Methodological Approach to Risk Assessment in Building Security

Zdenko Adelsberger[1], Gojko Grubor[2] and Ivan Nađ[3]

[1] Bluefield d.o.o., Zagreb, Croatia
[2] Singidunum University, Belgrade, Serbia
[3] University of Applied Sciences Velika Gorica, Velika Gorica, Croatia

A B S T R A C T

Building object (or asset) security has always been a burning subject in all systems and regimes since ancient times, and will always be. The reason for this lies solely in the fact that these objects have a high material, historical, cultural and other value. Therefore, the owners of such buildings, regardless of whether they are the public, civic or some other social institutions, organizations or individuals, have always paid, more or less, attention to the issue of security of such objects. The amount of attention given to the security of these structures in general depends on the current situation of the external and internal environment of the object, relative to the degree of security threats to it. Certain organizational – technical activities are being performed with the aim to protect such objects. Up to which extent they will be used, depends on the level of risk assessment of those objects that will show the possibility that incidents might occur with harmful consequences. Poor risk assessment results in many unnecessary investments in the security, or lack of it, which does not offer the necessary optimum of security. Hence, risk assessment in building security is considered to be a highly significant and crucial matter. This paper presents a methodological approach to risk assessment in the overall process approach to risk management in order to provide security to the objects. It delivers a critical overview of the methodological steps of risk assessment with the intention to achieve the most realistic assessment.

***Key words**: risk assessment, object protection, risk management, risk assessment methodology, security*

Introduction

Every object (including its asset) has some type of value that can be (and has to be) eventually expressed in quantifiable amount of money. According to the general principles of objects and its owner's relationship, such object value must be preserved. Preservation of the object value relies on its damage issue, which can decrease value and/or functionality of the object itself, as well as of another assets within that object, or directly related to the object. The object's owner obligation, in most cases, is formally regulated by a certain document that is given to the owner. Note that the term »owner« here means a person who is responsible for all issues related to the given objects value maintenance, or risk or object security.

The object value runs within the limits from minimal up to extremely high, or as it is sometimes known as endless value. Therefore, in respect to risk or security aspects, that value must be eventually quantified in some way. Consequently, it can be done by using either the quantitative or the qualitative method. Logically, the higher the object's value the more attention is needed, and it requires usage of more techniques and tools to secure the desired level of object's security or perceived risk.

The relationship between the levels of risk and security are reverse proportional, but both terms are directly related to the necessity of the object's value preservation. Mathematical expression for the relationship between the level of risk and security can be defined as follows:

$$\text{Risk} \times \text{Security} = \text{Constant} \quad (1)$$

On the other side, the relationship between the level of security and uncertainty is complimentary and can be shown by the following equation (in this case, constant refers to wholeness or completeness):

$$\text{Security} - \text{Uncertainty} = \text{Constant} \quad (2)$$

Received for publication November 29, 2013

In various literatures many different definitions of risk and security can be found. However, in this paper, the definitions given in standard ISO Guide 73 will be used[1]. According to that source risk is effect of uncertainty on objectives[1]. In the context of particular application area, this risk definition can be relatively easily adjusted to, but the essence of it should always stay the same. The object security area risk definition, which is compatible with ISO standard, could be as follows: risk is the effect of uncertaintyon the object functionality or value. It could be noted that each object has its objectives, which should be (has to be) achieved. For example, any object can have the following objectives: functionality, visual object form, preservation of other objects or asset inside or related to the considered one, etc.

In order to protect the object, it is necessary to give the risk owner an answer with what kind and which level of security should the object be secured with in order to minimize or accept a risk of incident. It is logical that, in case of unacceptably high risk level for incident occurrence related to the given object of protection, it is necessary to implement, as a rule, a different type of protection than in the case when the risks are low. On the other hand, any type of security tool implementation requires some financial investment. Generally, the more the object's security, the higher the financial investment. Therefore, the consequence of any security implementation is a trade-off between the required low risk level and the acceptable level of financial investment.

Physical risk principles

In order to confirm the risk level, or an object security level, it is necessary to use a methodology that is generally accepted and recognized. It is compulsory because of both the acknowledgments of the methodology results and comparison of the risk to another object's risk. The risk theory states two approaches to risk assessment that are well known – quantitative and qualitative[2,3].

According to its definition, quantitative method of risk assessment is based on measurable and objective data that is used to determine risk value parameters. Because of the objective data, the risk assessment results using quantitative method are entirely objective, too. Evidently, the aim of the quantitative method is to objectively calculate the numerous values for each risk parameter used in risk assessment context. Quantitative method for risk assessment is closely related to the mathematical model in which different components that influence the risk level are connected. These are eventually manifested with exact mathematical equation for risk level calculation. The nature of the quantitative method limits its application, though its accuracy is practically not questionable. The most often application of the quantitative method is in the financial risk area, while it is almost not applicable in object security area.

The qualitative method, opposite of quantitative method, does not try to confirm the exact financial amount of the asset's (object's) values, it's expected losses and necessary security measures. Instead, it utilizes some relative values. They are expressed descriptively, and their sizes are categorized according to rank. Examples of the ranks are typically as follows: neglected, low, medium, high, extreme, important, very important etc. The scale numbers of the ranks for a parameter are not determined by a rule. It is rather a choice of the company which uses the qualitative method. It is a general rule that, if there are more ranks on the descriptive scale for a particular risk parameter, there will be a bigger risk value area, which is actually quite good. However, a grate number of ranks on the scale for a risk parameter causes difficulties for users. They can hardly differentiate why acertain rank is associated to a certain parameter, and not to the previous or the following one[4].

Physical risk model for the qualitative assessment method is shown in Figure 1. Figure 1 illustrates all essential components and their relationship to risk assessment, based on qualitative method, as well as the security measures for risk mitigation, preferably on an acceptable level. Further, the figure also illustrates all the risk complexity and multidimensionality. For any risk analysis and assessment later on, it is necessary to first determine the object of the risk assessment, which can be literally anything or anybody, a material or nonmaterial thing. An object of risk assessment can be buildings, machinery, people, etc. It should be emphasized here that the object by itself is not directly the subject of analysis, it is rather the objective(s) related to the considered object at hand. Obviously, the choice of objects is unlimited. Actually, the only limitation related to objects is the knowledge or awareness ofthe object's value and the importance of its objectives achievement that should be analyzed within risk assessment context.

Consequence analysis that can appear if identified objectives are not achieved will be the next logical step related to the chosen object. If the consequences of an unfulfilled objective are neglectable, then that objective can be exempted from further analysis. This means that irrelevant consequences should not be considered at all[5].

As a next step, for a given object and its chosen consequences, we need to analyze which combination of threats and vulnerabilities can cause that very same consequence. The sources of threats generate one or more threat agentsthat can, more or less, jeopardize fulfillment of one or more objectives of the considered object. How serious is that threat agent for an object goals achievement depends on the object's sensibility to that threat agent. In the context of risk management, the term vulnerability is usually used for object's sensibility to various threats. The vulnerability to one threat can be small, but to another threat can be very high. This means that threats and vulnerabilities by themselves are not important for risks, but their combination certainly is. This is why they say: If a threat exploits the object's vulnerability and causes a consequences, this means thatan incidentor security relevant event with consequence for the given object's goal has occurred.

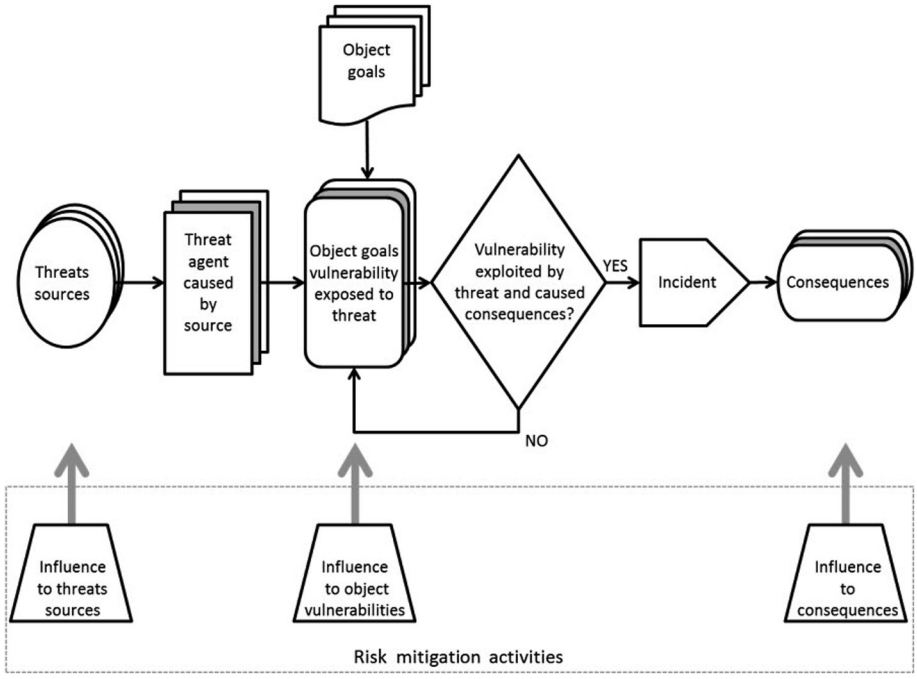

Fig. 1. Physical risk model for qualitative risk assessment method.

In this definition, there is a complete mechanism of risk development and its realization. To be precise, up to the point of the incident appearance, a risk with a certain likelihood for incident occurrence exists. An unpleasant fact that follows risk analysis is that there are a lot of threat sources, and each of them can generate more different threat agents. An object can be more vulnerable on a certain threat, that is to say one threat can exploit various vulnerabilities. Finally, each threat-vulnerability combination can cause more consequences. Therefore, in practice, risk analysis can be very complexand, as a rule, requires great effort, expertise and experience of all the participants involved in that process.

After all the potential risks and threat-vulnerability combinations that can cause relevant consequences are identified, it is possible to plan a defense. The risk mitigation on an acceptable level is primary stated under the term defense. In defense planning, or risk mitigation, it is possible to act against three factors – threats sources, object vulnerabilities and consequences. According to practical experience, the major effect on risk mitigation can be achieved through acting on vulnerabilities. A practical example of risk physical principles is shown in Figure 2.

The threat source (Figure 2) for an object (house) is an attacker (terrorist) who attempts to destroy the object by explosives. If the attacker succeeds in setting up the explosives and activates them, an incident – explosion will occur. At the same time, there will be some damages that causehigher or lower financial losses. Risk level

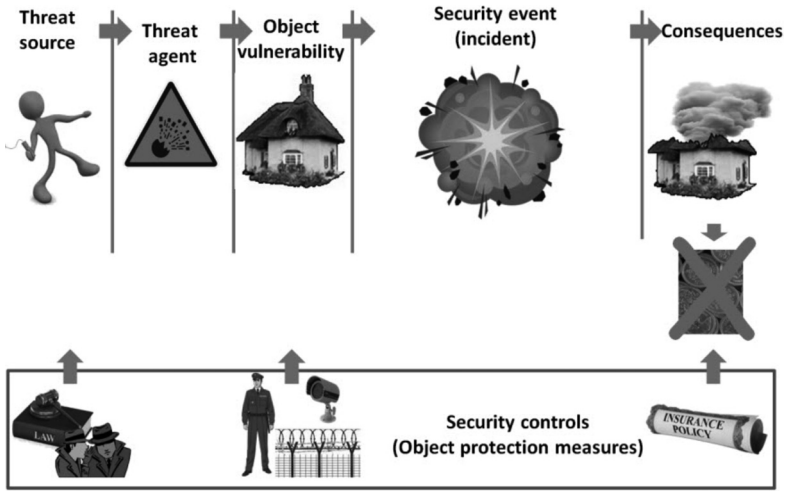

Fig. 2. A practical example of an object risk elements.

magnitude of such security event (incident) is expressed by likelihood. As incident likelihood is higher, the bigger damages of the given object will be. How can risk be reduced, or how can the object's damage probability be decreased? For example, some potential security measures that could be undertaken are shown in Figure 2. Subsequently, source threat impact on the object can be reduced by various legal regulations (sanctions), active intelligence, etc. Object vulnerability for such kind of threats and estimated consequences can be reduced by physical protection such as security staff, fence, video monitoring system, etc. The effects of consequences can also be reduced by taking out an insurance policy. Above stated are only examples given for illustration of risk manifestation reality and its analysis, including all major risk parameters in qualitative risk assessment method[6,7].

The qualitative risk assessment method most often uses two or three parameters. The two variants of this method are shown in Figure 3: one for three parameters application (a) – threat, vulnerability and consequences, and the other one for two parameters (b) – incident likelihood and consequences.

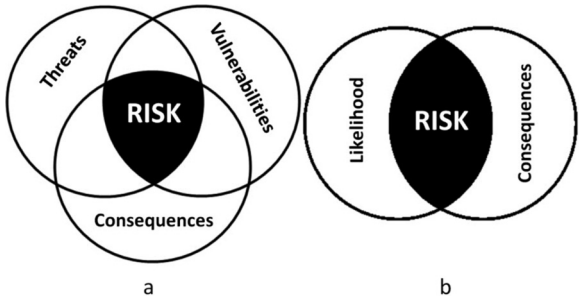

Fig. 3. Most frequent parameters for qualitative risk assessment method.

In any given case, risk exists only if all three or two parameters are important and if they are in interaction among themselves in the object at acertain time. If two parameters are used for risk assessment (Figure 3a) it will be easier to assess risk, but it will also be more difficult to determine why likelihood is so high. In that case, incident likelihood implicitly contents threat and vulnerability. In case of application of three parameters for risk assessment (Figure 3b), it is more difficult to assess risk, since more numbers of parameters must be assessed, but the implementation of security measures is simpler. Actually, it is possible to see directly why the risk is so high – because of either high threat, and/or high vulnerability, and/or high consequences. Hence, in the real environment of risk assessment, one method for risk assessment – with two or three parameters, should be chosen.

Mathematical Model of Qualitative Risk Assessment Method

The question is how is it possible to perform mathematical calculation of risk level, i.e. what is mathematical model of risk likelihood value calculation like. This is very important step in risk assessment process, since all later on activities connected to risk control or object security are based on calculated risk likelihood value. It may be said that badly calculated risk causes incorrect risk control and protection from it. The term badly implies that the calculated risk is unrealistically high or low. If calculated risk is unrealistically high, it will cause unnecessary investments and expenses for the object security measures, and the effects will be the same as if much less was invested in security based on the correct risk assessment. On the other hand, if calculated risk is too low, the main consequences will be insufficient investment (or expenses) in the object goal security, and hence, the responsible people will believe that quality protection based on this assessment has been provided. However, in that case, the risk would most likely be realized, and the resulting consequences could be numerous times more expensive than the money spend on security. Obviously, none of those two scenarios are acceptable. Therefore, it is necessary to pay close attention to the mathematical model and process of risk calculation. The model itself must be sufficiently accurate and to guarantee minimal number of acceptable error.

Traditional model of risk assessment is based on answers to the following three questions:

1. What can happen?
2. What is the likelihood for it to happen?
3. If that happens, what will be the consequences?

If all of the three questions can be answered, it can be concluded that the system risks are properly defined. From this approach, risk can be defined as a probability function of unwanted events and the significance of their consequences[8]:

$$R = \{ < Si, Pi, Ci> \} \quad (3)$$

Where Si is i's risk scenario, Pi – likelihood of that scenario, and Ci is the resulting consequence. In that equation, Si represents a set of all possible scenarios. Since that set is practically infinite, it is not possible to enumerate all of the plausible scenarios. As a result, and because of the fact that there must be set a limit that the scenarios are not inter-connected, the equation (3) will be modified as follows:

$$R = \{ < S\alpha, P\alpha, C\alpha > \}, \alpha \ ?A \quad (4)$$

Where α is a subset of practically infinitely large A set of all possible scenarios. In such manner of definition, it shows that a risk represents the set of risk values for each scenario. This indicates that there is not just one risk for a certain system, but rather theoretically numerous risk factors, one for every scenario. The term scenario implies a comprehensive set of conditions, circumstances and limitations, which lead to risk occurrence. In this paper, due to simplicity of analysis, all equations will rely on only one scenario, but at all time keeping in mind that besides that risk, there are many more of them for the same system (object).

Based on equations (3) and (4), a common and simplest equation can be derived as the function of two parameters – event likelihood and consequences:

$$R = f(p, c) \quad (5)$$

Where R = level of risk; p = likelihood of security events (incident occurrence); c = consequence of the incident; f = mathematical function that gives the level of risk in accordance to parameters values

As a rule, the type of mathematical function is defined not only by the nature of the risk, but also by the risk evaluation criteria. For example, it can be adding or multiplication function, or another complex formula. In case of adding or multiplication function, the risk could be calculated as follows:

$$\text{Adding function: } R = p + c \quad (6)$$

$$\text{Multiplication function: } R = p \times c \quad (7)$$

The equation (5) for risk calculation is related to only one incident likelihood, that originates from one source of threat. Since in practice, there are situations where many sources and many threats have affect on one object, and they can cause many consequences, the equation (5) is getting more complex and becomes a set of value couples, i.e. results in:

$$R = \{ f(p_1,c_1), f(p_2,c_2) \ldots f(p_n,c_n) \} \quad (8)$$

However, it is true only in case where the degrees of individual pairs are independent between themselves, and only the pertaining p and care to be determined. In case of new induced values of individual parameters which can happen due to incident occurrence of certain value pairs, the problem at hand becomes more complex and will not be considered in this paper.

The mathematical equation for risk calculation that uses only two parameters is not good enough in practice, because within each parameter there can be many others that are implicitly given. In that event, the simplest way is to identify the problem and concentrate all the activities for risk mitigation on the parameters with best effect. For example, let's take risk calculation with three parameters – threats, vulnerabilities and consequences. Then the mathematical equations (5) and (8) can be shown as follows:

$$R = f(t, v, c) \quad (9)$$

$$\text{f is adding: } R = t + v + c \quad (10)$$

$$\text{f is multiplication: } R = t \times v \times c \quad (11)$$

$$R = \{ f(t_1,v_1,c_1), f(t_2,v_2,c_2) \ldots f(t_n,v_n,c_n) \} \quad (12)$$

Where R = level of risk for one combination of threat/vulnerability/consequence; t=severity of threat; v = extent of vulnerability; c = significance of consequence

In the mathematical equation (9), the threats and vulnerabilities signify a scenario. Specifically, both the threat and the vulnerability in great extent define the scenario, which means a particular threat exploits certain vulnerability and causes therisk to be calculated in such way. At this point, many other various conditions related to the given risk scenario can emerge.

In the case of the three parameters included in the mathematical model, it is simpler to recognize risk physical nature and identify where to focus the optimal, and sometimes only possible, mechanisms for risk mitigation: to the source of threats, and/or reduction of either vulnerabilities or consequence, and/or some other combination of the later.

For both risk calculation models with two (5) and with three parameters (9), the functional connection between the probability and the combination pair of threat-vulnerability can be expressed by a new function:

$$p = k(t,v) \quad (13)$$

$$\text{k is adding: } p = t + v \quad (14)$$

$$\text{k is multiplication: } p = t \times v \quad (15)$$

Where p = security event likelihood; t = severity of threat; v = extent of vulnerability

According to mathematical equations (13) and (15), in case of one security event, risk can be calculated as follows:

$$R = f(t, v, c) = f(k(t, v), c) = f(p, c) \quad (16)$$

$$\text{f and k are adding: } R = t + v + c = p + c \quad (17)$$

$$\text{f and k are multiplication: } R = t \times v \times c = p \times c \quad (18)$$

However, the number of parameters that can be used within the risk calculation process is not at all limited to only two or three of them. How many parameters will be really used in a specific case depends on both the risk calculation problem and the risk analyst's approach to risk assessment. In this paper, only two and three parameters for risk calculation will be analyzed and calculated, not agreater number of parameters.

Practical methodical approach to risk assessment by qualitative method

The explanation of the qualitative risk assessment and analysis method is illustrated in Figure 4. The mechanism of risk calculation and the effect of security controls implementation for risk mitigation are shown. For risk assessment in this example, the three parameters – threat, vulnerability and consequence are used.

Prior to the implementation of security control, the risk is determined by three parameters R1 (t1,v1,c1), where t1, v1 and c1 are the initial values of threat, vulnerability and consequence, respectively. If one or more

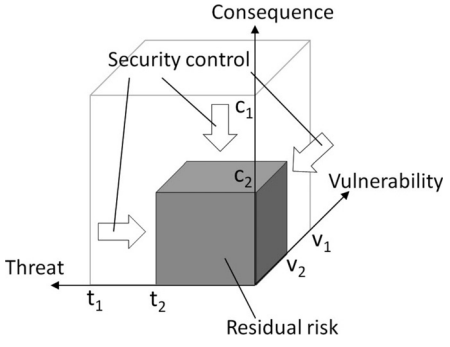

Fig. 4. 3-D diagram of risk in function of threat, vulnerability and consequence.

security controls that affect all risk parameters are applied to that risk, a new risk value determined by three parameters, R2 (t2,v2,c2) will be obtained. That risk, R2, is called residual risk and it represents the risk value after security controls are implemented onto the considered object.

The qualitative risk assessment method presumes that the weight of the parameter used in risk calculation is descriptively given in rated scale. An example of rated scale for any parameter for qualitative risk assessment method is shown in Table 1.

Number of rates in Table 1 is not limited, except by practicality of application which depends on chosen nature of the parameter, and compromise between wanted and possible accuracy. The bigger accuracy is required, the more rates there should be. However, there is a problem here. How can we make a unique description for the rate identificationin such way that rate k, but not k-1, or k+1 is assigned to a parameter. Minimal number of rates in a scale is two, and they can be described by features – »parameter has influence« or »parameter does not have influence«. This binary approach to parameter rating, as a rule, is unacceptable. Therefore, it may be said that the planning scale with minimum three rates is an opportunism.

Even or uneven number of rates on a scale objectively does not have any meaning, due to the fact that the numbers associated to the rates are not used either for some mean value calculation, nor for some other reason which would be in favor of even or uneven number of rates on a scale. After all, uneven number of rates in a scale usually prevails in practice.

Finally there is only one rule for defining number of rates in a scale – practicality and functionality, depending on parameter type and the possibility to define correctly theidentification of each particular rate in a scale. In practice, scales with 3 or 5 rates are used most often. However, usually there are more of them, especially in cases when some other numerical range that can be explicitly confirmed, can be used for rates description. Those are typical scale values of objects (and their assets), or similar to it. Practical applications of the risk assessment process, according to qualitative method, are shown in the following tables.

When defining the consequence parameter scale, it is very important to determine the financial losses caused by realized risk in a specific case. This means that the loss of 10,000€ can be a neglected consequence in some situations, but a very high one in some other circumstances. In case of a two parameter (likelihood and consequences) risk assessment method, the likelihood table can be presented as it is in Table 5. The consequence scale can be the same in both cases.

After risk assessment is performed and results are obtained for all risks related to an object, it is necessary to

TABLE 1
CRITERIA FOR DEFINING SCALE RATING OF PARAMETERS FOR QUALITATIVE METHOD

Rate No.	Textual rate	Description for category identification
1	Insignificant	Unique textual description by which rate 1 is assigned to the parameter
2	Low	Unique textual description by which rate 2 is assigned to the parameter
3	Medium	Unique textual description by which rate 3 is assigned to the parameter
…	…	…
n	Extreme	Unique textual description by which rate *n* is assigned to the parameter

TABLE 2
EXAMPLE OF THREAT PARAMETER SCALE FOR QUALITATIVE METHOD

Rate No.	Rate	Rate description	Description
1	L	Low	Very low likelihood occurrence of threat for object
2	M	Medium	Medium likelihood occurrence of threat for object
3	H	High	Very often or constant likelihood occurrence of threat for object

TABLE 3
EXAMPLE OF VULNERABILITY PARAMETER SCALE FOR QUALITATIVE METHOD

Rate No.	Rate	Rate description	Description
1	L	Low	There is no sensitivity to the threats, or very effective security controls have been implemented
2	M	Medium	Medium sensitivity to the threats, there is no protection, or security controls are poorly implemented
3	H	High	Very high sensitivity to the threats, there is no protection, or security controls are inefficient

TABLE 4
EXAMPLE OF CONSEQUENCE PARAMETER SCALE FOR QUALITATIVE METHOD

Rate No.	Rate	Rate description	Description
1	L	Negligible	Loss < 1.000 €
2	M	Low	Loss within limits 1.000–5.000 €
3	H	Significant	Loss within limits 5.000–12.000 €
4	E	Extreme	Loss higher than 12.000 €

TABLE 5
EXAMPLE OF VULNERABILITY PARAMETER SCALE FOR QUALITATIVE METHOD

Rate No.	Rate	Rate description	Description
1	L	Rare	Only in extraordinary circumstances
2	M	Possible	Could happen at any given moment
3	H	Likely	It will most likely happen in large number of cases
4	E	Almost certain	It is expected in most cases

TABLE 6
EXAMPLE OF QUALITATIVE MATRIX OF RISK ANALYSIS RESULTS

Risk = Likelihood × Consequences		Consequences			
		L	M	H	E
Likelihood	L	LL	LM	LH	LE
	M	ML	MM	MH	ME
	H	HL	HM	HH	HE
	E	EL	EM	EH	EE

Risk scale: Low Risk (LL,LM,LE,ML,HL,EL), Medium Risk (MM,MH,ME,HM,EM), High Risk (HH,HE,EH,EE)

rate the risks according to a criteria established by risk assessment team. The risk rate criteria is defined in the so called risk acceptable matrix (ISO 31000:2009). It is a two dimensional matrix determined by likelihood and consequence parameters.

One potential definition of risk acceptable matrix is presented in Table 6. The components of risk assessment matrix represent risk values, classified according to the rating scale. What the risk scale will be like mainly it depends on the security policy which is defined and enforced by the top management.

Depending on the defined risk scale, i.e. risk acceptable matrix, it is necessary to determine the security controls and in which cases risk should be reduced to unacceptable level. In Table 6, the risks in green fields are acceptable and they do not need any security controls. The risks in red fields are unacceptable, and they need to be treated urgently and reduced to an acceptable level. The risks in yellow fields should be mitigated to an acceptable level, provided there are enough resources, and they must be monitored all the time.

Undertaking measures to reduce risk is usually called risk treatment. Generally, there are four options for risk treatment:

a. Risk acceptance – no matter how high the risk is, it is accepted as it is, because it is within acceptable limits or within unacceptable limits, but there are no objective resources for its mitigation. In case that an unacceptable risk level is accepted, top management should issue a statement that they are awareofthe risk level and its consequences, and that the risk will not be reduced due to certain reasons.

b. Risk transfer – in this situation, a part of risk is transferred to some other external organization, for example to an insurance company. In this way the risks are objectively reduced, and first of all the consequences.

c. Risk avoidance – in this situation, occurrences of risk are disabled by different activities. As a rule, it is resolved by directives, orders, etc. For example, by a ban of bringing in open flames in a building.

d. Risk mitigation – in this situation, some procedural and technical controls are used to reduce risk, by influencing some of the parameters – threats, vulnerabilities, consequences and likelihood. Such risk reductions are performed by implementation of security controls. The term security controls implied needs for persistent control of risk (and security) level, and they are often called security measures.

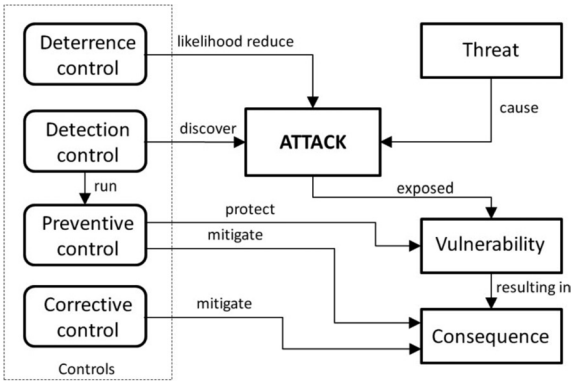

Fig. 5. Relationship of risk parameters, their occurrences and levels.

Relationships between risk parameters and security controls are shown in Figure 5, where a complete physical pattern of risk occurrence and control on an object can be viewed from.

Interpretation of the processes in Figure 5 can be simply done by following the string of arrows from a block. For example, a threat causes an attack to which a vulnerability is exposed and it results in a consequence.

Diagram in Figure 5 shows the complexity and the problems of risk analysis, risk level calculation and risk mitigation on an acceptable level as well. Unfortunately, risk mitigation is not always possible due to different reasons. Those are most often unacceptable expenses or investments in securityifpredicted losses are less then the security expenses.

All of the qualitative components of security risk assessment method are shown in Figure 6. This diagram can be applied to all types and classes of qualitative risk assessment method. The only difference is in the number and type of estimated objectives.

Project and process approach to security risk assessment

The main question in security risk assessment of an object is the choice of approach methodology. There are two possible options – project or process approach. According to international standards, the project and the process definitions are practically the same. Project (or process) is documented set of activities that transforms input into output values, with the help of resources and rules. In the field of risk assessment, both project and process approaches are presented in Figure 7.

The project and process approaches are shown in Figure 7a and Figure 7b, respectively. The difference between those two approaches are visible from diagrams in Figure 7. The project once it starts, ends after some time, meaning it is time limited. On the other side, the process has its beginning, but it does not have its end, because it is cyclically renewed in order to satisfy its input requirement. That is why it is called the period of the process cycle. There are no other significant differences. Sometimes it is said that a project is one time process. If somebody is to decide whether to apply process or project approach, it will depend on input requirements (see Figure 6). In project approach, the input requirements is the need for something to be done, and when it is done – the

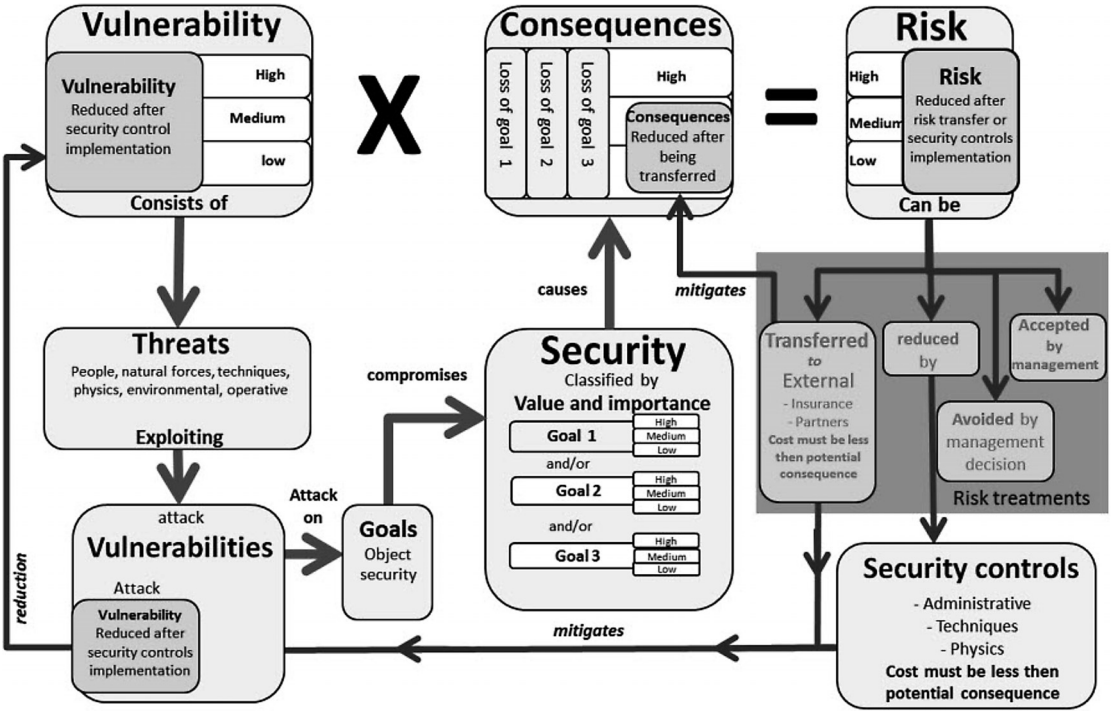

Fig. 6. Integrated presentation of risk assessment by qualitative method.

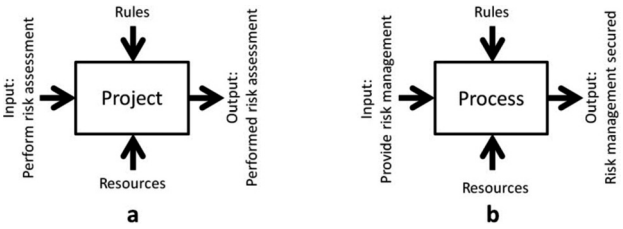

Fig. 7. Project and process approach to risk assessment.

project is finished. So, in Figure 7a the input requirement is to assess the risk. When risk assessment is finished, the project is finished, too. However, in process approach, the input requirement implies that constant process activities should be performed in order to accomplish input requirement. Thus, input requirement in process approach is to provide (persistently) risk management, or to control and retain the risk atan acceptable level all the time. The process is finished at apoint where there is no more need to fulfill input requirements.

Based on the above stated, it could be said that the project approach should be applied when a one time set of activities are needed to be achieved. Hence, risk assessment from flood, or risk assessment from football field devastation during asoccer game, are examples of security risk assessment. On the other hand, the process approach to security risk assessment should be applied when there is a need to secure some requirements persistently. For example, to provide protection from breaking into an object.

Due to its duration and repetition, process management can be continuously improved. That is why, during a process cycle, insufficiencies could be detected, as well as possibilities for improvement or optimization, and therefore various changes will be included in the next cycle. Thus, the new process cycle will run better, so possibility for continuous process improvement are based on that very principle. On the other side, one time projects can not have further improvements. If some insufficiencies are noticed during the project's flow, only some bad activity results can be eventually improved.

Since a project can be considered as a one time process, they are both almost the same. The fact that projects can not be improved is the only difference. Therefore, in this paper processes will be considered instead of projects.

There are many techniques and methods for process improvement. The most well-known among them is PDCA (Plan – Do – Check – Act) process model or The Deming circle. The PDCA model can be applied both for the implementation and the improvement of existing processes. The PDCA circle consists of the following four phases:

- Plan phase: In this phase, for completely designed processes, all resources and rules are identified and all activities in the process flow that have to be accomplished are approved.It is necessary to plan who and how will measure specific identifications in the process. The expected results should be planned as well.
- Do phase: In this phase all of the planned activities in the Plan phase must be practically implemented.
- Check phase: During this phase, it is verified whether the results obtained by planned measures are within the expected (planned) limits.
- Act phase: During this phase, all the reasons that lead to deviations from expected (planned) results are analyzed. Based on the result of the analysis, certain activities are planned to avoid repetition of such deviations. If there are deviations of results, some improvements (efficiency and/or effectiveness) will be planned.

At the end of the Act phase, a new Plan phase begins once again, with the aim to implement improvements of the results of the previous Act phase. In such manner, process performances are continuously and cyclically renewed.

The project approach has the same four phases too. However, there are no options for project improvement due to the fact that the project ends, after the Act phase is completed, and so there are no more new cycles[9].

If those components of process management theory are applied in the field of risk management, no matter for which purpose the risk assessment or the risk management are performed, they are achieved almost in the same way. That is the reason why there are a lot of efforts to define process managementand process assessment. The most well-known and generally accepted, among more or less many other successful approaches to define the risk management process, is the international standard ISO 31000:2009. It is not compulsory to apply that standard. It is rather a recommendation or best practice example, which assists users on how to implement the risk management process and continuously improve it. In practice, it means that it is not possible to certify activities according to that standard. However, today, it is impossible that any risk management is to be performed without ISO 31000:2009 standard's principles (see Figure 8). Besides risk management process, both risk management principles and risk management framework, according to ISO 31000:2009 standard, are also presented in Figure 8.

The PDCA process model is also used to manage risk management process, as shown in Figure 8. According to ISO 31000:2009 standard[10,11], in each particular phase of PDCA model, there are following process management activities:

- Plan phase: Risk identification, context determination, risk assessment, risk treatment plan, residual risk acceptance
- Do phase: Implementation of security controls according to risk treatment plan
- Check phase: Continuous risk monitoring and reviewing
- Act phase: Risk management process maintenance and improvement

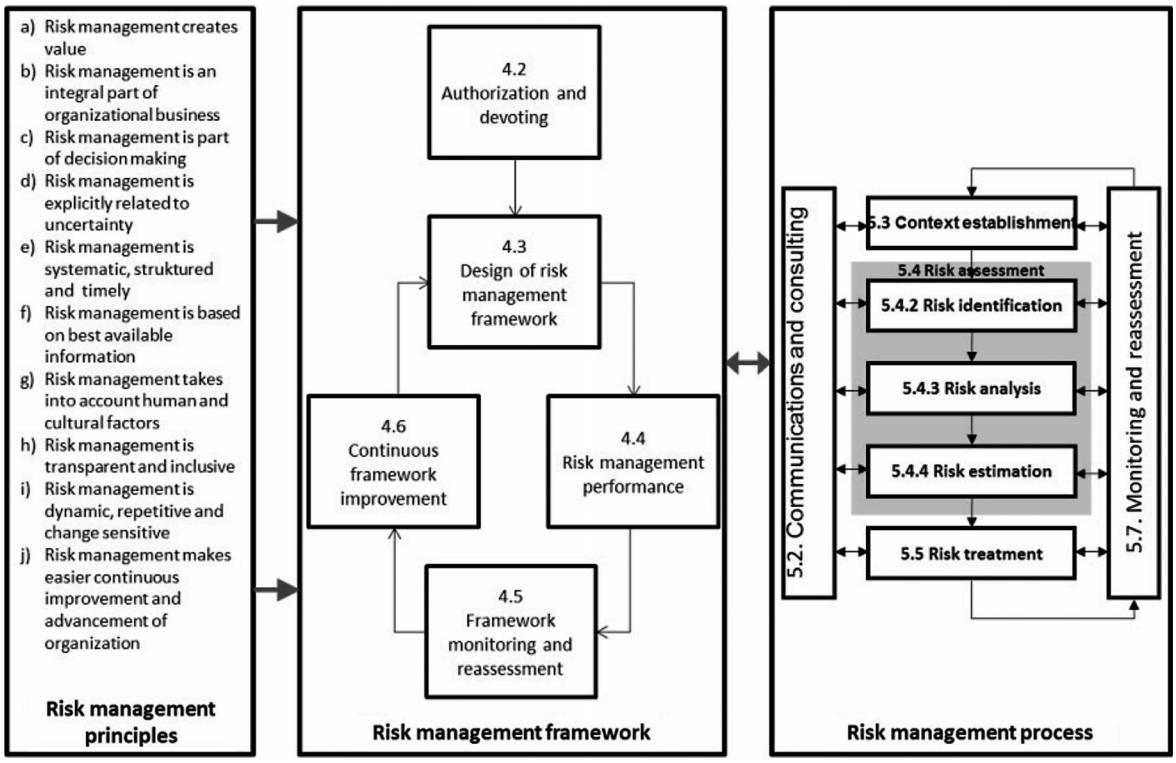

Fig. 8. Relationship between risk management principles, framework and process.

The basic activities of particular steps within the risk management process (see Figure 7) are as follows:

- Communication and consulting: It is correlated to internal and external stakeholders during all the step of the risk management process, and to the process as whole.
- Context identification: In this step, external, internal and risk management contexts (in which the rest of the process will be performed) are identified. The risk assessment criteria and risk analysis structure should be defined in this step, too.
- Risk identification: It is relayed on the identification of where, when, why and how a security event can be prevented, and/or mitigated, and/or shared, and/or accepted, in order to increasethe achievement of the objectives.
- Risk analysis: It includes identification and assessment of current security controls, and the determination of consequences, likelihood, and risk level. Potential consequences range and how they can occur, must be considered, too.
- Risk estimation: In this step, a comparison between assessed risk level and previously evaluated risk level criteria is done in order to balance benefits and disadvantages. It enables decision making on risk assessment range and risk treatment nature and priorities.
- Risk treatment: This step includes making and application of the effective and rentable strategies, specific expenses and action plans, in order to increase potential benefits and decrease potential expenses.
- Risk monitoring and reassessment: In this step, it is necessary to follow up the effectiveness of the overall risk management process steps. This is important for continuous improvement of the risk management process. To assure that any changes of circumstances can not change priorities, it is necessary to closely follow risk and security controls effectiveness.

According to the standard ISO 31000:2009 steps, block diagram of the processes in Plan phase (including related documentation) is shown in Figure 9.

It does not matter if it is risk management process or project, all the activities in the Plan phase and related documentation should be implemented (see Figure 8).

Methodological approach to risk assessment, based on ISO 31000:2009 standard, starts by risk range recognition, i.e. by range of risk assessment validity. It is related to accurate definition of physical and functional limits of the object for which the risk assessment is done. A formal document that includes such description is an output of this step. A formal definition of risk assessment objectives is the next step in that risk assessment process. The objectives are formally included in a document that is usually called risk assessment or risk management security policy. It is necessary to take into account that those defined objectives are measurable. Based on these measures, it can be confirmed whether risk assessment or risk management is effective. The next important step is

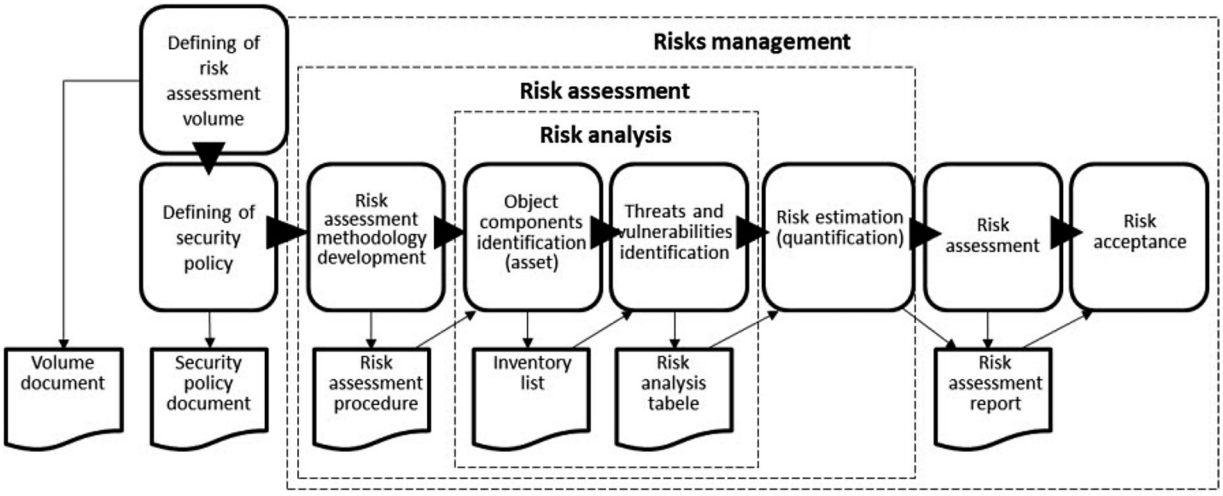

Fig. 9. Block diagram of Plan phase processes for risk management according to ISO 31000:2009

to define the methodology for risk assessment. The same risk assessment methodology often can not be completely applicable to every object. Therefore, the outcome of this step is a formal document »Risk assessment procedure«. Definition of the consequences, threats, vulnerabilities and likelihood scales is an integral part of that document. The next step is object (or its asset components) identification, which should be properly protected in order to achieve the objectives that are defined in the security policy. A list of asset inventory which isto be assessed is this step's outcome. In the risk analysis framework, the next step is determination of all the risk factors that could create losses. The risk estimation, based on the chosen methodology from the Risk assessment procedure, is the final step in the risk assessment process. During this step, calculation of the risk factors using all previous components is formally done. The document Risk assessment report is this step's outcome. Besides the risk estimation results, it also includes the estimated risk rating scale, in accordance to the risk level. If risk management is required, then it will be necessary to perform a risk treatment step. What should be done with each assessed risk is defined in this step. As it is mentioned before, acceptance, transfer, avoidance and mitigation are all possible options for risk management. For each of these options, it is necessary to mention who, when and how it will be performed, and what are the expenses and risk levels after risk management options are implemented, as well. The risk retained after risk management options implementation are called the residual risks. The results of that risk treatment step are also included in the Risk treatment report.

This final risk assessment report is sent for approval to the sponsor that has ordered the risk assessment to be done. Namely, the sponsor should accept all the risk assessment results, planned expenses, and effects of the security controls. If the sponsor is unsatisfied and refuses to accept the proposed security measures given in the report, this step goes back to the beginning and is repeated with adequate changes until the risk assessment report is accepted by sponsor. Most often, the sponsor is making atrade-off among expenses, timeframe and effectiveness of the implemented security controls and desired objectives. When the sponsor accepts The risk treatment report and signs it, then the planned security controls can be implemented. Hence, the sponsor is obliged to provide all of the needed material and financial resources for security control implementation.

From the above stated, it can be concluded that this methodological approach is completely logical and absolutely independent from the field of application, as well as from object (its asset) security. The main advantages of this risk assessment methodology is that it is based on ISO standards, as well as theclarity and lack of doubt for the risk assessment process. The number of assets to which this methodological approach can be applied is practically unlimited. Some of the examples of object security are the following: building protection (from fire, flood, burglary etc.), energy power protection, information security, drinking water protection, concerts and sports events protection, leaking of information from companies etc.

Risk assessment techniques and tools

Within the risk management process, risk assessment process is probably the most critical[12]. It means that any mistake made in these steps can cause wrong risk assessment results.That is why it is very important to approach properly risk assessment components by using adequate techniques and tools. Consequently, within standard ISO 31010:2009 many advices and instructions are provided. Directions for the choice of risk assessment methodology and techniques is one of them, too. A review of methods and techniques applicable for risk assessment are presented in Table 7.

Obviously, all methods and techniques shown in Table 7 are not used at every situation. Those that are optimally related to the given class of risk where a certain

TABLE 7
TOOLS FOR RISK RECOGNITION

Tools and techniques	Risk recognition process				
	Risk identification	Risk analysis			Risk assessment
		Consequence	Likelihood	Risk level	
Brainstorming	SA	NA	NA	NA	NA
Structured or semi structured interviews	SA	NA	NA	NA	NA
Delphi	SA	NA	NA	NA	NA
Check lists	SA	NA	NA	NA	NA
Hazard analysis	SA	NA	NA	NA	NA
A hazard and operability study (HAZOP)	SA	SA	A	A	A
Hazard analysis and critical control points (HACCP)	SA	SA	NA	NA	SA
Risk environment recognition	SA	SA	SA	SA	SA
Structure »What if?« (SWIFT)	SA	SA	SA	SA	SA
Scenario analysis	SA	SA	A	A	A
Business impact analysis	A	SA	A	A	A
Root cause analysis	NA	SA	SA	SA	SA
Failure mode and effects analysis (FMEA)	SA	SA	SA	SA	SA
Failure tree analysis	A	NA	SA	A	A
Event tree analysis	A	SA	A	A	NA
Cause and consequence analysis	A	SA	SA	A	P
Cause and result analysis	SA	SA	NA	NA	NA
Level of protection analysis (LOPA)	A	SA	A	A	NA
Decision tree	NA	SA	SA	A	A
Human reliability analysis (HRA)	SA	SA	SA	SA	A
Analysis »Bow tie« – graphical method of risk detection	NA	A	SA	SA	A
Maintenance based on reliability	SA	SA	SA	SA	SA
»Sneak« electro-mechanical assemble analysis	A	NA	NA	NA	NA
Markov analysis	A	SA	NA	NA	NA
Monte Carlo simulation	NA	NA	NA	NA	SA
Bayes network and statistic	NA	SA	NA	NA	SA
Graphic design of catastrophe-mortality relationship (FN curves)	A	SA	SA	A	SA
Risk indexes	A	SA	SA	A	SA
Consequences/likelihood matrix	SA	SA	SA	SA	A
Cost/benefit analysis	A	SA	A	A	A
Multi criteria decision analysis (MCDA)	A	SA	A	SA	A

(SA = Strongly applicable, NA = Not applicable, A = Applicable)

method is to be applied are usually chosen. Those techniques and tools with label AP are first choice criteria for certain class of problems – risk identification, consequences, likelihood, risk level or risk assessment[13]. If due to any reason, techniques and tools with label AP can not be applied, then those with label P should be chosen.

Conclusion

Risk assessment is inevitable and very often critical for any planning, especially in activities such as establishment and maintenance of object security systems. Basic rules of any organization's development includes the rule of proactive management where risk assessment is the source of all the following activities. Depending on the area of application, it is possible to use quantitative or qualitative risk assessment method. With type of problems such as object security, only qualitative method is acceptable, despite the fact that it contains the risk assessment evaluator's subjectivity and is based on insufficiently proved components.

Since objectively, there is no way to prove that the assessment is either accurate or wrong, the team of evaluators must be trustworthy in ordertothe risk assessment results to be accepted. Therefore, an expert that is trained for team work should perform risk assessment, since

every integrated risks is multidisciplinary. In team training, each team member or at least team leader must be highly educated and skilled for application of different risk assessment techniques and tools, and all the team members should think in similar way in order to avoid extremely pessimistic or optimistic attitude.

How important risk is, and in which way the risk assessment results will be used primarily depends on the awareness of the sponsor of the risk assessment and the underlining reasons for the assessment. The main problem is that many operative and, as a rule, all strategic decisions related to the object security are based on the risk assessment results. Hence, wrong risk assessment results could cause faulty decisions with consequences that could even destroy the object (or its asset).

REFERENCES

1. Guide 73:2009, Riskmanagement – Vocabulary, ISO, (2009). — 2. STACKPOLE B, OKSENDAHL E, Security Strategy – From Requirements to Reality (Taylor&Francis US, 2010). — 3. MAIWALD E, SIEGLEIN W, Security Planning And Disaster Recovery, (McGraw-Hill Osborne Media, 2002). — 4. Asset protection and security management handbook (POA Publishing, LLC, 2002). — 5. AVEN T, Risk Analysis: Assessing Uncertainties Beyond Expected Values And Probabilities (Wiley, 2008). — 6. SUTCLIFFE A, Scenario-Based Requirement Analysis, (European Commission ESPRIT 21903 »CREWS«). — 7. VOSE D, Risk Analysis – A quantitative guide, (John Wiley & Sons Ltd, 2008). — 8. JOHANSSON J, Risk and Vulnerability Analysis of Large-Scale Technical Infrastructures (Lund University, Sweden, 2007). — 9. LUND MS et al., Model-Driven Risk Analysis – the CORAS approach (Springer, 2010). — 10. ISO 31000:2009, Risk management — Principles and guidelines, (ISO, 2009). — 11. CHAPMAN RJ, Simple Tools and Techniques for Enterprise Risk Management (John Wiley&Sons Ltd, 2006). — 12. PFLUG GCH, ROMISCH W, Modeling, Measuring and Managing Risk, (World Scientific Publishing Company, 2007). — 13. YOUNG C, Metrics and Methods for Security Risk Management, (Elsevier Science & Technology, 2010).

Z. Adelsberger

Bluefield d.o.o., Trnsko 7B, 10020 Zagreb, Croatia
e-mail: zadelsbe@zg.t-com.hr

METODOLOŠKI PRISTUP PROCJENI RIZIKA KOD ZAŠTITE OBJEKATA

SAŽETAK

Zaštita objekata je oduvijek bila prvorazredna tema u svim sustavima i režimima od davnih vremena, a tako će uvijek i biti. Razlog za to leži isključivo u činjenici da takvi objekti imaju visoku materijalnu, povijesnu, kulturološku ili neku drugu vrijednost. Zbog toga su vlasnici takvih objekata, bez obzira da li su u pitanju države, neke druge društvena institucije, organizacije ili pojedinci, uvijek poklanjali manju ili veću pažnju zaštiti takvih objekata. Veličina pažnje zaštiti objekata općenito zavisi o trenutnoj situaciji vanjskog i unutarnjeg okruženja objekta, odnosno stupnju prijetnji sigurnosti objekata. U cilju zaštite objekata poduzimaju se određene organizacijsko – tehničke aktivnosti. U kojem obimu će se primjenjivati razni oblici zaštite objekata zavisi od procjene rizika da dođe do incidenta sa štetnim posljedicama. Loša procjena rizika ima za posljedicu da se nepotrebno mnogo investira u zaštitu, ili nedovoljno, a da se ne postiže optimalna zaštita. Zbog toga se i smatra da je u zaštiti objekata posebno značajna i presudna procjena rizika. U radu se prikazuje metodološki pristup procjeni rizika s procesnim pristupom cjelokupnom upravljanju rizicima u cilju zaštite objekata, te daje kritički osvrt na metodološke korake procjene rizika i to u cilju postizanje što realnije procjene.