Transactions of the VSB - Technical university of Ostrava Vol. VI, No. 1, 2011
Safety Engineering Series, ISSN 1805-3238 pp. 28 - 33, DOI 10.35182/tses-2011-0006

APPLICATION OF RISK ANALYSIS IN THE PHYSICAL PROTECTION OF PUBLIC UNIVERSITIES

Radomír ŠČUREK[1], Martin KONEČNÝ[2]

Review article

Abstract: This paper describes the possibilities of the application of risk analysis methods used in the industry for the risk assessment of illegal acts resulting from the situations of personal and property protection. It introduces the possibilities of involving these analyses in the practical assessment of particular hazards including the evaluation of human factor and the appraisal of influence significance.

Keywords: Hazard analysis, security threats, hazard identification, risk assessment, physical security.

Introduction

Humans and human behavior are primarily influenced by fear for our life, the lives of our family members and a sense of danger to our property. Human motivation to live in a safe and stable environment is determined (among others) using Maslow's hierarchy of needs, which puts the need of security immediately after the physiological needs to the second basic layer of the lower order needs which motivate human behavior. If we set this consideration to the specific degree of achieved technological and material level, including the level of knowledge, we can deduce that the human behavior in time and place has a principal significance on the creation of stable and secure environment. Within this context, it is in everyone's interest to keep his/her own personal security, depending on the knowledge level, to preserve the personal need to live safely. This necessity, or its degree, is given individually and therefore it is impossible to talk about fixed stability of a security in our society wherein the basic element will always be the individual person with democratically existent possibilities. Behavioral processes influenced by personal ideas and motivation, during which the individuals repress their need of security at the expense of other needs, cannot be standardized and mechanically solved with respect to their diversity. Although it is impossible to exactly describe processes connected with human motives, innovative methods or applications of well-proven tools used in other branch structures are sought, which may be applied to areas where they haven't been used till now. These methods goals are to specify and describe, at least partly, the processes connected with human factor.

Materials and methods

Characteristics of selected issue

If we hold to the human activity focused on security, thus to the system status at which the probability of detriment to protected interests is acceptable, we can submit that word meaning of security is propagated and interpreted from the standpoint of majority orientation of an organization which currently publishes materials about this phenomenon, or arranges conference and unfortunately views other safety subjects as less important. Many times are other natural segments of safety sidetracked as minor. In doing so we omit the complex character of safety while it is impossible to say that one part is more important than the other only with regard to what institution and which manager economically supports this part of safety or security. This also corresponds with different interpretations of safety when the standpoint of technical specialization disagrees with the human one. However the thief is a physical person who under the influence of his/her mental incentives often controls the technical instrument, so there are both human and technical parts of science. The complexity of safety arises from the fact that it presents a set of measures for the protection and development of human system, i.e. for the preservation and development of protected interests. This is followed up by a security that represents a state of human system in which the probability of damage to the protected interests is viewed as acceptable. In this article we will describe the application possibilities of well-proven technical methods used to assess technological hazards and to evaluate those hazards,

[1] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Ostrava, Czech Republic, radomir.scurek@vsb.cz

[2] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Ostrava, Czech Republic, martin.konecny.st2@vsb.cz

Safety Engineering Series, ISSN 1805-3238 pp. 28 - 33, DOI 10.35182/tses-2011-0006

that may be called personal and property protection hazards, or physical protection.

In the internal security subsystem of a state, in relation to the personal and property security, we can talk about few directions depending on the authorship. We can meet here the problem of uncontrollable migration and that of severe growth of criminality, growth of organized crime, terrorism (including cybernetic), culmination of political, economical or social situation in the state and growing number of attacks on institutional establishment, racial, religious and civil disturbances. Other sources, specifically the typology of security threats (for the year 2010) postulated by the Department of Security Policy of the Czech Ministry of Interior, determines as the most significant: terrorism, organized crime, cybernetic threats and civil aviation safety. More and more often we can hear about so called asymmetrical threats. Those are actions of minor tactical or operation forces against vulnerable places and their purpose is to achieve a very large effect. Presently there are six types of asymmetrical threats: nuclear, chemical, and biological weapons, information operations, alternative operational framework and terrorism.

However, the majority of authors generally agrees, that the current threats present terrorism, extremism, organized crime and criminality where characteristics of these threats blend together and we can in general use the term of illegal activities. At assessing and analyzing risks of physical security, i.e. personal and property protection, we deal with illegal activities that persons perform based on their incentives and motivation. Therefore, the evaluation mostly concerns procedural steps of offenders and it is impossible, due to the complexity of human thinking, to determine accurate results as can be done in the analysis in industry.

According to a dictionary, hazard is "a chance of bad consequences", or probability of specific undesirable phenomenon that generated during specific period or under specific conditions. The hazard is then an uncertainty multiplied by undesirable consequences. The minimization of hazard depends on protective measures, or in other words, on an optimization of protected system which can reduce, or divide, the hazard. According to the directive SEVESO II, which we apply also on the personal and property security, we can say that "hazard" is a probability of specific effects occurring during specific period or under specific conditions. The danger means a feature of subject or situation with the potential for the creation of damage.

At assessing the physical security of public universities (hereinafter called PU), as is generally done, it is necessary to identify a string "danger - threat - damage - loss". After that we need to appoint methods of analysis and calculation of hazards, including results verification. Then we review the hazards according to a scale and choose an optimal solution to minimize the hazard and install new measures (technical or organizational), as a staff training, completion of insurance and acceptance of necessary hazard. The final phase deals with a proposal of new infrastructure of the organization with a view to provide maximum level of safety. Evaluation methods aimed at PU hazards in respect to illegal acts are stochastic methods, engineering judgment, analogy and simulation (Loveček and Vel'as, 2010). The introduction of chosen measures for system optimization to practice is followed by the hazard management where hazards are monitored, reviewed and revaluated. The risk assessment has to be also adapted to changes that occurred under new conditions. Successful implementation of the process of risk management requires dividing the responsibilities according to the model "Plan - Do - Check - Act" = PDCA cycle. At assessing the project of PU security or organization security we follow three phases. In the first phase we investigate the system status, the environment condition and formulate intentions and security policy of the organization. In the second phase we execute a risk analysis and afterwards follows a third phase which consists of planning, creation of directions and regulations.

Results

The procedure of risk analysis applied to the physical protection of public universities

Analysis and risk assessment are procedures which serve for needs of management and form background for decision making process. Many methods and software tools are currently available for the analysis and risk assessment. In terms of desirable purpose of risk assessment, it is necessary to evaluate if the preconditions of methods are complied with, then evaluate if the available data and indications have informative value in terms of hazards and if the used data are applicable in chosen method. Only after that it is possible to perform the calculation. The interpretation of calculation result can be done within the extent identified by the method, but also by personal invention and judgment according to knowledge and experiences in this specialization. Individual methods of the risk analysis are only auxiliary tool of the reviewer who takes into account his/her practical experience, regulations and statistical data. It is a big advantage if the risk analysis realizes a group of reviewers to compare and evaluate the results.

Safety Engineering Series, ISSN 1805-3238 pp. 28 - 33, DOI 10.35182/tses-2011-0006

The procedure of risk analysis of PU includes problem definition, analysis of current status and the proposal of its optimization. The first step involves a determination of what has to be protected. The next step is a determination of what do we protect against (an attack, a hijack, housebreaking, or fire), and finally how do we ensure this protection. It is necessary to judge the value of probability that in the particular case (place, time, persons, terms etc.) these specific consequences will originate and how big and expensive they might be. Every existing method for hazard assessment was created for a specific problem. As mentioned above, there are all manner of risk analysis methods and their number increases. We can apply these methods to other objects as well but always with reference to the original purpose. A benchmark for method selection was actually their availability and expansion of their application in current security practice. Generally, we can say that risk analysis of illegal acts can be done in steps specified in the following block diagram.

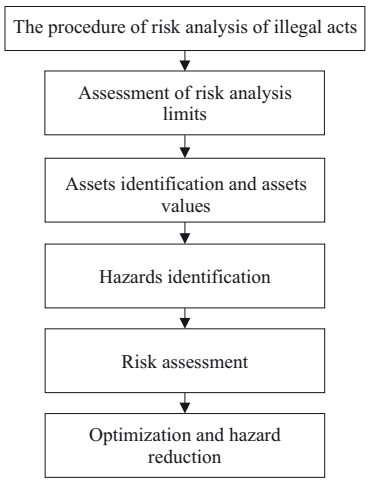

Fig. 1 Block diagram of a risk analysis of illegal acts at Public Universities

The risk analysis limit represents a boundary that separates assets which will be included to the analysis from other assets. The determination of analysis limits is based on management intentions or a security policy of organization. Assets identification consists of listing all assets occurring inside the risk analysis limit which is expressed from the economic aspect as a financial amount. This relates to the optimization and hazard reduction where it is necessary to reduce the risk to such a level when expenses for risk reduction become disproportionate in comparison with appropriate hazard limitation (ALARA principle). That means that from the economical aspect the expenses of system optimization should be around 10 % of the assets, in exceptional cases 15 %. Assessment of the assets value is based on the size of damage caused by the destruction or loss of assets. It is usual to proceed from the cost characteristics but it can be yield characteristics as well (if the asset brings well identified profits or other benefits). Then a process of hazard identification follows, during which we choose those that might threaten at least one of the assets. The identified hazards can be modeled for transparency. Every hazard is separately evaluated against every asset. It is suitable to perform approximate risk analysis first for the subsequent decision about the method option for the actual "big" risk analysis of specific PU.

Primarily we therefore perform preliminary risk analysis in order to determine which object is crucial for the PU activity and which subject is exposed to significant hazards. For these objects we will perform a detailed risk analysis that will be described later. It is probably an optimal procedure but it's undeniable that it is very lengthy and expensive process. Then a detailed valuation of identified hazards and determination of their sequence according to the relevance of their influence on PU assets follow. This relates to minimizing the worst risks that have the cost limit within the already mentioned 10 % cost limit (Reitšpis, 2004).

The actual risk analysis is based on the fact that we divide analysis methods in two large groups: qualitative and quantitative. Qualitative methods express hazards in defined range. They are for example given values from 1 to 10 or estimated by probability from 0 to 1 or verbally. The level is usually determined through qualified expert estimate (intuition). Qualitative methods are simpler and quicker but more subjective. Quantitative methods are in principle based on mathematical calculation of hazard from the point of the frequency of threat occurrence and its consequences and are more accurate. It is possible to solve overall PU risk analysis by both means. During selection of the method, especially objectives that are to be achieved by the risk analysis, including purpose, assets, for whom is the analysis addressed and investment volume, are decisive. However, in practice it can be found out that quantitative methods are not used very often in the risk assessment of physical security. It is especially due to the ignorance of these methods resulting from the fact that security managers (often ex-policemen) for so called risks of illegal acts are more likely educated in security and law rather than in technical or natural science fields and therefore they avoid calculations.

Returning to the common procedure of PU risk analysis, it is possible to state that preliminary, estimated risk analysis for the purpose of crucial assets determination and analysis method selection is generally realized in the form of qualitative analysis. Subsequent detailed analysis can also be qualitative,

or quantitative, depending on the ability and needs of reviewer. As already mentioned, it is always better when more independent experts perform the analysis.

Upon dividing the PU in smaller parts (assets) and after the determination of preliminary (qualitative) analysis, it is possible to proceed to the identification of hazards in the smaller unit. The reviewer himself/herself can perform the hazards identification provided he/she has got experience and the practice enables to do so, or it is possible to use more reviewers in methods like Brainstorming, Delphi (method of structured communication), Trends extrapolation, Scripts method, Heuristic methods, Panel discussion, Method of analogy, Comparative method and others (Plura, 2001).

During the risk identification we proceed on the basis of set objectives and risks. We identify at first from the procedural aspect, meaning we search for hazards caused by the human factor and consider these hazards more dangerous than the hazards identified from the structural (constructional) aspect that are caused by technical or structural errors. The example of danger assessment of PU from structural aspect is an identification of risks that are generated on the object perimeter, on the building's cladding (in the next phase of hazards identification) and hazards to the space and object protection. According to the Safety Pyramid we can, in each phase, identify hazards of classical and mechanical barrier systems, hazards of electric and electronic security, hazards of regimen protection etc., up to the so called residual hazards. During the risk identification of personal and property protection of PU from procedural aspect we search for hazards incurred by the process that is specific for the particular PU and its environment. For example, an angry employee or student having brought in an explosive system will cause panic and mob riots in an attempt to cause material losses and damage the goodwill of public universities, etc. In order to record all possible alternatives we identify and sort the hazards in procedural and structural categories, and then assess these risks in those subcategories while aware that the procedural hazards are more dangerous than the structural ones.

In the assessment of procedural hazards in personal and property protection (security) of PU, some point-by-point methods (for example FMEA) can also be used, which are usually employed only for structural hazards in industrial risks assessment. The selection of used method is only a recommendation with regard to the specificity of PU physical protection. Till now, the identified hazards of physical protection were generally reviewed only qualitatively, by a commentary, on the basis of the qualitative method output (WHAT IF, SWOT) or without any use of methods, only with commentary based on user's assessment. For structural hazards, especially in technological process, table values are used, for example fatigue limit, strength limit, simply limits of anything, and it is possible to attribute them with exact indexes of detectability based on their measurable and calculated values, which cannot be done in point-by-point methods. Regarding an intruder, we cannot exactly determine the values of indexes from these tables because it is impossible to measure a level of dissatisfied employee's intention to bring explosives to the PU premises. But we can estimate these indexes from statistics and experience. We can say that it is possible to exactly index constructional hazards (for example by use of breakthrough security). Procedural hazards cannot be indexed this way which is the reason why the use of quantitative methods in procedural hazards is less accurate to some extent. Although the classification of procedural hazards by quantitative methods is also somewhat intuitive, based on engineering, personal and practical knowledge, its use is not prohibited providing we are aware of possible error ratio. The use of quantitative point-by-point methods in procedural hazards is less accurate, but the result's interval is more accurate than the mere reviewer's wordy comment and the judgment without mutual mathematical conjunctions as we can see it happening in practice. From the practical point of view, we can compare the use of quantitative methods for procedural hazards to the use of the kitchen knife for releasing a screw with a cross recess. Knife as a tool is not designed for unscrewing, but if we do not have other available tool, some types of screws might be released with a certain degree of discomfort even with a knife. Likewise, it is possible to use a tool for risk assessment that is used for another purpose, but we have to be aware of certain discomfort.

In order to perform a risk analysis, the user needs hazard identification methods, particularly applied methods of graphically analytic hazard simulations. For example, the applied methods of Fault Tree Analysis (FTA) or a method of fishbone (so called Ishikawa cause-and-effect diagrams). For calculation and classification of identified hazards, it is possible to suggest a method of Failure Mode and Effects Analysis (FMEA). The solution starts with a progress from the aspect of the process that is happening in organization's systems and subsystems, and then with a progress from the aspect of structure, i.e. the perimeter, cladding of buildings, space protection and subject protection. Results of these analysis are evaluated by the "Pareto principle" (80-20 rule) and graphically in the "Lorenz curve". Result of this analysis is verified by the following calculations of the "Correlation method" (ČSN, 2007). Generally, we can summarize the whole progress of the PU physical protection risk analysis as follows:

- Identification of characteristic dangers and threats by using screening methods to identify characteristic elements and their verification.
- Division of systems to smaller parts. Assets determination. Preliminary qualitative estimation.
- Risk identification and its modeling with respect to procedural and structural approach and the determination of acceptable limits considering the cohesion of individual hazards.
- Risk assessment by qualitative or quantitative method considering priority and purpose. Results are subsequently compared from the aspect of acceptability (one is qualitative and two or more are quantitative or completed with a Software method).
- Risk evaluation includes characteristic consequences and their calculation. The user then has to determine a probability and their calculation including synergy.
- Compare accessible statistical data with results of several analyses. The user then has to choose identified hazards that were evaluated by several methods, as well as by statistical data, as the most severe.
- In the last phase, the user has to suggest a minimization of selected hazards to acceptable limit, considering costs of this optimization. It is necessary to reduce the hazard to such an level that expenses on decreasing the hazard become inadequate in comparison with hazard limitation (ALARA principle).

Analysis of defining human fault in the physical protection of Public Universities

In the following stage, we can define a human fault during evaluation of PU physical protection with respect to regimen security and physical security. This concerns behavior or attempted behavior when limit values of set system parameters are exceeded considering the human failure aspect. This can happen for example due to failure or momentary outage of attention while human intention is correct, but the procedure is wrong. Another possibility of human failure occurs due to insufficient training and instructions when the security guard does not know what to do or thinks that he might know it, but the reality is opposite. This type of failure is very dangerous because "the decision is wrong in the first place". Further, faults are caused by insufficient physical or mental ability due to bad predispositions for the job of security. Other faults are caused by insufficient motivation or by careful decision making that does not conform to directions (these faults are often called violations, but they tend to be created by bad estimation of the situation with consequent choice of wrong directive and incorrect progress). And last but not least there are faults caused by managers (providing unskilled training for security guard, wasting of experience from previous intrusions, or similar).

Quantification of human failure and estimates of its probability can be done providing that those estimates are based mainly on generic data supported by statistics. Resulting probability of failure consists of elemental human failures. Quantification can be supported by an experiment, calculations of human failure probability based on the hypothesis that faults will happen in the same ratio as in the past and its part is an assessment of uncertainties of the estimate.

The are many methods of quantification of human factor failure, for example a Method of statistical analysis of subjective estimation, Pair comparisons, TESEO method, THERP method, ASEP method, HEART method, IDA Diagrams of dependences, SLIM method, Correlation HCR method, Quantitative characteristics of human intervention database NUCLARR and others. From practice, it is possible to recommend for example the TESEO method thanks to its simplicity. This method determines a reliability of human factor by means of five factors dependent on each other. Factor types are: activities (performing activity), conditions and time (extraordinary conditions and normal conditions), personal qualities, distress, fatigue and stress and ergonomic factor. The result can be read from tables (sheets) based on the product of indexes we have read from the tables for individual factors. If the product of all five results comes to a numeric value greater than 1, we can suppose that the system failure will occur and it can cause emergency situation. The result within the range of 0.7 to 0.9 means a probability of emergency situation occurrence and the result within the range of 0 to 0.6 means no threat of an emergency situation.

The origin of human fault may be influenced by the environment and mutual interaction with subjects surrounding the security guard. In order to evaluate these influences, it is recommended to use the SHELL method. The method name hides a procedure, when the letter S means software (procedures, symbols), letter H means hardware (machine, for example central facility protection desk), letter E means environment (environment in which the security performs his/her job within the limits expressed by letters S - H - L), letter L symbolizes live ware (human, individuality in the centre of interest) and the next L means another people who the security can meet with. During the analysis we assess influences of each factor (letter) on human being. Thus the influence of clients on

the security guard (L - L) or the influence of display devices on human or the influence of the chair on his/her efficiency on the job (L - H). We can talk about relation and influence of non-physical aspects, for example manuals that security can use or an influence of catalogue sheets (L - S).

Methods of determining weights in the proposal of risk minimization

Other tools may be used in practice as well, for example "Determination of weights (priorities) in the proposal of risk minimization". Methods of importance assessment can be divided according to the information that is necessary to determine the importance. The more significant the criterion, the more importance (weight) we have to assign to it. We always choose weights (priorities) so that the total sum is equal to 1. At the situation when user cannot decide about the importance of criteria he/she has to associate each criterion with the same value of weight. Another alternative is to determine the importance from the ordinal information on criteria preferences, when the user is able to determine a sequence of criteria importance. It is possible to apply a Sequence method in which the criteria are ranged in descending order according to their importance, or a Pair comparison method (Fuller method) in which each criterion is compared with another one and then it is determined which criterion is more important in each pair. The last option is weight assessment from the cardinal information about criteria preferences where the user is able to determine not only importance sequence, but also an importance ratio between particular criteria. The user can use The Point-by-point method in which the criterion importance is rated by number of points and the more significant the criterion is, the more points are assigned to it. Another option is the Metfessel allocation method of 100 points which evaluates the criterion importance by number of points and the sum of all points has to equal 100. Again, the more significant the criterion is, the more points are assigned to it. The use of Quantitative method of pair comparison (Saaty method) is also possible. The user compares each criterion with all others. In addition to the selection of preferred criterion, we determine the size of this preference for each couple of criteria.

Conclusion

The article was focused on selected instruments, methods and analysis for risk assessment, which represent significant solutions of Risk Management of PU. In this sphere there are many security risks, some of which may seem insignificant and difficult to detect in sporadic analysis. The main aim of the article was to point out the possibility of applying selected risk analysis, representing the continuous monitoring and risk assessment, which forms the basis of comprehensive risk management of each organization.

Acknowledgments

The article is published with the same focus as the project titled „Assessment and standardization of physical protection of the object of public universities" within the security research program in the Czech Republic for the years 2010 - 2015" under the grant number VG20102013036.

References

ČSN EN 60812:2007. *Techniques for analysis of system trouble-free operation - Failure Mode and Effects Analysis*. (in Czech)

LOVEČEK, Tomáš, VEĽAS, Andrej (2010). Technical security of mail services, *Trilobit*, Zlín, 2010, roč. 10, č. 1, s. 1-5. ISSN 1804-1795. (in Czech)

PLURA, Jiří (2001). *Planning and continuous quality improvement*, 1. edition. Praha: Computer Press, 2001. 244 s. ISBN 80-7226-543-1. (in Czech)

REITŠPIS, Josef et al. (2004). *Management of security risks*. 1. edition. Žilina: Žilinská universita, 2004. 296 s. ISBN 80-8070-328-0. (in Slovakia)