Utilization of the EASI model in the matters of critical infrastructure protection and its verification via the OTB SAF simulation tool

LUDEK LUKAS, MARTIN HROMADA
Tomas Bata University in Zlín
T.G.Masaryka 5555, 760 01 Zlín
CZECH REPUBLIC
lukas@fai.utb.cz, hromada@fai.utb.cz, http://web.fai.utb.cz/

Abstract: The importance of critical infrastructure protection is perceived mainly through the lens of sustaining a functional continuity of society from economical and social standpoint. This fact has contributed to the creation of legislative, normative and institutional tools which are to form security environment and real approaches to critical infrastructure protection. It is obvious that the utilization of physical protection systems is one of the significant aspects of critical infrastructure protection, however, it is necessary to say that it lacks a comprehensive approach to determining optimal structural and functional demands on these systems. This article focuses on the utilization of the EASI model in the context of structure and functionality verification of the proposed physical security system of an component of the critical infrastructure and on verification of the outputs emerging from the EASI model via the OTB SAF simulation tool.

Key-Words: Critical infrastructure protection, physical security systems, EASI model, OTB SAF simulation tool, mechanical safety device, technical safety devices.

1 Introduction

Critical infrastructure protection is currently guided by an implementation of a 2008/114/ES directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In Slovakia, the implementation process is perceived through a passing of a law 45/2011 Coll. on critical infrastructure which specifies the identification and designation process of both the national and European critical infrastructures. Despite these facts, it lacks a comprehensive approach to protection and the process itself will be formed after the above-mentioned identification and designation process will be completed. The law makes it clear that one of the possible aspects of protection is utilization of security devices, by which (from §10 par. 2) "mechanical barrier systems, technical security devices, physical protection, administrative measures, schedule measures and their combination"[1] are understood.

This formulation, however, does not specify the optimal combination or its relation to functionality, neither does it set the necessary usage range of the mentioned security measures groups. It is obvious that in this process it will be necessary to use a simulation tool which, after having specified individual entities that will be entering the simulation process, would be a suitable means for the verification of the security measures structure and functionality and the operation of physical protection in case of breach into the protected space.

2 Physical security system of an element of the critical infrastructure

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

ISBN: 978-1-61804-004-6

routine measures; parameter – the time needed for the guards to transfer from A to B [2].

After this process implementation, a referential model of critical infrastructure element was created. It was subsequently divided into 8 security zones (Fig. 1.)

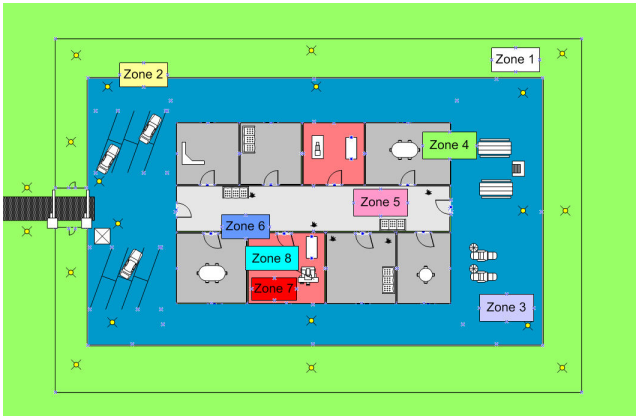

Fig. 1: Referential object divided into 8 security zones

Each of the defined zones was subsequently assessed by parameters (the adversary detection probability – technical security devices, breaking resistance – mechanical barrier systens, time needed to verify the alarm information – CCTV, adversary and guards time dependence in the guarded object and successful communication probability of the guards as well as standard deviations from these parameters) for individual sub-systems of the physical security system of the element KI. Based on this process, a physical protection system structure of a critical infrastructure component was determined. Fig. 2

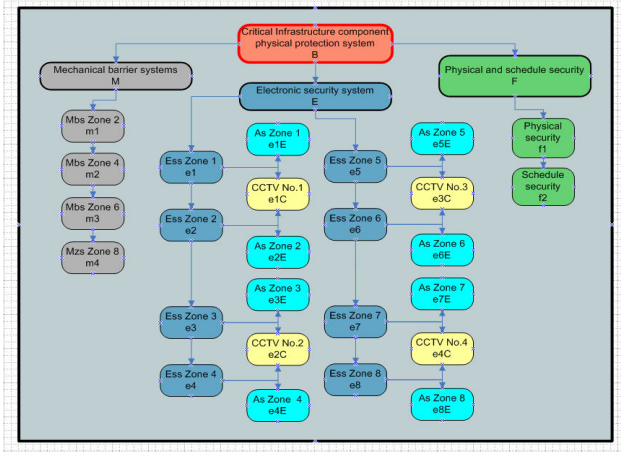

Fig. 2: The determined physical protection system structure of a critical infrastructure component

3 Evaluation of the system structural properties for physical protection of the critical infrastructure component

The actual process of evaluation of structural properties is seen as assigning point value to a particular component of the physical protection system according to its properties and determination that is expected with the distribution of critical infrastructure component into security classes, reflecting the growing criticism of the objects. Point values will be in the range of 1-4, where the value of 4 reflects the usability of security systems in the highest security for the largest class of criticality of the element.

While respecting the defined structure of the physical protection, the whole value system can be expressed in points of relations (1) and Table 1[3]:

$$B = \sum_{i=m1}^{m3} M_i + \sum_{i=e1}^{e8} E_i + \sum_{i=f1}^{f2} F_i \qquad (1)$$

B -Numeric value of security system
Mi -Numeric value of mechanical barrier systems
Ei -Numeric value of electronic security systems
Fi -Numeric value of physical and schedule protection.

Table 1 Maximal and minimal values of critical infrastructure components physical protection system

Minim. value Mbs	**Minim. value Ess**	**Min. value F**	**Security level SL**	**Minim. value** Ps	**Maxim. value** Ps
13	51	7	**IV**	71	**88**
9	35	5	**III**	49	70
5	19	3	**II**	27	48
3	15	2	**I**	**20**	26

Mbs – mechanical barrier systems, SL – security level, Ess – Electronic security systems, F – physical and schledule security, Ps – Critical Infrastructure component physical protection system,

In cases of application of the same procedure in the evaluation of other systems for physical protection of critical infrastructure elements in the sector, it is possible to express the average level of protection of critical infrastructure in this sector, then this value is qualitatively expressed (see Table 2).

ISBN: 978-1-61804-004-6

$$B_{norm} = \frac{B - B_{\min}}{B_{\max} - B_{\min}} \qquad (2)$$

B -Numeric value of security system
B_{norm} -Normative numeric value of security system
B_{min} -20 – minimal value of security system
B_{max} -88 – maximal value of security system

$$O_{ki} = \frac{1}{K}\sum_{k=1}^{K} B_{norm}, k \qquad (3)$$

O_{ki} -Numeric value of the security level in critical infrastructure sector
K -The number of critical infrastructure components in a given sector

Table 2 Quantitative explanation of security level in critical infrastructure sector [3]

Interval	**Levels of KI protection in the sector**
<-0,294; -0,014>	Poor
<0; 0,088>	Low
<0,103; 0,412>	Low to medium
<0,426; 0,735>	Medium to high
<0,750; 1>	High level of protection

4 Model EASI (Estimate of Adversary Sequence Interruption/ pravdepodobnosť prerušenia činnosti narušiteľa)

According to the above, structural assessment of the physical protection system of a critical infrastructure component lacks assessment of its functionality which specifies both the relation between the activity of the adversary and the guards and at the same time takes into account and utilizes the dependencies that emerge from basic structure and functionality demands and main system functions, which has been presented in the previous parts of this text. These dependencies may also be expressed by this relation:

$$P_D = P_S * P_T * P_A \qquad [4/51]$$

P_D - Probability of detection,
P_S - Probability of detection ability,
P_T - Probability of successful transfer,
P_T - Probability of successful assessment,

For this reason, an EASI (Estimate of Adversary Sequence Interruption) model was chosen. This model assesses and works with already determined parameters of the physical security system components where the outcome is estimation of adversary sequence interruption which is today used by National laboratories, Sandia USA and was published by M. L. Garcia, The Design and Evaluation of Physical Protection Systems, 2007. Fig. 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

Fig. 3: EASI model

5 EASI model output verification process via OTB SAF simulation tool

In order to raise the EASI outputs relevance and value of estimate of adversary sequence interruption in the object, it is necessary to simulate the movement of the adversary and guards with a simulation tool which works with parameters specified for the EASI model and with real conditions. In this context, the OTB SAF simulation tool (OneSEMI-Automated Forces Testbed / OneSAF Testbed Baseline; Science Aplications International Corporation San Diego California USA; national representative Lynx Ltd. Košice), in which a physical protection system built-in by a penetration test is defined, enters the process of physical protection system functionality assessment of the critical infrastructure elements and EASI model outputs verification.
The critical infrastructure element penetration tests of the physical security system were carried out in the referential object in Fig. 4. These tests were also considered to be a form of the EASI model verification.

ISBN: 978-1-61804-004-6

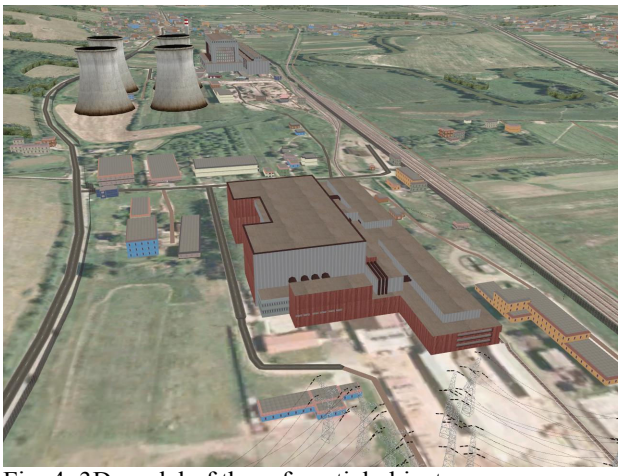

Fig. 4: 3D model of the referential object

According to the carried-out simulations, the EASI model is, in the context of verification of the physical protection systems functionality, an applicable model. This is in relation to potential purloin or destruction of the protected interest in terms of the critical infrastructure component. The following tables and graphs give the evidence.

Table 3 Security level I - asset abstraction

Number of zones overcome	EASI model output – estimate of adversary sequence interruption	EASI model simulation verification via OTB SAF tool
0	0,9699352	1
1	0,9693818	1
2	0,9640465	1
3	0,9137656	1
4	0,7589453	1
5	0,0223934	0
6	0,0123595	0
7	0,0000000	0
8	0,0000000	0

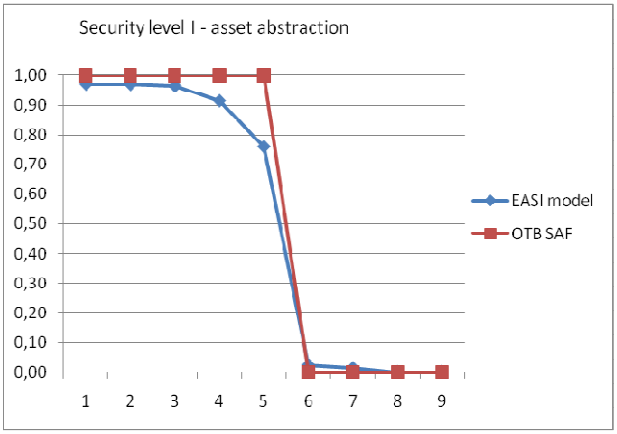

Fig. 5: Graph of EASI model verification via OTB SAF tool for Security class I – asset abstraction

Table 3 Security level I – detonating system

Number of zones overcome	EASI model output – estimate of adversary sequence interruption	EASI model simulation verification via OTB SAF tool
0	0,9699352	1
1	0,9693818	1
2	0,9640465	1
3	0,9137656	1
4	0,7589453	1
5	0,0223934	0
6	0,0123595	0
7	0,0000000	0
8	0,0000000	0

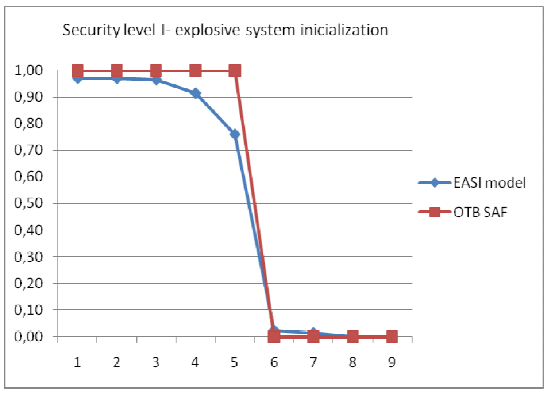

Fig. 6: Graph of EASI model verification via OTB SAF tool for Security class I – detonating system initialization

ISBN: 978-1-61804-004-6

According to the tables and graphs it follows that in the case of 2 security zones being overcome, the physical protection system functionality was not substantially impacted (see Fig. 7), which was confirmed by the EASI model outcomes – 0,9460 and also the simulation itself.

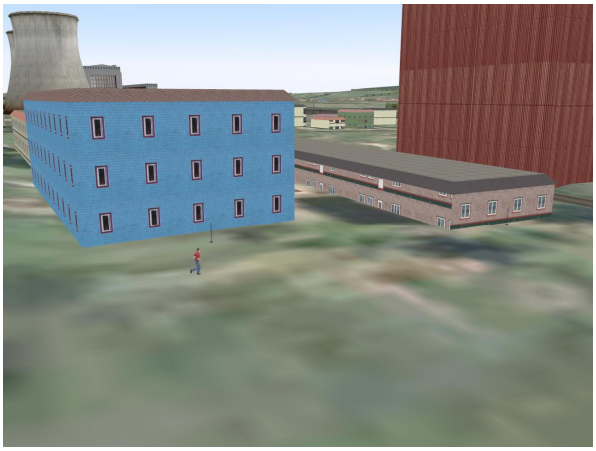

Fig. 7: Penetration tests of the FO system proposed

In the case of 4 security zones being overcome (Fig. 8), the probability dropped to 0,7597 and in certain extreme cases the physical protection system was partially breached.

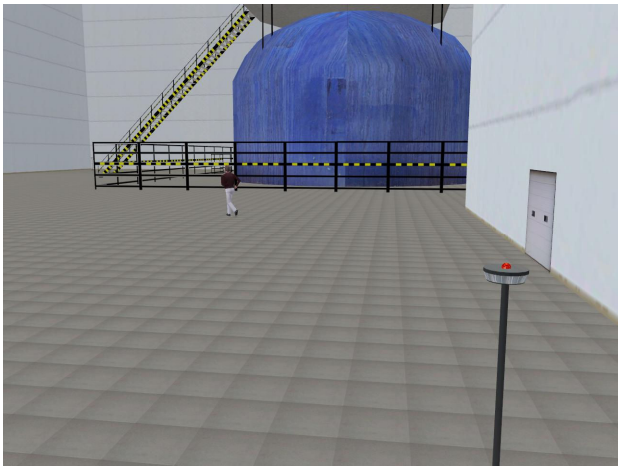

Fig. 8: Adversary's activity in the protected object

Only when 5 security zones were overcome, the probability of sequence interruption represented by the EASI model was 0,0227 which was confirmed by the simulations whose output was initialization of a detonating system and destruction of the protected interest (Fig. 9).

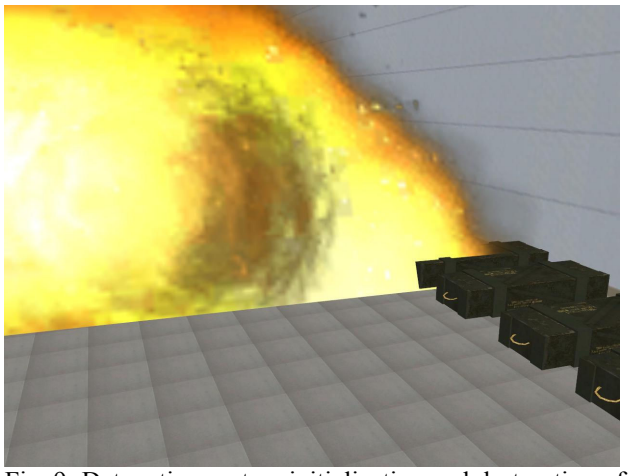

Fig. 9: Detonating system initialization and destruction of the protected interest

6 Conclusion

The proposed structure and physical protection system function parameters of a critical infrastructure component are acceptable mainly on the base of the carried-out verification, which was perceived as a synthesis of existing approaches to property and person protection in the civil and military sector.

According to the conclusions, the crucial aspect in verifying theoretical basis not only in relation to generating input parameters into the chosen EASI model but also to individual outputs verification following from the EASI model was the application of OTB SAF simulation tool for the verification of the physical protection system functionality and structure as a critical infrastructure component.

A significant contribution of the simulation tool can be seen mainly in the possibility to verify a defined system in terms of multiple substantial threats such as purloin or manipulation with the protected interest or its destruction by the detonating system.

One of the possible alternatives in the simulations (in relation to the detonating system application intent) was the physical annihilation of the adversary, but with regard to the character of activity of private security agencies, this form of stopping the adversary was relinquished.

With support of 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] SR. Zákon 45/2011 o kritickej infraštruktúre : Zbierka zákonov č. 45/2011. In *Zbierka zákonov č. 45/2011*. 2011, Čiastka 19, s. 434-442. Dostupný také z WWW: <http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=210111&FileName=zz2011-00045-0210111&Rocnik=2011>.

[2] GARCIA, M. L. The Design and Evaluation of Physical Protection Systems, Second edition, Sandia National Laboratories, 2007, p. 273-289, ISBN – 10: 0-7506-8352.

[3] HROMADA, M. Stanovení odolnosti kritickej infraštruktúry – praktický príklad /Critical Infrastructure Resilience Determination – Practical example /. In: Security Magazín, 2010, num- 92, p. 25-27, ISBN – 1210-8723..

[4] GARCIA, M. L. The Design and Evaluation of Physical Protection Systems, Second edition, Sandia National Laboratories, 2007, p. 275, ISBN – 10: 0-7506-8352.

[5] LUKÁŠ, L., HROMADA, M. Možnosti hodnocení odolnosti kritické infrastruktury/ Evaluating the Resistance of Critical Infrastructure. In: Bezpečnost v informační společnosti, Brno, 2009, p. 56, ISBN 978-80-7231-653-3