Information Support System Development in Relation to Critical Infrastructure Element Resilience Evaluation

Martin Hromada
Department of Security Engineering
Faculty of Applied Informatics, Tomas Bata University in Zlin
Zlin, Czech Republic
email: hromada@fai.utb.cz

Abstract— **Evaluating and ensuring the resilience of critical infrastructure is essential in terms of maintaining vital societal functions. This fact increases the importance of developing relevant mathematical models and their implementation to software tools. This article therefore discusses the development process of a critical infrastructure resilience evaluation mathematical model as a basis for information support system development. The article addresses both the description of selected resilience evaluation attributes as well as the possible structure of the information support system.**

Keywords- critical infrastructure; resilience evaluation; information support system.

I. INTRODUCTION

Critical infrastructure as a system is an essential part of society functional continuity, its economic or social structure and systems. In relation to this fact, approaches and tools were proposed, which reflect the above mentioned essentiality and create the framework for a risk assessment system, which should positively affect the functionality and resilience. Critical Infrastructure Protection in the Czech Republic is regulated by Act no. 430/2010 Coll., which can be seen as an implementation of Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, which provides a framework for creating a common European access to Critical Infrastructure Protection. This Directive establishes certain instruments for the identification and designation of an European and national infrastructure (sector and cross-cutting criteria), as well as instruments for increasing the protection of Critical Infrastructure in the context of the need to maintain functional continuity of the society (Operator Security Plan, Security Liaison Officer, Public Private Partnership and etc.). These instruments can also be seen from the resilience evaluation perspective, where, as it was said, resilience is seen as an indicator that quantifies the ability to provide functionality in terms of internal and external factors negative effects, provided to the need of establishing the limits, when degradation of system functionality is acceptable and when it is not [3]. Relevant approaches which were the philosophical baseline and the concept for security research project were presented in several articles. The most appropriate are RAMCAP Plus Approach [2] or D., Rehak P., Senovsky [10]. The rest of the paper is structured as follows. The first section provides the theoretical input to the resilience evaluation process in the context of information support. The second part is focused on resilience terminology specification. The third part then discusses and presents the security research outcome – Methodology for the Resilience Evaluation System of the Critical Infrastructure Elements and Networks in Selected Areas in Czech Republic as a unique and new approach to resilience evaluation and its implementation to decision support calculator as a relevant information support system.

II. RESILIENCE

"System resilience" in relation to critical infrastructure is a relatively new term, but, in principle, there are some accepted definitions:

Resilience is the „ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions" according to the U.S. Department of Homeland Security Risk Steering Committee [1].

Resilience is „both the inherent strength and ability to be flexible and adaptable after environmental shocks and disruptive events"according to Tierney and Bruneau [1].

Resilience is understood as „the ability of systems, infrastructures, government entities, businesses, and society to adapt to adverse events, to minimize the impact of such events (keeping the system running), and also to anticipate future adverse events and be able to prevent them"according to the CRN Report, Focal report 6, Risk Analysis, Resilience – trends in Policy and Research [1] [2].

III. CRITICAL INFRASTRUCTURE ELEMENT RESILIENCE EVALUATION METHODOLOGY ALGORITHMS

One appropriate approach, which was a philosophy baseline for our new approach for resilience evaluation was All-hazard risk and resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach [2]. The RAMCAP Plus process avoids unnecessary detail, precision and cost by focusing on the most critical assets at a facility and keeping the approach relatively simple and intuitive. There are numerous other risk methodologies in use by specific industries, but their results are generally not comparable with other industry sectors or, in some cases, with other facilities within the sector. Many are qualitative,

 ISBN: 978-1-61208-493-0

producing relative results that can be compared only locally, if at all. Moreover, several of the available methods require the assistance of specialized consultants and/or considerable amount of time, money and personnel resources, which discourages their use and makes them costly to use on a regular basis. The RAMCAP Plus process – through the cost-effective application of common and consistent terminology and metrics – provides a basis for using existing data and reporting results in a consistent, quantitative, directly comparable manner [2]. Depending on the purpose, the resilience of critical infrastructure element or elements evaluation should be done as an external or internal evaluation. It should be based on knowledge of nature and basic functional, technological and spatial attributes of the evaluated critical infrastructure elements. Next, we will therefore present a unique approach which reflects actual security, safety and resilience issues in Czech Republic in relation to critical infrastructure stability and functional continuity.

Multi-criteria evaluation is one of the appropriate methods for evaluating the resilience of critical infrastructure element and system. This method allows implementation of a comprehensive evaluation of relatively independent indicators and parameters. It uses a semi-quantitative expression of the individual indicators value. Its disadvantage is a lower resilience level performance. It allows to rate a critical infrastructure element in an appropriate range of resilience levels. The result of evaluation unfortunately does not specify how long the element of critical infrastructure can withstand the influence of negative factors. The advantage is the evaluation of the protection measures quality in relation to identified threats and risks [3].

It is obvious that the multi-criteria evaluation should be related to the security areas, which have a positive impact on the resilience level (robustness and preparedness), including their components. Every area of security and safety should have a positive impact on the robustness and preparedness level. The assessment should therefore establish standards (criteria) for the selected security and safety areas, through checklists. A comprehensive evaluation requires the expression of the risk value (coefficient) and its relationship and impact on the selected element or sector of critical infrastructure resilience. This highlights the fact that the final system resilience level is the average value of resiliencies related to selected risks. For complex multi-criteria critical infrastructure element or sector resilience evaluation, a mathematical relationship was established, represented by following equation:

$$ODP = \frac{\sum OD_i}{x_i} \quad (1)$$

where:

ODP - is the resilience value of the evaluated critical infrastructure elements,
OD_i - is the resilience value of the critical infrastructure element in relation to the selected (i-th) risk
x_i - is the number of selected risks [4].

The mathematical expression of critical infrastructure elements resilience in relation to the i-th risk is:

$$OD_i = \frac{(1 - H_{RZi}) + (1 - K_S) + (K_{RO} * V_{RO} + K_{PR} * V_{PR})}{3} \quad (2)$$

where:
H_{RZi} - is the risk value of i-th risk
K_S - is correlation coefficient,
K_{RO} - is the robustness coefficient,
V_{RO} - is the weight of robustness,
K_{PR} - is the preparedness coefficient,
V_{PR} - is the weight of preparedness [2][3].

A. *Analysis and Risk assessment*

Analysis and risk assessment in the context of the above-mentioned methodology is based on a two steps process:

1. Semi-quantitative risk analysis,
2. Qualitative risk correlation analysis (QARS)

In the first instance, the risk is semi-quantitatively expressed by the relationship:

$$R = P * N \quad (3)$$

where:
R - Risk value,
P - The probability of threats application,
N - Impact value

In risk and vulnerability evaluation process is necessary to use relevant methodology for the expression of the mutual relationships and interdependencies between identified risks. For this purpose, the (QARS) methodology was selected.

The importance of this methodology is especially in connection with the diversification of risk based on level of risk activity (the risk ability or potential to cause further risks) and passivity evaluation (possibility that the risk may be caused by other risks) in relation to other risks.

The process of implementation of the QARS analysis is a multi-steps process, with the first step being the creation of a list of possible risks.The next step is focused on the expression of importance relations and interdependencies between the identified risks in the form of spreadsheet correlation Table 1.

 ISBN: 978-1-61208-493-0

TABLE 1. LIST OF RISKS

	Index	1	2	3	4
Index.	The Threat Of	High temperature	Lightning	Tree fall	Operating error of third parties
1	High temperature	x			
2	Lightning	1	x	1	0

x - Reflects the fact that the risk itself cannot cause,
1 - Is the real possibility that the risk Ri may cause risk Rj,
0 - Expresses a condition where there is no real possibility that the risk Ri may cause risk Rj
Coefficients of the correlation and interdependencies calculation are based on the equations:

$$C_A R_i = \frac{\sum R_i}{x-1} \qquad C_P R_i = \frac{\sum R_i}{x-1} \tag{4}$$

where:
$C_A R_i$ is the value of activity coefficient,
$C_p R_i$ is the value of passivity coefficient,
$\sum R_i$ is the sum of risks,
x - total number of risk.

After adding values to the correlation table for the tree fall risk, the horizontal axis (activity coefficient) and vertical axis (passivity coefficient), and after using the above equations, we have the following parameters (presented in Table 2):

TABLE 2. COEFFICIENTS AND RISK INDEX

The Risk Index		1	2	3	4	5	6	7	8	9	10
Activity Coef.		0,00	0,22	0,44	0,44	0,56	0,56	0,67	0,56	0,11	0,11
Pasivity Coef.		0,67	0,00	0,11	0,44	0,67	0,00	0,44	0,33	0,44	0,33

Subsequently, the coefficient values are plotted on a graph, which ultimately enables the identification of the most significant risks in terms of their potential (high activity and passivity potential).

For the risk evaluation or for the process of determinig the most significant risks, the graph must be divided into segments that differentiate risks according to their significance. To divide the graph into 4 segments, it is necessary to define S1 and S2 lines that divide the graph itself and the risks to the segments where it is assumed that in the first segment will be 80% if major risks.

To express the parameters for lines S1 and S2, we use the equations:

$$S_{1/2} = C_{A/P\max} - \frac{(C_{A/p\max} - C_{A/P\min})}{100} * 80 \tag{5}$$

where:
$C_{A\max}; C_{A\min}$ - minimum and maximum values of activity coefficient,
$C_{P\max}; C_{P\min}$ - minimum and maximum values of passivity coefficient,

Then, the lines are implemented and divide the risks in 4 segments (Figure 1) that represent the level of risks:

1. I. Segment - Primarily significant risks – the highest activity and passivity coefficients,
2. II. and III. Segment – Secondary significant risks,
3. IV. Segment – Tertiary significant risks – low value of activity and passivity coefficients,

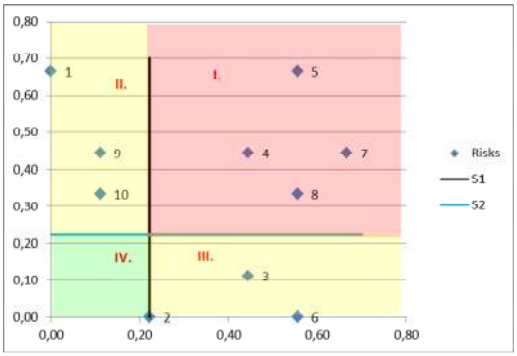

Figure 1. Division into 4 risk segments

This process allows us to divide risks by the highest potential in relation to system functionality degradation due to domino efect, which can be seen as an expression and evaluation of the vulnerability parameter (Vi) [3][4].

B. *Software application*

In relation to above-mentioned procedure, the second step of risk analysis and assessment is the risk list creation. This method is based on the use of simple mathematical equations. In connection with this fact, the excel calculator was selected, mostly because it provides easy editing and graph work. The resulting Table 3 was:

TABLE 3. RISKS CORRELATION TABLE

i	Table of correlations	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	Energetics																										
1	Short-term electricity outage			✔																							
2	Long-term electricity outage				✔																						
3	Outage of water supply					✔						✔				✔		✔									
4	Outage of gas supply						✔																✔				
	Natural impacts																										
5	Flood																										
6	Prolonged drought																										
7	Extreme heat and drought								✔												✔			✔			
8	Thick frost									✔					✔												
9	Pandemic, epidemic																										
	Risks associated with the human factor																										
10	Conflagration																										
11	Explosion																										
12	Robbery																										
13	Leaks of pollutants in the area																										
14	Outage in logistics																										
15	The virtual attack			✔								✔															
16	The terrorist attack				✔								✔														
17	Disruption of public order																										
18	Unavailability of staff			✔																							
19	Sudden rush of patients					✔																					
20	Technical failures						✔																				
21	Sabotage			✔																							
22	Violent criminal activity												✔	✔													
23	Acts of vandalism																										
24	Plundering			✔	✔																						
25	Reserve 1					✔											✔	✔									
26	Reserve 2						✔														✔						

Reset

After inputting the values in the table and using appropriate mathematical background, the resulted graph (Figure 2) and risks segmentation was:

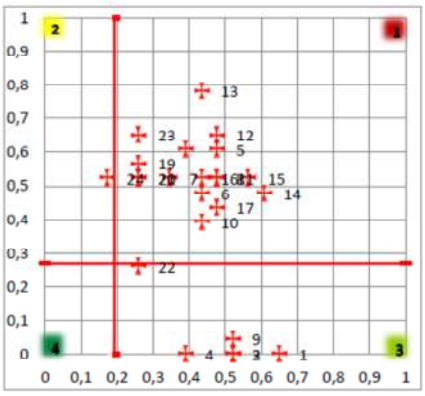

Figure 2. Risks correlation graph

where the segment properties presented in Figure 3 are:

S	Segment properties
1	Areas of primary and secondary dangerous risks
2	Areas of secondary dangerous risks
3	Areas of primary dangerous risks
4	Relatively safe area

Figure 3. Segment properties

For the process of determining the value of the risk coefficient/parameter HRzi, we select risks which can be considered critical - located in I. quadrant of QARS. These risks values are seen through first phase of risk assessment and analysis, which takes into account the degree and significance of the selected risks impact to the system. For the determination of the risk value the following equation was applied:

$$H_{RZi} = \frac{H_{Ri}}{H_{Ri\max}} \quad (6)$$

where:
H_{RZi} - is the risk value of i-th risk in range <0,1>
H_{Ri} - is the original risk value expressed in the first phase of the risk analysis
H_{Rimax} - the maximum attainable risk value within the value range.

The final list for evaluation of critical infrastructure element risk value is presented in the Figure 4:

i	Risks	Active	Passive	S
	Energetics			
1	Short-term electricity outage	0.04	0.00	2
2	Long-term electricity outage	0.04	0.00	2
3	Outage of water supply	0.17	0.22	1
4	Outage of gas supply	0.09	0.13	1
	Natural impacts			
5	Flood	0.00	0.09	2
6	Prolonged drought	0.00	0.04	4
7	Extreme heat and drought	0.13	0.04	3
8	Thick frost	0.04	0.00	2
9	Pandemic, epidemic	0.00	0.04	4
	Risks associated with the human factor			
10	Conflagration	0.00	0.04	4
11	Explosion	0.00	0.00	2
12	Robbery	0.00	0.09	2
13	Leaks of pollutants in the area	0.00	0.09	2
14	Outage in logistics	0.00	0.09	2
15	The virtual attack	0.13	0.04	3
16	The terrorist attack	0.09	0.00	1
17	Disruption of public order	0.00	0.04	4
18	Unavailability of staff	0.04	0.00	2
19	Sudden rush of patients	0.04	0.04	4
20	Technical failures	0.04	0.00	2
21	Sabotage	0.04	0.04	4
22	Violent criminal activity	0.09	0.00	1
23	Acts of vandalism	0.00	0.04	4
24	Plundering	0.09	0.00	1

Figure 4. Risks assessment list

C. *Correlation value*

Determination of correlation coefficient K_s is an important aspect that expresses the position of the linkages and dependencies within the critical infrastructure system. Generally, the main linkages and dependencies areas are:

a) Logical linkages and dependencies,
b) Physical linkages and dependencies,
c) Territorial linkages and dependencies.

To determine the value of correlation parameter the following equation is applied:

$$K_s = \frac{\sum Si}{S_{\max}} \quad (7)$$

where:
K_s - correlation parameter value
Sum Si - the sum of the dependence degree of the i-th CI elements groups to other CI areas
S_{max} - is the maximum value of correlation

After the mathematical expression of correlation value parameter, the final list for critical infrastructure element correlation value calculation was (Figure 5):

 ISBN: 978-1-61208-493-0

Product or Service	Is the element Hospital care dependent on another product		Dependency
Electricity supply	yes	no	0
Gas supply	yes	no	0
Water supply	yes	no	8
Food supply	yes	no	6
Functionality of communication networks	yes	no	4
Access to data services	yes	no	0
Availability of staff	yes	no	0
Supply of medical materials	yes	no	7
Forecasting and warning service	yes	no	1
Public Administration	yes	no	3
Transportation	yes	no	0
	Reset	Ks	0.26

Figure 5. Correlation value

D. Robustness coefficient evaluation

The robustness expressed by $K_{RO,}$ represents strength, durability, resistance to deformation. It is the ability to resist and withstand the effects of negative events without significant function degradation. In this methodology, the CI element robustness is divided into structural robustness and security robustness. These two areas, respectively, their expressions, form a relationship for the evaluation of the system robustness:

$$K_{RO} = K_{RZ} * K_{SR} \quad (8)$$

where:

K_{RO} - is the robustness coefficient,
K_{RZ} - is the structural robustness coefficient,
K_{SR} - is the security robustness coefficient.

The evaluation of security robustness coefficient K_{RZ} in relation to the resilience evaluation is seen from a wider context. The security robustness coefficient expresses the extent and quality of the critical infrastructure element security in connection with identified risks. Individual measures, according to their nature and effect, are divided into specific security areas. There are areas of physical security, information security, administrative security, personnel security, etc. For each type of critical infrastructure element, different security areas should be defined. The security robustness coefficient basically consists of:

- level of physical security M_{FB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element physical security,
- level of information security M_{IB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element information security,
- level of administrative security M_{AB} - which is an expression of the extent and quality of the measures taken under the critical infrastructure element administrative security,
- level of personal security M_{PB} - which is an expression of the extent and quality of the measures taken in the critical infrastructure element personnel security.

The importance (weight) of individual security area components of the security robustness is as individual as the status and importance of robustness and preparedness in relation to the selected critical infrastructure element resilience. The importance determination, that is, the weights determination of security robustness for individual components, is realized using pair wise comparison (Fuller triangle).

In the case of any two security robustness components comparison of the n components, we select all combinations of two elements of n, where the total number of combination is equal to (figure 6):

$$K = \frac{n * (n-1) * (n-2)!}{2!\,(n-2)!} = \frac{n * (n-1)}{2} \quad (9)$$

1	1	1	1	1	1	1	1
2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	
3	4	5	6	7	8	9	
3	3	3	3	3	3		
4	5	6	7	8	9		
4	4	4	4	4			
5	6	7	8	9			
5	5	5	5				
6	7	8	9				
6	6	6					
7	8	9					
7	7						
8	9						
8							
9							

Figure 6. Example of Fuller triangle

Therefore, weights assessment may be calculated by the following equation:

$$V_i = \frac{m_i}{\sum_{i=1}^{k} m_i} = \frac{m_i}{K} \quad (10)$$

Mathematical expressions of weights determine the safety and security areas that are relevant for the evaluation process which influence the final value of the resilience (in the case that the weight of administrative security is 0, it is clear that we would not evaluate the measures provided by this security area).

For security robustness evaluation, a process has been formulated following the relationship:

$$K_{RZ} = M_{FB} * V_{FB} + M_{IB} * V_{IB} + M_{AB} * V_{AB} + M_{PB} * V_{PB} \quad (10)$$

where:

V_{FB} - is the weight of physical security,
V_{IB} - is the weight of information security,
V_{AB} - is the weight of administrative security,
V_{PB} - is the weight of personal security,
M_{FB} - concerns the determination of the physical security measures quality,
M_{IB} - concerns the determination of the information security measures quality,
M_{AB} - concerns the determination of the administrative security measures quality,
M_{FB} - concerns the determination of the personal security measures quality [3].

Regarding the software application of security robustness expression, we used selected security areas importance comparison by Fullers triangle (Figure 7.):

Compare the importance of individual areas			
Physical and object security	●	●	IT security
Physical and object security	●	●	Business continuity management
Physical and object security	●	●	Administrative security
IT security	●	●	Business continuity management
IT security	●	●	Administrative security
Business continuity management	●	●	Administrative security

Figure 7. Security areas importance comparison

and the selected security areas checklist fulfilment is represented in Figure 8:

IT security	Yes	No
Antivir	●	●
Firewall	●	●
Identification and authentication	●	●
RAID	●	●
Access control	●	●
Traffic Control	●	●
256-bit encryption	●	●
Ensuring sterility of environment	●	●
Staff training	●	●
Prevention	●	●

Figure 8. Selected security areas checklist

E. Structural robustness coefficient evaluation

Resilience of critical infrastructure element is the ability to ensure functionality in terms of external and internal factors effects. Each resilience value should have a point featured element (building, room), surface element (agricultural fields, complex reservoirs), line element (pipeline, pipeline) and element with the network characteristics (Radiation Monitoring Network). The level of element resilience is related to the security measures, but also reflects the systemic, structural and technological characteristics. A critical infrastructure element with network character structure will be able to withstand the effects of natural disasters without serious function degradation, if it will be able in terms of its structure, redirect the flow of technology and alternative way to bridge the shortfall of transit components. To determine the degree of influence, it is necessary to reflect those characteristics that are part of normal operation and are immediately available to use and do not require extensive activation of forces and means. These characteristics determine the structural robustness of a critical infrastructure element.

In the process of assessing structural robustness, it is possible to use the so-called macro-view approach. Widely distributed critical infrastructure element deployed on a large territory (region, country) is more vulnerable than a point element (Department Building). The probability that it will deal with the effects of natural disasters is higher, also has given his blanket deployment of more vulnerabilities.

Structural robustness of critical infrastructure element expresses the ability to withstand the effects of negative factors due to its structure, system and technology properties. It also includes the ability to withstand the effects of negative factors without function degradation, potential of deploying the redundant subsystems to isolate the failure (to prevent their spread) and flexibility to redirect service. In relation to this fact, the critical infrastructure elements have the character of the building, technological unit, staffed technical system, processes, systems or services, the assessment of structural robustness should be determined by a multi-criteria evaluation.

The evaluation process is represented by scoring of the main attributes that determine the magnitude of the structural robustness. The structural robustness coefficient K_{SR} varies in the interval 0.8 – 1. Structural robustness coefficient K_{SR} expresses the influence of topological structure, complexity and other properties or characteristics of the deterioration of protective measures effect of evaluated critical infrastructure element. If the coefficient of structural robustness K_{SR} is lower, the more attention should be paid to emergency preparedness. The main attributes by which the evaluation of the structural robustness should be performed include:

- type of topological structure,
- complexity,
- number of key technologies
- flexibility
- redundancy
- perimeter protection.

Topological structure type of element is a topological expression of its physical appearance. The type of topological structure is evaluated by the topology index value I_t. Determination of the topological structure type is carried out by using the system architecture, implemented in the system analysis. Based on the analysis of sectoral criteria, we distinguish between four types of topological

 ISBN: 978-1-61208-493-0

structures of the critical infrastructure elements. These include point, area, line and network structures. Topological structure type is reflected in the range of elements, the degree of centralization and density of components of critical infrastructure elements, etc. Index topology I_t has values in the range 0 – 3. Value of I_t is determined by identifying the type of evaluated element topology (point, area, line and network) and the specifications of its size. The network character elements I_t are determined by using partial methods. Next, we characterize all four types of topological structures.

The point structure element is an element that forms a centred closed unit, located on a small area. Usually, it may be protected as a whole against external events. This category includes critical infrastructure elements represented by building, group of buildings, building with mast etc. The closeness and separation from the outside boundary elements improves the conditions for the functioning and reduces its vulnerability. For such elements, structural robustness may not be in high demand. Index topology I_t of elements with an area up to 1000 m^2 takes the value 3, with area over 1000 m^2 has a value of 2, and the maximum size of the point element is 1 hectare.

The surface structure element has the character of surface unit. The dimensions of element length and width are comparable in size. The geometric shape is not clear, it may take the form of rectangles, squares, triangles and polygons, etc. Such an element occupies a large and geographically compact area. Element target function is associated with a wide area of space. The surface dimensions are so large, and it usually means that the physical security provided around the perimeter is difficult to achieve, but not always. Examples of surface structure element with ensured physical security may be airports, especially international flights. An example of element which is not ensured by physical security is an important agricultural field. Elements topology index I_t of area to 1 km^2 takes the value 2, the area between 1-10 km^2 has a value of 1 and a surface of 10 km^2 has a value of 0.

The line structure element is characterized by a line arrangement. It represents an element which ensures transmission, supply or transport between two physically separate locations. This kind of element is not usually possible to protect as a whole. Its interruption causes degradation of transmission, delivery or transportation. Only local points on the line should be protected, such as compressor stations, booster stations, etc. In terms of its nature it is the most vulnerable category of critical infrastructure elements and ensuring their resilience requires high preparedness to function restoration. Structural robustness coefficient should reduce the overall resilience value of the element represented by the protective measures and preparedness to restore function. Linear character element topology index I_t with a length of 10 km takes the value 1, with a length of 10 km has the value 0.

The network structure element is characterized by a network structure. It consists of several components (nodes) which are interconnected. The network is characterized by a topological structure that expresses the nature and type of interconnection nodes. We distinguish between tree, star, polygon and bus structures. If the network is dense, it is less vulnerable and can better adapt to the failure of one of the nodes or edges. Element resilience significantly reflected the ability of technologies in the area of routing. If the technology in the network allows automatically or at least automated forwarding, element resilience is greatly increasing. Resilience is also affected and have irreplaceable role in relation to the importance of each node in the network. A key role in these elements plays a central node, which collects data, evaluates and presents it for further use. Failure of the central node can mean functionality disruption of the whole critical infrastructure element. Therefore, it is important that the network functions of the central node are backed up. Another structural robustness characteristic of the network is the uniformity of edges distribution. If there are nodes in the network with the number of edges significantly higher than the rest, the failure of nodes should significantly degrade the quality of the provided function of evaluated critical infrastructure element than the other. Index I_t of network topology structure element is determined by the partial multi-criteria methodologies. Depending on the type of network topology, the number of core nodes, the total number of nodes and the average number of edges per node should the topology index I_t takes values from 0 - 3.

Element complexity integrates a number of categories (types) of components and their total number. The level of complexity is evaluated using the complexity index value I_s. If the system is complicated, it is more vulnerable and less resilient. A number of complications may occur at the interfaces between the components and technologies. A complex system also requires a higher degree of specialization of the individual components, which degrade the interchange ability of components. Extensive systems tend to be prone to restructured complexity. Simple systems take the complexity index I s value 2, medium (medium complexity) systems take value 1 and 0 value is for complex systems. The criterion for determining the degree of complexity can also be the number of employees.

In addition to the complexity of critical infrastructure element, the resilience is significantly affected by the number of key and support technologies that ensure the fulfilment of its key function. For example the key technology of electricity production dispatching is an information technology as a Local area network. The number of key technologies is identified in the system analysis in the specification of technology architecture. Generally, the more complex systems are more vulnerable. Mostly the technological dependence of society, forced the establishment of critical infrastructure protection. Just a limitation of raw materials for key technology elements of

 ISBN: 978-1-61208-493-0

critical infrastructure is degrading its functionality. Similarly, the failure of one technological unit should spread failures by domino effect in other technological units. The increasing number of technologies leads to increased vulnerability and limited element resilience. Technological complexity of evaluated critical infrastructure element is evaluated using the key technologies index I_{kt}. If the element contains less than 2 key technologies take the key technologies index I_{kt} value 2, when the number of technologies is 3-4 is an index of key technologies I_{kt} assigned with value of 1, and if the number of key technologies is 5 and more the index value is 0.

Flexibility as a general feature means adapting of the building operations in relation to changes in conditions, the input variables and its structure and other key features. Flexibility is reflected by critical infrastructure elements adaptation to new conditions. It ensures the implementation of the target element function and in the case of breakdown or failure of some critical infrastructure elements component. It provides flexibility in redirecting the flow in case of failure of one of its nodes. Flexibility properties should be considered to technologies ensuring the fulfilment of the objective function. For example the high voltage transmission system ability is to bridge the section shortfall by redirection and the use of other sections for power transmission. The ability of critical infrastructure flexibly is evaluated by the flexibility index I_f. If key technologies allow the flexibly adaptation of their activities, the flexibility index If is assigned the value 2, in the absence of flexibility potential¸ flexibility index I_f takes the value 0.

Redundancy generally means excrescence. In the field of critical infrastructure elements, redundancy means the extension of the structure of the key components backup. The purpose of redundancy is to create the conditions where the failure of a key component will be immediately substituted by using redundant (backup) components. Implementation of redundancy principle can be seen through a backup operation control, which assumes the management after failure of the main control room. Applying the principle of redundancy is an important characteristic to ensure structural robustness of critical infrastructure element. Using redundant principal components is expressed by the redundancy index I_r. Redundancy index I_r takes the value 1, when the redundancy principle is applied. In the case when element does not have any redundant key technologies, redundancy index I_r is assigned by the value 0.

The geographic scope of the evaluated critical infrastructure elements translates into the possibility of ensuring the physical security by perimeter protection. If there is a feature on a relatively small area, it is economically viable to ensure the physical security as a whole. In the case where the element is located on a large area or a long line, it is not economically viable to protect it as a whole. The monitoring networks elements can be protected by local perimeter protection. The structure and use of perimeter protection is evaluated by a perimeter protection index I_{po}. If the critical infrastructure element does not build the perimeter protection, the perimeter protection index I_{po} is assigned by the value 0. If is the perimeter protection is local,, the perimeter protection index I_{po} takes the value 1, and in case of a complete perimeter protection, the index value is 2.

The values of topology index I_t, complexity index I_s, key technologies index I_{kt}, flexibility index I_f, redundancy index I_r and perimeter protection index I_{po} are listed in following Equation 11 [3].

$$K_{SR} = 0{,}8 + \frac{I_t + I_s + I_{kt} + I_f + I_r + I_{po}}{60} \quad (11)$$

K_{SR} - structural robustness coefficient[5]

Software application of structural robustness evaluation is divided into two parts. The first part is the highest hierarchical level and it is presented in Figure 9:

Type of topology	point		area		
	> 1000 m2	< 1000 m2	> 1 km2	1 – 10 km2	< 10 km2
	●	●	●	●	●
Complexity	simple (under 10 employees)			medium (10-100 em	
	●			●	
Number of core technologies	0-2 of technology			3-4 of technolc	
	●			●	
Flexibility	no				
	●				
Redundancy	no				
	●				
Perimetric protection	unprotected			local	
	●			●	
	K_{SR}			0.93	

Figure 9. Structural robustness evaluation

In the case when the topological type is a network, it is necessary to fulfil additional information, as shown in Figure 10:

Type of topology	bus	star / circle
	●	●
Number of core nods	1 node	2 nodes
	●	●
The number of nodes	to 5 nodes	6 - 15 nodes
	●	●
The average number of edges per node	to 1,5 edge	1,6 - 2,2 edges
	●	●

Figure 10. Additional table for network structural robustness evaluation

F. Preparedness coefficient evaluation

Preparedness of critical infrastructure element expresses its ability to restore its function after its degradation by the effects of negative factors (risks). Preparedness is evaluated through the preparedness parameter/coefficient K_{PR}, which can be understood as an expression of the ability to adequate reaction respectively response to the outbreak of an

emergency or incident as well as the ability to recover and return to desired system functionality.

The mathematical expression of preparedness of the selected critical infrastructure (CI) element is given by:

$$K_{PR} = \frac{K_r + K_p + K_i}{3} \quad (12)$$

where:

K_r - coefficient of identified risks accuracy,
K_p - CI subjects crisis preparedness plan quality coefficient,
K_i - CI subjects crisis preparedness plan implementation quality coefficient,

Each part (defined coefficients) of the preparedness coefficient has a different check list. For this reason, we presented the example of a selected one (Figure 11) and the final software application of critical infrastructure element preparedness coefficient evaluation.

Crisis preparedness	Yes	No
Security audit	●	●
Identification of possible events	●	●
Contact Information	●	●
Organization structure	●	●
Insurance contracts	●	●
Description of the main activities	●	●
Probability of events occurrence	●	●
List of procedures	●	●
List of needs and resources	●	●
Determination of responsible persons	●	●

Figure 11. Crisis preparedness plan quality coefficient

The final software application of critical infrastructure element, the preparedness coefficient evaluation, is as an important aspect of specific critical infrastructure resilience evaluation (Figure 12):

Number of risks identified by control authority in first segment	6
K_R	0.83
K_P	0.6
K_I	0.8

Figure 12. The final preparedness coefficient evaluation

G. Critical infrastructure element resilience evaluation

It is obvious that the multi-criteria evaluation should relate to the areas of security, which have a positive impact on the level of resilience (robustness and preparedness), including their components. Each area of security, having a positive impact on the robustness and preparedness should be assessed in relation to the established standards (criteria), for selected area through checklists. A comprehensive evaluation requires expressing the value (coefficient) of the risk and its relationship and impact to the value of resilience in relation to selected element or sector of critical infrastructure. This highlights the fact that the total value of resilience under evaluated system is the average value of resilience in relation to i-th risk. For a complex multi-criteria evaluation of selected CI element or elements the resilience was established by the following mathematical relationship:

$$ODP = \frac{\sum ODi}{xi} \quad (13)$$

where:

ODP - selected CI element resilience value
ODi - CI element resilience value in relation to selected i-th risk
xi - number of selected risks

The mathematical expression of CI elements resilience in relation to the i-th risk is:

$$ODi = \frac{(1 - H_{RZi}) + (1 - K_S) + (K_{RO} * V_{RO} + K_{PR} * V_{PR})}{3} \quad (14)$$

where:

H_{Rzi} - the value of i-th risk,
K_s - correlation parameter,
K_{RO} - robustness parameter,
V_{RO} - robustness weight,
K_{PR} - preparedness parameter,
V_{PR} - preparedness weight,

Equations (1- H_{Rzi}) and (1- K_s) reflect the fact that risk and correlation value negatively affect the value of the critical infrastructure element resilience.

The presented facts are the basis for the final evaluation of the critical infrastructure element or group of elements resilience in the relevant sector.

The final qualitative evaluation will be presented in the software application part of final critical infrastructure element resilience evaluation.

For final critical infrastructure element resilience evaluation, we used the above-mentioned facts and mathematical expressions and they are presented in Figure 13:

 ISBN: 978-1-61208-493-0

i	Risks	S	P	N	H_{RZi}	Odi
	Energetics					
1	Short-term electricity outage	1	3	1	0.12	0.77
2	Long-term electricity outage	1	2	3	0.24	0.73
3	Outage of water supply	1	3	1	0.12	0.77
4	Outage of gas supply	1	3	2	0.24	0.73
	Natural impacts					
5	Flood	1	2	2	0.16	0.76
6	Prolonged drought	2	3	2	X	X
7	Extreme heat and drought	3	1	0	X	X
8	Thick frost	2	2	0	X	X
9	Pandemic, epidemic	2	2	0	X	X
	Risks associated with the human factor					
10	Conflagration	2	0	0	X	X
11	Explosion	2	0	0	X	X
12	Robbery	1	2	1	0.08	0.78
13	Leaks of pollutants in the area	1	2	3	0.24	0.73
14	Outage in logistics	2	0	0	X	X
15	The virtual attack	1	3	2	0.24	0.73
16	The terrorist attack	1	3	1	0.12	0.77
17	Disruption of public order	2	0	0	X	X
18	Unavailability of staff	1	0	0	0	0.00
19	Sudden rush of patients	1	0	0	0	0.00
20	Technical failures	1	0	0	0	0.00
21	Sabotage	3	0	0	X	X
22	Violent criminal activity	1	3	4	0.48	0.65
23	Acts of vandalism	2	0	0	X	X
24	Plundering	1	3	1	0.12	0.77
			ODP			**0.59**

Figure 13. Final resilience evaluation

Qualitative expression of critical infrastructure element resilience evaluation is represented by Figure 14:

Resilience evaluation	Value of ODP	Verbal rating	The minimum value of the robustness	The minimum value of the robustness of security	The minimum value of preparedness
Great (A)	0,8– 1	system is ready for all identified risks, none risks was neglected	0.5 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.5 as a result of the relationship $K_{PR}*V_{PR}$
Very good (B)	0,6 – 0,8	system is ready for all of the important identified risks	0.4 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.4 as a result of the relationship $K_{PR}*V_{PR}$
Good (C)	0,4 – 0,6	systém is ready for the most of important identified risks	0.3 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.3 as a result of the relationship $K_{PR}*V_{PR}$
Enough (D)	0,2 – 0,4	system is ready for the most of the identified risks	0.3 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.3 as a result of the relationship $K_{PR}*V_{PR}$
Unable to resist (E)	0 – 0,2	system is not ready for the majority (more than half) of the identified risks	0.2 as a result of the relationship $K_{RO}*V_{RO}$	Is given by the weights of individual parameters $V_{FB}, V_{IB}, V_{AB}, V_{KO}$	0.2 as a result of the relationship $K_{PR}*V_{PR}$

Figure 14. Qualitative expression of resilience evaluation

Figure 14 presents the qualitative expression of resilience evaluation as a final step of comprehensive approach for resilience evaluation. The approach was validated in selected critical infrastructure element as a reflection to practical model implementation ambition.

IV. CONCLUSION

As it was stated in the introduction, the resilience of critical infrastructure is a major aspect of critical infrastructure protection level improvement and assurance and maintenance of functional continuity. The paper presented selected facts and knowledge of the evaluation process in connection with selected attributes of methodological resilience evaluation. The evaluation process was followed by the software application and implementation of the presented mathematical relations. These facts should allow and provide a basis for information support system development. The presented model and resilience evaluation methodology was an outcome of security research project, where the main aim is to develop an unique and new approach and model to define and evaluate the critical infrastructure resilience. In relation to this fact, it is necessary to mention that resilience evaluation methodology was certified by Ministry of Trade and Business and Ministry of Interior of Czech Republic. The above mentioned model presents the mathematical modelling which is presently the framework for Dynamic Resilience Evaluation in new security research project RESILIENCE 2015.

ACKNOWLEDGMENT

This work was supported by the research project VI20152019049 "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems", supported by the Ministry of the Interior of the Czech Republic in the years 2015-2019.

REFERENCES

[1] CRN Report, Focal report 6, Risk Analysis, Resilience – trends in Policy and Research, Commisioned by the Federal Office for Civil Protection Zurich, pp.25. April 2011

[2] ASME Innovative Technologies Institute, LLC,. All-hazard risk and resilience : Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach. 1. New York : ASME, 2009. 155 p. ISBN 978-0-7918-0287-8

[3] M., Hromada, L., Lukas Conceptual Design of the Resilience Evaluation System of the Critical Infrastructure Elements and Networks in Selected Areas in Czech Republic, The twelfth annual IEEE Conference on Technologies for Homeland Security (HST '12), will be held 13-15 November 2012 in Greater Boston, Massachusetts. Pp. 353-358, ISBN 978-1-4673-2707-7

[4] M., Hromada Knowledge sharing in the risk analysis proces in energy sector, 3rd EU-US-Canada Expert Meeting on Critical Infrastructure Protection (CIP) May 22nd – 23rd 2012, Brussels

[5] M., Hromada, L., Lukas, The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation, The 13th annual IEEE Conference on Technologies for Homeland Security (HST '13), held 12-14 November 2013 in Greater Boston, Massachusetts. Pp. 589-594, ISBN 978-1-4799-1533-0

[6] E. G., Vugrin, D.E., M. A., Warren Ehlen, R. C., Camphouse A Framework for Assessing the Resilience of Infrastructure and Economic Systems, In: Sustainable and Resilient Critical Infrastructure Systems, 1st Edition, pp. 84-85,April 2010,ISBN 978-3642114045

[7] M., Hromada, L., Lukas Critical Infrastructure Protection and Resilience as an Actual Challenge of Security Education,

Computers and Technology in Modern Education, Kuala Lumpur, Malaysia, April 23-25, 2014, p. 62-69, ISBN: 978-960-474-369-8

[8] L., Lukas, M., Hromada, Simulation and Modelling in Critical Infrastructure Protection, In: International Journal of Mathematics and Computers in Simulation, Issue 1, Volume 5, p. 386-394, 2011, ISSN: 1998-0159, http://www.naun.org/journals/mcs/

[9] L., Lukas, M., Hromada, Resilience as Main Part of Protection of Critical Infrastructure, In: International Journal of Mathematical Models and Methods in Appliad Sciences, Issue 1, Volume 5, p. 1135-1142, 2011, ISSN: 1998-0140, http://www.naun.org/journals/m3as/

[10] D., Rehak P., Senovsky Preference Risk Assessment of Electric Power Critical Infrastructure. Chemical Engineering Transactions, 2014, Vol. 36, pp. 469-474. ISSN 1974-9791. DOI: 10.3303/CET1436079