Critical Infrastructure Protection and the Evaluation Process

Martin Hromada and Ludek Lukas

Department of Security Engineering
Faculty of Applied Informatics, Tomas Bata Univerzity in Zl ń,
Nad Str ánĕmi 4511, Zlín, Czech Republic
hromada@fai.utb.cz, lukas@fai.utb.cz

Abstract

Critical Infrastructure Protection importance is seen as basic element of maintaining vital societal functions from social and economic perspective. In relation to the needs of optimal and relevant protection and security measures selection is necessary to establish framework for Critical Infrastructure protection evaluation in relation and interconnection to risk assessment. This article discuss about conceptual approach of Critical Infrastructure Protection measures evaluation, which should be seen as an above-mentioned framework development, which it is based on the actual state of knowledge in Czech Republic.

Keywords: *Critical Infrastructure Protection, Physical Protection Systems, Administrative Security, Information Security*

1. Introduction

Critical infrastructure as a system is the essential part of society functional continuity, its economic or social structure and systems. In relation to this fact, there were created approaches, tools, which reflect above mentioned essentiality and created the framework for risk or those factors assessment system, which are able to affect the functionality and resilience. Critical Infrastructure Protection in the Czech Republic is guided by the Act 430/2010 Coll., which is seen as the 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 a European and national infrastructure (sectorial and cross-cutting criteria) as well as tools 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). These tools can be seen also from resilience evaluation point of view, where as we said before resilience is seen as an indicator that quantifies the ability to provide functionality in terms of internal and external factors effects, provided to the need of establishing the limits, where degradation of system functionality is acceptable and when it is not [1].

2. Critical Infrastructure Protection Structure

The main aim of Critical Infrastructure protection process is to reach the relevant security and protection level in relation to critical infrastructure functional continuity. Another goal is to ensure the disaster recovery process in case of the system function degradation. Identified and designated system components must withstand the effects of all threats and risks, that is seen as a principle of All Risk approach.

In relation to previous facts, we are able to say that the main usable aspect for optimal Critical Infrastructure protection level is combination of:

- Physical protection systems,
- Information security,
- Business continuity planning/management,
- Administrative and personal security,

2.1 Physical Protection Systems

In order to articulate the optimal system structure and functionality of the physical protection system of an element of the critical infrastructure, it is necessary to define the key functions of the already mentioned system and its sub-systems. In association with the comprehensive utilization of the physical protection system, three main system functions and its sub-systems parameters are considered:

- Detection – detection of an adversary with the use of technical security devices (AIR, PIR, MW Bistatic, MW Monostatic, dual sensor, etc.) and verification of the alarm information via the closed-circuit television (CCTV); parameter – probability of detection, the time needed for the verification of alarm information and probability of successful communication.
- Delay– hindering of the adversary with the use of mechanical barrier systems (fences, gates, barriers, grids, security doors, glass and other); parameter – breaking resistance
- Response – the response of the object’s guards – preventing or interrupting the activity of the adversary or his arrest even with the use of routine measures; parameter – the time needed for the guards to transfer from A to B [2].

The standard object of a critical infrastructure element is in relation to the needs of our research and in accordance with existing expert opinion is divided into 8 security zones Figure 1.

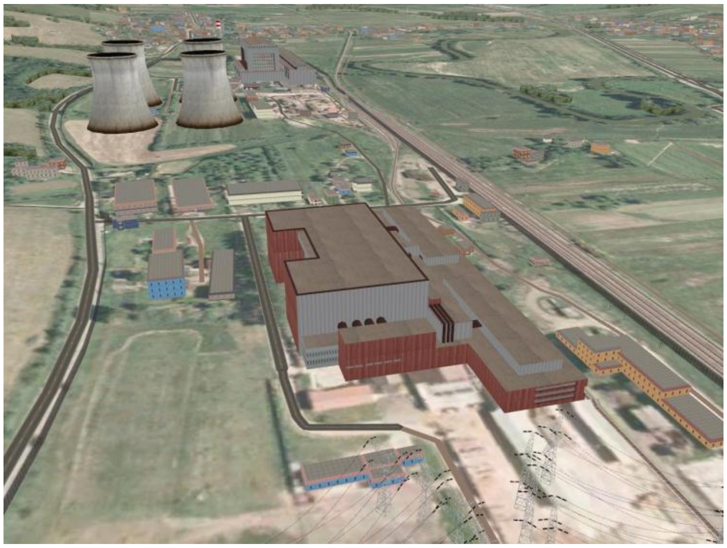


Figure 1. Critical Infrastructure Object Divided to 8 Security Zones

Each zone has its specific functional and structural parameters that affect the success of the intruder in achieving his aims. From the functionality point of view, we are talking about probability of detection, breakthrough resistance and time availability of response team.

Based on this approach the structure of the physical protection system was required, which is then subjected to the evaluation process; see Figure 2 [2].

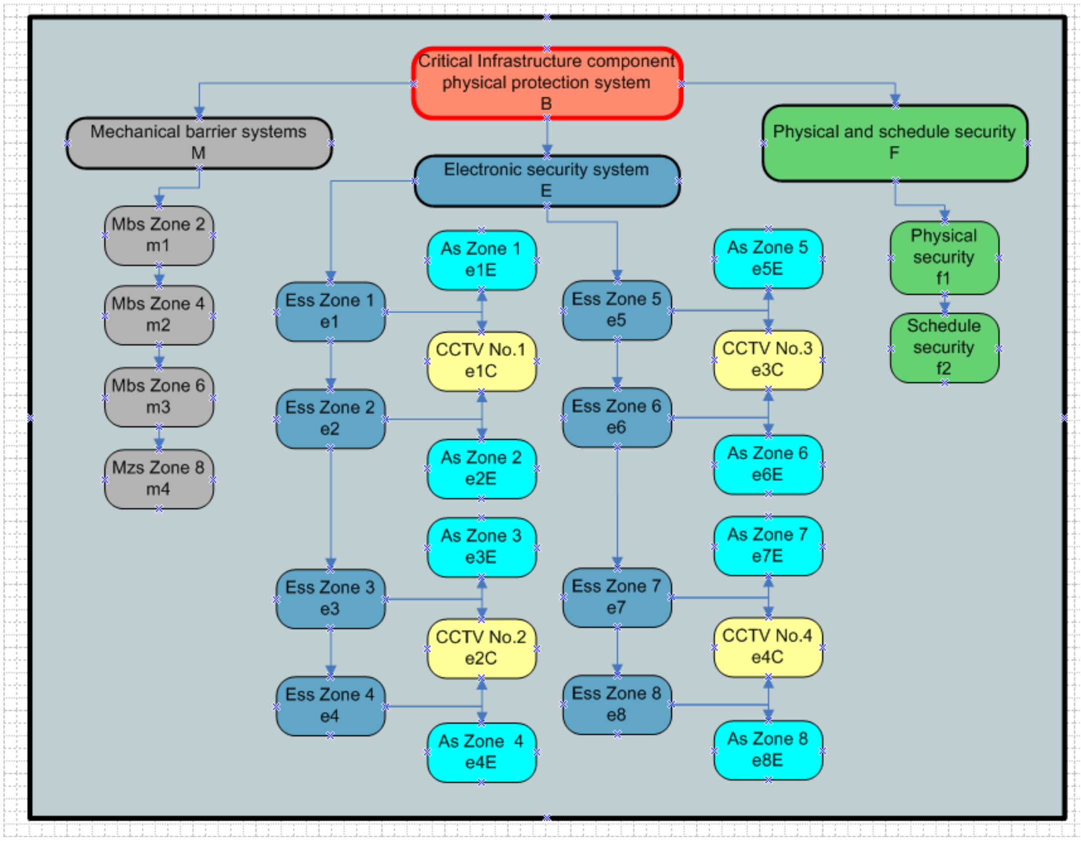


Figure 2. Critical Infrastructure Element Physical Protection System Structure

2.2 Information Security

Establishment and formulation process of information risk assessment system or information security management system is an important aspect of setting uniform standards to ensure the critical infrastructure entities information systems functionality. Information systems complexity and current trends in ICT increased emphasis on building security standards. Information (ICT) security is one of the cornerstones of the critical assets protection whether through the provision of security systems connectivity, or providing information protection maintained within the databases and information systems [3].

Following text identifies areas of information security management system, that are able to assess wide range of information risks and are relevant for critical infrastructure protection and security management system.

Table 1. Information Security

Information security	
Identification and authentication,	**Management control system,**
Management of logical access	**The security of routing tables,**
Audit,	**Operational control,**
The integrity of the software,	**Public key infrastructure,**
Backing up data,	**Check for software changes ,**
The resilience of the network,	**Customer authorization,**
System posting,	**Analysis of vulnerabilities,**
Testing of the system,	**Document/media**
Protection against malicious programs,	**Control users,**

2.3 Business Continuity

Business continuity is another important aspect of security and protection in terms of identifying needs and requirements to ensure functional continuity and system recovery of Critical Infrastructure in the event of disruption or interruption. The requirements formulation is crucial in relation to ensure the essential functions in the event of an emergency, area restoration and time intervals definition that are shorter or equal length than a specified maximum function acceptable time failure [4].

In relation Critical Infrastructure Protection evaluation, we defined areas, for better business continuity management system implementation:

Table 2. Business Continuity Management System Structure

Business continuity	
Business continuity management system (BCMS) structural requirements definition	**Crisis situation response team management level**
Personal structure of BCMS	**Crisis situation level**
Personal structure of crisis response team	**Crisis situation management and recovery**
Structural requirement of business continuity planning	

2.4 Administrative Security

The major part of protection and security management system related to selected area of Critical Infrastructure includes administrative aspects of security that addresses the process of ensuring adequate protection of documents in paper and electronic form and their creation, receipt, recording, processing, transmission, transportation, transfer, storage, shredding, and so on [5].

The main and perspective administrative security areas are presented in Table 3.

Table 3. Administrative Security Areas

Administrative security	
Responsibilities and duties	**Loss of documents and storage media**
The labeling and classification of documents	**Administrative security of personal changes**
Manipulation with documents	

2.4 Personnel Security

On the basis of previous project activities and consultations with the responsible authorities in selected area of Critical Infrastructure was like another part of comprehensive security and protection management system selected the area of personnel security, This area is perceived as a system of individuals selection in relation to access to information assets of Critical Infrastructure element, verification conditions for information access, protection and relevant education. The requirements focus on minimizing the impact of human errors, potential theft, fraud or abuse of information resources of the organization [6]. In relation to this fact, the main personnel security areas were defined.

Table 4. Personnel Security Areas

Personnel security	
Responsibilities and duties	Staff training
Employee screening	Responding to security incidents and failures
Agreements on the information security	The disciplinary process
Conditions for work activities	Termination of employment relationship

3. Critical Infrastructure Protection Evaluation

This chapter will discuss about approaches which should be used in relation to Critical Infrastructure protection management system evaluation where the structural properties in selected areas of each security or protection aspects should be seen as comparative criteria for process of multicriterial evaluation of Critical Infrastructure element protection management system. Each area should be for the process of evaluation concretized and compared by checklists [7].

3.1 Physical Protection System

Evaluation of functionality of these systems will be based on breakthrough resilience, detection probabilities, the probability of response team communication interconnection and temporal accessibility of the response team in respect of specific objects, that were defined for each security level and for the each security zones of Critical Infrastructure element on the basis of presented actual approaches to designing the physical protection systems. For purposes it is possible to use some relevant simulation tools.

3.1.1 EASI, ASD, SAVI (SANDIA NATIONAL LABORATORIES, USA)

These three closely interconnected methodics are based on detection of path with lowest cumulative probability of detection up to critical point of detection and are intended for evaluation of technical effectiveness of nuclear facility security. They utilize central division of security zones with one zone containing protected asset in middle of whole system and are based on intruder's familiarity with the security system.

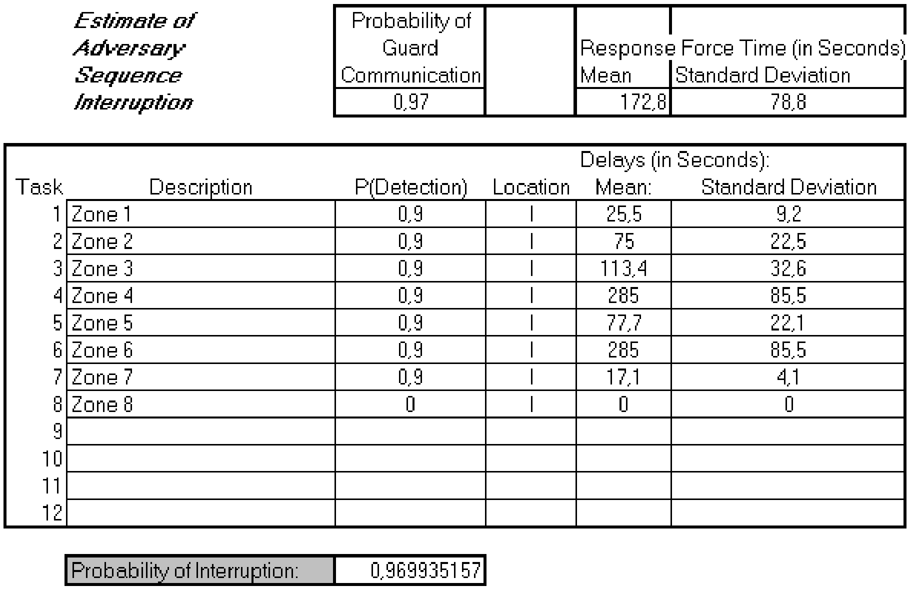
According to terminology used in these methods the path with lowest cumulative probability of detection up to critical point of detection is called critical path or path with lowest cumulative probability of interruption [9]. Detection before critical point of detection is called timely detection [8]. EASI method (Estimation of Adversary Sequence Interruption) allows calculation of probability of interruption only on one predefined path. ASD Method (Adversary Sequence Diagram) is method for graphic representation of possible intruder paths in security system. ASD describes facility and its security system as layers that separate external intruder from his target inside facility. Individual physical areas are separated by protective barriers that include everything that may delay or detect intruder [9].

SAVI method (Systematic Analysis of Vulnerability to Intrusion) combines EASI and ASD methods and evaluates every possible path to central zone from the viewpoint of probability of interruption, and creates list of ten most vulnerable paths according to their possibilities of interruption [8]. If values of probability of interruption are equal, it lists paths according to total length of attack. Main SAVI program is accompanied by extensive database of delay and detection parameters of most commonly used protection elements [9].

SAVI method implements also sensitivity analysis. Given that most critical parameter is time required for response, for sensitivity analysis SAVI uses different values of response force time. Output is of course probability of interruption.

From the viewpoint of modeling the main method of evaluation of effectiveness (calculation of probability of interruption) may be identified as suitable, but models do not completely reflect demands of systems for protection of persons and property from the viewpoint of modeling of protected area. Stated disadvantage (even from viewpoint of nuclear facilities) is absence of probability of intruder elimination calculation [10].

For purposes of further process the model EASI was used (Estimate of Adversary Sequence Interruption - Garcia M.L., The Design and Evaluation of Physical Protection Systems, 2007) [7], the output of which is the probability of successful interruption of an adversary activity (see Figure 3).



Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0,97		172,8	78,8

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Zone 1	0,9	I	25,5	9,2
2	Zone 2	0,9	I	75	22,5
3	Zone 3	0,9	I	113,4	32,6
4	Zone 4	0,9	I	285	85,5
5	Zone 5	0,9	I	77,7	22,1
6	Zone 6	0,9	I	285	85,5
7	Zone 7	0,9	I	17,1	4,1
8	Zone 8	0	I	0	0
9					
10					
11					
12					

Probability of Interruption:	0,969935157

Figure 3. EASI Model

3.2 Information Security

Each defined area of information security should be in the next evaluation process divided and concretized for better understanding and for evaluation process optimization by creating relevant checklist. Each positive answer is in the process of information security system evaluation considered as a point and the value (sum of the points) of selected information security system is divided by defined maximal value of information security system.

$$Iss = \frac{\sum IP_i}{IP_{\max}} \qquad (2)$$

Iss - information security system quality index,

$\sum IsP_i$ - the sum of positive answers,

$IsP_{\max}$ - defined maximal value of information security system

Formulation of the basic requirements for information security is another area of optimal security management system and Critical Infrastructure protection. For the purpose of Critical Infrastructure protection evaluation system will be this approach considered as an entry approach.

3.3 Business Continuity

Each defined area of business continuity should be in the next evaluation process also divided and concretized for better understanding and for evaluation process optimization by creating relevant checklist. Each positive answer is in the process of business continuity evaluation considered as a point and the value (sum of the points) of business continuity area is divided by defined maximal value of business continuity.

$$Bc = \frac{\sum Bc_i}{Bc_{\max}} \qquad (3)$$

Bc - business continuity system quality index,

$\sum Bc_i$ - the sum of positive answers,

$Bc_{\max}$ - defined maximal value of business continuity

3.4 Administrative and Personnel Security

Also in the process of administrative and personnel security aspects evaluation each defined area of these security aspects should be in the next evaluation process divided and concretized by creating relevant checklist. Each positive answer is in the process of administrative and personnel security aspects considered as a point and the value (sum of the points) of administrative and personnel security aspects area is divided by defined maximal value of business continuity.

$$As = \frac{\sum As_i}{As_{\max}} \quad Ps = \frac{\sum Ps_i}{Ps_{\max}} \qquad (4)$$

$As; Ps$ - Administrative and Personal security quality index,

$\sum As; Ps_i$ - the sum of positive answers,

$As; Ps_{\max}$ - defined maximal value of Administrative and Personal security [7]

4. Critical Infrastructure Protection and the Evaluation Process

For the purpose of multicriterial evaluation of Critical Infrastructure element protection it is necessary to define and establish relevant mathematical approach. In relation to previous text chapters, it is crucial to define optimal mathematical interconnections between these indexes.

Pss - physical protection system quality index,

Iss - information security system quality index,

Bc - business continuity system quality index,

$As; Ps$ - Administrative and Personal security quality index,

The first acceptable mathematical explanation of the Critical Infrastructure element protection level evaluation (CIP) is the basic multiplication by equation:

$$CIP = Pss * Iss * Bc * As * Ps \qquad (5)$$

We assume that in the case of probabilistic approach, the multiplication cumulating the probabilities which reduces the total probability and distorts the perception of the overall critical infrastructure protection level.

The second possible approach that is based on the current state of the knowledge is the expression of an average value of defined indexes:

$$CIP = \frac{Ps_S + Iss + Bc + As + Bs}{x} \tag{6}$$

x – number of defined indexes

It necessary to say, that there are a variety of possible mathematical approaches which can be used for Critical Infrastructure element protection level evaluation process, but it is not easy to select those that reflect the requirements of critical infrastructure owners/operators and their need for simplicity the evaluation process.

The relevant selection of the objective mathematical model will be based on practical verification of mathematical models in real objects (Critical Infrastructure element) and further discussions with responsible entities [7].

5. Conclusion

Article “Critical Infrastructure Protection and the Evaluation Process” discusses about the possible way how to develop relevant framework for Critical Infrastructure protection evaluation mostly in relation to increasing the resilience of its functional continuity.

The text is focusing on relevant areas which are usable also for resilience evaluation. We identified and established the security and protection measures areas that could be seen as relevant in present state of knowledge and based on actual requirements of Critical Infrastructure owners and operators.

Last part of the text is related to evaluation process in connection with Critical Infrastructure protection and security management system where the mathematical models were presented. We expect that all approaches would be confronted with real conditions and environment and also with simulation and modeling tools to reach optimal project results and outcomes.

Acknowledgements

This work was supported by the Ministry of Interior of the Czech 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.

References

[1] M. Hromada and L. Lukáš, “Conceptual design of the resilience evaluation system of critical infrastructure elements and networks in selected areas in Czech republic”, IEEE International Conference on Technologies for Homeland Security, **(2012)** November 13-15, Boston, USA.

[2] M. L. Garcia, “The Design and Evaluation of Physical Protection Systems”, Second edition, Sandia National Laboratories, **(2007)**, pp. 275, ISBN – 10: 0-7506-8352.

[3] M. Hyslop, “Critical Information Infrastructures, Resilience and Protection”, Springer, Middlesbrough, 1st ed., **(2010)** November, pp. 288, ISBN 978-1441944191.

[4] K. J. Engeman and D. M. Henderson, “Business Continuity and Risk Management, Essentials of Organizational Resilience”, Rothstein Associates, 1st ed., **(2011)** September, pp. 370, ISBN 978-1931332545.

[5] Decree No. 529/2005 Coll. On administrative registers and security of classified information, as amended (hereinafter the "Decree").

[6] Czech National Bank, “Principles of Security Policy of the CNB”, http://www.cnb.cz/cs/o_cnb/principy_bezpec_politiky.html.

[7] M. Hromada and L. Lukas, “Multicriterial Evaluation of Critical Infrastructure Element Protection in Czech Republic”, Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity, International Conferences, ASEA and DRBC 2012, Held in Conjunction with GST 2012, Jeju Island, Korea, **(2012)** November 28-December 2, Proceedings, pp. 361-368, 978-3-642-35267-6.

[8] Physical Protection of Nuclear Facilities and Materials, Albuquerque, New Mexico, USA.

[9] Analýza účinnosti systému bezpečnostní ochrany jaderných zařízení a jadrných material, **(1991)**, Ústav jaderných informácí

[10] T. Loveček, J. Vaculík and L. Kittel, “Qualitative Approach to Evaluation of Critical Infrastructure Security Systems”, European Journal of Security and Safety, **(2012)**.