RISK ASSESSMENT IN THE AREA OF PUBLIC UNIVERSITIES

Martin KONEČNÝ[1], Ondřej STONIŠ[2], Radomír ŠČUREK[3]

Review article

Abstract: The article deals with the application of risk analysis for the identification and assessment of unlawful acts within the premises of public universities (referred to as PU). The subject of this article are options for increasing security level of these buildings, and thus it also provides an overview of potential involvement of selected risk analysis in practical assessment of security risks.

Keywords: Physical protection, university, identification, risk analysis.

Introduction

Public universities can certainly be included in the category of buildings that may be a target to potential illegal activity. In addition to conventional illegal acts in terms of threat to life and health (theft, vandalism, etc.), there is also an imprescriptible risk of more significant threat with greater impact to the society. This group of security risks includes terrorism, organized crime or the use of weapons of mass destruction. Important thing which confirms this statement is the fact that during the day tens to hundreds of people, especially students, staff and the public are present in these types of buildings. These institutions are also frequently visited by prominent politicians and statesmen during various lectures, conferences and formal events, being important potential targets of terrorist attack and thus a threat to the PU building itself and to all the people who are present there at the moment. However, PU buildings are not exposed to external threats only. Significant risks to security are violence and aggression of students or teachers, which are in most cases more difficult to detect than in case of a standard offender. Many incidents from abroad are pointing the fact that it might be only a matter of time before similar cases of violence occur at universities in the Czech Republic (CR), which is also confirmed by a recent knife attack at elementary school teacher in Havířov to whom the offender caused a series of cutting and stab wounds. Currently there are 26 public universities in the Czech Republic (Ščurek and Konečný, 2011).

The actual level of security at individual universities is not optimal, the technique is outdated, current regime measures are insufficient and can hardly detect and reveal a more capable offender. Virtually every public university implements physical protection through the guard service, which provides physical security and protection of the building. However, eligibility of the guards to respond to the alarm and any action against the perpetrators is often insufficient. Given these facts, attacks of a similar nature cannot be excluded in the future and it is necessary to take all possible preventive measures.

Materials and methods

Characteristics of preventive measures to increase the level of safety

From the perspective of security of PU we need to seek possibilities of using innovative elements in security technology field, where the development is focused on the introduction of new access systems (e.g. biometrics, radiofrequency identification and localization). Other areas of interest should be the technology searching and profiling potential offenders, or the intention to carry out an attack on a protected building. It concerns a development of contactless devices allowing the detection of negative intentions of people (the terrorist's revelations, etc.) through sensors. These systems allow the registration of non-verbal body demonstrations undetectable to human eye (body temperature, the contraction of facial muscles, etc.). If the sensors identify the sensed parameters are abnormal, the system activates an alarm signal. In the area of physical protection we can also use RFID technology, through which the

[1] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Ostrava, Czech Republic, martin.konecny.st2@vsb.cz
[2] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Ostrava, Czech Republic, ondrej. stonis@vsb.cz
[3] VŠB - Technical University of Ostrava, Faculty of Safety Engineering, Ostrava, Czech Republic, radomir.scurek@vsb.cz

organization will obtain contactless identification of persons and property, or their location within the building in real time (Finkenzeller, 2003). The spectrum of RFID utilization is diverse and in cooperation with the optimal settings of mode measures this technology represents an efficient system that enables the control of entry, exit and movement of staff, students and visitors within the premises of public universities. Another important precautionary element in physical protection is the risk management. Here it is necessary to choose the appropriate strategy and the definition of effective security measures leading to the optimization of risk and losses generated by adverse incidents. However, despite all precautions that the organization dedicated to the risk management a number of negative phenomena cannot be excluded, which can lead to serious threat to personal health and threat to other assets of PU. Those phenomena are emergency situations that are artificially induced, random, unexpected and socially dangerous, in respect to a significant effect on human health, property and the environment. This category includes an explosion of trip explosive system (referred to as TES), burglary, theft, sabotage and other illegal activities. Perpetrators of these crimes can be divided into external and internal attackers, or a combination of both of these types, which is very efficient in terms of successful implementation of the attack. With a large number of persons moving around the public universities are very vulnerable, open to all visitors and thus an easy target of terrorist attack and other forms of crime. To ensure complete safety of the organization it is therefore necessary to ensure mutual cohesion of various components of security and adapt their interactions to selected building. In the event that one component is not optimal, this gap cannot be effectively replaced by another and the system cannot be further considered safe and reliable (Ščurek and Konečný, 2011). Therefore the prevention is necessary, whether in the form of risk analysis or innovative means of technical protection, enhancing monitoring, identification and locating of people in buildings of this nature.

Results

Application of selected risk analysis

Risk analysis is a procedure that is used for the management and forms a basis for the decision-making process of the organization. For analysis and risk assessment are currently available many methodics and software tools. In terms of desirable purpose of risk assessment it is necessary to evaluate if the expectations of methodics are executed, then evaluate if the available data and indications have informative value in terms of hazards and if used data are applicable in chosen methodics. Individual methods of the risk analysis are only auxiliary tool of the reviewer who takes into account his/her practical experiences, regulations and statistical data (Rafferty, 1994). It is a big advantage if the risk analysis realizes a group of reviewers to compare and evaluate the results. The procedure of risk analysis of PU includes problem definition, analysis of current status and 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.) will originate these specific consequences and how big and expensive they might be. Every existing method for hazard assessment was created for a specific problem. As mentioned above, there is all manner of risk analysis methods and their number increases. Methods of risk assessment of public universities include probability methods, engineering judgment, analogy and model (Loveček and Veľas, 2010). We can apply these methods on 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. Within the evaluation and risk assessment of PU it is necessary to define the string "danger - threat - fault - damage". In general, the procedure of risk analysis of unlawful acts is shown in the following block diagram.

Boundary of risk analysis is a limit defining assets to be included in the analysis. To this closely relates the optimization of the risk when the risk must be minimized to such level that the reduction of costs does not become disproportionate in comparison with the corresponding risk limitation (ALARA principle). From the economic point of view, the expenses on system optimization should be around 10 % of assets, in exceptional cases may reach 15 %. Subsequently, detailed identification of risks is done, when we select risks that could threat at least one of the assets. Then a detailed assessment of identified risks is conducted, determining their order of significance of the impact on public universities assets, which is related to minimizing the most serious that fit into the above mentioned 10 % cost limit (Reitšpís, 2004). Prior the "big" risk analysis of PU it is recommended to carry out preliminary risk analysis in order to determine which one of the buildings is crucial for the functioning of PU and is exposed to significant risks. Preliminary risk analysis

is usually done in the form of qualitative analysis. Appropriate method is for example a risk modeling with Ishikawa diagram that defines the various causes of risk, leading to security threats to PU.

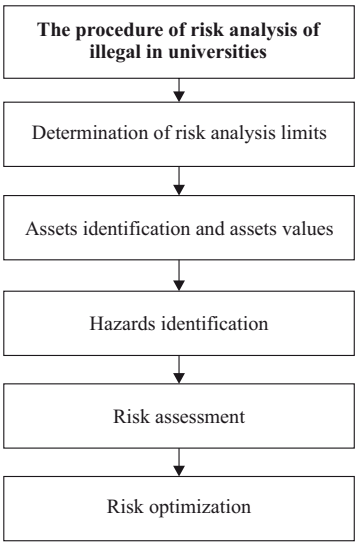

Fig. 1 Block diagram of risk analysis procedure (Ščurek and Konečný, 2011)

leads to a simple understanding of the behavior of the system and the factors contained therein. Illustrative example of application of this method is shown in the following block diagram.

Detailed analysis can be qualitative, same as already mentioned preliminary analysis. Many evaluators, however, prefer for the purposes of risk assessment of buildings of similar nature as public universities, quantitative methods. One of them is the analysis of the causes of failures and their consequences (referred to as FMEA), which is a quantitative method of risk assessment based on the analysis of failure modes and their consequences, enabling identification of consequences and causes based on systematically and structurally managed failures. It also serves to control individual elements of the system and its operation, where it identifies basic faults. During FMEA the risks are first evaluated in terms of process (caused by human factor) and then in terms of structural point caused primarily by technical or structural fault. Example of PU risk assessment in terms of structure can be risks generated on the perimeter or cladding of the building or risks of area or subject protection.

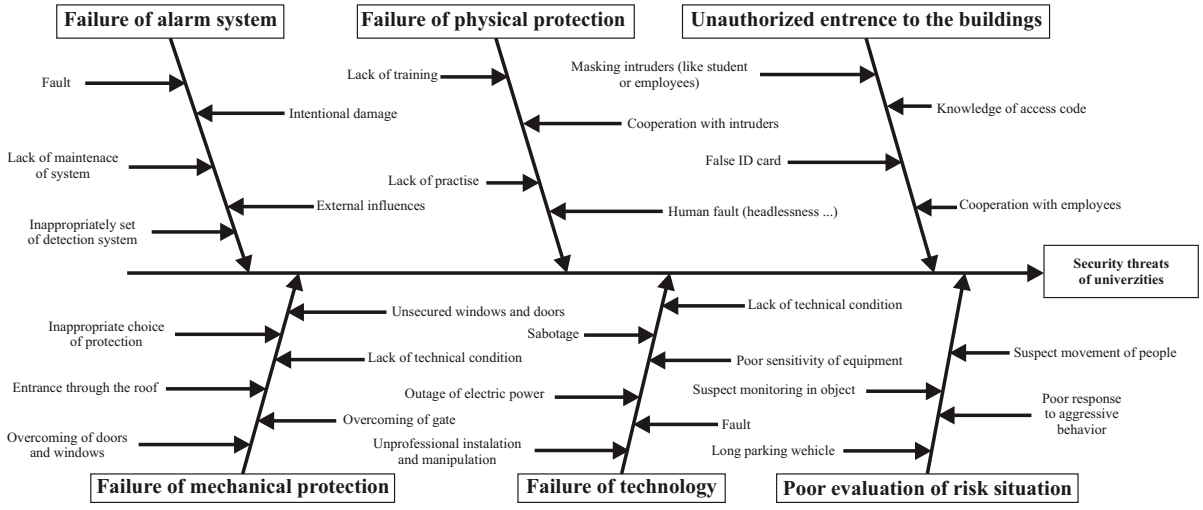

Fig. 2 Risk identification by Ishikawa diagram (source: Author)

Another preliminary risk analysis using scientific approach suitable to use is the fault tree analysis (referred to as FTA). This method is highly systematic and allows you to analyze various factors, including physical phenomena and human interactions. Using a "top-down" approach, it focuses on those consequences of faults that are directly related to the top event, such as the explosion of TES. In general, this analysis provides the evaluators with an overview of possible causes leading to an adverse phenomenon with a comprehensive overview and reflection on its creation. Graphical representation

In terms of process it concerns risks generated in the process specific for certain public university and its environment (e.g. sabotage of discontented employee). Due to possible variations, the risks are identified and divided into aforementioned process and structural categories, followed by the assessment of individual risks is carried out with the knowledge that the process risks pose greater threat in terms of security than structural risks do (Ščurek a Konečný, 2011). The output of this analysis is a table with subsequent graphic output of identified risks and those are evaluated by "80/20 Pareto principle" (see example in Tab. 1).

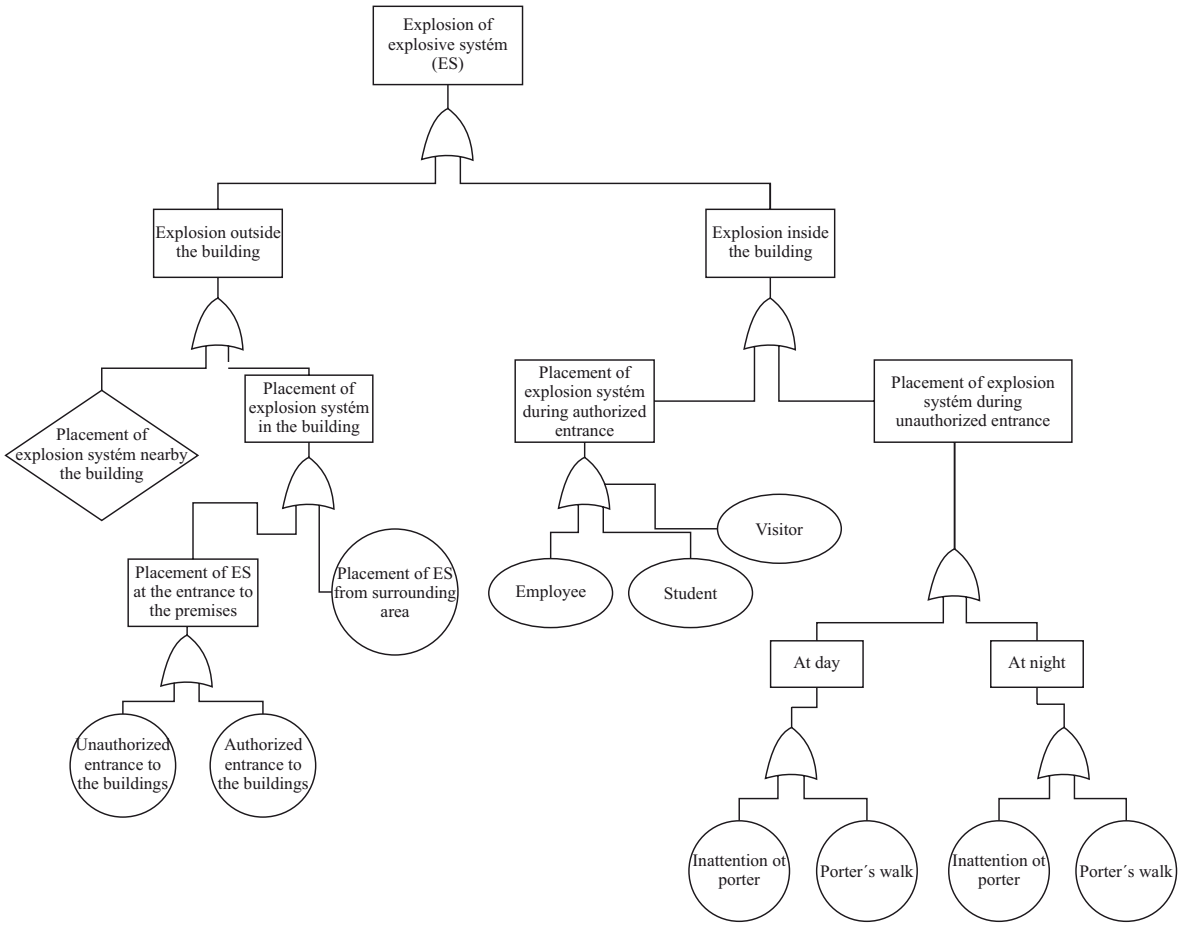

Fig. 3 Risk of explosion of TES by FTA method (source: Author)

Tab. 1 Process risks assessment (source: Author)

No.	Event	Evaluation			R	Pareto Principle 80/20 [%]
		P	N	H		
1	Unauthorized entry through the lodge	4	5	5	100	**34.48**
2	Failure of key mode	3	3	4	36	**12.41**
3	Theft of property or other assets	3	4	3	36	**12.41** **to 80 %**
4	Insufficient control of people	3	3	3	27	**9.31**
5	Human factor failure (negligence)	3	3	3	27	**9.31**
6	Failure of alarm security and emergency system	4	2	3	24	8.28
7	Sabotage of employees with the offender	3	2	3	18	6.21
8	Wrong evaluation of risk situations	4	2	2	16	5.52
9	Power outage	2	2	1	4	1.38
10	Random fire due to short circuit	1	2	1	2	0.69
∑					**290**	

The significance of risks listed in the table is graphically shown by “Lorenz curve” in Fig. 4, which illustrates the risks in red letters, requiring the implementation of preventive measures that would lead to optimization of risk.

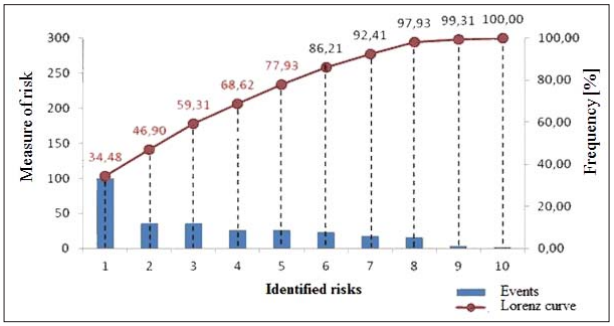

Fig. 4 Pareto analysis in terms of process (source: Author)

It should be noted that the index values for an offender cannot be accurately determined, because it is impossible to accurately measure for example the intention of discontented employee who wants to smuggle explosive in public university building. However, indexes of risk of this nature can be estimated from statistics and experience. It can be said that the structural risks can be indexed accurately (e.g. using breakthrough security), but we cannot do the same with process risks. The use of quantitative methods for process risks is therefore less accurate, but the interval of the result will undoubtedly be more accurate than a mere verbal comment of the evaluator, which would be based only on an estimate without mutual mathematical relationships. From a practical point of view, we can compare an application of quantitative methods to process risk to using a kitchen knife for loosening a cross-headed screw. The knife is not a tool primarily intended for loosening screws, but if we do not have another more suitable tool, we can still achieve our objective with some limitations.

Conclusion

The article dealt with the assessment and identification of security risks in the public universities. In terms of physical protection it can be stated that there is a wide range of potential risks in this area, when some may seem insignificant and difficult to identify in sporadic analysis. In the area of physical protection of public universities, there is a wide range of security risks, some of which may appear to be insignificant, and in sporadic analysis difficult to identify. The subject of this article was to point out the potential application of selected tools and methods of risk analysis, representing the continuous monitoring and risk assessment, which is the basis of risk management of each organization and it means to optimize the security level in the environment of public universities.

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 program security research in the Czech Republic for the years 2010 - 2015 under the grant number VG20102013036.

References

FINKENZELLER, Klaus (2003). *RFID Handbook, second edition*. Germany 2003. 419 p. ISBN: 0-470-84402-7.

LOVEČEK, Tomáš, VEĽAS, Andrej (2010). Technické zabezpečenie ochrany poštových prevádzok. In: *Trilobit*, Zlín, 2010, roč. 10, č. 1, s. 1-5. ISSN 1804-1795 (in Slovak)

RAFFERTY, J. (1994). *Risk Analysis in Project Management*. E&FN Spon, London. 1994.

REITŠPÍS, Josef et al. (2004). *Manažérstvo bezpečnostných rizík*. 1. vyd. Žilina: Žilinská universita, 2004. 296 s. ISBN 80-8070-328-0 (in Slovak)

ŠČUREK, Radomír, KONEČNÝ, Martin (2011). Aplikace analýzy rizik v oblasti fyzické ochrany veřejných vysokých škol. In: *TRANSACTIONS of the VŠB - Technical University of ostrava, Safety Engineering Series*, 2011, pp. 27-32. ISSN 1801-1764. [cit. 2012-06-10]. Available at: http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/cs/sys/resource/pdf/veda-a-vyzkum/sbornik/2011-1-sbornik.pdf (in Czech)