CHEMICAL ENGINEERING TRANSACTIONS
VOL. 86, 2021
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Sauro Pierucci, Jiří Jaromír Klemeš

ISBN 978-88-95608-84-6; **ISSN** 2283-9216
DOI: 10.3303/CET2186093

Assessing the Resilience of an Acute-care Hospital in the Context of Current Security Threats

Alena Splichalova[a,*], Katerina Vichova[a], Jarmil Valasek[b], Frantisek Paulus[b]

[a]Charles University, Faculty of Social Sciences, Smetanovo nabrezi 6, 110 01 Prague 1, Czech Republic
[b]Population Protection Institute, Na Luzci 204, 533 41 Lazne Bohdanec, Czech Republic
alena.splichalova@vsb.cz

Acute-care hospitals are the most important elements of the critical infrastructure in the area of healthcare in the Czech Republic. The disruption or failure of the services they provide would have a significant impact on the lives and health of the population. In recent years, these hospitals have often been threatened by the effects of various disruptive events, e.g. cyber attacks, disruptions of electricity supply or physical attacks. For this reason, it is necessary that hospitals have an adequate level of resilience, which would allow them to reduce the magnitude and/or duration of the disruptive events. The effectiveness of hospital resilience depends on their ability to anticipate, absorb, adapt to and/or rapidly recover from disruptive events. Currently, however, there are no available data about the resilience of hospitals of this type. For this purpose, the article is aimed at assessing the resilience of selected acute-care in the context of current disruptive events. Resilience is assessed using the CIERA method in the context of the effects of selected security threats, i.e. cascading, cybernetic and physical.

1. Introduction

Acute-care hospitals provide health care on a continuous basis. For this reason, their infrastructure must be highly resilient to the effects of security threats that may cause disruption or failure of the healthcare provided (Jouini and Rabai, 2016). These have mainly been cyber attacks (e.g. Czech Republic, March 2020; United Kingdom, May 2017), electricity supply disruptions (e.g. United Kingdom, August 2019; Michigan, August 2003) or physical attacks (e.g. Czech Republic, December 2019; Illinois, October 2018).
The effective protection of hospitals from these threats is achieved with an adequate level of infrastructure resilience (NIAC, 2009). The starting point for infrastructure resilience management is their evaluation/measurement. Currently, there are also already several technical methods for assessing resilience that are able to assess the statistical level of resilience, though so far none of them have been used in this context. These include, in particular, the Critical Infrastructure Elements Resilience Assessment “CIERA method” (Rehak et al., 2019), Availability-based engineering resilience metric and its corresponding assessment methodology (Cai et al., 2018), Resilience Capacities Assessment for Critical Infrastructures Disruption: The READ Framework (Kozine et al., 2018), A Quantitative Method for Assessing Resilience of Interdependent Infrastructures (Nan and Sansavini, 2017) and others such as (Bertocchi et al., 2016; Prior, 2015; Petit et al., 2013).
The aim of this article is to perform an assessment of the resilience of the hospital with acute care in the context of current threats through a selected technical method. The resilience was assessed using the CIERA method (Rehak et al., 2019), namely in the context of cascading, cyber and physical threats. Weaknesses were identified and recommendations given for increasing resilience based on the results of the assessment.

2. Perception of resilience in the context of critical infrastructure

In the context of the critical infrastructure, resilience represents the internal preparedness of elements (it means important objects which ensuring the course of the whole critical infrastructure system) for disruptive events. It is also the ability of these subsystems to ensure and maintain their function during the course of the

Paper Received: 16 August 2020; Revised: 29 January 2021; Accepted: 15 April 2021
Please cite this article as: Splichalova A., Vichova K., Valasek J., Paulus F., 2021, Assessing the Resilience of an Acute-care Hospital In the context of Current Security Threats, Chemical Engineering Transactions, 86, 553-558 DOI:10.3303/CET2186093

negative impacts of the internal/external factors. Resilience can therefore be defined as the opposite of vulnerability; resilience and vulnerability are inversely related (Rehak et al., 2018a). Vulnerable subsystems lack resilience and, conversely, resilient subsystems aren't overly vulnerable.
On the basis of definition "the ability to absorb, adapt to and/or rapidly recover from a potentially disruptive event" (NIAC, 2009), it is evident that the resilience of individual elements is determined by their robustness, recoverability and adaptability.
Factors determining the resilience of elements of the critical infrastructure can be divided, on the basis of the definition given by the National Advisory Council (NIAC, 2009), into three basic groups: (1) factors determining robustness, i.e. ability of an element to absorb the effects of disruptive events, (2) factors determining recoverability, i.e. ability of an element to recover its function to the original (required) level of service provision after the end of the effects of the disruptive event and (3) factors determining adaptability, i.e. ability of an entity of critical infrastructure (organization) to prepare an element for the recurring effects of a disruptive event that has already occurred. The first two groups of factors determine the so-called technical resilience (Rehak et al., 2018a) and the third group of factors determines organization resilience (Denyer, 2017; Rehak, 2020). Technical resilience represents the protection of elements from the effects of disruptive events and their subsequent recovery, while organizational resilience consists in creating conditions in which elements may adapt to disruptive events that have already occurred. The individual factors and their components are presented in Figure 1.

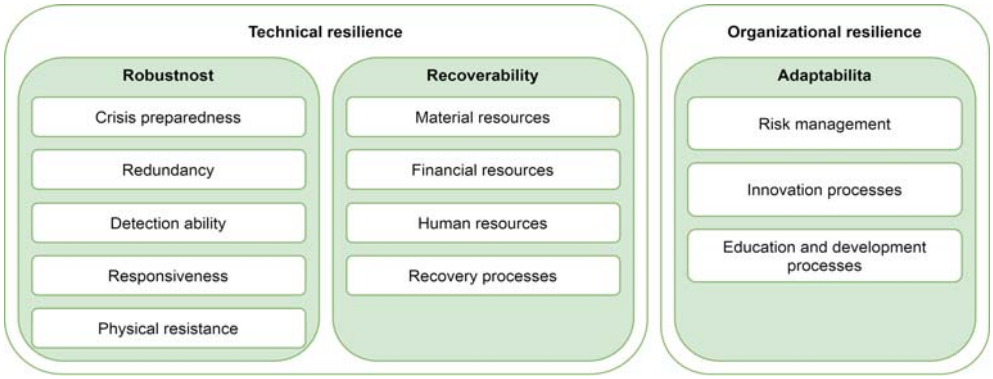

Figure 1: Factors determining the resilience of critical infrastructure elements (Rehak et al., 2018a)

Crisis preparedness is a set of measures for increasing the preparedness of an element of the critical infrastructure for disruptive events. Redundancy represents the ability of the immediate substitution of power of a disruptive part of an element or the strengthening of its capacity. Detection ability represents the probability and/or time of detection of a disruptive event. Responsiveness represents the probability and/or time of intervention leading to the elimination of the cause of the disruptive event or the minimization of its consequences. Physical resistance represents a set of technical means and organization or regime measures for the increase of physical resistance to elements of the critical infrastructure from disruptive events.
Material resources represent the availability of necessary components for the repair or replacement of damaged or destroyed parts of the element. Financial resources represent the availability of funds, or reserves, making it possible to finance a quick recovery of the element. Human resources represent the availability of staff with necessary qualifications. Recovery processes support the quick recovery of the required performance of the element.
Risk management represent significant internal organizational processes that are necessary for ensuring safety and increasing resilience in the prevention stage (Rehak et al., 2016). This management consists of the coordination of actions of the leadership and management of the organization with regard to risks (ISO 31000, 2018). The most important innovation processes, in terms of strengthening resilience, can be considered process and organizational, focusing on reliability and external security of technologies (OECD/Eurostat, 2005) Education and development processes can be divided into three main categories (Armstrong, 2014), which are knowledge (explicit and tacit), skills (e.g. technical, managerial, analytical, conceptual) and attitudes (reflecting the values that a particular person recognizes).

3. Case study of the Czech Republic

The following text is focused on the assessment of the static resilience of an acute-care hospital within the context of selected current security threats. Resilience is assessed using the CIERA method (Rehak et al., 2019) which is presented in Figure 2.

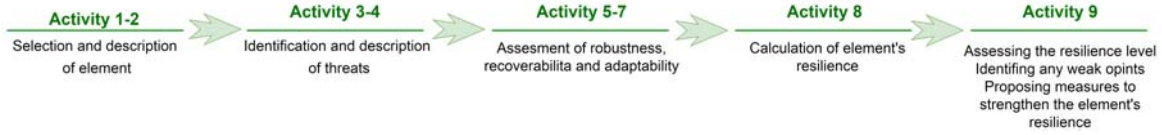

Figure 2: Procedure for assessing the resilience of critical infrastructure elements (Rehak et al., 2019)

An anonymized acute-care hospital located in an unnamed region of the Czech Republic was selected for the resilience assessment (Activity 1). The measurement of the resilience of this station was done in collaboration with the crisis manager of the assessed hospital.
Subsequently, a description of this hospital was made, consisting of its classification in the structure of the critical infrastructure and the description of its structural and performance parameters (Activity 2). The structural parameters of this hospital specify its topological structure and number of key technologies, i.e. departments. The performance parameter of an element is the number of inhabitants for which the hospital can provide care (see Table 1).

Table 1: Description of the assessed element of critical infrastructure

Element name	Acute-care hospital
Sector/Subsector	Healthcare/Provision of health services
Topological structure	Area element
List of key departments	1. Department of Neonatology; 2. Cardiac surgery; 3. Urgent admission; 4. Surgery; 5. Intensive Care Unit
Performance parameter	1.2 million inhabitants

The assessment of the resilience of this element will carried out against three selected threats, which were identified on the basis of their timeliness in the context of the current security situation (Activity 3). Specifically, these are cascading threats (Vichova and Hromada, 2019; Rehak et al., 2018b), cyber (Mantzana et al., 2020) and physical threats (Kampova et al., 2020). A description of these threats (Activity 4) is presented in Table 2.

Table 2: Description of threats against which the resilience of the element was assessed

	Description of selected current threats		
Threat:	Disruption of electricity supply	Cyber attack	Terroristic attack
Threat category:	Technogenic	Anthropogenic	Anthropogenic
Threat type:	Cascading	Cybernetic	Physical
Threat specification:	Disruption of electricity supply for 24 hours	Disruption of the internal system of information and communication technologies	Lone shooter terrorist attack

The following section presents the results of the assessment of robustness, recoverability and adaptability of the selected hospital. The first was the assessment of the robustness of this element (Activity 5), which consisted in assessing the current state (level) of the individual variables. Due to the large number of measurable items and intermediate calculations, only the final percentage results for selected threats are presented in the following Table 3. Subsequently, an assessment of the hospital's recoverability was carried out (Activity 6), which consisted in assessing the current state (level) of individual variables, i.e. material resources, financial resources, human resources and recovery processes, again for each threat separately. The results of the assessment of the recoverability against selected threats are presented Table 3.
The last component of resilience assessed was the adaptability of the hospital, i.e. organizational resilience of the hospital (Activity 7). This assessment was common to all selected threats and the assessment consisted of the assessment of the current state (level) of individual variables, i.e. risk management and innovation, education and development processes. The resulting level of organizational resilience of the hospital was calculated to be 64% against selected threats.
The main step of the assessment was the calculation of the resilience of the element (Activity 8). The level of resilience of the evaluated hospital was calculated as a weighted arithmetic mean of the factors by which it is determined (for more details see Rehak et al., 2019). The results of the assessment are presented in Table 3.

Table 3: Level of the hospital's resilience to selected threats

Selected current threats	Level of robustness	Level of recoverability	Level of adaptability	Resilience
Disruption of electricity	67 %	78 %	64 %	70 %
Cyber attack	76 %	79 %	64 %	73 %
Terroristic attack	56 %	66 %	64 %	62 %

The final activity of the hospital's resilience assessment was the evaluation of the level of resilience, identification of weak points and a proposal of measures for strengthening the resilience of the element (Activity 9). The assessment of the resilience level was calculated consecutively on the basis of comparative values (see Table 3) on three levels and the level of resilience is presented Table 4.

Table 4: Comparative table for assessing the resilience of the element (Rehak et al., 2019)

Selected current threats	Percentage level of robustness
High level of resilience	85 - 100%
Acceptable level of resilience	69 – 84%
Low level of resilience	53 – 68%
Unsatisfactory level of resilience	37 – 52%
Critical level of resilience	≤ 36%

The highest level where the resilience is calculated is the level of the element. In this case it can be stated that the hospital's resilience to a disruption of the electricity supply reached the level of 70% and disruption of the internal system of information and communication technology, the hospital's resilience reached the level of 73%, which represents an acceptable level of resilience duration throughout of the threat. In the case of a terrorist attack of a lone shooter, the hospital's resilience reached 62%, which represents a low level of resilience, which would have a negative impact on the provision of health care services.

Subsequently, it is possible to assess the resilience on the level of factors in order to identify weaknesses. The resilience of the majority of the variables reach high or acceptable levels. However, in the identification of weak points, it is necessary to focus attention on those factors that reach insufficient or critical levels of resilience. An overview of these factors is presented in Table 5.

Table 5: Identification of weakness in resilience of the assessed element of the critical infrastructure

Threats	Components of resilience	Factor with insufficient level of resilience	Factors with level of resilience
Disruption of electricity supply for 24 hours	Robustness		Time characteristics of the use of linkage and Technical means
	Recoverability	Allocation of the financial resources/reserves for recovery Preparedness of financial resources/reserves in time of need	
	Adaptability	Level of scenarios for disruptive events Implementation of management systems Evaluation of the training's effectivity	
Disruption of the internal system of ICT	Robustness	Evaluation/audit of the security and risk analysis Firewall/demilitarized zone	
	Recoverability	Allocation of the financial resources/reserves for recovery Preparedness of financial resources/reserves in time of need	
	Adaptability	Level of scenarios for disruptive events Implementation of management systems Evaluation of the training's effectivity	
Lone shooter terrorist attack	Robustness	Technical means Protective measures Regime measures	Cumulative probability of intruder detection The probability of intruder elimination
	Recoverability	Time horizon of repairing or replacing key technology Allocation of the financial resources/reserves for recovery Preparedness of financial resources/reserves in time of need Availability of human resources with required qualification Capacity of human resources	
	Adaptability	Level of scenarios for disruptive events Implementation of management systems Evaluation of the training's effectivity	

As there are three types of threats, the total number of factors analyzed in the robustness calculation is different. In the case of disruption of electricity supply for 24 hours there were analyzed in total 8 factors, disruption of the internal system of ICT 17 factors and lone shooter terrorist attack 12 factors. Recoverability was calculated from a total of 17 factors and adaptability from 16 factors.

After identifying weaknesses, it is necessary to create a draft of measures for strengthening the hospital's resilience. In cases where factors reached an insufficient level of resilience, it is appropriate to focus attention on the allocation of financial resources/reserves for recovery, the preparedness of financial resources/reserves in time of need, the specification of scenarios of expected disruptive events (IEC, 2010; IEC 2006), the implementation of management system (Jonker et al., 2017) and the evaluation of the training's effectivity of employees (Sarre et al., 2018).

In contrast, factors that reached a critical level of resilience are either completely absent or show critically low parameters. In terms of the electricity supply, it is appropriate to pay attention to predictive indications of a disruption of this supply (Rehak et al., 2017) and the technical means of physical resistance (ISO 8528, 2018; IEC, 2017). In terms of a terrorist attack, it is appropriate to pay attention to the implementation of measures leading to an increase in the cumulative probability of the detection of an intruder and the probability of his elimination (Siser et al., 2018; Lovecek et al., 2013). These items need to be entirely revised and the process of setting them up or recovering them must be initiated as soon as possible.

4. Conclusion

The elements of the critical infrastructure in the healthcare sector, especially acute-care hospitals, are currently the ones that are most vulnerable because this infrastructure is included to soft targets. For this reason, in recent years they have been a highly attractive target not only for physical attacks, but also cyber attacks.

Given these facts, the aim of this article was to perform a resilience assessment of the selected acute-care. The Resilience was assessed using the CIERA method in the context of current selected security threats. Specifically, these were the disruption of the electricity supply for 24 hours, the disruption of internal information and communication technology and the lone shooter terrorist attack.

The assessment shows that the hospital's resilience to the disruption of the electricity supply and to the disruption of the internal system of information and communication technology is at an acceptable level. The critical factors in this area are only the high dependence of the hospital on electricity and information and communication technology. However, the resilience to a terrorist attack by a lone shooter reached a low level, which would have a negative impact on providing health care services. The critical factors negatively affecting the resilience level were identified as low, particularly in the cumulative probability of the detection of an intruder and the probability of his elimination. This situation exists due to the insufficient security level of health care facilities in terms of technical means of physical protection and protective and regime measures.

Acknowledgments

This work was supported by the Ministry of the Interior of the Czech Republic [VI20152020009].

References

Armstrong, M., 2014, Armstrong's Handbook of Human Resource Management Practice, 3rd edit., Kogan Page, London.

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

Cai, B., Xie, M., Liu, Y., Liu, Y. and Feng, Q., 2018, Availability-based engineering resilience metric and its corresponding evaluation methodology, Reliability Engineering & System Safety, 172, 216-224. https://doi.org/10.1016/j.ress.2017.12.021

Denyer, D., 2017, Organizational Resilience: A Summary of Academic Evidence, Business Insights and New Thinking, BSI and Cranfield School of Management, Cranfield.

IEC 61025, 2006, Fault Tree Analysis (FTA), International Electrotechnical Commission, Geneva.

IEC 62040, 2017, Uninterruptible power systems (UPS), International Electrotechnical Commission, Geneva.

IEC 62502, 2010, Analysis techniques for dependability – Event Tree Analysis (ETA), International Electrotechnical Commission, Geneva.

ISO 8528, 2018, Reciprocating internal combustion engine driven alternating current generating sets, International Organization for Standardization, Geneva.

ISO 31000, 2018, Risk management – Guidelines, International Organization for Standardization, Geneva.

Jonker, E., Koopman, Ch., van der Nagel, N. and Schoorl, M., 2017, An Integrated Quality Management System for Healthcare, Open Medicine Journal, 4, 86-92. https://doi.org/10.2174/1874220301704010086

Jouini, M. and Rabai, L.B.A., 2016, Threats Classification: State of the Art, Gupta, B. (Ed.), Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, Hershey, PA, pp.368-392. https://doi.org/10.4018/978-1-5225-0105-3.ch016

Kampova, K., Lovecek, T. and Rehak, D. 2020. Quantitative Approach to Physical Protection Systems Assessment of Critical Infrastructure Elements: Use Case in the Slovak Republic, International Journal of Critical Infrastructure Protection, 30, Article No. 100376. https://doi.org/10.1016/j.ijcip.2020.100376

Kozine, I., Petrenj, B. and Trucco, P., 2018, Resilience Capacities Assessment for Critical Infrastructures Disruption: The READ Framework, International Journal of Critical Infrastructures, 14(3), 199-220. https://doi.org/10.1504/IJCIS.2018.10015604

Lovecek, T., Velas, A., Kampova, K., Maris, L. and Mozer, V., 2013, Cumulative Probability of Detecting an Intruder by Alarm Systems, In: 47th IEEE International Carnahan Conference on Security Technology (ICCST), 1-5. https://doi.org/10.1109/CCST.2013.6922037

Mantzana, V., Darra, E. and Gkotsis, I., 2020, Cyber-Physical Security in Healthcare, In: Rehak, D., Bernatik, A., Dvorak, Z. & Hromada, M. (Eds.), Safety and Security Issues in Technical Infrastructures, IGI Global, Hershey, PA, 63-87. https://doi.org/10.4018/978-1-7998-3059-7.ch003

Nan, C. and Sansavini, G., 2017, A quantitative method for assessing resilience of interdependent infrastructures, Reliability Engineering & System Safety, 157, 35-53. https://doi.org/10.1016/j.ress.2016.08.013

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

OECD/Eurostat., 2005, Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd edit., OECD Publishing, Paris. https://doi.org/10.1787/9789264013100-en

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

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

Rehak, D., 2020, Assessing and Strengthening Organisational Resilience in a Critical Infrastructure System: Case Study of the Slovak Republic, Safety Science, 123, Article No. 104573. https://doi.org/10.1016/j.ssci.2019.104573

Rehak, D., Hromada, M. and Novotny, P. 2016. European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice, Chemical Engineering Transactions, 48, 943-948. https://doi.org/10.3303/CET1648158

Rehak, D., Hromada, M. and Ristvej, J., 2017, Indication of Critical Infrastructure Resilience Failure, In: Cepin, M. & Bris, R. (Eds.), Safety and Reliability – Theory and Application (ESREL), 963-970.

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

Rehak, D., Senovsky, P., Hromada, M., Lovecek, T. and Novotny, P., 2018b, Cascading Impact Assessment in a Critical Infrastructure System, International Journal of Critical Infrastructure Protection, 22, 125-138. https://doi.org/10.1016/j.ijcip.2018.06.004

Rehak, D., Senovsky, P., Hromada, M. and Lovecek, T., 2019, Complex Approach to Assessing Resilience of Critical Infrastructure Elements, International Journal of Critical Infrastructure Protection, 25, 125-138. https://doi.org/10.1016/j.ijcip.2019.03.003

Sarre, S., Maben, J., Aldus, C., Schneider, J., Wharrad, H., Nicholson, C. and Arthur, A., 2018, The challenges of training, support and assessment of healthcare support workers: A qualitative study of experiences in three English acute hospitals, International Journal of Nursing Studies, 79, 145-153. https://doi.org/10.1016/j.ijnurstu.2017.11.010

Siser, A., Maris, L., Rehak, D. and Pellowski, W., 2018, The Use of Expert Judgement as the Method to Obtain Delay Time Values of Passive Barriers in the Context of the Physical Protection System, In: Rich, B. (Ed.), 52nd IEEE International Carnahan Conference on Security Technology (ICCST), 126-130. https://doi.org/10.1109/CCST.2018.8585718

Vichova, K. and Hromada, M., 2019, Power outage in the hospitals, In: International Conference on Intelligent Medicine and Image Processing (IMIP), 15-20. https://doi.org/10.1145/3332340.3332345