Simulation and Modelling in Critical Infrastructure Protection

Lukas Ludek, Hromada Martin

Abstract: Critical Infrastructure Protection is currently considered an important aspect of solving security issues of EU countries, even given that its role is perceived in terms of maintaining functional continuity of the economic and social terms. It is therefore clear that the responsible entity will use all available approaches to ensure an acceptable level of security and protection of important elements of national as well as transnational (European) critical infrastructure. Among the useful approaches you can use appropriate forms of simulation and modelling tools. It is clear that the analysis of current approaches to protection of property points to the fact that the physical protection systems could be considered as an one aspect of a comprehensive protection system also useful in the present issue. Therefore, in this article we consider the use of modelling and simulation tools in the context of determining the optimal structure of the physical protection system of critical infrastructure elements. For the purpose of fulfilling this goal, we chose an EASI model and OTB SAF simulation tool.

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

I. INTRODUCTION

The complexity of critical infrastructure as a system created a framework to formulate an approach which would unify the identification and designation process of the European critical infrastructure and consequently national infrastructure in an adequate way. It is therefore necessary to describe this process in relation to the need to determine optimal security and protection precautions.

A. *Conditions for the marking and identification of the European critical infrastructures.*

Each member state was obliged (based on a Directive 2008/114/ES) to finish the identification and designation process of the European critical infrastructures by January 12, 2011. These infrastructures are considered for being critical infrastructures located in member states and whose disruption or destruction would have significant consequences in at least two member states. The severity is evaluated based on cross-cutting criteria. This identification process may be divided into more steps:

- each member state will (in relation to the aim to realize the first selection of European critical infrastructures) apply and use sectorally specific criteria (national sectoral and cross-cutting criteria)
- if there are elements selected in the first step, these elements are marked according to paragraph 2, letter a) as critical infrastructure,
- subsequently, cross-cutting criteria for determination of the European critical infrastructures are applied and used and thus selected elements are marked as European critical infrastructure according to paragraph 2, letter b)

In relation to the designation process of the European critical infrastructures, each member state on whose territory there is a potential European critical infrastructure is obliged to create a framework for uni- and multi-lateral deliberation with states which might be impacted by this infrastructure. In connection with this step we often encounter the fact that government authorities strive to not identify (not apply the cross-cutting and sector criteria and ignore the identification process) the European critical infrastructure, thereby divesting the obligation following from it. It is necessary to realize, however, that each member state which assumes it could be threatened by potential critical infrastructure of another state, has the right to ask the Committee to create a kind of a pressure on the member state which did not correctly design and identify the European critical infrastructure for the purpose of repeated identification [6].

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.

L. Lukas. Author was with University of Defence in Brno, Czech Republic. He is now associate professor with Faculty of applied informatics, Tomas Bata University in Zlin, Czech Republic. (corresponding author to provide phone: +420-576035248, e-mail: lukas@fai.utb.cz).

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

B. Cross-cutting criteria

The cross-cutting criteria are criteria which were determined in connection with the common and unified identification and designation process of the European critical infrastructures. In order to streamline the identification and marking process of the European critical infrastructures, a manual on implementing Directive 2008/114/ES was made. Based also on this manual, the criteria are divided and described in these groups:

- Casualties criterion,
- Economic effects criterion,
- Public effects criterion,

Casualties criterion

In accordance to the manual, the amount of dead and injured in a member state is considered significant if:

- Potential amount of dead and injured in a member state in relation to the loss of activity in the given ECI is higher than the set top limit based on an individual evaluation of the member state.
- At least two states are significantly struck by the loss of activity of the ECI in relation to the set top limit under the death toll criteria.
- As a consequence of a significant strike of the ECI and an absence of the boundary value, the amount of deaths may be counted in several hundreds and the amount of injured in several thousands.

Within the manual, limits were set: for injured – 5000, while 50% is in another member state and for dead – 500, while 50% is in another member state.

Economic effects criterion

Economic losses are defined as losses which did not emerge directly as a consequence of the ECI functionality disruption and are built on the impact of the disruption on dynamics of national economies. These losses are considered serious if:

- Potential economical loss of a member state as a consequence of the given ECI disruption is higher than the set top limit 500 million Euro or 0.5% GDP.
- Total economic loss of impacted states exceeds a total limit of 1 bil. Euro.

Economic losses as a consequence of the service's or product's unavailability

The initial stage is considered to be a state when disfunctionality or destruction of an ECI element has an impact on the services or products accessibility and when their potential severe unaccessibility has a negative effect on a supply chain and economic stability.

Environmental impacts

For the purpose of defining environmental impacts we evaluate:

- Losses of landscape/land which are defined as an economical value of landscape/land expressed by a potential utilization of the given landscape/land in relation to national incomes of the member states.
- Moved-out population – where economic expenses related to moving out of people and their impact on national economy are assessed.

Public effects criterion

- In a member state, as a consequence of a disruption or destruction of the ECI element, the value expressing the amount of impacted population under physical suffering as well as under disruption of the quality of every-day life over 250 000 people
- Is a value expressing the amount of impacted population as well as under disruption of the quality of every-day life on the level or above the level for medium intensity.

After applying these criteria, the state should mark the chosen elements of national infrastructural as potential European critical infrastructures and subsequently inform the provider of such infrastructure about this marking. This information is assumed to be adequately confidential.

II. CRITICAL INFRASTRUCTURE PROTECTION

Critical infrastructure protection is perceived from a perspective of a need to make a complex system of critical infrastructure protection that is in the context of the state's security environment, while it is supposed that the making of such a system will follow from the current legislative environment [10].

A. Critical infrastructure protection system building

The aim of the process of protecting critical infrastructure is to ensure the desired degree of physical security and resilience for critical infrastructure elements. The aim is also to ensure the recovery process in case of the degradation function of elements. Designated elements must withstand the effects of all threats. This is the principle All Risk.

The basic standards and rules for the protection of critical infrastructure are included in content of the process of creating a security framework for the system of protection of critical infrastructure. There is included:

- Establishment of systems and institutions for the protection of critical infrastructure,
- Selection of elements for the protection of critical infrastructure, ensuring their protection and recovery functions in case of degradation.

Security framework for the protection of critical infrastructure represents the definition of critical infrastructure and its relation to the state and society. The framework defines the position of critical infrastructure

in the state security system. There is emphasized the reasons for its protection and risks for the society at time of its disposal.
Creation of juridical environment for critical infrastructure protection includes the development and adoption of the law and other standards activities in this area. The laws and standards should have set objectives of the process, elements and areas of critical infrastructure, institutions for the protection of critical infrastructure and their actions towards the protection and restoration functions. Protection of critical infrastructure is related to crisis management and the efforts of rescue and protection of the population [8].

B. Legislative environment of the critical infrastructure protection

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.

This directive defines and formulates the rights and obligations of the European critical infrastructure provider which point to the need of making an OSP (Operator Security Plan) which defines components of the critical infrastructure element, security solutions and other measures connected with protection, the SLO (Security Liaison Officer) who is considered to be a certain communication entity between the provider and state or a contact point for ECI protection.

OSP (Operator Security Plan)

In relation to objects problems, The Operator Security Plan should include an identification of the critical infrastructure components and existing security measures or solutions as well as their forthcoming addition and renovation. As for processing, the following steps are recommended:

- Identification of important equipment,
- Carrying out of a risk analysis in relation to main threat scenarios, vulnerable parts of individual systems as well as defining possible consequences of these threats,
- Identification or selection of suitable counter-measures, processes and activities, while it is possible to divide these counter-measures into:
    - permanent security measures which are specified as investments and resources inevitable in relation to the ECI effective protection. It is primarily technical measures (means of detection, access control, protection and informing), organization measures (procedures for warning a critical management), control and monitoring measures, professional training and security of the information and communication systems
    - gradatory security measures – primarily those measures whose activation will depend on the current risk measure.

SLO (Security Liaison Officer)

According to the Direction 2008/114/ES is the Security Liaison Officer considered as a security officer who is a contact point within the matters and steps related to security between the provider or owner of ECI and state's entities or with a contact point for ECI protection (under the contact point we understand Ministry of Internal Affairs or another responsible state authority also authorized to coordinate activities within the ECI protection. The provider’s liaison officer can be, according to the already mentioned Directive, an existing person responsible for security, mainly in order to minimize expenses on work positions. Based on this fact it is assumed (not given or defined in relevant documents related to ECI protection) that such officer will meet the following requirements:

- Person eligible to carry out legal actions
- Person who is unimpeachable
- Person who has university degree or bachelor’s degree of an adequate technical field,
- Person who has completed professional training,
- Person who has professional eligibility.

Further obligations of the ECI provider

Among other obligations of the provider, which are, however, not further described in detail by the Directive, may be considered:

- To apply the best available technology for allowing adequate protection of the element during its construction or modernization.
- To secure the construction of a security plan and present it to the central authority within six months from receiving an announcement of the element's designation and of its integration into a sector; reassess the security plan and, if necessary, ensure the security plan update and present it to the central authority.
- Inform its employees about the security plan.
- To drill a threat situation of disruption or destruction of the element according to the security plan at least once a year
- To appoint a person who makes, processes and acquaints themselves with sensitive information as well as to appoint a contact person, if the element in question is one of the European critical infrastructure.
- Provide the central authority and ministry with cooperation, especially as for data, records and explanations needed for:
    - designation of an element and its integration into a sector, as well as elimination of an element from a sector,
    - assessment of the element's security,
    - making of the risk analysis,

  - keeping a register according to this law,
- Proceed according to the security plan in case of a threat of disruption or destruction of the element [9].

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.

III. Physical Protection System of Critical Infrastructure Element

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].

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

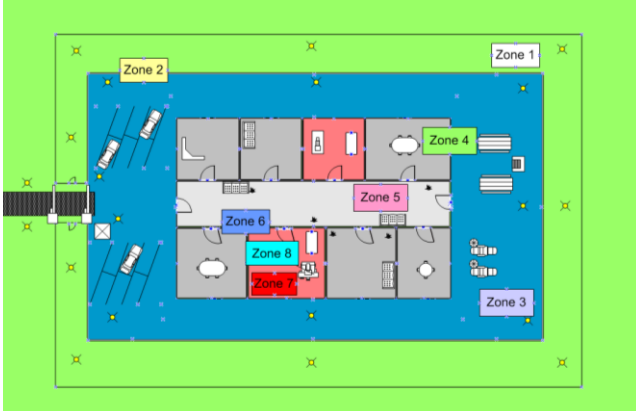


Fig. 1: Referential object divided into 8 security zones

Each of the defined zones was subsequently assessed by parameters (the adversary detection probability – technical security devices, breaking resistance – mechanical barrier systems, 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

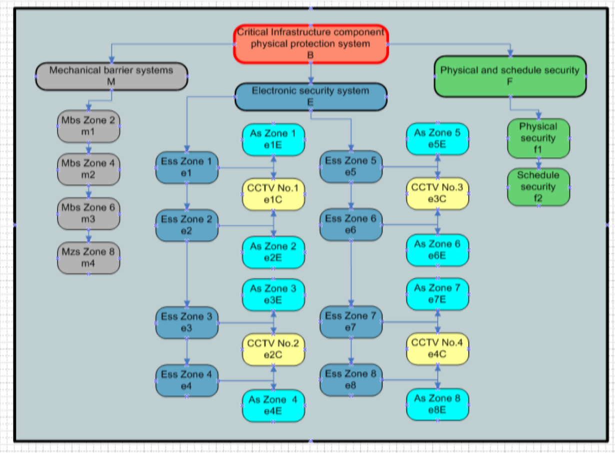


Fig. 2: The determined physical protection system structure of a critical infrastructure component

IV. Structural Properties Evaluation of Physical Protection System of the Critical Infrastructure Element

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.

Fence	Security class and its value			
	I - 1	II - 2	III - 3	IV - 4
The total high of fencing	min. 220 cm above ground,	min. 230 cm above ground,,	min. 240 cm above ground,,	min. 250 cm above ground,,
Anti –burrow board	min. 20 cm above ground,	min. 20 cm above ground,	min. 30 cm above ground,	min. 30 cm above ground,
Mechanical barrier on the crown	One side bavolet	One side bavolet	Both sides bavolet	Both sides bavolet
Maintained band	120 cm to both sides	120 cm to both sides	150 cm to both sides	150 cm to both sides

Fig 3: Fence – Security class and its value

Entrances and driveways	Security class and its value			
	I - 1	II - 2	III - 3	IV - 4
The total high of fencing	min. 220 cm above ground,	min. 230 cm above ground,,	min. 240 cm above ground,,	min. 250 cm above ground,,
Anti –burrow board	min. 20 cm above ground,	min. 20 cm above ground,	min. 30 cm above ground,	min. 30 cm above ground,
Mechanical barrier on the crown	One side bavolet	One side bavolet	Both sides bavolet	Both sides bavolet
Locking system or padlock	Class 4	Class 5	Class 5	Class 5

Fig. 4: Entrances and driveways – Security class and its value

Then they were subsequently formulated the requirements for individual components of the physical protection of critical infrastructure elements:

- Mechanical barrier systems

Value of Mbs for Zone 2 m1	Value of Mbs for Zone 4 m2	Value of Mbs for Zone 6 m3	Value of Mbs for Zone 8 m4	Security class	Minim. Value of MBS SC	Maxim. Value of MBS SC
4	3	3	3	IV	13	16
3	2	2	2	III	9	12
2	1	1	1	II	5	8
1	1	1	0	I	3	4

Fig. 5: Mechanical barrier systems minimal and maximal values

- Electronic security system

Value of Ess for Zone 1 e1		Value of Ess for Zone 2 e2		Value of Ess for Zone 3 e3		Value of Ess for Zone 4 e4		Security class
8	e1E - 4	7	e2E - 3	6	e3E - 3	6	e4E - 3	IV
	e1C - 4		e1C - 4		e2C - 3		e2C - 3	
6	e1E - 3	5	e2E - 2	4	e3E - 2	4	e4E - 2	III
	e1C - 3		e1C - 3		e2C - 2		e2C - 2	
4	e1E - 2	3	e2E - 1	2	e3E - 1	2	e4E - 1	II
	e1C - 2		e1C - 2		e2C - 1		e2C - 1	
2	e1E - 1	2	e2E - 1	2	e3E - 1	2	e4E - 1	I
	e1C - 1		e1C - 1		e2C - 1		e2C - 1	
Value of Ess for Zone 5 e5		Value of Ess for Zone 6 e6		Value of Ess for Zone 7 e7		Value of Ess for Zone 8 e8		Security class
6	e5E - 3	6	e6E - 3	6	e7E - 3	6	e8E - 3	IV
	e3C - 3		e3C - 3		e4C - 3		e4C - 3	
4	e5E - 2	4	e6E - 2	4	e7E - 2	4	e8E - 2	III
	e3C - 2		e3C - 2		e4C - 2		e4C - 2	
2	e5E - 1	2	e6E - 1	2	e7E - 1	2	e8E - 1	II
	e3C - 1		e3C - 1		e4C - 1		e4C - 1	
2	e5E - 1	2	e6E - 1	2	e7E - 1	1	e8E - 0	I
	e3C - 1		e3C - 1		e3C - 1		e3C - 1	

Fig. 6: Electronic security system – values of ESS for each zone

Security class	Minim. Value of ESS SC	Maxim. Value of ESS SC
IV	51	64
III	35	50
II	19	34
I	15	18

Fig. 7: Electronic security system – minimal and maximal values

- Physical and schedule security

Value of F f1	Value of F f2	Security class	Minim. Value of F	Maxim. Value of F
4	3	IV	7	8
3	2	III	5	6
2	1	II	3	4
1	1	I	2	2

Fig. 8: Physical and schedule security – minimal and maximal values

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]:

$$B = \sum_{i=m1}^{m4} M_i + \sum_{i=e1}^{e8} E_i + \sum_{i=f1}^{f2} F_i \qquad (1)$$

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.

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

Fig. 9: Maximal and minimal values of critical infrastructure components physical protection system

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).

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

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

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

Fig. 10: Quantitative explanation of security level in critical infrastructure sector [3]

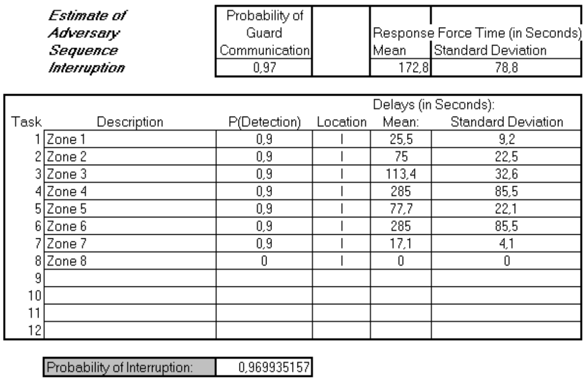
V. MODEL EASI (ESTIMATE OF ADVERSARY SEQUENCE INTERRUPTION)

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. 11.



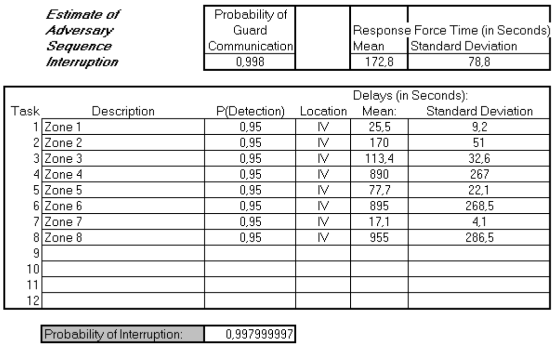
Estimate of Adversary Sequence Interruption

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

				Delays (in Seconds):	
Task	Description	P(Detection)	Location	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. 11: EASI model security class I



Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Mean	Force Time (in Seconds) Standard Deviation
0,998		172,8	78,8

				Delays (in Seconds):	
Task	Description	P(Detection)	Location	Mean:	Standard Deviation
1	Zone 1	0,95	IV	25,5	9,2
2	Zone 2	0,95	IV	170	51
3	Zone 3	0,95	IV	113,4	32,6
4	Zone 4	0,95	IV	890	267
5	Zone 5	0,95	IV	77,7	22,1
6	Zone 6	0,95	IV	895	268,5
7	Zone 7	0,95	IV	17,1	4,1
8	Zone 8	0,95	IV	955	286,5
9					
10					
11					
12					

Probability of Interruption: 0,997999997

Fig. 12 EASI model security class IV

VI. EASI MODEL OUTPUT VERIFICATION PROCES 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 Applications 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 and this simulation tool can be also used for many kinds of training scenarios operations realization [11].

The critical infrastructure element penetration tests of the physical security system were carried out in the referential object in Fig. 13. These tests were also considered to be a form of the EASI model verification.

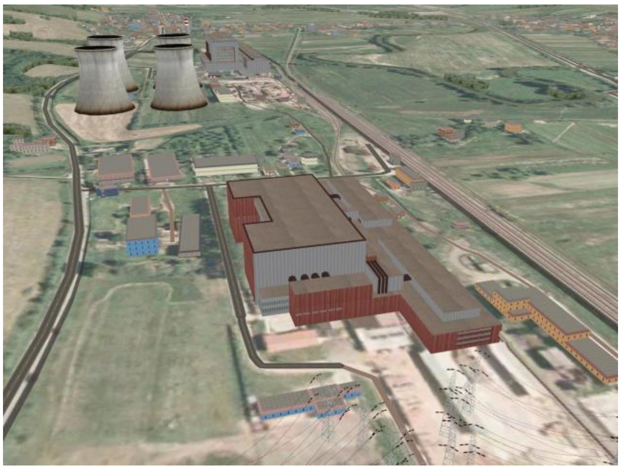


Fig. 13: 3D model of the referential object

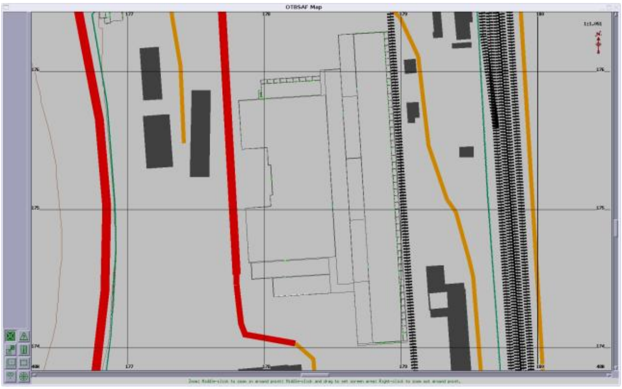


Fig. 14: 2D model of the referential object [14]

Fig. 15: Response team base

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.

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. 16: EASI model output – security level I – asset abstraction

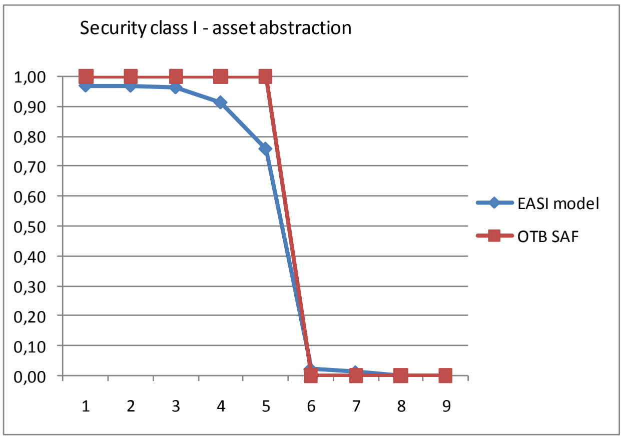


Fig. 17: Graph of EASI model verification via OTB SAF tool for Security class I – asset abstraction

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. 18: EASI model output – security level I – detonating system initialization

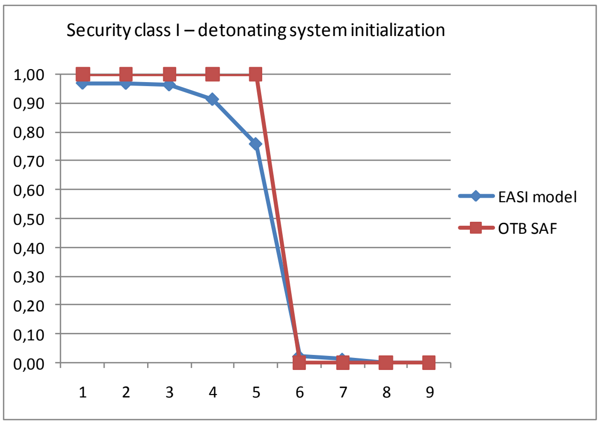


Fig. 19: Graph of EASI model verification via OTB SAF tool for Security class I – detonating system initialization

Number of zones overcome	EASI model output – estimate of adversary sequence interruption	EASI model simulation verification via OTB SAF tool
0	0,9979	1
1	0,9979	1
2	0,9979	1
3	0,9979	1
4	0,9976	1
5	0,9919	1
6	0,9447	1
7	0,0134	0
8	0	0

Fig. 20: EASI model output – security level IV – asset abstraction

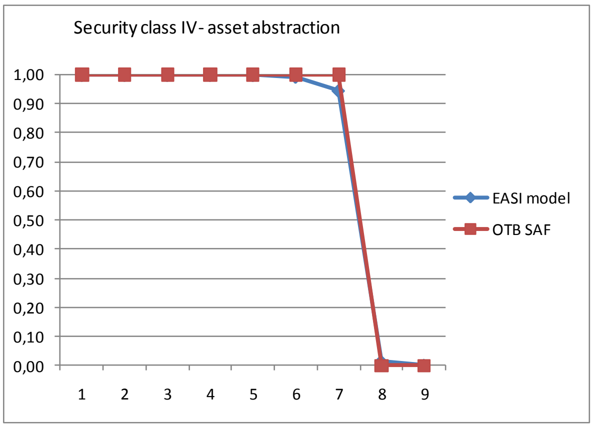


Fig. 21: Graph of EASI model verification via OTB SAF tool for Security class IV – asset abstraction

Number of zones overcome	EASI model output – estimate of adversary sequence interruption	EASI model simulation verification via OTB SAF tool
0	0,9979	1
1	0,9979	1
2	0,9979	1
3	0,9979	1
4	0,9976	1
5	0,9919	1
6	0,9440	1
7	0	0
8	0	0

Fig. 221: EASI model output – security level I – detonating system initialization

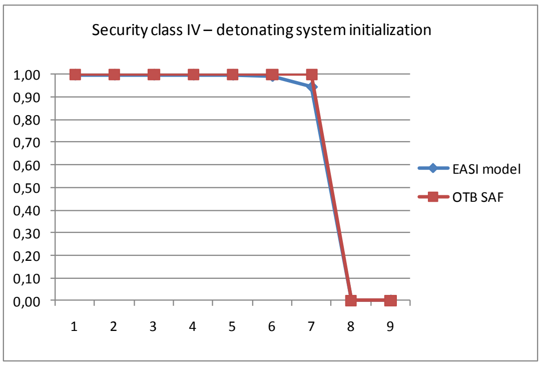


Fig. 23: Graph of EASI model verification via OTB SAF tool for Security class IV – detonating system initialization

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. 24), which was confirmed by the EASI model outcomes – 0,9460 and also the simulation itself.

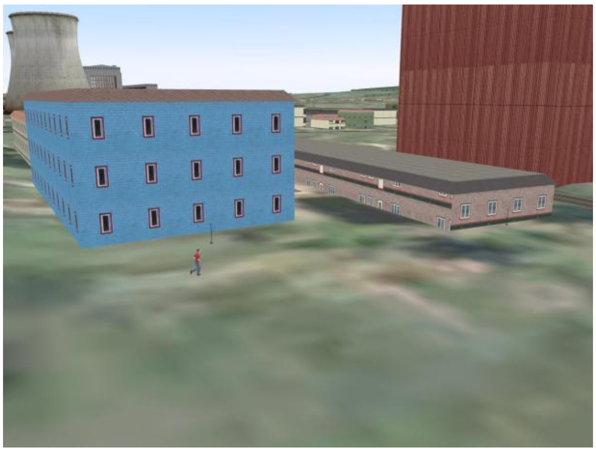


Fig. 24: Penetration tests of the FO system proposed [14]

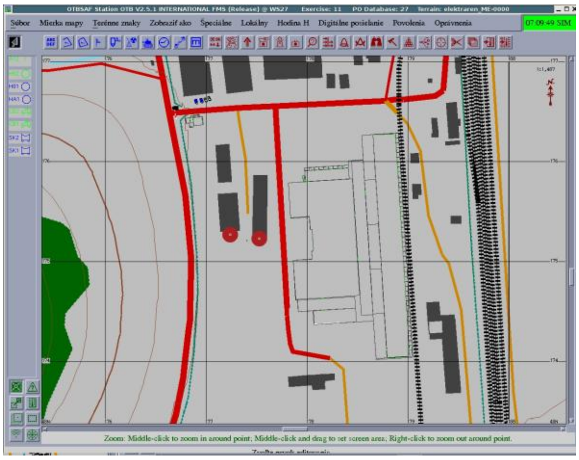

OTBSAF Station OTB V2.5.1 INTERNATIONAL FMS (Release) @ WS27 Exercise: 11 PO Database: 27 Terrain: elektraren_ME-0000
Súbor
Mierka mapy
Terénne znaky
Zobraziť ako
Špeciálne
Lokálny
Hodina H
Digitálne posielanie
Povolenia
Oprávnenia
07:09:49 SIM
Zoom: Middle-click to zoom in around point; Middle-click and drag to set screen area; Right-click to zoom out around point.

Fig. 25: Detection system activation

In the case of 4 security zones being overcome (Fig. 26), the probability dropped to 0,7597 and in certain extreme cases the physical protection system was partially breached.

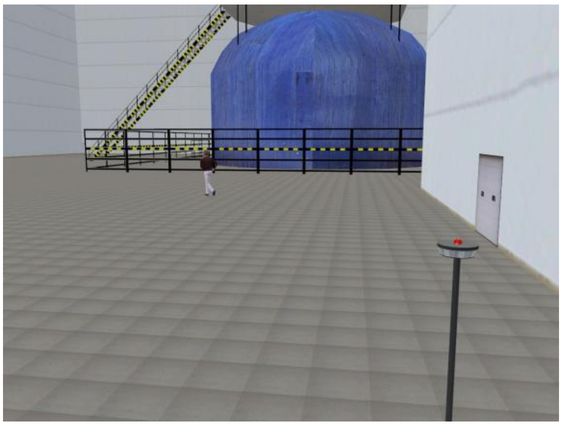


Fig. 26: Adversary’s activity in the protected object

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. 27) [13].

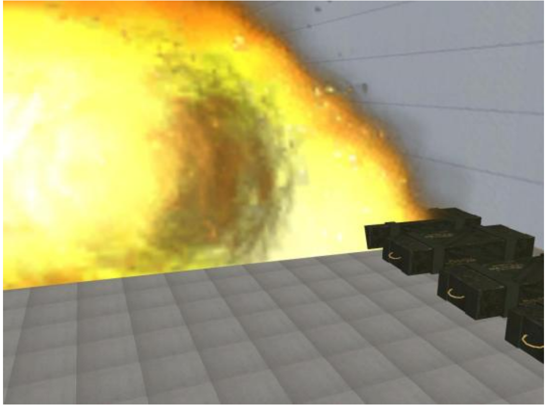


Fig. 27: Detonating system initialization and destruction of the protected interest [14]

VII. 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 also in connection to e-learning systems development [12].

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 abstraction 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.

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. Avaliable from 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

[6] EU. Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In *Council directive 2008/114/EC. 2008*, 345, s. 75-82. Available from WWW: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF>

[7] EU. Non – Binding Guidelines For application of the Council Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

[8] LUKÁŠ, L., HROMADA, M. *Management of Protection of Czech Republic Critical Infrastructure Elements*, In: 13th WSEAS Internationa Conference on Automatic Control, Modelling & Simulation (ACMOS´11), Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, , p. 306-309, 2011, ISBN: 978-1-61804-004-6

[9] HROMADA, M.,*Povinnosti prevádzkovateľa Európskej kritickej infraštruktúry/The European Critical Infrastructure Operator Duties*, In: Security Magazín, No. 95, p. 52-55, 2010, ISBN – 1210-8723

[10] NECESAL, L., LUKÁŠ, L., *Entities of critical infrastructure protection,* In: 13th WSEAS Internationa Conference on Automatic Control, Modelling & Simulation (ACMOS´11), Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, , p. 383-386, 2011, ISBN: 978-1-61804-004-6

[11] CIRULIS, A., GINTERS, E., *Training Scenario Operations Ralization in Virtual Reality Enviroment*, In: 13th WSEAS Internationa Conference on Automatic Control, Modelling & Simulation (ACMOS´11), Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, , p. 39-44, 2011, ISBN: 978-1-61804-004-6

[12] LAUBERTE, I.,, A., GINTERS, E., *Agent-Based TemPerMod Simulator Cell Architecture*, In: 13th WSEAS Internationa Conference on Automatic Control, Modelling & Simulation (ACMOS´11), Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, , p. 75-79, 2011, ISBN: 978-1-61804-004-6

[13] LUKÁŠ, L., HROMADA, M. *Utilization of the EASI model in the matters of critical infrastructure protection and its verification via the OTB SAF simulation tool*, In: 13th WSEAS Internationa Conference on Automatic Control, Modelling & Simulation (ACMOS´11), Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, , p. 131-136, 2011, ISBN: 978-1-61804-004-6

[14] KELEMEN, M., HROMADA, M., NECAS, P., ANDRASSY, V., SOUSEK, R., PETZ, I., *The ONESAF OTB modeling and simulation tool for the defence and critical infrastructure component physical and technical protection system verification*, In. Brno, ICMT, 2011, p.1215-1223, ISBN 978-80-7231-787-5

Ludek Lukas - (LTC ret.) was born in 1958. He graduated university studies in 1981 at Military Technical University in Liptovsky Mikulas (Slovakia) and doctoral studies in 1993 at Military Academy in Brno (Czech Republic).

During his working at the Military Academy in Brno (1991 - 2005) he held the function of lecturer, group leader, head of department and vice rector for study affairs. He currently works at the Tomas Bata University in Zlín as associate professor. His scientific research, publishing and educational activities are focused into area of C2 communication and information support, information management, physical security and critical infrastructure protection.

Martin Hromada - Was born in 1983. In 2008 completed a master's degree in security technologies, systems and management at the University of Tomas Bata in Zlin, where he currently serves as an internal PhD student. The object of his interest in the protection of critical infrastructure in terms of technological aspects, modelling and simulation.