Quantitative assessment parameters of the protection level of national strategic sites in the EU

T. Loveček[1] & J. Ristvej[2]
[1]*Department of Security Management, Faculty of Special Engineering, University of Žilina, Slovakia*
[2]*Department of Crisis Management, Faculty of Special Engineering, University of Žilina, Slovakia*

Abstract

Property protection against deliberate human acts, such as terrorist attacks, thefts or vandalism, is governed in manifold legal regulations, technical standards and professional publications. Nonetheless, none of those tackles the property protection issues comprehensively, nor provides any satisfactory answer to the question of the optimal design of those systems from the perspective of their technical efficiency and economic effectiveness.

Since the 1990s, the University of Žilina, in cooperation with certifying authorities and experts of the National Security Authority, has been developing mathematical models to determine the protection level of national strategic sites. From the long-term perspective the research aims to develop specific mathematical models based on breakthrough resistance of passive protection components, probabilities of violator detection by active protection components in the respective zones of protected area, and intervention unit response times. Those models will facilitate assessment of property security levels and quality from the technical-economic perspective.

Any mathematical property protection system model works with input and output parameters. This article illustrates the basic parameters that can be used in the assessment of technical efficiency of a new or a proposed protective system of national strategic sites. The principal measurable parameters considered herein are: protective measure efficiency coefficient, total breakthrough time of passive protection components, probability of violator elimination, cumulative

WIT Transactions on Information and Communication Technologies, Vol 43, ©2010 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK100071

probability of (correct) violator detection or probability of successful intervention of intervention unit, or critical detection point.

One of the principal reasons for absence of such a tool for assessment of the level of protective systems is the necessity to join experts, funds and competences from various industries, such as the security industry, electrical power industry, building industry, engineering industry or economy or applied mathematics. For this reason, the University of Žilina, apart from its scientific and research activity, creates communication space for discussion also via the European project: Competency Based e-portal of Security and Safety Engineering, which aims to create a network of educational, research and financial institutions operating in the security field in the EU.

Keywords: quantitative assessment parameters, protection level, national strategic sites.

1 Introduction

Currently, the EU, Russia and the USA apply three basic approaches towards national strategic site protection: a directive approach (the required protection level is defined exhaustively in the relevant general binding regulation), a variant approach (the required protection level is sufficient in case the stakeholder reaches a sufficient number of points in a beforehand predefined scale) and a variable approach (an approach based on comparison of intervention unit response times, passive and active protection components). The variable approach is considered the most effective approach as its flexibility enables one to design a system in a way to satisfy the stakeholder's requirements, conditions and possibilities as best as possible. The variable approach to property protection is based on the presumption that it is necessary to use many passive and active protection components so that the violator could be detected and detained by the intervention unit before achieving their intent. The fact that the national security authorities of the EU members states declare in their further direction concepts that the method of classified information protection requires a change to the effect that its protection level be derived from the response times of passive or active components of the protective system affirms the aforementioned statement [5]. Detailed requirements for the method of determination of the national strategic site protection level are declared only generally in the Green Paper on a European Program for Critical Infrastructure Protection, approved in 2005 by the European Commission. Nonetheless, no methodology, guidelines, guidance or any other instrument, which would define in detail and enable one to apply the variable quantitative approach to national strategic site protection, based on exact methods, has been yet developed in Europe. A kind of resort may be found in the methodologies developed in the 1970s in the US Sandia National Laboratories, which had been developed for needs of protection of nuclear material and facilities. When applied to national strategic site protection, these tools imply certain deficiencies or disadvantages:

- developed to protect specific materials and non-commercial facilities and not to protect other infrastructure types,
- not developed to assess protection level in multilevel infrastructures,
- do not take into account the European technical norms, standards and certifications used in property protection,
- do not take into account random impacts, such as the decision of a violator under conditions of uncertainty,
- do not take into account the economic effectiveness of the entire protective system.

Given the above, all those European institutions that deal with the issues of strategic site protection should exert efforts to develop a tool to provide quantitative assessment of the technical efficiency of the protective system of a strategic site [5].

2 Property protection system efficiency assessment

In technology (and metaphorically also in economics, etc.), the efficiency term is defined as a dimensionless number that describes how close an ideal concept of a process is to its actual manifestation in the assessed machine or facility. The efficiency is calculated as a ratio of the monitored parameter on the facility output to the monitored parameter on the facility input in the same time interval. The efficiency of an ideal process is 100%. Any system where the aggression time T_N, or total breakthrough time of internal and external passive protection components T_{PRL}, is longer than the intervention unit response time or physical protection T_{FO}, i.e. $T_N > T_{FO}$ or $T_{PRL} > T_{FO}$ [1] is considered an efficient property protection system[1].

Fulfilment of the above condition needs not to be sufficient at all times. Nonetheless, it is the precondition to any affirmation of efficiency of protective systems. In the first case ($T_N > T_{FO}$), it is sufficient to detain the violator during the aggression time T_N, which takes into account attack time $T_{\text{út}}$ and escape time $T_{\text{ún}}$. Thus the disposal time of intervention unit T_{FO} is extended, and thus also the probability of the violator detention. In this case we are dealing with a violator whose intent is to steal some protected interest to sell it later for money. In the second case ($T_{PRL} > T_{FO}$), the violator must be detained before the breakthrough time of all internal and external passive protection components T_{PRL}. In this case an attack with the intent of sabotage, industrial espionage or terrorist attack is expected, i.e. a destructive manipulation with some protected interest, which can be in contravention of the state interest or can endanger life and health of population.

Thus, the basic criterion for assessment of property protection system efficiency is the relationship between times T_N or $T_{PRL\ \text{and}}$ T_{FO}. We need to implement parameters/coefficients, which would convey the overall system efficiency, to express their mutual relationship as a quantity. The protective measure efficiency coefficient Q_{ochr} is a significant parameter that describes the system efficiency. In case of violator detection by active protection components, the **protective measure efficiency coefficient $\mathbf{Q_{ochr}}$** can be defined either as (1) or (2).

$$\mathrm{Q_{ochr}} = \frac{T_N}{T_{FO}} = \frac{T_P + T_{PRES} + T_{út} + T_{ún}}{T_{pop} + T_{ver} + T_{pres} + T_{zás}} \quad \text{pre } \mathrm{T_N > T_{FO}}, \tag{1}$$

$$\mathrm{Q_{ochr}} = \frac{T_{PRL}}{T_{FO}} = \frac{T_P + T_{PRES}}{T_{pop} + T_{ver} + T_{pres} + T_{zás}} \quad \text{pre } \mathrm{T_{PRL} > T_{FO.}} \tag{2}$$

Time T_N is the total time of the violator's aggression since the moment of the violator detection at time t_{DET} by active protection components until the violator leaves the protected area. Time T_{PRL} is the total breakthrough time of passive protection components, i.e. the time required for the violator to approach the protected interest up to a distance of direct threat. This time is composed of the breakthrough time of all passive protection components T_P (object, perimeter and enclosure) since the detection moment at time t_{DET} and the total time T_{PRES} required for the violator transfer to the protected interest since the detection moment. $T_{út}$ is the attack time, i.e. the time which the violator needs to achieve their intended attack (e.g. protected interest theft, damage or destruction). $T_{ún}$ is the escape time, i.e. the time which the violator needs to leave the protected area. It is crucial that we realise why it is necessary to base our calculations on the detection time t_{DET}. The first reason is the fact that the intervention unit, with a certain probability, becomes activated at that time. The second reason is based on the presumption that where there is not any detection, there cannot be any intervention, and where there is not any intervention, then it is irrelevant to take into account or invest into passive components from the perspective of comprehensive protection. Each passive component has its breakthrough resistance, the overcoming of which is only a matter of time and unless the violator is or has already been detected by an alarm system, it is irrelevant to include their resistance in the total time T_N or T_{PRL}. Time t_{DET} plays a crucial role in including the time $T_{P1,}$ i.e. the breakthrough of the first passive component to reach the protected interest. T_{FO} is the total intervention unit response time, which is composed of:

- alarm announcement time T_{pop}, i.e. the time which has expired since the detection moment at the time t_{DET} until alarm condition announcement,
- transmission time T_c which is required to transmit a signal/message to the permanent physical protection service point in the protected area, the transmission time is the interval since the moment of display of change in the alarm system condition in the communicator interface and in the transmission alarm device interface and the indication and display device in the alarm transmission centre,
- aggression verification time T_{ver}, i.e. the time required to assess whether a real aggression by a violator or a false alarm is concerned,

- time of transfer to the place of intervention T_{pres}, i.e. the time required for the intervention unit to transfer to the place of intervention against the violator,
- time of intervention against the violator T_{zas}, i.e. the time required for efficient intervention against the violator, acts of violator deterrence, detention or paralysation, or ensuring security of the protected interest can be considered efficient acts of intervention.

Given the above, if Q_{ochr} is lower than 1, then protective measures are insufficient, and, to the contrary, the higher than 1 Q_{ochr}, the higher the efficiency of protective measures. According to professional literature, the protective measure efficiency coefficient should oscillate from 6 to 12, however, no more detailed exact reasoning is provided. Even in case the condition of $Q_{ochr} \geq 1$ is fulfilled, protective measures can be inefficient. In case great knowledge of active protection components on the part of the violator can be expected, the probability of their sabotage increases. Therefore any protected areas, in which sabotage of active components is expected, require physical protection to check them directly visually, or the active components must have the features against masking (antimasking), sabotage or replacement of individual components. The time interval for this check should ensure timely detection of aggression even in case of elimination or replacement of active protection components and thus to fulfil the basic condition ($T_N > T_{FO}$ or $T_{PRL} > T_{FO}$). Foreign literature states rather the parameter expressing the minimum time of delay on the part of violator to reach the protected interest T_D (*Time Delay*), defined as 3, than the coefficient Q_{ochr}.

$$T_{MIN} = \sum_{i=1}^{n} \Delta t_i \tag{3}$$

where:

Δt_i - the time of delay on the part of violator to overcome individual protective measures of the system or the distances between the individual zones.

Given the formula, this time is identical with the time T_{PRL} (total breakthrough time of internal and external passive protection components). The disadvantage of stating only this parameter is the fact that it does not take into account the probability of violator detection on their way to the target, neither the time of intervention unit. For these reasons, we find it more appropriate to use the coefficient Q_{ochr} that takes into account also the time of intervention unit.

Another significant parameter, which describes the protective system efficiency, is the **probability of violator elimination P_I**. This parameter defines the probability of the violator detention or other kind of elimination on their way to the protected interest. Contrary to the aforementioned parameters, it takes into account the probability of violator detection, the probability of successful response of intervention unit and the impact of stochastic phenomena.

Parameter P_I is based on the basic assessment criterion of property protection system efficiency T_{FO} as well, i.e. $T_N > T_{FO}$ or $T_{PRL} > T_{FO.}$ This criterion implies the conditions under 4 (in view of the fact that an analogical procedure is concerned in both the cases, we will consider hereinafter only the condition of $T_{PRL} > T_{FO}$).

$$T_N - T_{FO} > 0 \text{ resp. } T_{PRL} - T_{FO} > 0 \tag{4}$$

The times T_{FO} and T_{PRL} are independent random parameters, by rule implying parameters μ, σ^2. Thus, giving rise to a new random parameter X of the identical division as the given times. The new random parameter X is calculated as 5.

$$X = T_{PRL} - T_{FO} \tag{5}$$

$$\mu_X = E(T_{PRL} - T_{FO}) = E(T_{PRL}) - E(T_{FO})$$

$$\sigma_X^2 = Var(T_{PRL} - T_{FO}) = Var(T_{PRL}) + Var(T_{FO})$$

where:

μ – middle random parameter X value
σ – random parameter X range of scatter (dispersion, variation).

As already mentioned in the previous section, the probability of violator elimination P_I is based on the probability of violator detection and probability of successful response of intervention unit (6).

$$P_I = P_D * P_P * P_{PPS} * P_{\mathrm{R|D}} \tag{6}$$

where:

P_I – probability of violator elimination
P_D – probability of detection by alarm system
P_P – probability of failure free condition of alarm system
P_{PPS} – probability of alarm signal transmission via alarm transmission path to distant alarm receipt centre (PPC)
$P_{R|D}$ – probability of successful response of intervention unit

Intervention unit is successful if the random parameter X is higher than 0 (X>0). Given this, we can calculate the probability of successful response of intervention unit (formula 7) [1].

$$P_{R|A} = P(X > 0) = \int_0^\infty \frac{1}{\sqrt{2\pi\sigma_X^2}} * e^{\frac{-(x-\mu_X)^2}{2\sigma_X^2}} dx \tag{7}$$

The formula 7 describes the probability of violator elimination only for one detection by an alarm system. Nonetheless, the violator can on their way to the protected interest pass several detection zones. In case the violator passes two detection zones on their way to the target, the probability of violator elimination can be calculated as (8)

$$P_I = P_{D1} * P_{P1} * P_{PPS1} * P_{\mathrm{R|D1}} + (1 - P_{D1}) * P_{D2} * P_{P2} * P_{PPS2} * P_{\mathrm{R|D2}} \quad (8)$$

Detection can occur under a certain probability on a first detector and under a certain probability on a second, third or nth detector. In case detection occurs as soon as on the first detector and the intervention unit would respond adequately, no response to the alarm signal/message from the second detector is required. Although the probability of detection by alarm system is quite high ($P_D \cong 1$), there is still the possibility that the first detector would not respond. In this case, there are other detectors available in the order depending on the specific way passed by the violator to the target (the so-called cumulative probability). For this reason, a variable ($1-P_{D1}$) is included in the formula9. In general, the probability of violator elimination can be calculated as formula 9:

$$P_I = P_{D1} * P_{P1} * P_{PPS1} * P_{\mathrm{R|D1}} + \sum_{i=2}^{n} \left(P_{Di} * P_{Pi} * P_{PPSi} * P_{\mathrm{R|Di}} * \prod_{j=1}^{i-1} (1 - P_{Di}) \right) (9)$$

Since overcoming the protected area perimeter until reaching the protected interest, the violator often passes several detection zones of various probability of detection P_{Di}. In this case of multiple detection we consider the so-called **cumulative probability of violator detection P_{KDET}**, which represents the overall probability of violator detection before reaching the target. This parameter can be calculated as (9).

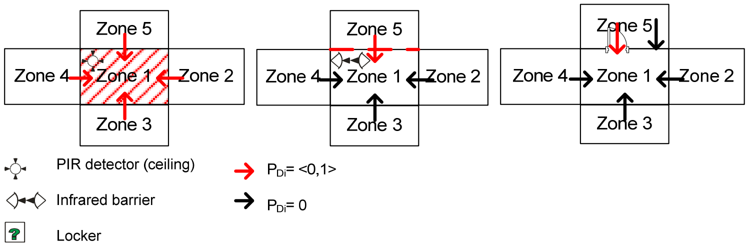
$$P_{KDET} = \left[1 - \prod_{i=1}^{n} (1 - P_{Di}) \right] * P_{PPS} * P_P * P_{LF} \quad (10)$$

where:

P_{KDET} – cumulative probability of violator detection
n – number of detection zones on the violator's way
P_{Di} – probability of correct detection by active component (e.g. PIR detector) in ith detection zone on the violator’s way
P_P – probability of failure free condition of alarm system or PPS
P_{PPS} – probability of alarm signal transmission via alarm transmission path to distant alarm receipt centre
P_{LF} – human factor reliability

From the perspective of cumulative correct probability of violator detection P_{KDET}, the time of detection of violation protected area will be a crucial condition for us, i.e. the correct alarm condition expressed by **probability of violator detection by alarm system in detection zone on a particular way of violator** $P_{Di.}$

According to the method of detection in area, alarm systems can be divided into (figure 1):



a) “3D” b) “2D” c) “1D”

Figure 1: Alarm system division by detection method.

- object protection alarm systems– “1D”,
- perimeter protection alarm systems – “2D”,
- area protection alarm systems – “3D”.

This method of alarm system division takes into account whether the violator is detected in the buffer zone, when passing the detection zone, or in case of change in the protected interest area condition.

In case of object protection alarm systems (“1D”), the probability P_{Di} applies exclusively to one place, point or facility, for which conditions characterising the protection status are preset (e.g. opening filling in closed, secured or locked condition, hanged picture). Electric security systems (e.g. detectors for protection of pieces of art, picture frame mouldings) or entrance control and management systems (e.g. code or biometric lock) are used most often as “1D” alarm systems. Electronic security systems (ESS) (e.g. ESS detectors to protect glass areas, infrared gates and barriers, underground pressure hoses), which monitor any motion between two detection zones, are used most often as (“2D”) perimeter protection alarm systems. Camera systems and ESS systems (e.g. security cameras, passive infrared/ultrasound/microwave ESS area detectors), which monitor motion in a particular detection zone, are used most often as (“3D”) area protection alarm systems.

The probability P_{Di} of respective “D1”, “D2” or “D3” alarm systems depends also on the particular used technology. The below text illustrates P_{Di} calculation for camera alarm system (11), which can be considered one of the most difficult ones.

$$P_{Di} = \frac{S_{Zi}}{S_{FPi}} * P_{DvOi} \qquad (11)$$

where:

P_{Di} – probability of violator detection by alarm system in ith detection zone on the violator's way to the protected interest,
S_{Zi} – camera footprint in ith detection zone [m^2],
S_{FPi} – total area of ith detection zone [m^2],
P_{DvOi} – probability of violator detection in an area/characteristics in ith detection zone.

The probability of violator detection by camera (P_{DvOi}) depends on the distance of violator from the camera. The graph in figure 2 illustrates the dependence between the violator's distance from the camera and the probability P_{DvOi}. This graphic dependence is not the same with all camera types. For this reason the individual P_{DvOi} values must be obtained by practical measurement in view of the distance Lx under various operating conditions.

We can consider two monitoring types in relation to the monitored scene (Figure 3).

With the so-called local monitoring, the footprint camera is of a trapezoid shape and the monitored scene horizon is bounded (e.g. monitoring the entrance to the infrastructure). The trapezoid area can be calculated under the formula (12). In this monitoring type, the upper limit of the monitored picture angle is >90° to the supporting construction (e.g. wall, column, pole, a fence).

$$S_{Zi} = \frac{O_S}{2*f} * \left[\frac{1}{\sin(\beta+\gamma)} + \frac{1}{\sin\gamma} \right] * \left[\sqrt{\left(\frac{v_K}{\sin\gamma}\right)^2 - v_K^2} - \sqrt{\left(\frac{v_K}{\sin(\beta+\gamma)}\right)^2 - v_K^2} \right] \quad \beta = 2*arctg\frac{O_V}{2*f} \tag{12}$$

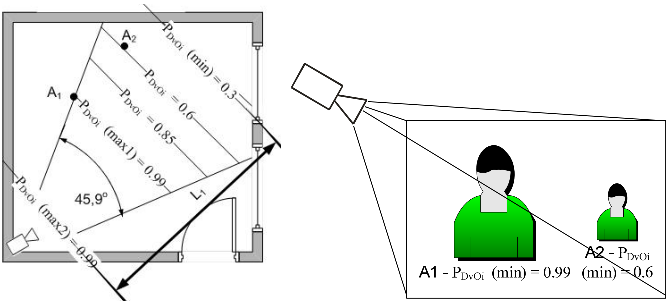


Figure 2: Example of mutual dependence between the probability of detection and the camera-monitored area.

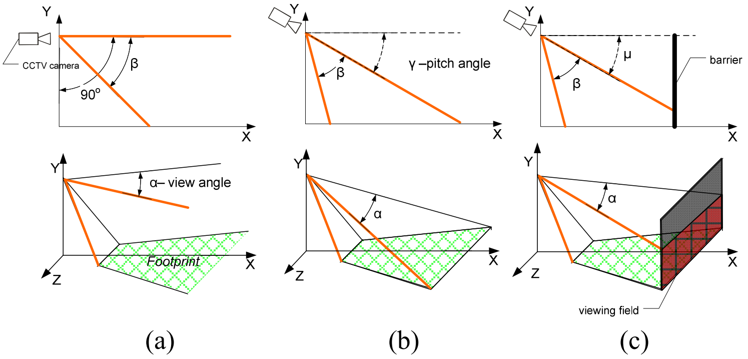


Figure 3: (a) Area monitoring; (b) local monitoring; (c) local monitoring blocked by an obstacle.

where:

S_{Zi} – monitored foot area – *footprint* [m^2],
V_K –camera installation height [m],
f – focal distance of lens [mm],
O_S – focal plane width – optical sensor [mm],
O_V – focal plane height – optical sensor [mm],
γ –camera inclination angle [^{o}].

The second possible monitoring type is the so-called area monitoring where the monitored scene horizon is not bounded. In this monitoring type, the upper limit of the monitored picture is at least in the right or obtuse angle to the supporting construction (e.g. when monitoring access roads to the perimeter). Often, the angular field of the monitored scene is obstructed by a non-transparent obstacle (e.g. wall, fence, opposite building) (Figure 3c) in both these monitoring types. In this case the footprint will be calculated as (13)

$$S_{Zi} = \left[\frac{O_S * V_K}{2 * f * \sin(\beta + \gamma)} + \frac{O_S * V_K}{2 * f * \sin\gamma} - \frac{\sqrt{\left(\frac{v_K}{\sin\gamma}\right)^2 - v_K^2} - s}{\sin\left(\frac{180 - \alpha}{2}\right)} * \sin\frac{\alpha}{2} \right] * \left[s - \sqrt{\left(\frac{v_K}{\sin(\beta + \gamma)}\right)^2 - v_K^2} \right]$$

$$\alpha = 2 * arctg \frac{O_S}{2 * f} \tag{13}$$

where:

S_{Zi} – monitored foot area – *footprint* [m^2],
V_K –camera installation height [m],
f – focal distance of lens [mm],
O_S – focal plane width – optical sensor [mm],
O_V – focal plane height – optical sensor [mm],
γ –camera inclination angle [^{o}],
s – distance of the obstacle or violator.

We can derive **probability of intervention by executive unit $\mathbf{P_Z}$** (14) from the probability P_{KDET}. In many cases, the intervention unit directly assesses the alarm signal. Nonetheless, in practice we often encounter cases when the signal recipient only mediates the information on the alarm condition to the intervention unit. The recipient can be either an organisation having its alarm system connected to the security service PPC, or an organisation where the operator themself, an own security guard (e.g. a gateman) or a random passer-by contacting the intervention unit (e.g. the Police Force of the SR) is the mediator of the information on the alarm condition.

$$P_Z = P_{KDET} * P_R \tag{14}$$

where:

P_Z – probability of intervention of intervention unit,
P_{KDET} – cumulative probability of violator detection,
P_R – probability of timely and correct assessment of alarm condition.

The last parameter to assess the technical efficiency infrastructure protection system is the **critical detection point CDP** [1]. CDP expresses the system property that should a system be effective, detection must occur at latest at this point /component or previous active components. The point/active component position *k-1* is based right on fulfilment of the condition that the time delay of violator when transferring and overcoming passive protection components (T_{PRLmin}), from that point to the protected interest (point *n*), has just exceeded T_{FO} (15).

$$T_{PRL\,\mathrm{min}} = \sum_{i=k}^{n} \Delta t_i > T_{FO} \tag{15}$$

where:

T_{PRLmin} – minimum total breakthrough time of passive protection components,
Δti – sum total of all breakthrough times of passive protection components times and times of transfer of violator on the way to the protected interest that fulfil the condition that their sum total is just higher than intervention unit response time,
T_{FO} – total intervention unit response time,
n – total number of passive protection components,
k – passive component protection before which violator must be detected in order the system be efficient (from the perspective of system breakthrough resistance and intervention unit response time).

3 Conclusion

This article reflects the author's long-term scientific and research activity in the field of physical and building security to create formal mathematical models of property protection systems to determine exactly their effectiveness and efficiency in relation to the protected interest. These models can be used for protection of components of critical or defence infrastructures, buildings of special significance at the resorts of the Ministry of Economy, the Ministry of Defence, the Ministry of Interior and the Ministry of Transport, Posts and Telecommunications, and last but not least, classified information protection under the charges of the National Security Office of the SR. This article describes output parameters models to assess the property security level and quality based on input parameters that take into account:

- violator's intent (attack with the aim to damage/destruct the protected interest or attack with the aim to steal it),
- protected interest nature and value,
- violator's decision making process under conditions of certainty, uncertainty or ambiguity,
- breakthrough resistances of passive system components dependent on the violator's skills, physical condition and type of used tools,
- method of detection and assessment of protected area violation,

- possibility of dividing the protected area into zones,
- protected area dislocation.

The scientific asset of this article consists in the fact that such a systematic approach to property protection against deliberate human acts, such as thefts or vandalism and terrorist attacks and many others has not been elaborated in detail in any legal regulation, technical norm, guidelines, or resort methodology. Even if there are certain procedures based on expert estimates in practice, their efficiency or effectiveness cannot be proved exactly and only the professional competence of their creators can be relied on. One of the main reasons for this unfavourable condition is the absence of real values of model input parameters, principally, probability of violator detection and breakthrough resistance of passive protection components. This situation is caused mainly by a high number of possible combinations of existing protective means and tools to be overcome on the market. Therefore a network of all stakeholders, who would join their human, technical, but also financial capacities, should be created. For this reasons as well, the University is implementing the European Competency Based e-portal of Security and Safety Engineering project.

Acknowledgement

With the support of the Lifelong Learning Programme of the European Union, Project Competency Based e-portal of Security and Safety Engineering – eSEC, 502092-LLP-1-2009-1-SK-ERASMUS-EMHE.”

References

[1] Garcia, M. L. 2001. The Design and Evaluation of Physical Protection Systems. USA: Elsevier.2001. ISBN 0-7506-7367-2.
[2] Hofreiter, L. 2003. Nové determinanty ochrany objektov. In. Zborník z 8. vedeckej konferencie s medzinárodnou účasťou: Riešenie krízových situácií v špecifickom prostredí. Žilina: EDIS. 2003.
[3] Kružliak, Ľ. Sivák, J., Vrbičan, P.: Model stanovenia komplexnej efektívnosti stráženia objektov osobitnej dôležitosti. In. Zborník z 4. vedeckej konferencie s medzinárodnou účasťou: Riešenie krízových situácií v špecifickom prostredí. Žilina: EDIS. 1999.
[4] Sivák, J.: Systém komplexnej ochrany majektu. In. Zborník z 4. vedeckej konferencie s medzinárodnou účasťou: Riešenie krízových situácií v špecifickom prostredí. Žilina: EDIS. 2000.
[5] Koncepcia ochrany utajovaných skutočností v Slovenskej republike. [online]. [cit. 7. 07. 2008]. dostupné na: <http://www.nbusr.sk/ipublisher/files/nbusr.sk/legislativa/docs_leg/ku180607/vlastny_material.pdf>
[6] Kampová, K.: Methods of Simulations in Risk Analysis / Metódy simulácie v analýze rizík. In: RSK, Žilina, 2009. ISBN 978-80-554-0014-3