Tomas Lovecek *

PRESENT AND FUTURE WAYS OF PHYSICAL PROPERTY PROTECTION

Nowadays in the territory of Slovak republic, the property protection and security systems design lies in realization of requirements following from security requirements specifying details of tangible property protection (Law, Risk Analyze, Internal regulations of the company). In this article, three basic approaches to secure physical protection of property will be introduced. There is directive-oriented, variant-oriented and variable way of physical protection. For the most effective way of protection we can consider the variable way of protection, which allows due to its flexibility designing of the system in such a way, that it best suits requirements, conditions and possibilities of the subject.

1. Introduction

Nowadays in the territory of the Slovak republic, the property protection and security systems design lies in realization of requirements following from security requirements specifying details of tangible property protection. The security requirements come from the following three basic sources:

- legal aspects of property protection (e.g., law, ordinances, regulations, guides, business-law relations),
- independent evaluation of threats and their risks (security audit),
- set of principles, goals and requirements for property protection, which were developed by a given organization to support its operation.

Generally, binding legal directives define property protection only in certain areas (e.g., protection of classified information, critical/defending infrastructure, financial institutions). These are areas where the state has dominant interest in protection of its or private property against attack, misuse, damage or theft by other person or organized group. In case the state with the help of legal directives does not define a specific methodology of property protection (e.g., security standard of physical security and object security), there is a possibility to proceed according to requirements (e.g., insurance conditions, certification requirements according to ISO 27001) or proposals (e.g., designed or performed project of security system) of third subjects (e.g., insurance company, technical service for property protection). In case the state does not define a way of property protection against intentional threats, we can talk about so-called private security [6].

2. Property protection from confidential information point of view

The fact that the biggest attention in case of state property protection is dedicated to the classified information protection (under board of NBÚ SR), confirms that these problems are related to approximately 16% of organizations in the SR. Classified information (US) can be information (e.g., content of a document/drawing/map/photography, content of electrical/electromagnetic or other physical transport medium) or object (e.g., product, equipment, realty) [7]. From its beginning the classified information protection was subject to several changes from object and physical security point of view. The respective executing regulation specifies details about specifications of buildings and space where the classified information is located and details about the way of their protection. The main difference between the pilot regulation and later regulations (including the currently valid regulation) lies in the way how the creators of the regulation approached the classified information protection [8]. They used a *directive-oriented approach*, which caused problems for some subjects, related to holding the letter of the law, either from realization or financial position. For particular protection interests, specific precautions were defined. These were not allowed to be omitted or replaced by different ones. This approach was changed in the next execution directives [8] and for the evaluation of the US protection level the spot system has begun to be used, which allowed choice of various security variants. The spot system allows choosing such a combination of security precautions with respect to the specific conditions, which suits best the given circumstances. For objects and protected space the smallest spot values are defined, which are necessary to reach. The mathematical method is used which assigns spot evaluations to respective security precautions. Their sum is evaluated in a respective way. Precautions defined as optional do not have to be realized, but the prescribed total number of points must be reached. The philosophy of such *a variant-oriented way* of physical protection is built on the fact that the subject has to reach a necessary number of points with respect to local conditions. An example of possible variant of protection security corresponding to the US classification degree “confidential” or “reserved” is illustrated in Fig. 1. The spot system of security standard allows choosing, with respect to specific conditions, various combinations of protection

* **Tomas Lovecek**
Department of Security Management, Faculty of Special Engineering, University of Zilina, Slovakia, E-mail: Tomas.Lovecek@fsi.uniza.sk

precautions. It only depends on the given subject which combination will be chosen so that the summary point evaluation is equal or a higher than the minimum required value for respective amount of risk, which is a result of risks analysis.

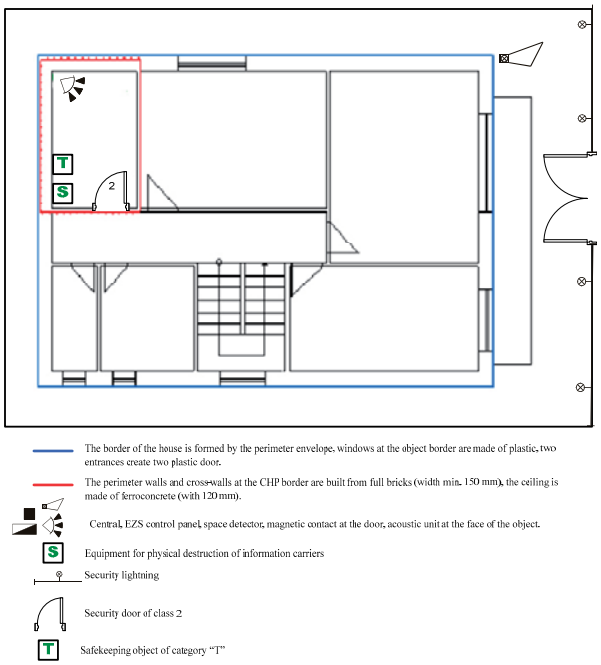

Fig. 1 Example of protected space of category classified

3. Property protection from financial institutions point of view

A combined method of directive and variant way of property protection security is used for example by financial institutions. The national bank of Slovakia (NBS) issued a precaution n. 12/2005 dealing with the analysis of risks related to the security of bank operation space where both the contact with clients and manipulation with financial cash (business office) is realized. This analysis of risks in connection with business office includes the technical-building fabrication of the object, passive and active security components of inner/outer environment, physical protection and organizational-regime precaution for employees, clients and other persons. A bank subject is, on the basis of the bank law, obligatory [9] to realize respective precautions and to discuss these precautions with a respective unit of police force. On the basis of this information, the office of judicial and criminal police of police force presidium has elaborated methodical directives for security of a unified procedure of the police force units at a risks analysis discussion which are related to the security of operational bank space. The directive part of a property protection way follows directly from the law [9] which obliges banks to secure the business office with a security and alarm system and to connect them to an alarm registration central. Furthermore, the law orders to secure the place with a camera monitoring security system in 24 hours recording time in a quality which allows distinguishing a specific person. The variant way of the bank and clients property protection security lies in the fact that the law orders to accept other security precautions which are results of risks analysis needs. A designated police officer at the risks analysis discussion uses the material presented by a bank and the methodological directive in which inner and outer environment of the bank subject is evaluated. In case the total level of risk is lower than the before set value presented in the methodological directive, the bank must accept only the directive protection precautions presented in the law. However, in case the total level of risk is higher, the bank must accept other protection precautions, which directly lower the risk level (e.g., optimization of financial cash according to operational needs of the business office, using safety caskets, transport containers and other technical means designated for financial cash protection, existence of means for financial cash devaluation, etc.).

4. Property protection from insurance companies point of view

A significant factor which influences security requirements for protection of both private and state property are conditions of insurance companies defining the security requirements for individual insurance events. Each insurance company has processed its own requirements for individual types of protection precautions with respect to the value of protected interest. Certain necessary conditions are set which the object must satisfy so that the insurance company can agree to the insurance contract. Unlike Czech insurance companies, Slovak insurance companies present only a type of necessary precautions (e.g., security door, IDS connected to the alarms registration central), but they do not present a level of protection for individual security precautions. The Czech association of insurance companies issued for insurance companies needs a so called security pyramid which declares both equality of protection elements with respective ČSN norms and respective degree of protection. On one hand, for each process of property protection and also design of security system is the owner (caretaker) of the property who has certain security requirements following either from generally binding legal directives or their internal needs. On the other hand, there is a designer/person realizing the project who comes with certain conceptual proposal how to satisfy requirements of the property owner. In practice, the fulfillment of criteria of binding legal directives and contracts (e.g., criteria following from law, executing regulations, insurance agreement, work contract) is a dominating security requirement. Let's assume that the goal of the purchaser is not only the fulfillment of the criteria of binding legal directives and contracts, but also the economic and functional effectiveness of the whole security system. We have used the word "assume" because in practice it is common that it is not possible to identify the given person from the recordings of security camera, while general conditions presented in the insurance agreement were satisfied. In the same way it is not a problem to meet the private security service, which wasn't successful at any of its "sharp" actions, while, again, general conditions presented in the insurance agreement were satisfied. From my own experi-

ence I can say, regardless the satisfaction of agreement requirements, not always the injured receives compensation. This fact is usually caused by inexact and generally formulated requirements of the respective insurance company, which are concretized by its legal and technical assistants only in case an insurance event occurs. From the presented examples follows that it should be in the personal interest of every subject which wants to insure his or her property, to include the whole effectiveness of the proposed or realized security system.

5. Property protection from critical infrastructure point of view

Also not all the state and private subjects can afford to secure their property only on the basis of requirements of insurance companies. It is about subjects which, on the basis of their activity, significantly influence the operating of the state, i.e., they influence lives of big amount of people. These subjects become on the basis of nature of their activity part of so called critical/defensive infrastructure. Under critical infrastructure we understand a set of physical or virtual systems, organizations, directives and other services, whose disruption, deficiency or destruction could cause disorganization of the society stability and state security, develop crisis or seriously influence functioning of the state administration and autonomy in crisis [5], [11]. On the basis of the given definition we can say that the following subjects come under critical infrastructure: subjects whose activity interfere in the area of providing basic goods and services with sectors, e.g., energetics, transportation, supplying with fuel and food, medical services, financial services, communication services, etc [4]. The question is how to secure property of these subjects, when insurance conditions aren't sufficient and no legal directive defines specifically the way and form of protection, as it is defined, for example, in the case of law of classified information protection. The existing legal directives define the way of property protection more or less in a proclaiming way and they do not present any concrete solution proposals. An example of such legal directive could be nuclear law [10]. It is set down in a proclaiming way in one of its executive regulations that the subject must secure by an appropriate combination of IDS effective enough and mechanical debarment means detection of violators and slowing down their progress and, in this way, enable the action unit to stop the violator's progress even before its manipulation with the subject of protection. Here, we have an interesting and important condition – even before its manipulation with the subject of protection. We can call this way of protection a *variable way* of physical protection, i.e., it is required to use enough passive and active elements of protection so that the violator is stopped by an action unit even before the individual manipulation with the subject of protection. The problem is the fact, in which a ratio the individual protection elements must be represented in the system. The law solved this problem by means of executive regulation where it sets down again, in a directive way, specific conditions of physical protection of the given subject.

In order to secure physical protection in a variable way, software tools were created, which use qualitative-quantitative methods, evaluating the existing or proposed security system, following from certain measurable values like Probability of Detection PDi, Response Force Time (RFT), Delay Time (DT) a Probability of Correct and Timely Guard Communication PC. On the basis of these data the Probability of Interruption P_I is estimated. In USA until the year 2004, 76 studies, methodologies, pieces of software or reports were developed, which engage in problems of attacks against a subject coming into contact with nuclear material [1]. Most of these studies were designated for development and implementation of computer models or decision trees, using mostly stochastic mathematical methods (e.g., Monte Carlo). The so called **EASI model** (*The Estimate of Adversary Sequence Interruption*) is used as basic methodology for judging the effectiveness of the security system which is integrated also in more complex methodologies, for example, in software tools **SAVI** (*Systematic Analysis of Vulnerability to Intrusion*) and **ASSESS** (*Analytic System and Software for Evaluation of Safeguards and Security*). The three given software tools come from the workshop of American laboratories Sandia National Laboratories [11]. These laboratories conduct research in the area of nuclear weapons, military technologies, energetics and critical infrastructure in the area of national security and protection.

The EASI Model is a stochastic method using mean values and standard deviations of above described times where in the mutual relation with Probability of Detection provides estimation Probability of Interruption P_I. Its disadvantage is the fact that it is

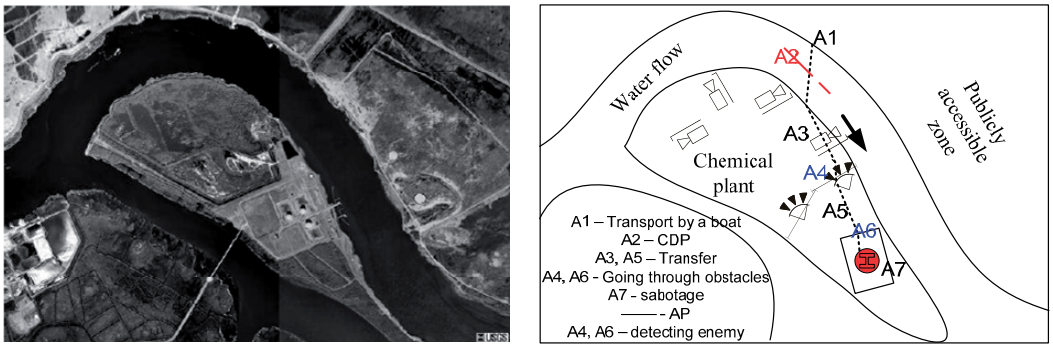

Fig. 2 a) Aerial photograph of a chemical plant b) Block diagram of eventual attack

able to estimate P_I only in one adversary path. The process of adversity is usually recorded into the so called *Adversary Sequence Diagram*. These deficiencies are removed in already mentioned SAVI and ASSESS methodologies [3]. Philosophy of the EASI module follows from the following equations:

$$PI = f\left[RFT, DT, P_{Di}, P_C, E(DT) > E(RFT)\right],$$

where *RTF* and $DT \in N(\mu, \sigma^2)$

$$P_I = \left[1 - \left(\prod_{i=1}^{j}(1 - P_{Di})\right)\right] * P_C$$

Fig. 2 a) presents an aerial photography of a chemical plant, while Fig. 2 b) shows a possible path of attackers and individual activities which they have to execute in order to reach their goal, which, in this case, is destroying the storage tank of detrimental chemical substance. Fig. 3 illustrates attackers' path with the help of a sequential diagram ASD.

SAVI software tool gives security system effectiveness estimation or vulnerability estimation, with respect to intentionally active outer or inner attackers, while it takes into account attacks type of damage or theft of given asset. Effectiveness or vulnerability of the security system is estimated on the basis of probabilities of attacker's elimination for individual possible paths of violation. The ASSESS methodology replaced the previous SAVI methodology, which didn't take into account some of the important factors (e.g., cooperation of an internal employee with an external violator). ASSESS is a software tool which evaluates the way of physical protection of nuclear material against theft and sabotage. The program consists of six modules *Facility* (the module enables analysis of elements of all system, e.g., protective elements and building constructions), *Insider* (the module enables definition of personal authorities and responsibilities of internal employees, furthermore it enables a definition of possibilities of internal employees to use slyness and falsehood to reach their goal), *Outsider* (the module enables to estimate probability of thwarting intentional security incident), *Neutralization* (the module enables to estimate probability that the action unit neutralizes attacker and stabilizes the situation) and *Hand-Off Collusion* (the module enables to assume cooperation of internal employee helping the outer attacker).

Nowadays the sections of the ministry of energetics in USA use the simulation software tools JCATS (*Joint Conflict And Tactical Simulation*), which started in 90's (JTS). JCATS is helping software tools, developed for training commanders and their action units in commands and directives during the action. Software tools take into account both actions from the ground and from the air, while it takes into account action of fire service unit. JCATS was developed on the basis of its predecessors JTS (*Joint Tactical Simulation*), UCCATS (*Urban Combat Computer-Assisted Training System*) or SEES (*Exercise and Evaluation System*). Other software tools which will be in the future used at simulations of action units look bit futuristic, but their time as the consequence of new technologies development will come (see Fig. 4). These tools are not directly used for judging the state of property physical protection, but they have to help architects in order to map the given object and to eventual simulation of already arisen security incident [2].

Apart from the already mentioned tools used for evaluation of security systems' effectiveness, it is appropriate to mention some other tools, methodologies and software dated earlier (70's and 80's of the 20th century), e.g., methodology BATLE (*Brief Adversary Threat Loss Estimator*), VISA (Vulnerability of Integrated Security Analysis), ISEM (*Insider Safeguards Effectiveness Model*) or FESEM (*Forcible Entry Safeguards Effectiveness Model*) [1].

6. Conclusion

In this article, three basic approaches to secure physical protection of property were introduced. There is a directive-oriented, variant-oriented and variable way of physical protection. For the most effective way of protection we can consider the variable way of protection, which allows, due to its flexibility, the designing of

a) b)

a)*Fig. 3 a) Block diagram of ASSESS b) screenshot taken from JCATS software*

a) b)

Fig. 4 a) CRIAISMASTERTM b)ADEPT
(source: http://www.dtic.mil/ndia/security2/jaeger.pdf)

the system in such a way that it best suits requirements, conditions and possibilities of the subject. However, on the other hand, there doesn't exist any publicly accessible general methodology, handbook, manual or other tool which would define a detailed procedure at realization of physical protection of property. Certain possibilities and solutions are offered by system tools which were developed for needs of protection of nuclear material and equipment. Here, we point out some of its deficiencies or disadvantages. We can mention for example:

- tools were created for protection of specific materials and non-commercial pieces of equipment,
- they haven't been modified from the time of their creation (EASI – 1980, SAVI – 1987, ASSESS - 1989), which also indicates critics of individual authors and users,
- they don't enable evaluation of danger level in multi-level objects,
- the tools require a big amount of expert evaluation and the fact that resulting evaluation is based greatly on mathematical statistics and probability theory can lead to inexact or misleading conclusions (e.g., in case incorrect inputs' interpretation or absence of relevant data),
- the tools do not take into account the European technical norms and standards used in the area of physical protection of property.

In spite of the above mentioned deficiencies or better said disadvantages, it is necessary to prefer and further elaborate the variable way of physical protection, which is also affirmed by the fact that the new security conception of the NBU SR (National Security Agency of the Slovak Republic) declares a change of variant-oriented way of classified information protection to the variable one. The necessity of physical protection has to be derived from reaction times of passive or active elements of the security system.

References:

[1] BAGNALL, A. M., WILBY, J., GLANVILLE, J., SOWDEN, A: *Scoping Review of Sabotage and/or Tampering in the NHS,* [on line]. Centre for Reviews and Dissemination. Report25. [cit.10.10.2007], <http://www.york.ac.uk/inst/crd/pdf/report25.pdf >, 2004
[2] PHILLIPS, G., MAY, D., GOLDEN, M., MASTON, M.: *New Vulnerability Assessment Technologies vs the Old VA Tools,* [on line], NATIONAL SECURITY PROGRAM. [cit.10.10.2007], <http://www.projectenhancement.com/new.pdf>, 2004
[3] GRANT III, F. H., MINER, R. J., ENGI, D.: *A network modeling and analysis technique for the evaluation of nuclear safeguards systems effectiveness,* ACM Press, New York, NY, USA. ISSN 0163-6103, 1978
[4] HOFREITER, L.: *Safety, risks safety and threats (in Slovak)*, ZU, ZILINA, 2004, 146 S., ISBN 80-8070-181-4(23/23)
[5] MIKOLAJ, J., HOFREITER, L., MACH, V., MIHOK, J., SELINGER, P.: *Terminology of management safety (in Slovak)*, Vykladovy slovnik, Kosice, Multiprint s.r.o. 2004. ISBN 80-969148-1-2, 2004
[6] REITSPIS, J. et al.: *Managing of safety risks (in Slovak)*, EDIS, ZU, Zilina, ISBN 80-8070-328-0, 2004
[7] *Act NR SR Nr. 215/2004 Z.z. at security of classified materials (in Slovak)*
[8] *Public notice NBU Nr. 336/2004 Z.z. at physical safety and a objects safety (in Czech)*
[9] *Act NR SR 483/2001 Z.z. at banks (in Czech)*
[10] *Act NR SR Nr. 541/2004 Z.z. at peaceful exploitage nuclear energy (atomic act) – in Czech*
[11] *Sandia National Laboratories [online], SNL. [cit. 10.10.2007], www.sandia.gov.*