International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:9, No:3, 2015

Application Potential of Selected Tools in Context of Critical Infrastructure Protection and Risk Analysis

Hromada Martin

***Abstract*—**Risk analysis is considered as a fundamental aspect relevant for ensuring the level of critical infrastructure protection, where the critical infrastructure is seen as system, asset or its part which is important for maintaining the vital societal functions. Article actually discusses and analyzes the potential application of selected tools of information support for the implementation and within the framework of risk analysis and critical infrastructure protection. Use of the information in relation to their risk analysis can be viewed as a form of simplifying the analytical process. It is clear that these instruments (information support) for these purposes are countless, so they were selected representatives who have already been applied in the selected area of critical infrastructure, or they can be used. All presented fact were the basis for critical infrastructure resilience evaluation methodology development.

***Keywords*—**Critical infrastructure, Protection, Resilience, Risk Analysis.

I. Introduction

UNDERSTANDING the importance of critical infrastructure and its position in relation to society and societal needs can be objectively stated by motto: When we flip a switch, we expect light. When we pick a phone, we expect a dial tone. When we turn a tap, we expect drinkable water [1], [8].

These basic expectations and needs best express the importance of critical infrastructure for the maintaining of elementary functions and society. It is therefore clear that States have a need to create and build a system that will institutionalize the protection of critical infrastructure in the national legal environment.

One of the tools of critical infrastructure protection in the Czech Republic is the critical infrastructure body emergency preparedness plan, where legally required part of the basic structure withstands relevant application tools and information support for risk analysis. The following text will therefore present selected application tools useful in the context of risk analysis in selected areas of critical infrastructure as an outcome of security research project related to critical infrastructure resilience evaluation system development [6], [7].

II. SRC (Security Risk Scorecard)

One suitable methodology respectively information support in relation to risk analysis which fulfills the above mentioned conditions already defined is the SRC (Security Risk Scorecard). This scorecard is a key part of the methodology to better evaluate our security risks. It is designed to identify and assess the security risks that the Group faces. The scorecard will be the mechanism used to gather the information necessary to develop an overall view of the Group's risk profile. The scorecard focuses on assessing the following key determinants of security risk:

- Economic impact - maximum level of impact (financial and non-financial) that could be suffered if a security incident occurred, given the current level of controls,
- Vulnerability - circumstances that impact the likelihood of threats materializing (including the status of controls; actions to enhance controls which have been completed, are planned or are in progress; special circumstances such as outsourcing),
- Frequency of occurrence - incident history as an indicator of the likelihood of threats materializing,
- Impact of occurrence - incident history as an indicator of the business impact of such events.

This scorecard considers five categories of security risks:

- Theft & fraud,
- Information security,
- systems security,
- Protective security.

A one page questionnaire is attached for each of the security categories detailed above. The questions address each of the key determinants of security risk:

A. Economic Impact

It is a maximum level of impact that the business unit could suffer, in context of a security incident occurrence. Factors considered are legal liabilities, increased expenditure or financial loss, degraded performance, impaired growth, loss of management control, brand/reputation damage, regulatory requirements and investigation/resolution.

B. Vulnerability

It means status of the current measures, as well as any actions to enhance the measures, which have been completed, initiated or planned.

C. Frequency of Occurrence

It summarizes the number of incidents, which have compromised security arrangements.

D. Impact of Occurrence

This section, completed last, uses the information provided by the level of threat section, to estimate the impact of historic incidents on the business. As for Economic Impact, Impact of

M. Hromada is with Faculty of applied informatics, Tomas Bata University in Zlin, Czech Republic (e-mail: hromada@fai.utb.cz).

Occurrence considers legal liabilities, increased expenditure or financial loss, degraded performance, impaired growth, loss of management control, brand/reputation damage, regulatory requirements and investigation and resolution. It also considers the impact of 'near misses'.

E. Near Misses

Near misses are defined as identified unresolved security exposures, including outstanding audit issues. To prevent double counting, identified attempted breaches of security have not been included in near misses as it is anticipated that they will be incorporated in 'vulnerability'.

This scorecard should be completed by, or on behalf of, the primary 'owner' of security for each Business Unit. The completion of the scorecards for each Business Unit will be coordinated by the Divisional Operational Risk Managers. The scorecards will also be subject to a quality assurance review by the Divisional Operational Risk Managers. The results will then be consolidated and summarized. The scorecard results will be analyzed to provide insight into:

- Actual risk profile versus acceptable risk tolerance faced at the Group, Division, and Business Unit levels,
- Actual risk profile versus acceptable risk tolerance faced at the Group, Division, and Business Unit levels,
- Areas of risk that may require further review or investment on security initiatives,
- Achievements of security 'owners' who are managing their risks within acceptable levels [2].

Security Risk Category 2: Information Security

Economic Impact & Impact of Occurrence	What is the maximum level of impact that the Business Unit **could** suffer if an information security incident occurred?		What impact (if any) **did** the incidents experienced over the last 12 months have on the business? (complete this section last)	
			Actual	
	4	Legal liabilities (also fines, penalties and compensation)	1	1 - Positive or Insignificant negative impact
	2	Increased expenditure or financial loss (loss of business, increased cost, asset damage/writedown)	1	2 - Minor impact
	3	Degraded performance (failure to achieve targets, loss of productivity)	3	3 - Serious impact
	1	Impaired growth (delayed new products or business lines)	1	4 - Very serious impact
	1	Loss of management control (over financial risks)	1	5 - Extreme impact
	3	Brand/reputation damage	1	X - Don't know
	2	Regulatory requirements	1	
	2	Investigation and resolution	1	

Fig. 1 Security Risk Scorecard – Economic impact [2]

III. Property Security Risk Survey

Other risk analysis methodology developed and used by Deloitte Advisory is just methodology Property Security Risk Survey. In relation with the physical protection is one of the most detailed. Its level of detail creates a framework for comprehensive risk analysis and in response to these risks, assessing the level of accepted safety/security measures by the quantitative approach.

Estimate the number of security incidents that have occurred in the last 12 months.

Refer individual Division guidance for category definitions	None		1-10		11-50		51-100		101+		Don't know	
	Actual	*Near Miss*	*Actual*	*Near Miss*	*Actual*	*Near Miss*	*Actual*	*Near Miss*	*Actual*	*Near Miss*	*Actual*	*Near Miss*
Kidnap/ransom	X											
Abuse/threats					X							
Assault	X											
Theft	X											
Accidents			X									
Availability of access (potential to damage)	X											
Unauthorised access (actual access but not damaging)	X											
Vandalism	X											
Fire	X											
Malicious destruction	X											

Fig. 2 Security Risk Scorecard - Frequency of occurrence [2]

For the purposes of this methodology were formulated following terminology areas:

A. Event

Occurrence of a particular set of circumstances; the event can be certain or uncertain; the event can be a single occurrence or a series of occurrences,

B. Hazard

It can be presented as a source of potential harm.

C. Likelihood

It is general description of probability or frequency. It can be expressed qualitatively or quantitatively.

D. Consequence

It is an impact of an event. There can be more than one consequence from one event. Consequences can range from positive to negative. Consequences can be expressed qualitatively or quantitatively. Consequences are considered in relation to the achievement of objectives.

E. Risk

The chance of something happening that will have an impact on objectives. A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. A risk is measured in terms of a combination of the consequences of an event and their likelihood. A risk may have a positive or negative impact.

F. Risk Treatment

The measures selection and implementation process to modify risk level. The term 'risk treatment' is sometimes used for the measures themselves. Risk treatment measures can include avoiding, modifying, reducing, eliminating, sharing, transferring or retaining the risk.

G. Inherent Risk

It is a risk, which is an intrinsic component of an event. It can be also seen through the implementation of risk treatment measures.

H. Residual Risk

The risk remaining after the risk treatment measures

implementation.

This terminology base is then applied to each portion of the risk analysis process in areas which are also perceived as separate units. It is mainly related to the following units:

- Building details,
- Base building,
- Perimeter security,
- Floor security,
- Area security,
- Protective lighting,
- Emergency,
- Key control, locking devices,
- Control of personnel and vehicles,
- Safety of personnel,
- Cafeteria,
- Car park and loading bay,
- Hijack controls,
- Theft,
- Visitors and mail,
- Plant,
- Locker rooms,
- Security guard forces,
- Security culture.

For each of the above mentioned areas are formulated relevant questions that define certain parameters assessed quantitatively evaluating their level.

Where is the cafeteria located?	
What are the hours of operation?	
Is it company or concession operated?	
What security measures are in place of cash proceeds from sales?	
What security measures are in place for security of foodstuffs?	
What is the method of supply of foodstuffs?	
How are garbage and trash removed?	
Where is the location of vending machines?	
Where is the change maker, if any?	
Score:	

Fig. 3 Property Security Risk Survey – issues [3]

Another important part, which formulates and qualitative approach to risk assessment is to determine the classification of assumptions and categories of priority areas:

- Qualitative measurement of "Event Likelihood",
- Qualitative measurement of "Event Consequence or Impact",
- Qualitative risk Analysis Matrix,
- Inherent risk Treatment Strategy.

Descriptor	Description
Almost Certain	The event is expected to occur at **least daily**
Likely	The event is expected to occur at **least weekly**
Possible	The event is expected to occur at **least monthly**
Unlikely	The event is expected to occur **once every 1 to 9 years**
Rare	The event is expected to occur **once every 10 years or greater**

Fig. 4 Qualitative measurement of "Event Likelihood" [3]

LIKELIHOOD	CONSEQUENCE				
	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
A - Almost Certain	HIGH	HIGH	EXTREME	EXTREME	EXTREME
B - Likely	MEDIUM	HIGH	HIGH	EXTREME	EXTREME
C - Possible	LOW	MEDIUM	HIGH	EXTREME	EXTREME
D - Unlikely	LOW	LOW	MEDIUM	HIGH	EXTREME
E - Rare	LOW	LOW	MEDIUM	HIGH	HIGH

Fig. 5 Qualitative risk Analysis Matrix [3]

	TIMING OF RESPONSE	NEXT ON SITE INSCPETION
EXTREME	Improved actions, resources and strategies are required to be implemented IMMEDIATELY to reduce, transfer or control the level of risk	Every 3 months
HIGH	Existing actions, resources or strategies must be modified AS SOON AS POSSIBLE to reduce, transfer or control the risk	Every 6 months
MEDIUM	CONTINUE to implement actions, resources and strategies to prevent and/or reduce the level of risk	Annually
LOW	MAINTAIN current actions, resources and strategies to prevent the escalation of the level of risk	Bi Annually

Fig. 6 Inherent risk Treatment Strategy [3]

It is clear that the methodology Property Security Risk Survey is especially useful in the context of assessing the relationship between the identified risks and security measures adopted. Its level of detail can be used in the assessment and physical inspection of selected objects in a selected area of critical infrastructure [3], [5].

IV. Sphere – Energy

Software tool SPHERE - ENERGY is a form of expert analytical tools for risk analysis. Analytical method is based on a compilation of several analytical methods for analyzing threats and risks with a focus on energy entities. This program resp. tool is a specific approach to data collection within a system and the subsequent implementation of these data into the program.

The program itself is divided into five areas respectively parts that are logically linked in sequence workflow in the implementation of risk analysis. The program is divided into the following parts:

- Window matrix - for creating Pivot Tables
- Window relationships - for displaying instantaneous connections between elements,
- Window entering data wizard - to edit the names of the threats created tables for the effectiveness of selection of relevant threats in the system under consideration,
- Window element values - for entering other parameters for individual elements,
- Results window - for displaying output in graphical form or in a tree correlations.

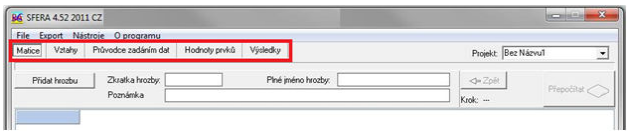

Fig. 7 Window matrix - for creating Pivot Tables [4]

A. Threats Database

Threat database is an important part of the aforementioned tools, where you can view the database of data entry divided into two basic groups. The first group consists of data that can be viewed from the perspective of coding threats and a second group of data characterizing a particular threat. For correct functionality of the program is expected in a given instrument that the draw key to encrypt individual threats, what ultimately allows selecting threats conveniently.

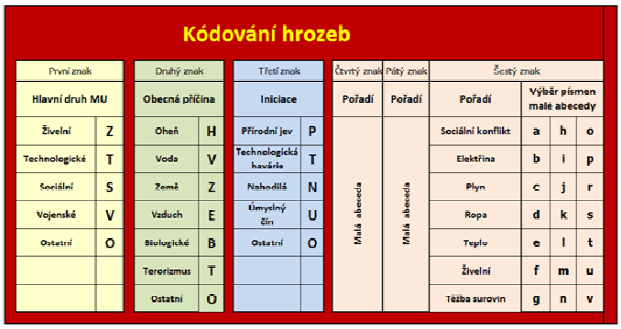

Fig. 8 Encryption of individual threats [4]

The first character key is the designation of main categories, which divides threats according to the type to natural, technological, social, military, and other. Each of these five groups are further subdivided by cause, therefore, according to the potential effects of the phenomenon on issues related to fire, water, etc.

The default database, which is primarily focused on the energy sector, includes over 500 items that are all the same for each threat. Created database is not a closed database, and it is possible to supplement and expand the range of other threats.

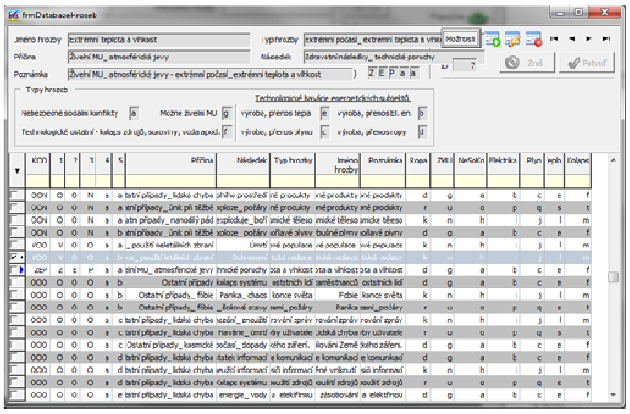

Fig. 9 Default threats database [4]

As mentioned at the outset, this analytical technique or tool is a form of a compilation of several analytical methods where significant aspect is the possibility of threats decomposition. Decomposition of the threat is within the scope of this tool is perceived as a state where the threat inserted to analyze to create a Pivot Table causes some form of feedback between one or more already embedded threats that the current system of threats divided input threat into two threats, one part of the threat system affects and the second part is influenced by threats system.

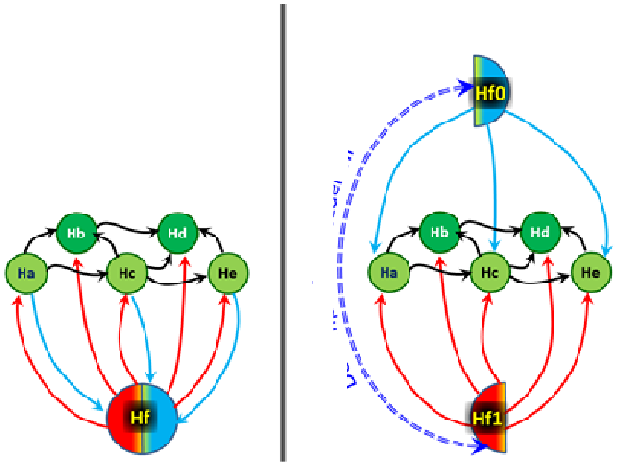

Fig. 10 Risk decomposition [4]

An important analytical process is the expression of complex cycles between contexts and threats in areas of:

- the threat affect - Which threats affects the identified threat,
- the threat does not affect- - Which threats does not affect the identified threat
- the threat is affected - Which threats directly affect identified threat, or may make its existence,
- the threat is not affected - Which threats do not directly affect the identified threat,
- feedback - Which threats affect the identified threat and simultaneously are affected by the same time.

At the finalization of the analytical process is the formulation of vulnerability criteria, which can be seen as important in determining the economic size of each of the selected threats, and thus determine the level of probabilities of occurrence of the threat, which is selected or manually defined by the length of the period in which it is expected, that a particular threat occur. Last part of this analytical process is an expression of the value of funding to prevention.

Visualization is output through the final ranking chart of tree correlations, where they present the results and possible impacts of assessed threats [8].

Software tool SPHERE-ENERGIE is an analytical tool for comprehensive vulnerability assessment and potential impacts or correlations of assessed threats to the selected system in the critical infrastructure energy sector energy. Its complexity creates a presumption to use its philosophical perspective to support the process of determining the methodology for critical infrastructure resilience evaluation for selected areas and elements, and also in relation to the fact that vulnerability is seen as important parameter of system resilience evaluation [4], [5].

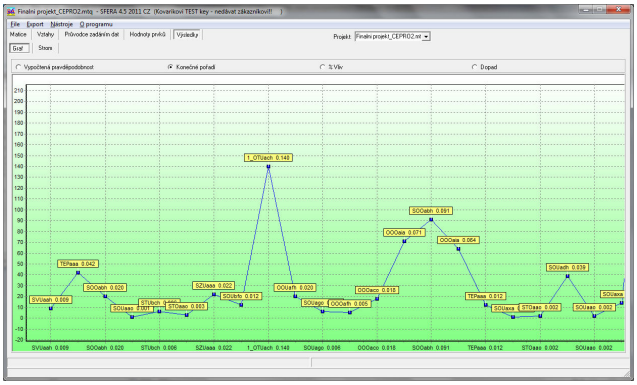

Fig. 11 Final ranking chart of tree correlations [4]

V. Conclusion

These publications presented and discuss potential application of selected tools of information support for the implementation and within the framework of risk analysis and critical infrastructure protection. Contribution of the text is viewed from the perspective of fulfillment of the selected part of the critical infrastructure subject emergency preparedness plan elaboration. Text describing the generally applicable methods to the most specific, also from the perspective of information support use in context of risk analysis. The text makes it clear that in the energy sector can be applied a wider range of approaches to risk analysis, which highlights its complexity and linkages with other areas of critical infrastructure.

Acknowledgment

The work was performed with financial support of research project NPU I No. MSMT-7778/2014 by the Ministry of Education of the Czech Republic and also by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

[1] USA, The physical protection of Critical Infrastructures and key Assets, 2003
[2] DELOITTE, SRC (Security Risk Scorecard)
[3] DELOITTE, Property Security Risk Survey
[4] Kovářík, f., zíchová, l. SFÉRA-ENERGIE, User Manual for the program,
[5] Rehak D, Danihelka P, Bernatik A. Criteria Risk Analysis of Facilities for Electricity Generation and Transmission. In Steenbergen et al. (eds). Safety, Reliability and Risk Analysis: Beyond the Horizon (ESREL 2013), 2014, pp. 2073-2080. ISBN 978-1-138-00123-7.
[6] Bernatik A, Senovsky P, Senovsky M, Rehak D. Territorial Risk Analysis and Mapping. Chemical Engineering Transactions, 2013, Vol. 31, pp. 79-84. ISSN 1974-9791.
[7] 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
[8] 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