RISK ANALYSIS OF A CRITICAL INFRASTRUCTURE FACILITY

Radomir SCUREK
radomir.scurek@vsb.cz

Delivered 2011-03-14, revised 2011-06-08, accepted 2011-06-16.
Available at http://www.population-protection.eu/ attachments/038_vol3n1_scurek_eng.pdf.

Abstract

The article is focused on the characteristics of risk analysis applicable to the identification of the risk of illegal acts occurring in critical infrastructure facilities protection. It provides information on connection possibilities of these risk analyses in a practical review of individual risks including human factor rating and the importance of the influences.

Key words

Risk analysis, security threats, risk identification, risk assessment, physical protection.

Introduction

A human being and human behavior is influenced first of all by the fear of life, life of relatives and by the feeling of the threat to the property. The motivation of a person is to live in a safe and stable environment and is basically determined (among others) by the Maslow´s pyramid of needs which classifies the need for the safety after physiological needs right on the second level of needs of a lower class motivating human benavior. As long as this consideration is placed to a certain degree of technological and material level including the level of cognition, it is possible to deduce that the creation of a stable and secure environment is basically influenced by human behavior at time and place. Regarding this, it is therefore a personal interest of everybody to keep inside the own degree of safety in dependence on the level of their cognition in order to sustain a personal need to live safely. This need, its degree then, is given individually and therefore it is not possible to talk about a firm stability of security in society where the basic cell is always an individual with democraticly given possibilities. The processes of behavior, influenced by thoughts and motivation of individualities where they suppress their need for safety to the prejudice of their other needs, are not possible to normalize and solve by rote with regard to their diversity. The processes connected with human incentives are not possible to record; however, the innovation methods or applications of proof tools used in the structures of other branches which are applied to areas where they have not been used so far are sought after. The objective of these methods is at least to specify and identify the

risks connected with action scenarios therefore with phenomena of human behavior.

As long as we consider human behavior aimed at safety (the condition of a system where the probability of the rise of the detriment on protected interests is acceptable), we find out, that the meaning of the word safety is perceived only as a specific segment responding to a professional focus of an organization which right now talks about this phenomenon, or it holds a conference and many times the safety of other sections is not regarded as the same important as it is the focus or education of managers of a given organization. Other natural segments are this way shifted to the margin as less important. Hereat a complex character of safety is overlooked when it is not possible to talk that one part is more important than the other just with regard to the fact which institution and which manager economically supports this area of security. This also corresponds to various interpretations of safety when sometimes the technical viewpoint differs from the humane one. A thief or a terrorist is a physical person who under the influence of psychical incentives operates a technical device and there the area of both humane and technical sciences is represented. The complexity of safety comes out of the fact that it is a set of measures for protection and development of a human system, i.e. for protection and development of protected interests. This is also connected with security which is a condition of a human system where the probability of the rise of the detriment on protected interests is acceptable. The possibilities of the application of proof methods used for the assessment of technological and managerial risks will be described in this article together with the evaluation of the risks which are possible to call ciritical infrastructure risks from the viewpoint of physical protection.

In the subsystem of internal security of a state related to critical infrastructure protection it is possible to talk about several focuses in the dependence on the authorship. We may encounter with the issue of uncontrolled migration of persons and a steep growth of criminality, the growth of organized criminality, terrorism, escalation of political, economical or social situation inside the state, increasing assaults on constitutional system, racial, religious or civilian disturbances. Other sources, specifically the typology of security threats determined by the Department of Security Policy of the MoI of the CR specifies that among the most significant security threats especially belong - terrorism, organized crime, cybernet threats, extremism and the security of civil aviation. More and more we talk about so called asymmetric threats. They are the actions of smaller tactic or operation forces against vulnerable places whose purpose is to achieve a disproportionally huge effect. At present there are six asymmetric threats, they are nuclear, chemical and biological weapons, information operations, alternative operation conceptions and terrorism.

Generally the professional public agrees upon the fact than among actual threats belong – terrorism, extremism, organized crime and criminality when the characters of these threats blend together. Generally these threats can be called illegal activities. When assessing and analyzing the risks of critical infrastructure security we deal with illegal activities committed by persons on the base of their

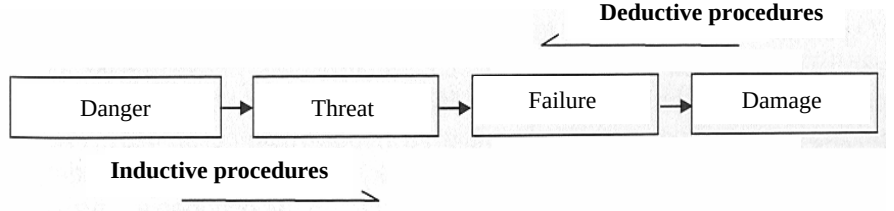
incentives and motivations. The evaluation therefore concerns mostly the procedural steps of perpetrators and it is not possible by reason of unseizurability of human thinking to determine precise results as it is with the analyses e.g. security of industrial technologies.

The risk depends, as long as its decrease is concerned, on protective measures or in other words on the innovation of a protected system by which this risk may be lowered and divide. The risk is the uncertainty multiplied by undesirable consequences and according to the directives SEVESO II, which have been apllied, it is possible to say that the "risk" is the probability of specific effects occurring during a specific period or under specific conditions. The danger is the characteristic of an object or a situation with the potential to cause damage. The security is generally defined as an agreggate description of determinants which are necessary to keep in the acceptable limits of a resting state or the security is a state where the rise of the detriment of people´s lives and health, the environment, society and critical infrastructure has been of an acceptable probability.

The procedure of the risks analysis applied to physical protection of a critical infrastructure subject

The security as a concept has not been specified yet in the CR legal system. However, the amendment of a Crisis Act and amendments of the Government Resolution say that the critical infrastructure subjects have to come out of the risks analysis.

When assessing the protection of a critical infrastructure subject it is necessary to identify the chain "danger – threat – failure – damage".



Next we determine an appropriate method of an analysis and the calculation of a risk including the verification of results. After we assess the risk according to a scale we choose an optimal solution for minimization of a risk and introduce new measures (technical or organizational), personnel schooling, resp. insurance completion and the adoption of the acceptable risk. In the final phase we present an optimized proposal of the company infrastructure with regard to the assurance of maximal security. The methods of evaluation focused on the risks of an critical infrastructure object with regard to illegal actions will be the methods of probability, engineering judgement, analogy and a model. [3]

After implementing the chosen measures for the optimization of a system, the risk management is the next. It includes risk monitoring, researching and re-evaluation of risks and adaptation of risks evaluation to changes which began under new circumstances. Successful introduction of a procedure of risks analysis requires the division of responsitilities. In a model "Plan – Do – Check – Act" = PDCA When assessing the project of critical infrastructure object or organization security we come out from three phases. In the primary phase we investigate the condition of a system, environment and enunciate the aims and security policy of an organization. In the secondary phase we start risks analysis and consequently the tercial phase deals with planning and determination of guidelines and regulations.

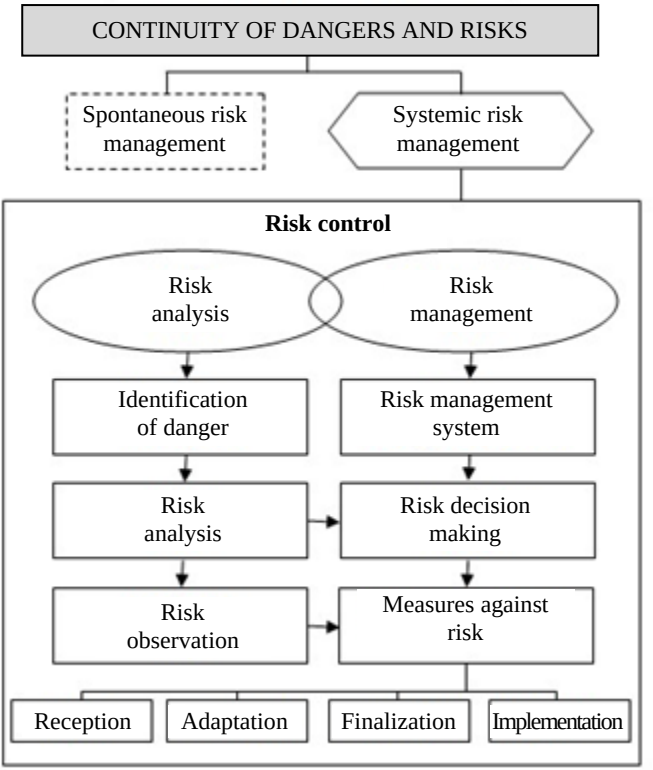


Fig. 1
Block scheme – continuity of the danger and risks

The analysis and risks evaluation are procedures which are necessary for the management and serve as the groudwork for the decision making processs. At

present there is a number of methodologies and software tools for the analysis and risks evaluation. From the viewpoint of the objective, it is necessary to evaluate first, if the hypotheses of an existent methodology are fulfilled, then evaluate if the information and data available are relevant from the viewpoint of risks and if these data are applicable with a chosen methodology.

Only after this, it is possible to carry out the calculation. The interpretation of the results of the calculation is possible to carry out within the range which is determined by a method but also by personal invention and deduction of the investigators who acquired it through the practice and knowledge. Individual methods of risks analysis are therefore only a supportive tool of the reviewer who uses also own practical experience, regulations and statistic data. It is beneficial if the risks analysis is shared with more reviewers in order to compare the results and evaluate them.

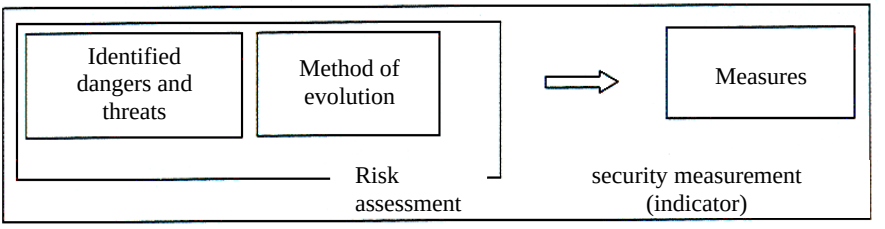


Fig. 2
Risks analysis methodology

In order to solve risks analysis in a critical infrastructure object, the procedure consisting in the problem defining, analysis of a current situation and suggestions for the measures is opted.

The first step is the determination of assets; therefore, the objects that are supposed to be protected. Further against what we protect ourselves (assault, kidnapping, robbery, fire) and in which way to ensure the protection. It is necessary to assess how high is the probability that in a specific case (place, time, persons, circumstances etc.) the consequences will occur and how extent and costly they might be. Each of existing methods for the determination of risks was developed for a specific problem. As mentioned above, it is a wide range of the methodologies for the analysis and risks evaluation and the other ones appear. These methods are applicable if needed for other objects; however, always with regard to a primary purpose. The criteria for the selection of methods was just their availability and extention of their application at present security practice. Generally it is possible to say that the risks analysis of illegal actions is possible to carry out in this order:

1. Determination of a risk analysis boundary
2. Identification of assets and the value of assets (also orientation analysis)
3. Identification of risks and the risk modeling
4. Evaluation of risks, vulnerability and the probability of the phenomenon
5. Risk decreasing

The boundary of risk analysis is a margin separating assets which will be included into the analysis from the other assets. During the determination of the analysis boundary we start from the intentions of the management, in some case from the security policy of a critical infrastructure facility. The identification of assets consists in the creation of a list of all assets being inside the risk analysis boundary, expressed from the economic viewpoint by a financial amount. This is connected with the risk decreasing when the risk is necessary to decrease to such a level where the expenses on the risk decrease become disproportionate in comparison with the relevant risk restriction (the principle ALARA), therefore from the economic viewpoint the expenses on the optimization of a system should be about 10 % of assets, exceptionally up to 15 %. The evaluation of the value of an asset is based on the extent of the damage caused by the destruction or by the loss of an asset. Usually during the determination of the value of an asset we start from the expenses characteristics, however, we can also start from the profits characteristics (as long as an asset brings easily identified profits or other benefits). The next part is the risks identification which is performed by selecting those risks which might threaten at least one of the assets. For the lucidity, the identified risks might be modeled here as well. Each risk is evaluated against each asset separately. It is suitable to make at first an orientation risk analysis for the consequent decision on the selection of a method for the following own “complete” risk analysis of a specific critical infrastructure facility.

Primarily it is therefore made an orientation risk analysis in order to evaluate which of the facilities is a key one from the critical infrastructure viewpoint and which is exposed to considerable risks. For these facilities consequently a detailed risk analysis will be made which is mentioned further. Despite the fact that it is the most suitable procedure, we cannot deny that his procedure is lengthy and therefore expensive. Afterwards there is a detailed evaluation of identified risks with a consequent determination of their order according to the seriousness of their impact on the asset of a critical infrastructure facility which is connected with the minimization of the most serious ones which with the expense limit will not exceed the permitted expenses. [4]

During the respective risk analysis we start form the fact that the risk analysis methods beside others are divided into qualitative, semi-qualitative and quantity analyses. For qualitative methods it is typical that the risks are expressed in a specific extent (e.g. they are marked <1 to 10>, or they are determined by the probability <0; 1> or verbally). The level is usually determined by a qualified expert estimate (intuition). Semi-qualitative methods complete qualitative evaluation by point values. The objective is to create point scales which are more detailed and the potential of verification between facilities is higher than it is with a qualitative analysis.

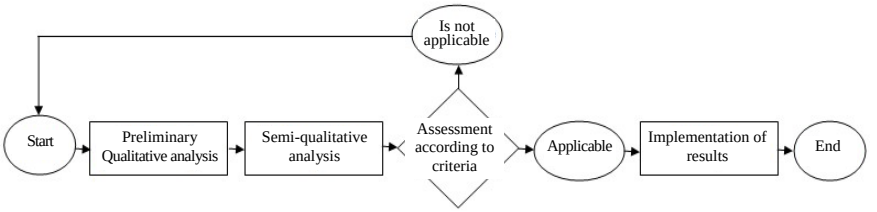


Fig. 3
The application of the risk analysis for the evaluation of identified risks and dangers

Qualitative methods are simpler and faster but more subjective. Qualitative methods are based usually on a mathematical calculation of a risk from the frequency of the occurrence of a threat and its impact and they are much more precise. Globally the risk analysis of a critical infrastructure facility is possible to solve through both ways and especially the objectives which are to be achieved are decisive when choosing the method, including the purpose for whom the analysis is designed and the volume of investments. However, the practice shows that semi-quantitative and qualitative methods are not much applied when evaluating the risks in the area of physical protection. This is especially due to the complexity of these methods which means also the fact that security managers are rather educated in legal affairs than in security-engineering or in natural science. With regard to the fact that it is not possible to define exactly in numbers e.g. the magnitude of the disclosure as well as the limit of the strength in a machine part, for the purposes of physical protection the semi-quantitative method might be used where the index is or else set guessingly but through a qualified estimate and it is already justified by the handler and controlled by an auditor. It is suitable to combine the team of risks evaluators from both technically and humanitarianly educated experts. [5]

Going back to a general procedure of a risk analysis of a critical infrastructure facility it is possible to say that first the orientation and preliminary risk analysis is made in order to find out the key assets and the choice of an analysis method. This is basically in the form of a qualitative analysis and the consequent detailed analysis may be already qualitative, semi-qualitative, or quantitative according to the abilities and needs of evaluators (it is always better when the analysis is made by more independent experts as already mentioned above).

After the division of a critical infrastructure facility into smaller units (assets) and the determination of the orientation (qualitative) analysis it is possible to start the identification of risks in a given lower unit. The evaluator himself is able to identify the risks as long as he is experienced and it is practicable or it is possible to use for this some methods encompassing more evaluators such as

Brainstorming or Delphi method, Trends Extrapolation, Scenarios method, Heuristic method, Panel discussion, Analogy method, Comparative method etc. [2]

During the risks identification we proceed on the base of determined objectives and risks are identified first of all from the process point of view, therefore we search risks caused by a human factor and these risks are considered to be much more dangerous than the following risks identified from the structural (construction) point of view. As an example of the assessment of the danger of a critical infrastructure facility from the structure point of view we can introduce the risks identification arisen on the outside and inside perimeter of the critical infrastructure facility, in the following phase we can introduce the identification of risks on the surface sheet of a critical infrastructure facility, risks of spatial and subject protection and here we can again according to the pyramid of security in each phase identify risks of classical and mechanical barrier systems, risk of electrical and electronic security, risks of the regime protection, physical guarding, insurance up to so called residual risks. During the identification of risks of protection of persons and property in the critical infrastructure facility we again search for risks arisen in the process specific for a given company and environment. For example an angry employee or a client brings into a facility an explosive system, he damages the products in order to do harm to the company´s name etc. In order to catch up all potential variants we identify risks and classify them into process and structural categories and then in these sub-categories we make also the evaluation of these risks knowing that the process risks are much more dangerous than the structural risks.

During the evaluation of a process risk from the area of the security of persons and the property in the critical infrastructure facility we may apply also some point methods (e.g. FMEA), which are during the evaluation of industrial risks basically applied only to structural risks. The selection of a used method is only a recommendation with regard to specifics of so called physical protection of a critical infrastructure facility. Mostly so far identified risks of physical protection have been assessed only qualitatively, therefore through the commentary, on the base of the output of the qualitative method (WHAT IF, SWOT) or without the application of methods only through the commentary based on practical assessment of an evaluator. With structural risks, thus especially in a technological process the tables such as the tiredness limit, the strength limit, the whatever limit are used. Through them on the base of measurable and calculated values it is possible to allocate the precise indexes of the disclosure etc.

With thieves we are not able to determine from the tables indexes values exactly, because it is not possible to measure the intention of a dissatisfied employee to bring in a critical infrastructure facility the explosion; however, we are able to estimate these indexes from the statistics and practice for which just semi-quantitative methods are suitable. We may say that structure risks can be precisely indexed (e.g. via the break-through security) and the processed ones cannot. This is also the reason why the application of quantitative point methods in process risks is less precise. Despite the fact that the evaluation of process risks by semi-quantitative methods is made to a certain degree intuitively on the base of

engineering, personal and practical knowledge, we accept here a certain amount of mistakes. The application of semi-quantitative point methods in process risks will be less precise, but the interval of a result will be undoubtedly more precise than in a poor verbal commentary of an evaluator, as it has been so up to now. From the practical point of view we can compare the application of a semi-quantitative method to a process risk to the application of a knife to loosen a cross slot screw. The knife as a tool is not designed to loosen a screw, but as long as we do not have any other tool, this knife fulfills with a certain limitation of the comfort its purpose for some types of screws. The same way it is possible to use as a tool the method of risk evaluation used for other purpose with the realization of certain discomfort.

To analyze risks we can e.g. apply the method of risk identification, specifically the applied method of graphically analytical risk modeling. For example the applied method "tree failure" (FTA) or the method "fishbone ", so called Ishikawa cause and effect diagram. For the calculation, evaluation of identified risks we may suggest the method "failure mode and effects analysis" (FMEA). The solution starts first with the procedure from the processes viewpoint proceeding in systems and sub-systems of the critical infrastructure facility and consequently with the procedure from the structural viewpoint, therefore perimeter surface sheet protection of buildings, spatial protection and object protection. The results of this analysis are more over evaluated by a "Pareto principle 80/20" and graphically visualized by a "Lorenz curve". The result of this analysis is verified by the following calculations using the Method of "correlation". [1] Generally the whole procedure of risk analysis of physical protection of a critical infrastructure facility may be summarized into the points:

1. The identification of typical dangers and threats by applying screening methods for the identification of typical elements and their verification.
2. Division of systems into smaller units. Determination of assets. Preliminary qualitative evaluation.
3. Preliminary orientation risk analysis and the selection of methods.
4. The identification of risks and their modeling with regard to a process and structural approach and determination of a boundary of the acceptability with regard to interlacing of individual risks.
5. Evaluation of risks through a qualitative or semi-qualitative method with regard to the priorities and the purpose. The results are then compared from the aspect of acceptability (e.g. one qualitative and two or more semi-quantitative, in some case a method in Software is added).
6. Risks evaluation includes characteristic effects and their calculation. After it follows the determination of probability and its calculation including synergy respecting.
7. Available statistic data are compared to the results of several analyses. Selection of identified risks which were evaluated as the most serious in several methods and also in statistic data.
8. To suggest for such selected risks their minimization on the acceptable boundary with regard to expenses of this optimization. The risk must be lowered up to such level when the expenses on the risk decrease become

uneven in comparison with relevant limitation of a risk (principle ALARA "As low as reasonably achievable").

The analysis of a defined human fault in physical protection of a critical infrastructure facility

In the following (extra standard) phase it is possible when assessing physical protection of a critical infrastructure facility have a respect to, with regard to regime protection and physical guarding also defining a human fault. It means acting or an attempt of acting where the marginal values of given parameters of a system from the human fault aspect are stepped over. This might happen due to a failure or a momentary disable state of the attention when the intention of man is right but the procedure is wrong or the schooling or instructions are inadequate when the guards do not know what to do or they think they know it but in fact they do not. Making mistakes of such a kind is very dangerous because *"already the decision itself is wrong"*. Further there are mistakes made due to the lack of physical and psychical resilience which is caused by unsuitable abilities of the guards for this specific activity. Then there are mistakes made due to the lack of motivation or too cautious decision making which does not follow the instructions (they are often called an offence but they are usually mistakes caused by the wrong estimation of a situation and the following selection of a wrong guidance and a wrong procedure and last but not least the mistakes of managers (improperly made plans, insufficient assurance of guard schooling, not applying lessons learned from previous infringements etc.).

Quantification of a human failure and estimations of the probability of the failure of man is possible to carry out supposing that the estimates are mostly based on the generic data supported by the statistics. The resulting probability of the failure is composed of elementary human failures. The quantification may be supported by an experiment. The calculations of a human failure probability come from the supposition that the failures will occur in the same proportion as in the past and the part of it is the evaluation of the uncertainty of the estimate.

There is a wide range of methods of quantification of a human factor failure, for example the Method of a statistic analysis of subjective estimates, Pair comparisons, Method TESEO, Method THERP, Method ASEP, Method HEART, Method of diagrams of dependencies IDA, Method SLIM, Method HCR correlations, Database of quantitative characteristics of human acts NUCLARR and others. Based on the practice we can recommend thanks to its simplicity e.g. Method TESEO which determines the reliability of a human actor through 5 factors which are mutually dependent. It is an activity factor (carried out activity), further according to a condition and time factor (extraordinary conditions and current conditions), a personal quality factor, an anxiety factor, a tiredness and stress factor and an ergonomic factor. The result is the subtraction from the tables based on the product of indexes also subtracted from the tables with individual factors. As long as the product reaches all five results of a numeric value higher

than 1, we suppose that the failure of a system will occur, therefore an extraordinary event. As long as the result is in the interval 0.7 – 0.9, there is the probability of the rise of an extraordinary event, the range in the interval between 0 and 0.6 means that an extraordinary event is not probable.

Also the environment may influence and may cause the rise of a human failure as well as mutual interaction with objects surrounding a guard. For the assessment of these influences we recommend to apply Method SHELL. In the name also a procedure is hidden, where the symbol S means software (procedures, symbols etc.), symbol H expresses hardware (a machine, e.g. an operator panel of a centralized protection), further E means the environment (the place where the guard performs within limits of S-H-L), further L means liveware (man, a person in the center of an interest) and a second L means other persons with whom a guard comes into a contact. In the analysis we assess the influences of individual factors (letters) on man. Therefore it is the influence of clients on the guard (L-L), the influence of display devices on man or the influence of a chair on the performance of a dispatcher (L-H), we can also talk about the relation and the influence of man and non-physical aspects, e.g. manuals which the guard may use, the influence of catalogue pages, etc. (L-S).

The methods of the importance determination when suggesting the risks minimization

In the practice we can also use other tools e.g. “Importance (priorities) determination when suggesting the risks minimization”. The methods for the determination of the importance may be divided according to the information which is necessary for this importance determination. The more important the criterion is the more importance we have to allot. The importance, therefore the priorities are always chosen so that the sum of the importance of all criteria was 1. We can talk here about the determination of the importance of criteria, without the information on the criteria preference when the responsible person is not able to decide about the importance of criteria for the assessment of the variants and to each criterion the same importance is allotted.

The other variant is the importance determination from the ordinal information on preference criteria where the responsible person is able to determine the order of the criteria importance and here we can apply the Method of order where the criteria are arranged in a descending way according to their importance, or the Method of Pair comparisons (Fuller method) where we use the comparison of each criterion with another and determine which criterion of a given couple is more important.

The last variant is the determination of the importance from the information on the preference of criteria where the responsible person is able to determine not only the order of the importance but also the proportion of the importance between individual criteria and he will apply either the Method of points where the importance of a criterion is evaluated by the number of points

from an in advance determined interval. The more significant the criterion is, the more points are allotted to it, because according to the Metfessel allocation of 100 points where the importance of a criterion is evaluated by the number of points, whereas the sum of all points must equal 100. It is also possible to use the Method of quantitative pair comparisons (Saaty method), where we compare each criterion with another. Besides the selection of a preferred criterion we determine for each couple of criteria also the size of this preference.

Résumé

Nowadays the issues of risk management studies on physical protection of critical infrastructure is more and more actual. The qualitative methods are mainly used in practice. The qualitative methods and semi qualitative analyses are far less used in systems of risk management. The article is focused on these risk analysis methods applicable to the identification and review of illegal act risks occurring particularly in physical protection of critical infrastructure facilities. The work also acquaints with the assessment and rating of a human factor and with the phenomenon of threats in critical infrastructure facilities. A lot of methods of risks evaluation have been applied especially in a technological sector focused on aviation and work safety, and they have been used rarely in the evaluation of physical protection of critical infrastructure. Therefore the paper offers the alternative and the methodology in a risk management system with the application of derived methods from other spheres of safety.

Literature

[1] CSN EN 60812. *The technique of the analysis of the reliability of systems – The procedure of the ways of the analysis and the consequences of failures (FMEA).* Prague: Czech Standards Institute, 2007.

[2] PLURA, J. *Method FMEA and FTA.* Ostrava: DTO CZ, Ltd. Supportive education texts for BONATRANS GROUP Inc. Bohumin.

[3] LOVECEK, T., VELAS, A. Technical assurance of the protection of postal services. In *TRILOBIT professional research journal.* Zlin: The Faculty of Applied informatics UTB in Zlin, 2010. ISSN 1804-1795.

[4] REITSPIS et al. *Management of security risks.* 1. edition Zilina: Zilin University in Zilina. ISBN 80-8070-328-0.

[5] SMEJKAL, Vladimir, RAIS, Karel. *Procedure and methods of risks analysis.* (cit. 2008-02-03). Available at WWW: http://www.businessinfo.cz/cz/clanek/rizeni-rizik/postup-a-metody-analyzyrizik/ 1001617/42741/.