Determinants of Dynamic Resilience Modelling in Critical Infrastructure Elements

David Rehak

Faculty of Safety Engineering, VSB-Technical University of Ostrava, Czech Republic. E-mail: david.rehak@vsb.cz

Vendula Onderkova

Faculty of Safety Engineering, VSB-Technical University of Ostrava, Czech Republic. E-mail: Vendula.onderkova@vsb.cz

Veronika Brabcova

Faculty of Safety Engineering, VSB-Technical University of Ostrava, Czech Republic. E-mail: veronika.brabcova@vsb.cz

Resilience is an important factor in protecting critical infrastructure elements against the negative effects of disruptive events. The higher the resilience level, the longer the element can withstand disruptive events. Consequently, the impact of disruption to the functionality of services necessary to the population is minimized. However, resilience is dependent on the action of the disruptive event, and as a result, its level is developed dynamically over time. This dynamic development is influenced by several positive and negative factors. Based on the above, the article examines the issue of modelling dynamic resilience in critical infrastructure elements. Particular attention is paid to the factors influencing resilience in critical infrastructure elements and the harmful nature of disruptive events. Using these factors, the basis of dynamic resilience modelling is then defined.

Keywords: Critical infrastructure, Resilience, Elements, Determinants, Disruptive event, Dynamic modelling.

1. Introduction

Several recent professional publications investigate the evaluation of static resilience in critical infrastructure elements (Rehak et al., 2018b; Bertocchi et al., 2016; Prior, 2015; Petit et al., 2013). Static resilience is evaluated during the zero-intensity phase of a disruptive event, that is, at the moment when it has not yet started affecting the critical infrastructure element.

The static resilience level is an important starting point for dynamic modelling, but it loses its predictive value when the course of the disruptive event has already started affecting the critical infrastructure element, consequently making it impossible to observe the dynamic development of resilience and predicatively identify weak points that may be the cause of inadequate protection, followed by the failure of the critical infrastructure element's performance.

Drawing on this observation, the article defines the determinants and basis for dynamic resilience modelling in critical infrastructure elements dependent on the effect of a disruptive event. The article can thus be seen mainly as the basis for subsequent establishment of appropriate methodology and the process of dynamic resilience modelling itself.

2. Methods of modelling the progress of functions

Modelling the progress of functions is currently necessary for supporting predictive engineering in the field of security engineering and can be applied to both the occurrence of disruptive events and resilience of critical infrastructure elements. Methods used for this purpose include graphical-analytical methods (e.g., network analysis), statistical methods (e.g., Bayesian kernel, testing of statistical hypotheses) and mathematical methods (e.g., topology, Euler's method and pair comparison for interdependence).

The first and most logical and practical method for modelling the progress of functions is network analysis. Work by authors Setola and Theocharidou (2016) more closely incorporates Input-Output Inoperability (IIM) and network-based methods. Other authors engaged in network analysis are Omer et al. (2014), who describe the methodology used to measure resilience in organizational networks. Inspired by graph theory, this method permits critical pathways to be created and then used to identify critical nodes that could cause significant network damage.

Baroud and Barker (2014) use statistical methods in their contribution, addressing the problem of resilience modelling with the Bayesian kernel method. Some publications

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

Published by Research Publishing, Singapore.
ISBN: 978-981-11-2724-3; doi:10.3850/978-981-11-2724-3_0070-cd

focus directly on dynamic resilience modelling and time projection in modelling. Wears and Perry (2006) apply statistics in their contribution by testing statistical hypotheses and focusing on dynamic modelling of systems, or more precisely, on resilience representation, and by examining the behaviour of the system as a whole and its reaction to change over time. This contribution focuses on the emergency department in the health care sector.

Buor (2015) and Bühne et al. (2003) deal with interdependence, which is modelled using Euler's method and the pairing method. Each solves a slightly different area while using similar approaches. Buor (2015) addresses the dynamic modelling of systems to analyse the structural behaviour of the model by interacting with disaster preparedness, environmental instability and resilience. He uses Euler's numerical method of analysis to validate and check the model, i.e., the technique for quantitative evaluation of the structural behaviour of inventories acting as variables that modify certain input values based on the results of interviews. By contrast, Bühne et al. (2003) are concerned with identifying common types of dependencies that are useful to the community for modelling functions expressing the interdependence between variation points and variants.

The last significant method for modelling the progress of functions is the integration of relevant properties of topological network structures into spatial time modelling (Wei et al., 2013). The authors comment on the resilience of the power grid in the case of bad weather. This work develops an analytical formulation for a major failure and recovery of energy distribution during adverse weather. These characteristics represent new knowledge for dynamic failure and subsequent recovery. According to the proposed model, the authors define dynamic resilience. Their contribution also discusses failure and recovery processes, which they subject to further research using flexibility metrics to identify the least durable areas and the quickest recovery time.

3. Determinants of dynamic resilience modelling

The factors influencing performance of a critical infrastructure element can be classified into two basic groups: negative and positive. While negative factors cause a decrease in performance of the element through its vulnerabilities, positive factors prevent this decrease and keep the element in a fully functional state or mitigate impact on the element (Rehak et al., 2018a). These factors therefore determine the progress of dynamic resilience in critical infrastructure elements.

Negative factors are disruptive events (i.e. naturogenic, technogenic and anthropogenic), concrete factors that determine their hazard level. These factors include the intensity, progress of escalation, duration of exposure and progress of de-escalation of the disruptive event. These factors are further influenced by specific measurable items that determine the intensity and progress of a disruptive event in its individual phases.

Conversely, positive factors are measures and processes that lead to resilience in a critical infrastructure element (i.e. robustness, recoverability, adaptability). When a disruptive event occurs, however, only an element's robustness, its essence, will immediately mitigate the effects of a disruptive event. Factors determining an element's robustness include crisis preparedness, redundancy, detection capability, responsiveness and physical resilience. These factors are further influenced by specific measurable items that determine the static (i.e., default) level of robustness of the critical infrastructure element prior to the occurrence of a disruptive event.

3.1 *Factors determining the robustness of critical infrastructure elements*

The term resilience was first defined in 1973 in connection with the resistance and stabilization of ecological systems (Holling, 1973). Over time, the concept of resilience has been progressively applied to other disciplines such as sociology, psychology and economics, and later also in engineering. In the context of critical infrastructure, resilience was first defined in 2009 as "the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event" (National Infrastructure Advisory Council, 2009). Currently, Resilience in a critical infrastructure system can be viewed as a quality that reduces vulnerability, minimizes the consequences of threats, accelerates response and recovery, and facilitates adaptation to a disruptive event (Rehak et al., 2018a).

Resilience in elements of a critical infrastructure system is defined by three basic properties: robustness, recoverability and adaptability. Robustness is the ability of an element to absorb the effects of a disruptive event. These effects can be absorbed, for example, through the structural features of buildings or technologies used (i.e., structural robustness) or through security measures (i.e., security robustness) (Rehak et al., 2018a). Recoverability is the ability of an element to restore its activity to the original (required) level of service after a disruptive event ends.

Recoverability in critical infrastructure is seen as repairability; therefore, only repairing or replacing damaged or destroyed components is considered. Adaptability is the ability of a critical infrastructure subject (i.e., an organization) to prepare an element for the recurrence of a previous disruptive event (Rehak et al., 2018b). It represents the dynamic, long-term ability of an organization to adapt to changes in situations.

As noted above, absorbing the effects of a disruptive event is achieved solely through robustness. From this point of view, robustness is responsible for the rate of decrease in an element's resilience during a disruptive event. If a robustness level of 100 % is achieved, the element becomes fully resistant to the effects of the disruptive event. This means that it can withstand its effects completely without any appreciable negative effects on its service performance.

Robustness in a critical infrastructure system element is defined by five fundamental variables: critical preparedness, redundancy, ability to detect a disruptive event, responsiveness and physical resilience (Rehak et al., 2018b). Crisis preparedness is a set of measures to increase a critical infrastructure element's preparedness for disruptive events. Redundancy provides the ability to instantly replace the performance of the disrupted part of an element or to enhance its capabilities. The ability to detect a disruptive event is the probability or time to detect a disruptive event compared to responsiveness, which is the likelihood or the period of time of intervention that leads to eliminating the cause of the disruptive event or minimizing its consequences. The primary variable is physical resilience of the element, which represents a set of technical means and organizational or systemic measures to increase the physical resilience of a critical infrastructure element to disruptive events (Lovecek et al., 2010).

Static resilience in critical infrastructure elements can currently be evaluated through a number of specific methods. Critical Infrastructure Elements Resilience Assessment – CIERA (Rehak et al., 2018b), Resilience Measurement Index – RMI (Petit et al., 2013) and the Guidelines for Critical Infrastructure Resilience Evaluation (Bertocchi et al., 2016) are regarded as the most suitable.

3.2 *Factors determining a disruptive event's hazard level*

A disruptive event is defined as the harmful effects of forces and phenomena caused by human activity, natural influences and accidents that threaten a critical infrastructure element (Rehak et al., 2018b). The degree of a disruptive event's adverse effect on a critical infrastructure element is expressed as the level of hazard. In the context of evaluating dynamic resilience in critical infrastructure elements, hazard can be defined by four fundamental variables: escalation, exposure, de-escalation and intensity of the disruptive event. This view of the breakdown of disruptive events is according to the method of identifying common types of dependencies (Bühne et al., 2003).

Escalation is the initial phase of a disruptive event and determined by the escalation function and the level of its intensity reached in the final phase. Exposure is the duration of a disruptive event delimited by its escalation and de-escalation phases. This variable can be broken down into any number of sub-sections depending on the change in intensity of the disruptive event. This definition is based on Bayesian statistics, which works with probability in relation to unknown factors from the past and an estimate of resilience (Baroud and Barker, 2014). De-escalation is the final phase of a disruptive event and determined by the de-escalation function and the starting level of its intensity in the initial phase.

The final variable determining the hazard level of a disruptive event is its intensity. The intensity of a disruptive event is a common factor during escalation, exposure and de-escalation in a disruptive event. This factor describes the degree of damage caused by a disruptive event and its ability to impact negatively on a critical infrastructure element. During the progress of a disruptive event, the intensity level can vary greatly.

The hazard level of a disruptive event can currently be evaluated using several specific methods, such as Event Tree Analysis – ETA (IEC, 2010) or Fault Tree analysis – FTA (IEC, 2006).

4. Starting points for dynamic resilience modelling

The essence of a critical infrastructure element is its ability to permanently provide services necessary to the functioning of society. The indicator of the level of service provided is its performance, which is influenced by negative and positive factors. The effects of negative factors decrease an element's performance. These factors include components that determine the progress and intensity of a disruptive event. By contrast, the effects of positive factors mitigate the negative impact of a disruptive event on a critical infrastructure element and maintain the element's performance at a desired level. These factors are components that determine the element's resilience.

Mitigation of disruptive events, however, results in a dynamic decline in the level of resilience over time. The core of modelling dynamic resilience in critical infrastructure elements dependent on the occurrence of disruptive event is therefore the quantification of these factors and the mathematical expression of their correlation (Buor, 2015). Hence, dynamic resilience modelling is based on the correlation between the performance and resilience of the critical infrastructure element and the disruptive event (Fig. 1). Evaluating resilience in this way, however, is from a managerial point of view, and the result of evaluation consists only of weaknesses found without any deeper context of the negative impact of a certain disruptive event on the element's performance.

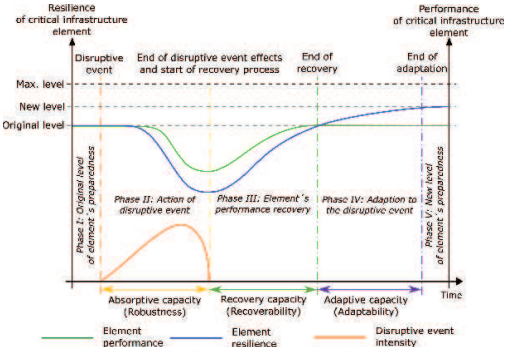

Fig. 1. Phases of the resilience cycle in relation to an intensity of the disruptive event and performance of a critical infrastructure element (Rehak et al., 2018b).

The starting point of modelling dynamic resilience in a critical infrastructure element dependent on the action of a disruptive event is to define the dependencies between resilience and disruptive events. A disruptive event's progress is characterized by three phases: escalation, exposure and de-escalation (Jeong, 2008). All three phases can occur with varying levels of intensity, which is thus a fourth change in evaluating a disruptive event's hazard level. Resilience evaluation, though, is done in four steps:

- Phases I and V: a disruptive event does not affect these phases and static resilience can be evaluated.
- Phase II: this is when the disruptive event occurs and when resilience or the factors of its one component, which is robustness, decreases.
- Phase III: this is the element's performance recovery phase, when resilience is restored to its original level.
- Phase IV: this phase is adaptation to the disruptive event, when resilience is strengthened (Labaka et al., 2015) against a specific disruptive event and results in a new, higher level of resilience in the critical infrastructure element.

Phase II is crucial for modelling dynamic resilience in a critical infrastructure element dependent on the occurrence of a disruptive event. During this phase, resilience declines dynamically because of a disruptive event. The initial resilience level (i.e., static resilience) is evaluated through a suitable methodology (e.g., Rehak et al., 2018b) in Phase I, when a disruptive event does not affect the element. The evaluation's result is an expression of percentage of the static element's resilience level relative to the potential impact of a particular disruptive event. This level is then dynamically modelled in Phase II in relation to the disruptive event's hazard level.

The core of dynamic resilience modelling is to divide the disruptive event into three phases: escalation, exposure and de-escalation (Fig. 2). Each phase evolves in a certain way over time, but in general, it can be said that escalation grows in intensity over time, whether as a rapid or gradual increase. Increased intensity during a disruptive event results in a directly proportional reduction in resilience. The exposure phase can take several forms, namely constant, increasing or decreasing, as a result of which the element's resilience is also variable. During the de-escalation phase, decrease in resilience is once again gradual until the intensity of the disruptive event reaches a zero value, when the resilience level either stagnates or slowly recovers (Labaka et al., 2015).

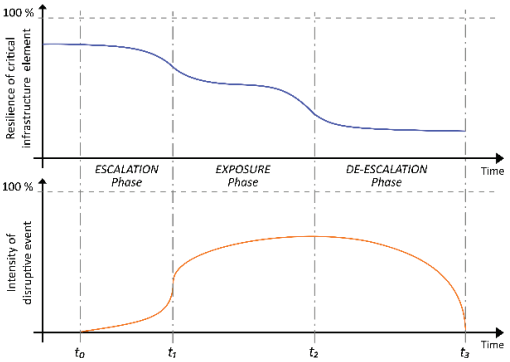

Fig. 2. Graphic depiction of dynamic resilience in response to a disruptive event.

Dynamic resilience is then expressed by a curve connecting the levels of static resilience values R_0 to R_n over time, and its function is derived from the disruptive event function. For example,

an exponential increase in the intensity of a disruptive event, which is initially gradual and then steep, will result in an exponential drop in the element's resilience, which is also initially gradual and then steep. Similarly, this will also be the case for a quadratic, linear, inverse quadratic or inverse power function (Fig. 3).

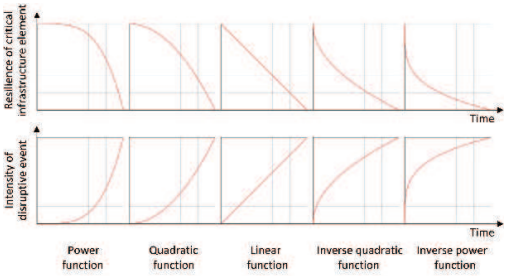

Fig. 3. Relationship between escalation functions of a disruptive event and dynamic resilience functions.

The value of the new R_{n+1} resilience level is always calculated from one phase of the disruptive event using direct proportionality and the expression of percentage of the dependence on development over time. To calculate a new resilience level R_{n+1}, the initial resilience value R_n, which at a given phase always has a certain level considered 100%, must therefore be known.

5. Conclusion

The performance of critical infrastructure elements is influenced by several internal and external factors that can be classified as positive and negative. While negative factors cause a decrease in performance of the element through its vulnerabilities, positive factors prevent this decrease and keep the element in a fully functional state or mitigate impact on the element. Positive factors include measures and processes that maintain the resilience of critical infrastructure elements.

Dynamic resilience modelling represents a significant shift in the area of critical infrastructure protection. The benefit of dynamic resilience modelling is the possibility to predictively evaluate resilience in critical infrastructure elements during a disruptive event in accordance with an assumed scenario. Based on the results of the evaluation, weaknesses can be identified, and adequate precautions applied to increase the resilience of an element to a disruptive event.

Acknowledgement

This research was supported by the Ministry of the Interior of the Czech Republic under Project VI20152019049 'RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems' and by the VSB–Technical University of Ostrava under Project SP2018/116 'Dynamic Modelling of Resilience of Critical Infrastructure Elements'.

References

Baroud, H. and K. Barker (2014). Bayesian Kernel Methods for Critical Infrastructure Resilience Modeling. In M. Beer, S. Au, and Hall, J.W. (Eds.), *Vulnerability, Uncertainty, and Risk: Quantification, Mitigation, and Management*, pp. 687-694. American Society of Civil Engineers. DOI: 10.1061/9780784413609.070

Bertocchi, G., S. Bologna, G. Carducci, L. Carrozzi, S. Cavallini, A. Lazari, G. Oliva, and A. Traballesi (2016). *Guidelines for Critical Infrastructure Resilience Evaluation.* Italian Association of Critical Infrastructures' Experts.

Buor, J.K. (2015). Applying System Dynamics Modelling To Building Resilient Logistics: A Case of the Humber Ports Complex, Doctoral Thesis, The University of Hull.

Bühne, S., G. Halmans, and K. Pohl (2003). Modelling Dependencies between Variation Points in Use Case Diagrams. In *Workshop on Requirements Engineering - Foundation for Software Quality (REFSQ '03)*, pp. 59-69. Klagenfurt/Velden.

Holling, C.S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics 4*, 1-23. DOI: 10.1146/annurev.es.04.110173.000245

IEC 61025 (2006). *Fault Tree Analysis.* International Electrotechnical Commission.

IEC 62502 (2010). *Analysis techniques for dependability – Event tree analysis.* International Electrotechnical Commission.

Jeong, H. (2008). *Understanding Conflict and Conflict Analysis.* SAGE Publications.

Labaka, L., J. Hernantes, and J.M. Sarriegi (2015). A framework to improve the resilience of critical infrastructures. *International Journal of Disaster Resilience in the Built Environment 6(4)*, 409-423.

Lovecek, T., J. Ristvej, and L. Simak (2010). Critical Infrastructure Protection Systems Effectiveness Evaluation. *Journal of Homeland Security and Emergency Management 7(1)*, Article No. 34.

National Infrastructure Advisory Council (2009). *Critical Infrastructure Resilience Final Report and Recommendations.* U.S. Department of Homeland Security.

Omer, M., A. Mostashari, and U. Lindemann (2014). Resilience Analysis of Soft Infrastructure Systems. *Procedia Computer*

Science 28, 873-882. DOI: 10.1016/j.procs.2014.03.104

Petit, F., G. Bassett, R. Black, W. Buehring, M. Collins, D. Dickinson, R. Fisher, R. Haffenden, A. Huttenga, M. Klett, J. Phillips, M. Thomas, S. Veselka, K. Wallace, R. Whitfield, and J. Peerenboom (2013). *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience.* Argonne National Laboratory.

Prior, T. (2015). *Measuring Critical Infrastructure Resilience: Possible Indicators – Risk and Resilience Report 9.* Eidgenössische Technische Hochschule Zürich.

Rehak, D., P. Senovsky, and S. Slivkova (2018a). Resilience of Critical Infrastructure Elements and its Main Factors. *Systems 6(2)*, Article No. 21. DOI: 10.3390/systems6020021

Rehak, D., P. Senovsky, M. Hromada, L. Pidhaniuk, Z. Dvorak, T. Lovecek, J. Ristvej, B. Leitner, E. Sventekova, and L. Maris (2018b). *Methodology of the Critical Infrastructure Elements Resilience Assessment.* VSB–Technical University of Ostrava.

Setola, R. and M. Theocharidou (2016). Modelling Dependencies between Critical Infrastructures. In R. Setola, V. Rosato, E. Kyriakides, and E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach*, pp. 19-42. Springer Nature. DOI 10.1007/978-3-319-51043-9_2

Wears, R.L. and S.J. Perry (2006). A Systems Dynamics Representation of Resilience. In *Resilience Engineering International Symposium.* Resilience Engineering Association.

Wei, Y., Ch. Ji, F. Galvan, S. Couvillon, and G. Orellana (2013). Dynamic modeling and resilience for power distribution. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 85-90. Institute of Electrical and Electronics Engineers. DOI: 10.1109/SmartGridComm.2013.6687938