Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2011

RISK ANALYSIS IN CONTEXT OF CRITICAL INFRASTRUCTURE PROTECTION

LUKAS, L[udek] & HROMADA, M[artin]

Abstract: *The Critical Infrastructure Protection is essential for maintaining society functional continuity from the economic and social terms. In relation to this fact is necessary to create a framework for the formulation and determination of approaches, which should be in an optimal way to provide the necessary level of protection. Article will therefore discuss and establish the basic framework and scope for a comprehensive risk analysis, which will be based on the current environment and security research*
Key words: *critical infrastructure protection, vulnerability, risk analysis, threats, asset*

1. INTRODUCTION

For optimal expression of security measures is necessary to establish the scope and framework for a comprehensive risk assessment of identified assets. Identification should be multi-level, which creates a framework for defining security classes that will represent the growing importance or severity of individual assets (Council Directive 2008/114/EC). After completing the identification and designation process, the range of threats affecting the functionality of this critical infrastructure sector is set appropriately. The last parameter to be determined in the context of assets risk evaluation in the particular area is expressing and evaluating vulnerability, which is perceived as an expression of a weak spot in the system (Hromada, M., 2010).
The value alone will be based on current attitudes of quantitative risk formulation, which means that the risk value will be a numerical expression of product of assets numerical value, threat and vulnerability according to a relation:

$$R = A \times T \times V \quad (1)$$

R – risk
A – asset value
T – threat
V – vulnerability

For individual risk values will be consequently created intervals which will divide the risk into groups qualitatively expressing the risk.

2. IDENTIFICATION AND DESIGNATION OF CRITICAL INFRASTRUCTURE THREATS

Designation and identification of threats is an important process not only in relation to creating and determining the extent of assets risk evaluation but also in relation to threats categorization in critical infrastructure as a system (Lukas, L., Hromada, M. 2011). In this way, it is supposed that the threats division into individual groups will have an influence on the total risk measure. In the context with critical infrastructure in the area of energetics but also in other areas, there were indetified these groups of threats (RAMCAP Plus Approach, 2009):

- Intentional human activity,
- Technological failure,
- Environmental threats,
- Mutual dependencies of territorial threats

2.1 Intentional human activity

Intentional human activity is one of the most significant threat groups which influence the total risk value. In regard to the variability of the individual types of intentional human activity, I divided this group in the following table, where the most greatly concerned is the terorristic activity which is, even from the perspective of other studies in the object area, considered as essential.

Intentional human activity				
Type of activity	Description of activity			
Naval attack	N1 Small ship	N2 Fast ship	N3 Boat	N4 Ship with high draft
Aerial attack	A1 Helicopter	A2 Small plane	A3 Regional cargo plane	A4 International cargo plane
Terrestrial motorized attack	T1 Car	T2 Van or Pick up	T3 Mid-sized truck	T4 Truck with trailer
Terrestrial unmotorized attack	P1 1 attacker	P2 2-4 attackers	P3 5-8 attackers	P4 9-16 attackers
Sabotage	S1 Physical - Inside	S2 Physical - Outside	S3 Cybernetical - Inside	S4 Cybernetical - Outside
Theft and embezzlement	K1 Physical - Inside	K2 Physical - Outside	K3 Cybernetical - Inside	K4 Cybernetical - Outside

Fig. 1. Intentional human activity

2.2 Technological failure

Technological failure is another significant aspect increasing the given asset risk. In this area I chose those of the whole amount of technological factors which directly relate to functionality and availability of electric power. For a detailed picture, I divided them into groups:

Technological failure				
Type of failure	Description of failure			
Traffic breakdown	TB1 Traffic breakdown with a consequent explosion	TB2 Traffic breakdown with a consequent fire	TB3 Traffic breakdown with a leak of petroleum substances	TB4 Traffic breakdown with a leak of toxic substances
Operational breakdown	OB1 Operational breakdown with a consequent explosion	OB2 Operational breakdown with a consequent fire	OB3 Operational breakdown with a leak of petroleum substance	OB4 Operational breakdown with a leak of petroleum substance
Destruction of buildings	D1 Destructions of small extent	D2 Destructions of medium extent	D3 Destructions of large extent	D4 Total destruction
Technical failure	TF1 Repairable within 8hrs	TF2 Repairable within 16hrs	TF3Repairable within 24hrs	TF4 Repairable after more than 24hrs
Connection failure	CF1 Repairable within 8hrs	CF2 Repairable within 16hrs	CF3 Repairable within 24hrs	CF4 Repairable after more than 24hrs

Fig. 2. Technological failure

2.3 Environmental threats

Present days are characteristic with frequent changes of meteorological and climatic conditions which often increase the risk following from environmental threats. For the need of the risk analysis in the area of energetics, I defined and determined these environmental threats:

Environmental threats				
Type of threat	Extent of threat			
Fire	F1 Local character	F2 County character	F3 Regional character	F4 Of a character exceeding the borders of a region
Floods	FI1Local character	FI2 County character	FI3 Regional character	FI4 Of a character exceeding the borders of a region
Extreme heat and drought	EH1 Local character	EH2 County character	EH3 Regional character	EH4 Of a character exceeding the borders of a region
Strong frost	SF1 Local character	SF2 County character	SF3 Regional character	SF4 Of a character exceeding the borders of a region
Epidemy	EP1 Local character	EP2 County character	EP3 Regional character	EP4 Of a character exceeding the borders of a region
Earthquake	EQ1 Local character	EQ2 County character	EQ3 Regional character	EQ4 Of a character exceeding the borders of a region

Fig. 3. Environmental threat

2.4 Mutual dependencies of teritorial threats

Territorial threats often influence the assets functional continuity alone in the object area of critical infrastructure. These facts created a need to determination and identification of this threats group, which creates a framework for understanding mutual dependencies and potential danger. The territorial threats in question are:

Mutual dependencies of territorial threats				
Type of threat	Description of threat			
Territorial threats	U1 Loss of electrical equipment	U2 Loss of suppliers	U3 Loss of Employees	U4 Loss of customers
	U5 Loss of traffic		U6 Near presence of a dangerous conveyance	

Fig. 4. Mutual dependencies of territorial threats

Determination of scope for threats identification in the area of production, transmission and distribution of power is the second step in determining the extent and framework for carrying out the assets risk evaluation in the object area of critical infrastructure. This conceptual design is a draft which should be adjusted based on a current state analysis which should follow also from meetings with individual providers of these assets.

3. EXPRESSION AND EVALUATION OF VULNERABILITY

Following from the previous paragraphs, for the final risk determination of identified assets it is necessary to define the vulnerability of these assets. Vulnerability is in this relation understood as a numerical expression of probability of the threats coming through which may be perceived also as an expression of a weak spot of an identified asset. Following from the regional approaches analysis for vulnerability determination, the vulnerability is expressed by a decimal value or successfulness of the given threat's application (MURRAY, A. T. GRUBESIC, T., 2010). In order to comprehend this statement and to create a framework for determining of vulnerability in relation to the object area of critical infrastructure, these statements are in question:

With this table, the process of determinating of the scope and creating of the framework in order to carry out the critical infrastructure assets risk evaluation in a selected area of critical infrastructure is finished. The next step should be the application of this conceptual base into the process of assets identification and classification process into individual security groups.

Determination of vulnerability			
Numerical value of vulnerability	Decimal value	Percentage value	Successfulness of the given threat's application
6	0.90 – 1.00	90 – 100	9/10 ≤ T ≤ 1
5	0.75 – 0.89	75 – 89	3/4 ≤ T < 9/10
4	0.50 – 0.74	50 – 74	1/2 ≤ T < 3/4
3	0.25 – 0.49	25 – 49	1/4 ≤ T < 1/2
2	0.125 – 0.249	12.5 – 24.9	1/8 ≤ T < 1/4
1	0.0625 – 0.124	6.25 – 12.4	1/16 ≤ T < 1/8

Fig. 5. Determination of vulnerability

Subsequently, the knowledge base contained in this document is confronted with actual and relevant threats presence in an environment where the operation and impact of individual assets is supposed and required.

The creating of a threats and assets catalogue should be consequently a foundation and entry information database for applying the manner of vulnerability evaluation which actually closes the identification process of risk constituents in relation to critical infrastructure in the selected area.

Based on these facts and knowledge, it is possible to optimize and complete the process of setting up and relevant security measures, which express the relationship of risk, asset and security measure.

4. SUMMARY

Critical infrastructure and its protection is important from the viewpoint of maintaining the functional continuity of society in all its aspects. It is very important to formulate approaches and methodologies that positivly shape the actual level of protection. Article discusses the process of determining the potential risk through the application of created threats catalog, vulnerability determination approaches to the identified assets properties. This process is based on the specific requirements of operators of critical infrastructure in the relevant sector and it is accepted as an essential step to determine the optimum security measures to protect critical infrastructure.

5. ACKNOWLEDGEMENTS

This work was supported by the Ministry of Interior of the Czechb Republic under the Research Project No. VG20112014067 and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

6. REFERENCES

Hromada, M., *The European Critical Infrastructure Operator Duties*, In: Security Magazín, Číslo 95, 2010, ISBN–1210-8723

Asme Innovative Technologies Institute, Llc, . *All-hazard risk and resilience : Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach*. 1. New York : ASME, 2009. 155 s. ISBN 978-0-7918-0287-8

Lukas, L., Hromada, M. *Resilience As Main Part Of Protection of Critical Infrastructure*, In: INTERNATIONAL JOURNAL of MATHEMATICAL MODELS AND METHODS IN APPLIED SCIENCES, Issue 1, Volume 5, p. 1135-1142, 2011, ISSN: 1998-0140

Murray, Alan T. Grubesic, Tony. *Critical Infrastructure : Reliability and Vulnerability*. 1. USA : Springer, 2010. 311 s. ISBN 978-3642087738

Macaulay, T. Critical Infrastructure : Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies. 1. USA : Taylor & Francis Group, 2009. 320 s. ISBN 978-1-4200-6835-1

*** (2008) COUNCIL DIRECTIVE 2008/114/EC http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF

*** (2011) Zakon c. 430/2010 Sb. http://esipa.cz/sbirka/sbsrv.dll/sb?DR=SB&CP=2010s430