Petr Novotny - Jiri Markuci - David Rehak - Ibrahim Almarzouqi - Lucia Janusova *

CRITICAL INFRASTRUCTURE DESIGNATION IN EUROPEAN UNION COUNTRIES: IMPLEMENTATION OF SYSTEMS APPROACH

The contribution deals with the issue of designating critical infrastructure elements in European Union Countries. Based on approach analysis in selected countries, where sufficient attention is paid to the area of critical infrastructure, the aim of the article is to propose a systems approach to critical infrastructure designation. The aim is determined by the fact that a significant number of EU countries do not currently apply the systems approach and designating of elements is realized via sectors approach, i.e. without taking possible bonds with other sectors into consideration. Therefore, using the systems approach may be a solution to realizing further necessary steps in the area of critical infrastructure protection, for example complementing the issue of resilience and modelling dependences in the area of critical infrastructure.

Keywords: *Critical infrastructure, designation, systems approach, European Union.*

1. Introduction

The primary demand for sustaining development of EU countries´ economy and sustaining required level of society´s welfare [1] is providing continual supply of commodities and services via the infrastructure system [2]. These infrastructures may be divided according to functional specifications into technical (e.g. energy, transport) and socioeconomic such as the health service or financial market [3]. The individual infrastructures then come into effect as to expanse and value of the area for which they provide their services (European, national, regional), as well as regarding the importance or indispensability of the given services [1 and 2]. Infrastructures are growing more and more interconnected and in some cases even mutually dependent [4 and 5]. Functionality of these infrastructures and providing continual supplies of products and services is continually exposed to the impact of natural and anthropogenic threats [6]. That is the reason why significantly more attention has been paid to chosen, vital, even critical infrastructures [7 and 8], as well as to methods of its risk analysis, critical elements evaluation and their protection [9 and 10].

Building protection and resilience [11] of critical infrastructure elements is above all based on identification of critical infrastructure elements themselves, which is carried out via various approaches in the European Union and other parts of the world. These approaches are based on risk analyses [12 and 13], criticality analysis via various criteria [3], cross-section and sectoral criteria [2] or modelling and simulations [14]. The core of various approaches comparison is its evaluation from the point of view of entrusted responsibility for the critical infrastructure as well as the way of marking elements on various vertical levels.

2. Description of the system approach in selected countries

The system of critical infrastructure determination in the European Union proceeds from historical connections and the presented Green Paper [1]. The European Union member countries are bound to implement the procedures stated in the directive [2]. Since individual member countries approach the critical infrastructure determination in different ways, four countries whose critical infrastructure determination is system based were selected. System approaches of these countries will be used as the basis for proposing a system solution of critical infrastructure determination for European Union member countries which have not had the system approach yet. The key to the choice of the system for critical infrastructure determination is the following. The Swiss system of critical infrastructure determination was chosen as a model one, because specific

* [1]Petr Novotny, [1]Jiri Markuci, [1]David Rehak, [2]Ibrahim Almarzouqi, [3]Lucia Janusova
[1]Department of Civil Protection, VSB-Technical University of Ostrava, Czech Republic
[2]Department of Geography and Environment, Northumbria University, Newcastle upon Tyne, United Kingdom
[3]Department of Technical Sciences and Informatics, Faculty of Security Engineering, University of Zilina, Slovakia
E-mail: novotny.petr@vsb.cz

authorities are involved in the whole system. On the other hand, the British model was selected as the representative of traditional involvement of state authorities and rescue services in the choice of the critical infrastructure determination. Further, the system approach in the Netherlands has been selected as a representative of the traditional system solution, which is specific for developed European countries. Last, but not least, there is the long-term approved system of critical infrastructure determination in New Zealand. To contrast the system approach, the way of critical infrastructure determination in the Czech Republic will be presented in the following chapter.

2.1. Switzerland

The critical infrastructure system in Switzerland has undergone an evolution. The Federal Council`s Basic for Critical Infrastructure Protection [15] (also used as "CIP") was the key foundation for processing the crucial document for critical infrastructure determination process, which is the method for creating critical infrastructure protection inventory (Schutz Kritischer Infrastrukturen – SKI) [16]. The method´s aim [16] is to determine elements of infrastructure which show a high level of criticality. Criticality is connected with consequences that may occur at failure, malfunction or destruction of the relevant infrastructure element, however, the probability is not considered (this classification should enable an adequate determination of funds and measures). Besides other things, critical infrastructure elements on a national or regional level are to be identified. During the inventory preparation there are three groups of participants [16]. The basic group, which works on the inventory development and creates the basics for a thorough analysis of individual processes, is an expert committee participating in critical infrastructure elements identification. The last group of participants is represented by cantonal contact authorities of the SKI inventory that may identify objects important from the cantonal point of view as well as critical from the national point of view.

Within critical infrastructure protection, a list of objects, by the failure or damage of which the population and their living conditions may be endangered, has been created. These are objects which are of great importance for basic goods and service supplies, and objects where dangerous substances are stored [16]. Identification of critical infrastructure elements [15] follows a standardized process on the basis of three unified criteria (quantitative evaluation, qualitative evaluation, potential threat) and it is based solely on detailed process analyses in individual sub-sectors which are created by authorized national subjects. Five following steps are taken in order to identify and classify critical infrastructure subjects in individual sub-sectors [16]: (1) Creating a functional group for criticality evaluation, (2) preparation for criticality evaluation, (3) detailed data gathering, (4) objects classification, (5) amendment for cantonal subjects. Such a list of critical infrastructure elements [15 and 16] is classified as top secret from the point of view of secret information protection. The creation of the inventory is carried out and managed by the basic group only.

2.2. Great Britain

The main responsibility for the matter in question is borne by the Cabinet Office (evaluation of critical infrastructure elements vulnerability). Monitoring is continually realized by the ministries and authorities, however, once in 5 years there is an overall inspection, so called National Risk Assessment, carried out [17], the outcome of which is evaluation of the found risks (natural disasters, serious accidents, deliberate attacks) which may affect the whole country or its significant part. The National Risk Register [17] has been processed since 2008 as meeting liabilities coming out of the National Security Strategy [18]. Local rescue services are integrated into the risk evaluation system. Each local rescue service publishes its own Community Risk Register [17] for its area of interest and for the relevant territory on web pages. Measures planned by all organizations and operators should draw from the National Risk Register. The document of Strategic Framework and Policy Statement [19] for the area of improving the critical infrastructure resistance to natural threat provides instructions for how to evaluate the criticality of critical infrastructure area to all subjects involved. The document outlines possibilities for regional critical infrastructure determination (the term Vital Infrastructure corresponding with local infrastructures is used).

The national critical infrastructure in Great Britain is divided according to the Criticality Scale [19] into 9 sectors and 29 sub-sectors, including determining responsibilities for sub-sectors in the whole kingdom and individual countries. Seven categories of criticality draw from such evaluation (CAT 0 – CAT 6). CAT 3 forms the border between the Critical National Infrastructure and an infrastructure that may be interpreted as a regional critical infrastructure, since the possible impact on a geographic region or several hundred thousand people is defined here. From this level downwards we speak about Wider National Infrastructure including the above mentioned vital infrastructures providing services in certain location [19]. The level of criticality is thus determined merely for the national level of critical infrastructure. Any criticality evaluation under this level means determining the infrastructure as Wider National Infrastructure, not as critical. For that reason, only the national level is determined as critical. The risk evaluation system is also projected in the system of infrastructure criticality determination [19]. The planned measures for critical infrastructure protection draw from risk evaluation. All activities in the sphere of CIP in Great Britain strictly stick to standards of the Business Continuity

Management (BS 25999). Therefore, following all determined processes from the level of central authorities down to the local level is emphasized. At the same time, doing all pre-determined duties is ensured.

2.3. Netherlands

The Government of the Netherlands - The Cabinet is an authority responsible for the area of critical infrastructure protection in the country and this authority approved the National Safety and Security Strategy in 2007 [20 and 21]. According to this strategy, the national safety cannot be taken out of the complex safety context which proceeds from the partnership within the EU and NATO member countries. The performance of some entrusted activities in the sphere of critical infrastructure also belongs to risk management authorities across the risk management levels, including the public administration authorities. In the Netherlands, the original definition of "critical infrastructure" [22] included only the areas of public administration and industry (including the ICT area) and the original plan comprised the following steps: a fast analysis of the Dutch critical infrastructure, stimulation of bonds between the public administration and private subjects, threats and vulnerability analysis, analysis of safety measures gaps. After fulfilling the National Safety and Security Strategy, [20] A Quick Scan was created and used [21]. Since cross-border bonds were found out, some of the materials were given to the European Union.

The Ministry of Security and Justice and Ministry of Interior and Kingdom Relations [20] bears the primary responsibility for determining critical infrastructure elements. In order to increase the system flexibility, two working groups were appointed across the central authorities, which are Interdepartmental Working Group on National Safety and Security and Steering Group on National Safety and Security. First, the working groups evaluate the possible dangerous scenarios on a national level, based on The National Safety and Security Method, then consequences are described and probabilities of relevant scenarios are evaluated. Such scenarios are projected in the National Risk Assessment and, consequently, final summary of scenarios and its evaluation with respect to interest and consequence (territorial safety, physical security, economic security, and ecological security, social and political stability) is carried out. After evaluating the consequences it is possible to use the gained data further on, e.g. for public administration purposes [20].

For the needs of critical infrastructure determination in Netherlands, a boundary was set between services and products that are vitally important on the national level and those which are "only" very important [21]. Because of bonds and dependencies, operation-oriented analysis is required, in which the ICT sector plays an important role, as it currently connects and controls most infrastructures. The process of determining the vitally important infrastructure had not been easy until "Vital Importance" was determined within a company. According to the definition, these are products and services which [21] contribute to providing basic services for a society and define the basic level of its providing for (1) national and international law, (2) public safety, (3) economics (4) public health, (5) environment. These products and services may also reduce providing services for the population or public administration below the minimum level also in the national scale.

11 vitally important sectors with 31 vitally important products and services (an analogue of sub-sector) have been determined for the national critical infrastructure of the Netherlands. From the point of view of the national critical infrastructure of the Netherlands, it is these vitally important products and services (direct and indirect ones) which form the core of the system, while other products and services (not of vital importance) supplement the function of the whole system [21].

2.4. New Zealand

The core document for the civil protection of New Zealand is the Civil Defence Emergency Management Act 2012 [23]. This crucial document determines authorities, responsibilities and involvement of all involved services in the civil protection in the country. Based on the provisions of sections 39 and 45 of the Civil Defence Emergency Act, a new National Civil Defence Emergency Management Plan [24] has been created, in which all substantial requirements for the area of critical infrastructure defense are elaborated and stated. The aim of the plan is to increase public awareness, understanding and readiness in the field of Civil Defence and Emergency Management (CDEM), to reduce risks, to increase capacities for emergencies control and to increase the capacity for recovery after emergencies. The CDEM Plan also states tasks and responsibilities of subjects involved in protection of critical infrastructure elements, such as the Ministry of Civil Defence and Emergency Management for the national level, Local Civil Defence Groups and Local Authority for the local level. The working authority is always the group appointed for the relevant level, the so called "CDEM Group". Thus, there are advisory authorities called Clusters, i.e. groups comprising agencies across sector in order to cooperate effectively and reach practical outcomes. The above mentioned authorities participate in CIP.

However, the term of critical infrastructure is not used in New Zealand [23]. On the contrary, it is common to label some subjects as Health infrastructures and the term Lifelines is used instead of the term of critical infrastructure to mark basic systems for which it is necessary to remain in function, e.g. water supplies, transport (road, rail, sea and air), gas supplies, communication networks and sewage systems (water and sewage management).

The primary aim of supporting the Lifelines evidence by Central authorities is recognition, effective evaluation and evaluation of the subject´s importance [23]. Individual regions thus carry out evaluation and report data to the central level of the Ministry of Civil Defence and Emergency Management. In case some of the Lifelines shows high criticality and the consequences of its failure affect society outside the region, we speak about the national level, etc. The term Lifeline Utilities is used for the national level of critical infrastructure in New Zealand. Another option to determine such infrastructure on a national level is a direct determination in a legal regulation [23], (for example, keepers of enumerated airports, harbors, gas suppliers, etc.) or subjects mentioned in the following part that run enumerated businesses (running a national motorway network, railway network, electricity and water suppliers, etc.). In total, we can categorize the elements into eight sectors (or, as the case may be, determine specific elements) [23 and 25].

Determining the criticality of Lifeline Utilities [26] is based on the CDEM Plan. Categorizing Lifeline Utilities into relevant categories is carried out according to the outcomes of criticality determination. Criticality 1 for the national level of Lifeline Utilities, Criticality 2 for the regional level of Lifeline Utilities, Criticality 3 for the local level of Lifeline Utilities. Runners of Lifeline Utilities are obliged to abide carrying out of the prescribed activities in New Zealand, e.g. constant verifying and developing emergency plans, risk evaluation and preparation for reaction including constant reporting of the updated data to the subjects responsible [25].

In the above mentioned crucial document, [23] the need to protect the so called *Assets* is also stated. These are key elements like cultural and historical heritage. These subjects may also be determined as "critical infrastructure" elements in New Zealand. On the other hand, another commonly used term of Infrastructure Hotspots means accumulation of entries into several "critical" infrastructures on a single location (e.g. harbors) [26]. A similar term is used in other countries, e.g. in relevant literature [27] such cumulative entries are called Hubs. At the same time, dependencies were determined under the term of Infrastructure Interdependencies across sectors and currently programs for resilience improvement are being specified [26].

3. Sector approach description in the Czech Republic

Since 2010 and with effect from 2011, the critical infrastructure in the Czech Republic has been in function by implementation of Directive requirements [2] into the National legislature via the Crisis Management Act [28] and its implementing regulation [29]. The Ministry of the Interior – General Directorate of the Fire Rescue Service of the Czech Republic is the guarantor of the critical infrastructure in the Czech Republic. Thus, in the Czech Republic, critical infrastructure elements are determined at two vertical levels by law (National and European), while the national level is the implicit one. In the Czech Republic, elements at the national level are determined in nine sectors altogether (Energy, Water management, Food Industry and agriculture, health service, transport, Communication and information systems, Financial market and currency, Emergency services, Public administration). The way of determining the elements for individual levels is, in accordance with the Directive, [2] based on cross-cutting and sectoral criteria [28 and 29]. The cross-cutting criteria serve to evaluate the impact caused by potential malfunction of the evaluated element of the relevant critical infrastructure sector. These criteria serve to evaluate the impact with regard to possible casualties, economic impacts and impacts on the public [30]. Limit values of these criteria at a national level are stated by a decree of the Czech Republic government [29].

In case the critical infrastructure subject (Owner, Runner) is an organization bureau of the state, ministries and other central administration authorities send their proposals for elements to the Ministry of the Interior that prepares a list based on these proposals. In the following stage, the list is presented to the government who adopts a resolution about the critical infrastructure elements whose runner is the organization bureau of the state [31]. In case of determining the critical infrastructure elements whose runner is not an organization bureau of the state, the decision-making process is realized by entrusted ministries and other central administration authorities. These, in accordance with the law, apply relevant definitions and criteria and subsequently determine elements by general measures and immediately inform the Ministry of the Interior about their decisions.

It is the critical infrastructure subject itself who bears the responsibility for the critical infrastructure element protection [28]. For this purpose, the subject is, apart from other responsibilities, obliged to make a plan for the crisis readiness of the critical infrastructure subject [32 and 33]. Within the plan, the following areas should be considered: (1) overview and evaluation of possible risk sources, (2) threat analyses, (3) possible risk impact on the subject´s activities (4) a list of critical infrastructure elements within the subject´s control, (5) identification of possible threats of individual elements of the critical infrastructure, (6) measure overview arising from the emergency plan of the relevant risk management authority, (7) ways of securing realization of the mentioned measures, (8) ways of securing the subject´s action readiness to realize the emergency measures and subject´s activity protection and (9) procedures of solving emergency situations identified in the threat analysis. The necessity to increase the resistance and protection of critical infrastructure elements to possible risks and securing a broader involvement of critical infrastructure subjects in the process of preparation for emergency situations is one of the strategic priorities of population protection stated within the current population protection concept [34].

4. Summary, Suggestion and Discussion

This chapter summarizes the above mentioned approaches as materials for creating a system approach proposal. From the point of view of the state administration involvement there were no fundamental differences found, since in the selected countries it is always the top authority that bears the responsibility on the national level, alternatively it is the authority affiliated to the top management level. The involvement of the home rule in the critical infrastructure determination system is similar, though there are minor differences among the individual systems. In several cases the rescue services are involved, in other cases the home rule is involved. The responsibility for critical infrastructure determination is more varied – it is possible to leave the responsibility on the central level, divide it between the state administration and the home rule, leave it on the created authorities, shift the responsibility to the relevant level of management, alternatively to the owners or runners themselves, or a combination of any of the above mentioned approaches.

The initial framework of determining critical infrastructure elements differs in individual countries. It may be a clearly stated procedure according to an obviously described manual with clear outcomes, or a procedure stated only by conceptual material. It is similar with the case of the methodology used, when individual countries use their own procedures. However, there is a significant difference in the terminology used in individual countries. It is not always "critical infrastructure" that is in question; the terminology may be set in a different way. The numbers of sectors vary in a narrow interval, just as the numbers of sub-sectors on a national level do not vary significantly. The number of levels does not vary much either. In the European Union countries it is obligatory to determine the supranational critical infrastructure (or the European level). From the national level upwards, the system stays similar – in most cases it is the national, regional, or local level (in some cases with different terminology though). In the Czech Republic there is no other critical infrastructure determined but national. For this reason, the proposal for determining the critical infrastructure on a regional level is justified further on in the contribution.

On the bases of comparison of the above mentioned approaches to determining the critical infrastructure, a general proposal has been created. This proposal may be applied in countries which do not have such elaborate systems, e.g. the Czech Republic (see Fig. 1).

From comparison of the approaches to determining critical infrastructure elements it is obvious that the first suitable step to assess which elements belong to which level (e.g. the regional level) is assessing their criticality. Such assessment is based on various principles in different countries (cross-cutting and sectoral criteria, assessment of impact and vulnerability, etc.). A common aspect can be seen in assessing the extent of impacts on protected interests (lives, health, properties, and economy). Assessing criticality should not be based on probability of occurrence of those impacts, which are mainly because of the fact that a failure of a critical infrastructure element is very improbable. Nevertheless, there is still little probability of its occurrence. During criticality assessment it is also suitable to implement the issue of mutual dependencies and perceive it from

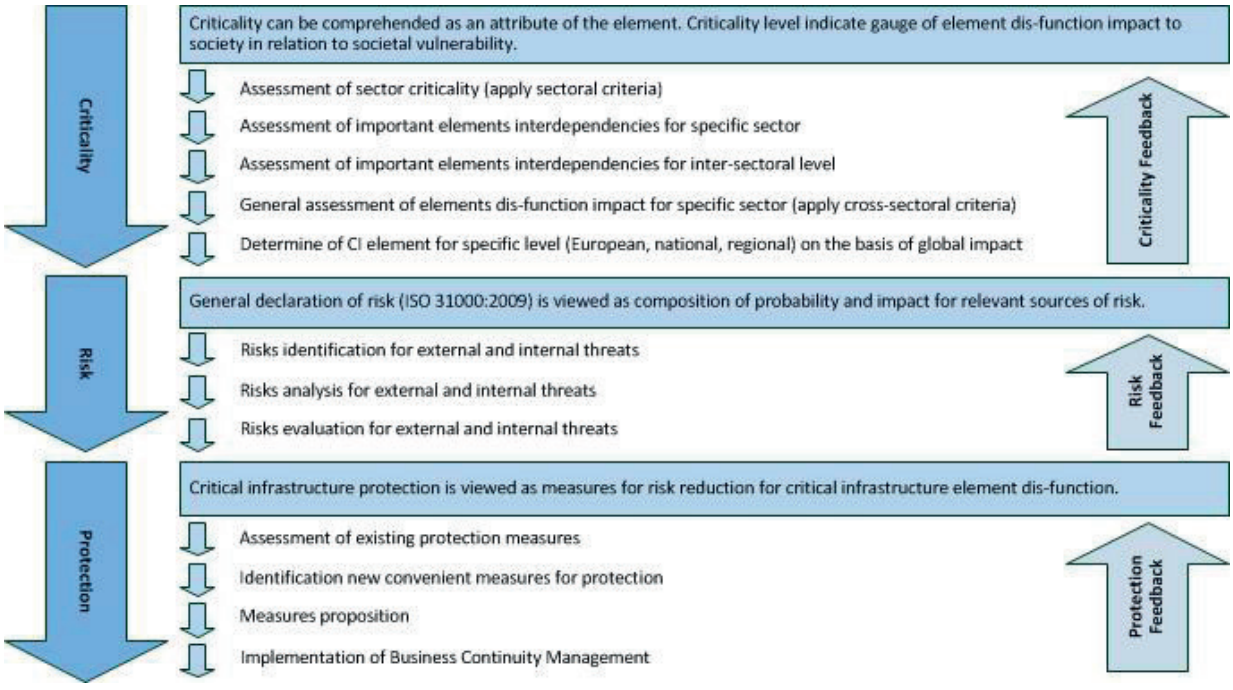

Fig. 1 Proposal of systems approach to critical infrastructure determination

the viewpoint of impacts that may be caused by bonds of the spreading disturbance among the critical infrastructure elements across the sectors (sub-sectors).

The second step is risk assessment [35] of a critical infrastructure element (determined according to step one) considering external as well as internal threats that may cause an element function disturbance. The risk extent is usually stated as a product of occurrence probability and impact extent. It is necessary to plan relevant measures based on the assessment. The planning documentation of critical infrastructure elements protection differs in individual countries (Operator safety plan, Emergency readiness of the critical infrastructure subject Plan, Business Continuity Plan). Nevertheless, the aim of all this documentation is identical – to provide a continuous supply of commodities and services [36] provided by the critical infrastructure element.

5. Conclusion

It is important to carry out critical infrastructure safety measures by relevant procedures, i.e. besides other things, make a suitable analysis, and not use common procedures without considering their suitability. Wrong usage of the Paret´s principle can serve as an example, which states that 20 % of causes bring about 80% of all effects. In spite of that, excluding all other causes and concentrating only on some of them may be a mere overlooking other causes, which does not lead to a system solution. A similar summary is presented in the risk matrix where the most numerous incidents do not cause any significant effects; on the other hand, rare incidents may cause extreme effects. For that reason, it is not purposeful to concentrate only on the most frequent causes and effects, but we should concentrate on system solution with all its causalities.

Based on the above mentioned approaches in selected countries, it would be suitable to set a system way of critical infrastructure determination that could be used e.g. in countries that do not have a similar system approach for all levels of critical infrastructure. In the Czech Republic, there has not unfortunately been a similar system way of critical infrastructure determination stated yet. The proposed Stating such approach would undoubtedly contribute to society´s safety and at the same time, it would increase the land potential as well as possible hidden drawbacks in the current way of critical infrastructure determination in the Czech Republic and elsewhere.

Acknowledgement

This article 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] Green Paper on a European Programme for Critical Infrastructure Protection (COM(2005)576). Brussels: Commission of the European Communities, 2005.

[2] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infra-structures and the assessment of the need to improve their protection.

[3] FEKETE, A.: Common Criteria for the Assessment of Critical Infrastructures. *Intern. J. of Disaster Risk Science*, 2011, vol. 2, No. 1, pp. 15-24, ISSN 2192-6395.

[4] RINALDI, S. M., PEERENBOOM, J. P. a KELLY, T. K.: Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, 2001, vol. 21, No. 6, pp. 11-25. ISSN 1066-033X. DOI: 10.1109/37.969131.

[5] PEDERSON, P. et al.: Critical Infrastructure Interdependency Modelling: A Survey of U.S. and International Research. Idaho: Idaho National Laboratory, 2006. 116 p.

[6] Global Risk 2014: Ninth Edition. Geneva, World Economic Forum, 2014. ISBN 13 92-95044-60-6.

[7] On the review of the European Programme for Critical Infrastructure Protection (EPCIP) (COM(2012) 190 final). Brussels: Commission of the European Communities, 2012.

[8] On a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure (COM(2013) 318 final), Brussels: Commission of the European Communities, 2013.

[9] LUKAS, L., HROMADA, M.: *Risk Analysis in Context of Critical Infrastructure Protection.* Annals of DAAAM for 2011 and 22nd Intern. DAAAM Symposium Intelligent Manufacturing and Automation: Power of Knowledge and Creativity, Vienna, November 2011, pp. 1469-1470. ISBN 978-390150983-4. ISSN 1726-9679.

[10] VIDRIKOVA, D., DVORAK, Z., KAPLAN, V.: The Current State of Protection of Critical Infrastructure Elements of Road Transport in Conditions of the Slovak Republic: Transport Means 2011, Proc. of the 15th intern. conference, Kaunas University of Technology, 2011.
[11] ROGERS, CH. D. F., BOUCH, CH. J., WILLIAMS, S. et al.: *Resistance and Resilience – Paradigms for Critical Local Infrastructure.* Proc. of the ICE - Municipal Engineer, 2012, vol. 165, No. 2, pp. 73-84. ISSN 0965-0903.
[12] REHAK, D., SENOVSKY, P.: Preference Risk Assessment of Electric Power Critical Infrastructure. *Chemical Engineering Transactions,* 2014, vol. 36, pp. 469-474. ISSN 974-9791.
[13] HOKSTAD, P., UTNE, I. B., VATN, J.: *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis*. Springer, 2013, 252 p., ISBN 978-1-4471-4661-2.
[14] OUYANG, M.: Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. *Reliability Engineering & System Safety*, 2014, vol. 121, pp. 43-60. ISSN 0951-8320.
[15] The Federal Council`s Basic Strategy for Critical Infrastructure Protection. Basis for the national critical infrastructure protection strategy. 2009, 8 p.
[16] Programm zum Schutz Kritischer Infrastrukturen. Methode zur Erstellung des SKI-Inventars, 17 p., 2010.
[17] Risk assessment: how the risk of emergencies in the UK is assessed. Detailed guidance - GOV.UK, 20th February 2013.
[18] A Strong Britain in an Age of Uncertainty: The National Security Strategy. 2010, 39 p.
[19] Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, London: Cabinet Office, March, 2010.
[20] National Safety and Security Programme: National Risk Analysis Method Guide, 2008. The Hague, 129 p., ISBN 978-90-5414-155-6.
[21] LUIIJF, E., BURGER, H., KLAVER, M.: Critical Infrastructure Protection in the Netherlands: A Quick-scan. Copenhagen: U. E. Gattiker (Ed.), EICAR Conference Best Paper Proc., 2003, 19 p., ISBN 87-987271-2-5.
[22] TWEEDE KAMER. Eerste voortgangsrapportage m.b.t. actieplan Terrorismebestrijding en veiligheid van 5 oktober 2001 [First progress report w.r.t. the action plan counter-terorism and safety dated 5 October 2001]. Tweede Kamer der Staten-Heneraal vergaderjaar 2001-2002, 27925(21), Hague.
[23] Civil Defence Emergency Management Act 2002. No 33. The Ministry of Civil Defence and Emergency Management, New Zealand, 2002.
[24] Revised National Civil Defence Emergency Management Plan. Wellington: Ministry of Civil Defence & Emergency Management, May 2014, 85 p., ISBN 978-0-478-43501-6.
[25] Lifeline utilities. Ministry of Civil Defence & Emergency Management. 2014.
[26] The Auckland Engineering Lifelines Project. Auckland: Auckland Civil Defence Emergency Management: Stage2, V1.1, Section 2, Feb 2014. 18 p.
[27] LEWIS, T. G.: *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Wiley - Interscience, 2006, 486 p., ISBN 978-0-471-78628-3.
[28] Act No. 240/2000 Coll. on Crisis Management and amending certain acts (the Crisis Act)
[29] Cabinet office directive No. 432/2010 Coll. On criteria for determining a critical infrastructure element
[30] DVORAK, Z., FUCHS, P., NOVAK, J., SOUSEK, R.: Individual and Social Risk During Transportation of Dangerous Substances, *Communications - Scientific Letters of the University of Zilina,* vol. 13, No. 2, 2011.
[31] Composite Authors:: *Critical Infrastructure Protection, 1st ed.* (in Czech), Prague: Ceska asociace bezpecnostnich manazeru, 2011, 189 p., ISBN 978-80-260-1215-3.
[32] Cabinet office directive No. 462/2000 Coll. for the implementation of § 27 para. 8 and § 28 para. 5 of Act no. 240/2000 Coll., on crisis management and amending certain laws (Crisis Act) as amended.
[33] DVORAK, Z., LUSKOVA, M., CEKEREVAC, Z.: *Risk Reduction in Critical Road Infrastructure in Central Europe,* WMSCI 2014 - the 18th world multi-conference on systemics, cybernetics and informatics, Orlando: Florida, pp. 234-239, ISBN 978-1-941763-05-6.
[34] *Population Protection Concept up to 2020 with Outlook to 2030 (in Czech),* Praha: Ministerstvo vnitra - generalni reditelstvi Hasicskeho zachranneho sboru Ceske republiky, , 61 p., 2013.
[35] ISO 31000:2009, Risk management - Principles and guidelines.
[36] STRELCOVA, S., REHAK, D., JOHNSON, D. E. A.: Influence of Critical Infrastructure on Enterprise Economic Security, *Communications - Scientific Letters of the University of Zilina*, 2015, vol. 17, No. 1, pp. 105-110, ISSN 1335-4205.