in the article, both resilience analysis and risk assessment employ quantitative, semi-quantitative and qualitative methods to track and evaluate risk. The IEC 31010:2019 Risk management – Risk assessment techniques standard [12] compliments the ISO/IEC 31000 norm and provides further guidelines for the selection and application of methods and techniques of risk assessment. The applicability of tools used for risk assessment was presented in Table 1.

Table 1. Applicability of tools used for risk assessment [12]. SA – strongly applicable, A – applicable, NA – not applicable.

Tools and techniques	Risk assessment process				
	Risk identification	Risk analysis			Risk evaluation
		Consequence	Probability	Level of risk	
Brainstorming	SA	NA	NA	NA	NA
Structured or semi-structured Interviews	SA	NA	NA	NA	NA
Delphi	SA	NA	NA	NA	NA
Check-lists	SA	NA	NA	NA	NA
Primary hazard analysis	SA	NA	NA	NA	NA
Hazard and operability studies(HAZOP)	SA	SA	A	A	A
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA
Environmental risk assessment	SA	SA	SA	SA	SA
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA
Scenario analysis	SA	SA	A	A	A
Business impact analysis	A	SA	A	A	A
Root cause analysis	NA	SA	SA	SA	SA
Failure mode effect analysis	SA	SA	SA	SA	SA
Fault tree analysis	A	NA	SA	A	A
Event tree analysis	A	SA	A	A	NA
Cause and consequence analysis	A	SA	SA	A	A
Cause-and-effect analysis	SA	SA	NA	NA	NA
Layer protection analysis (LOPA)	A	SA	A	A	NA
Decision tree	NA	SA	SA	A	A
Human reliability analysis	SA	SA	SA	SA	A
Bow tie analysis	NA	A	SA	SA	A
Reliability centered maintenance	SA	SA	SA	SA	SA
Sneak circuit analysis	A	NA	NA	NA	NA
Markov analysis	SA	SA	NA	NA	NA
Monte Carlo simulation	NA	NA	NA	NA	SA
Bayesian statistics and Bayes Nets	SA	SA	NA	NA	SA
FN curves	A	SA	SA	A	SA
Risk indices	A	SA	SA	A	SA
Consequence/probability matrix	SA	SA	SA	SA	A
Cost/benefit analysis	A	SA	A	A	A
Multi-criteria decision analysis(MCDA)	A	SA	A	SA	A

In order to ensure an effective way of managing risk, it is necessary to select an acceptable risk identification, analysis and evaluation method. The ISO 31010 norm [12] provides 31

methods for risk assessment, some of which are widely applied in terms of risk identification, evaluation and assessment, while others only focus on a certain risk assessment phase. From all of these methods, it is necessary to point out the FMEA (Failure modes and effects analysis) – which is a widely used method, applicable in all situations which can be used to identify significant number of errors within a system. There are no standardized approaches, methodologies and techniques for the evaluation of resilience, nor is a standardization of these methods foreseen in the versions of the ISO norms currently under development. In the literature authors list several methods which are applied in certain case studies as well as systematize approaches and methods to be used in different steps in the development of resilience management systems. Based on the literature reviewed, Figure 2, located below, provides approaches and methods for different steps which are considered to be relevant and potentially applicable for resilience assessments.

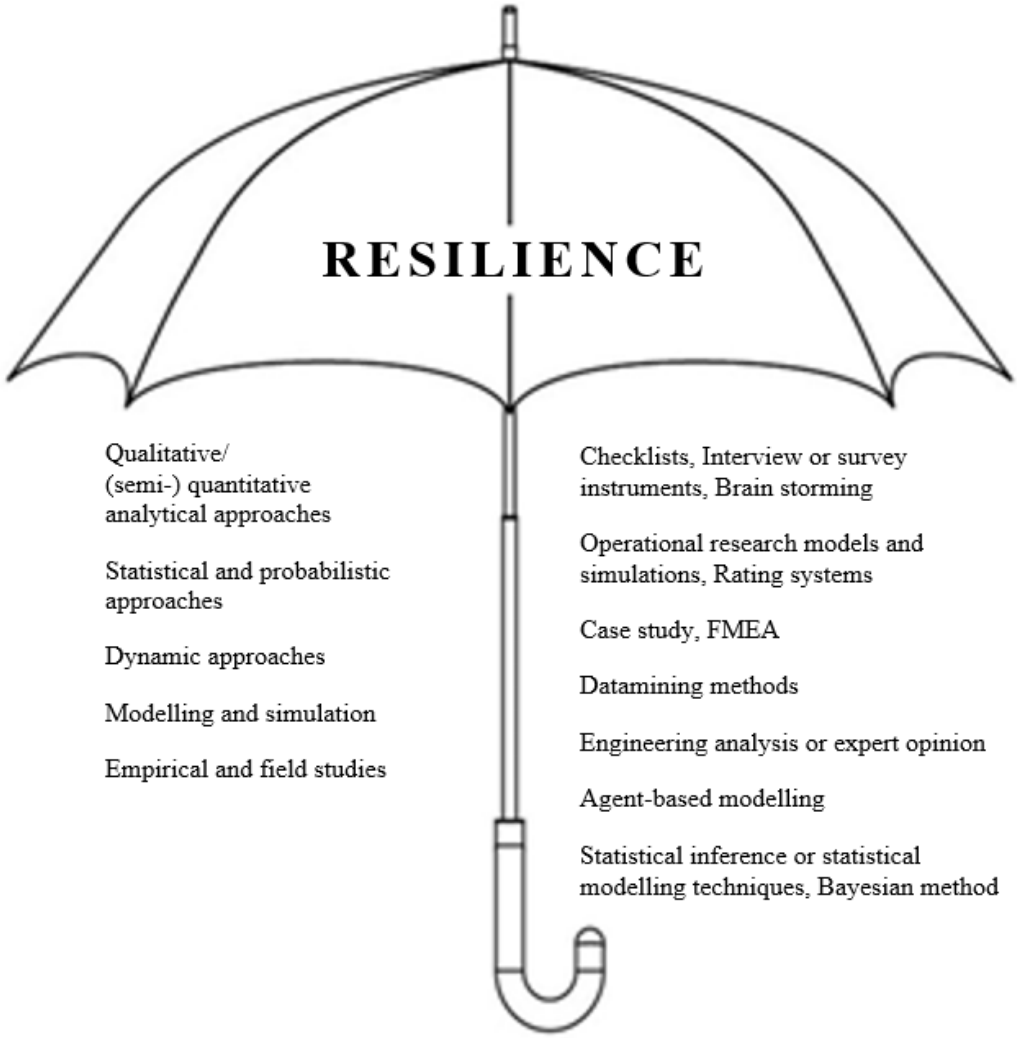

Figure 2. Approaches and methods (techniques) to resilience assessment.

In order for a certain approach or methodology to be fit for use, these are some of the key criteria which must be fulfilled:

1.) the application procedure of a certain methodology (method) must be clearly defined and understandable to the users,
2.) the methodology must ensure objective and repeatable results,
3.) the methodology must be successfully demonstrated both in a controlled and real world environment,

4.) the methodology must be independently evaluated,
5.) the methodology must demonstrate robustness,
6.) the results obtained via the application of different methods should be comparable.

Examples of resilience and risk assessment will be developed in further research using various methods. Examples for resilience assessments of materials to corrosion as well as risk assessment of the likelihood of corrosion will be provided using the Brainstorming technique, the Cause and effect analyses and the FMEA method.

CONCLUSION

Considering the analysis conducted in the article it is possible to concluded that demands to provide standardizations for the areas of risk and resilience are ever-increasing. A large number of norms pertaining to the area of resilience is currently being codified. As the article has demonstrated the initial analytical steps in the area of both risk and resilience share certain characteristics but differ in others. Risk assessment focuses on preventing failure of a specific system component, while resilience analysis focuses on preventing but also on recovering entire systems from low probability adverse events. Furthermore, the broader concept of risk management is focused more narrowly on individual system components while resilience management is more system focused. Despite their similarities, both approaches differ in terms of scale and the temporal dimension. As regards to the methodologies employed, both resilience analysis and risk assessment share a strong level of similarity in this domain as well, with both relying on quantitative, semi-quantitative and qualitative methods to track and evaluate risk. This being said it must be concluded that there is still no clearly defined delineation between the two concepts in the literature for which there is a pressing need due to their inherent difference and interoperability.

Taking all of this in to account it is possible to conclude that the risk assessment & management approach and the resilience analysis & management approach differ between each other, among other things, in terms of the level of analysis, the time-frame within which they study the impact of events as well as the steps they take to manage these concerns. Despite this, it is necessary to state that the resilience analysis and management approach can be applied to lower level system areas and can therefore function in the domain typically associated with risk assessment and in conjunction with it.

REFERENCES

[1] Linkov, I. and Palma-Oliveira, J.M., eds.: *Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains.* Springer Netherlands, 2017, http://dx.doi.org/10.1007/978-94-024-1123-2,
[2] Teoh, S.Y. and Zadeh, H.S.: *Strategic Resilience Management Model: Complex Enterprise Systems Upgrade Implementation.* PACIS 2013 Proceedings, 2013,
[3] ISO 22300:2021: *Security and resilience – Vocabulary*. https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en, accessed 8th April 2021,
[4] ISO/TS 22331:2018: *Security and resilience – Business continuity management systems – Guidelines for business continuity strategy*.
[5] ISO/TS 22375:2018: *Security and resilience – Guidelines for complexity assessment process.*
[6] ISO 22320:2018: *Security and resilience – Emergency management – Guidelines for incident management.*
[7] ISO 22316:2017: *Security and resilience – Organizational resilience – Principles and attributes.*

[8] ISO 22325:2016: *Security and resilience – Emergency management – Guidelines for capability assessment.*
[9] ISO Guide 73:2009: *Risk management – Vocabulary.* https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en, accessed 10th March 2021,
[10] ISO 9001: 2015: *Quality management systems – Requirements.*
[11] ISO 31000: 2018: *Risk management – Guidelines.*
[12] IEC 31010:2019: *Risk management – Risk assessment techniques.*
[13] Connelly, E.B., et al.: *Features of resilience.* Environment Systems and Decisions **37**(1), 46-50, 2017, http://dx.doi.org/10.1007/s10669-017-9634-9,
[14] Linkov, I. and Trump, B.D.: *The Science and Practice of Resilience.* Springer, 2019, http://dx.doi.org/10.1007/978-3-030-04565-4,
[15] Scholz, R.W.; Blumer, Y.B. and Brand, F.S.: *Risk, vulnerability, robustness, and resilience from a decision-theoretic perspective.* Journal of Risk Research **15**(3), 313-330, 2012, http://dx.doi.org/10.1080/13669877.2011.634522,
[16] Kinzig, A.P., et al.: *Resilience and regime shifts: assessing cascading effects.* Ecology and Society **11**(1), No. 20, 2006,
[17] Häring, I., et al.: *Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies.* In: Linkov, I. and Palma-Oliveira, J., eds.: *Resilience and Risk.* NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht, 2017, http://dx.doi.org/10.1007/978-94-024-1123-2_2.