Coll. Antropol. **38** (2014) Suppl. 1: 155–164
Review

Protection of Facilities and Risk Assessment Application

Ivan Nađ, Branko Mihaljević and Martina Mihalinčić

University of Applied Sciences Velika Gorica, Velika Gorica, Croatia

A B S T R A C T

The state of security on a specific area imposes the necessity for constant analysis of the existing system of protection of key state facilities, especially facilities of special significance for the defence. The facilities of special significance for the defence are an important part of the daily life, and enable smooth functioning of the economy and all other state activities. The protection of facilities of special significance for the defence is considered to be a system of obligatory measures which prevent the destruction or damage of the facilities as well as the disclosure of secret data regarding the facilities and activities performed within those facilities. Appropriate prevention protection measures need to be undertaken in case of each form of threat. The basic forms of possible threats to facilities which can cause major or minor damage, and which are within direct scope of physical and technical protection are various forms of terrorist activities, sabotage, diversions, explosions, major fires, natural disasters, burglaries and thefts, robberies, etc. The purpose of this paper is to display the responsibility of the crisis management for the facilities of special significance for the defence during threat assessment, and the development of the protection plans while applying risk assessment.

Key words*: protection of facilities, risk assessment, threat assessment, protection plan*

Introduction

The development of the society in general is accompanied by the monitoring and development of all kinds of crimes and a systemic growth in criminal activities may be expected in the future, especially in the field of property crime. Therefore, every state with their legal system, bodies of protection, standpoints and reactions to crime, have to provide protection of persons and property of citizens. Having in mind this condition, it has become normal in many countries today that enterprises and business and other organizations take care on their own about their property, and when this is not possible, they rely on the government institutions.

There is no country in which the police, regardless of their efficiency, may have the objective possibility of making their officers present at all those places where an incident may occur. This means that the protection of private property is the basic reason for the existence of private security. Private security is the most professional form of the organization of the society and individuals in the preventive and protection sense, whose scope of security is in many cases greater than the one offered by the state through its institutions.

Within its operation scope private security includes physical and technical protection of persons, objects and property. Within its segment physical protection means: protection of people and property performed by professional and adequately authorized persons – guards and security guards, securing peaceful demonstrations and public gatherings, securing residential and public areas, immediate physical protection, protection of natural assets and the environment, security and escort of cash, securities and valuables. In its segment the technical protection means the protection of persons and property with the use of various forms of technical equipment and devices. The system of technical protection, individually or in combination, as a rule, includes video surveillance system, burglar or counter-attack security system, access control system, fire alarm system or gas alarm system, working hours registration system and other technical equipment and devices.

Unfortunately, regardless of the increase in violence and other forms of crime, the practice has shown that today private security is primarily engaged by institutions and companies under legal obligation to do so, using often only the legal minimum.

Received for publication November 29, 2013

During the recent period the Republic of Croatia has recorded events of attacks on the property with the most severe consequences. Such events undoubtedly indicate the necessity of a different approach to the security culture in the behaviour of companies, financial institutions, and certain prominent individuals. Consequently, individuals and companies have to affect their security by a number of preventive measures and activities, which will reduce the possibility of realization of any forms of threats to a minimum. Implementing the protection of people, facilities and assets in companies is of extreme importance. The assets in residential areas and commercial premises often represent a significant value that needs to be adequately secured and protected. The protection of people, facilities and assets includes technical and professional planning of the security policy in enterprises, its implementation, vulnerability assessment, and creation of special teams that will respond in the protection adequately to the crisis. As a rule, this segment comprises the type of security, its scope, method of implementation and the holders.

The attacker on the interests of a company, including the facilities in its ownership, attacks the critical points, i.e. those points that feature the weakest security and pose the least risk to the attacker. An additional problem is caused by the fact that security implementation at companies represents an expense, in some cases a very large one, and it may seem unjustified to the management. However, it is certainly better to spend certain means to protect the facilities or assets, than to spend much larger funds to compensate for the damage and for subsequent implementation of protection.

This means that at companies and institutions private security and implementation of risk assessment in making the risk assessment play an important role, especially in raising the level of security and preventing possible threats to people and assets in compliance with the legal authority.

Term and Definition of Security

Today, the term of security includes a number of various aspects of human existence and activities in the society and nature. In modern times the term security started to be used in almost all the areas of human activities and the environment. Although being one of the most frequently used terms some authors believe that this is also one of the least explained terms[1].

Grizold determined conceptually that security is a situation which ensures balanced physical, spiritual and material survival of the individual and the social community in relation to other individuals, community and nature[2].

The term security originates from the Latin word *securitas* which literally means security (i.e. *securas*, Lat. secure, carefree, confident, fearless, strong, protected). In English and French the terms of the same meaning, security/securite, respectively, are also the terms safety and surete, which unlike the former ones which are related to aspects of security in relation to government, nation, political and social relations, are related to other aspects of absence of danger as the most general definition of the concept of security.

Although there are a number of definitions on security, there is no best or most precise one, and the authors believe that security is a condition and level of resistance and protection from threats and danger. It is therefore a condition which provides normal flow of all natural and social, vital and developed (usual, achieved) functions and maintenance of created, acquired values and qualities.

Security thus implies conditions of full balance between humans (society) and the nature and their interaction which does not lead to derogation of the nature and quality of life of the human community. Security is the fundamental and underlying category both to the individual and the community, as the possibility of their survival and existence, also including the activities, i.e. processes and activities which operationalize the survival towards other individuals, social, ethnic and interest groups of a society, towards other societies and towards natural environment.

Security can be classified with respect to entities that contribute to that security i.e. that in compliance with the legislation on obligations implement measures and activities that provide a certain level of such security, and that is: public and private security. Such a general definition of security says that security is actually the absence of harmful threats and as such it has a negative aspect of the definition since security as such is usually defined as a condition without danger or threat, as a feeling of safety, and as activity, i.e. system of realizing safety. The issue of the subject or object referred to by security, is the fundamental issue for considering these issues, i.e. seeking the answer to the question who or what does safety refer to, and it may include e.g. a human as an individual, certain social groups, society i.e. social community, government, international community, nature in general, world as a whole, security of ownership, etc.

Besides, it is necessary to determine also what kind of security is meant, i.e. whether it is the security of the subject or object in general which means survival or development or, a question of security from specific types of threats. Here one should keep in mind the levels of possible vulnerability in relation to various threats[3].

An important issue is also the question against whom and/or what one should advocate for the security of a certain subject. It is precisely the answer to this question which represents the introduction into the issue of threat which is an unavoidable factor in considering the phenomenon of security (security exists because threat exists). In this connection there are also questions necessary for analysing what the sources of threats, types of threats, directness or indirectness of threats, time or spatial vicinity of threats, probability of threat realization and level of its severity are.

One of the definitions of security is advocated by Milan Vršec (acc. to: Jurak)[4], who believes that security is »one of the central factors of the social life and work« and that security is also understood as one of the existential human problems that comes to the fore only when a person is faced by a critical situation (crisis).

Changes in the Modern World that Affect Security

Human civilization in the new millennium is characterized on the one hand by great advances in technology which is focused on the wellbeing of the humankind, and on the other hand, by a series of occurrences and phenomena which give it no credit since they are of a destructive or self-destructive character. The rich phenomenology of social and pathological phenomena and offenses with characteristics of violence indicates how human creativity can manifest itself in an extremely negative way. The group of such phenomena certainly includes theft, aggravated larceny, robbery, aggravated burglary, and murder as an act with extremely irreversible consequences.

According to Singer[5], crime as a social phenomenon and individual offenses as individual events cause growing distress of the states, their representative and presidential bodies, as well as concerns, feelings of threat and discomfort of every single citizen.

Crime is increasingly seen as a problem of national and international dimensions that disrupt the economic, social and cultural development of people and threaten the human rights and the fundamental freedoms[6].

Offences of violence in a civilized society represent a group of offences whose negative impact gives incentive to their study in order to use the modalities of execution of crime, scope and distribution, and characteristics of such acts, to approach the causes of such phenomenon and successful struggle of the society against such offences[7]. In practice as well as in literature that describe the offences of violence, it is obvious that persons who want to obtain illegal material gain through robbery or theft, differ greatly from the perpetrators of other crimes against property described in the Criminal Code.

Thus, one of the main forms of possible threats to facilities which is in immediate domain of private security are various forms of crimes in the economy, terrorist activities, burglaries, theft, theft of equipment and data, computer crime as a specific form of source of danger and robberies.

Terrorism is becoming one of the biggest problems of modern society which is imposed by various political groups, organizations and government as a means and method of achieving their goals, occurring as the direct consequence of the interests of individuals, forces and structures to change relationships in a certain community using force or violence against people or property.

Modern terrorism features some characteristics that distinguish it from other sources of threat, and that refer to: confidentiality of work, readiness to perform radical actions, good preparation for the action performance, frequent suffering of accidental civil casualties, high material damage, and all this with the aim of maximally intriguing the general public (international and domestic) and achieving high coverage of the media and substantial financial investments.

Crimes Involving Violence

According to analyses of property crimes committed on the Croatian territory, it was found that the most vulnerable facilities include: gas stations, shops, betting shops, jewellery stores, kiosks and other indoor facilities of commercial type, and such facilities are prevalent in the total mass of the committed crimes of theft and robbery in relation to other facilities of financial institutions. The perpetrators of such crimes are amateurs and professionals, or rather, along with proper criminals, all categories of criminals from the domain of property crime are recorded. Thefts and robberies are performed individually or in groups. The means of execution vary. The perpetrators of these offenses use physical force, knives, brass knuckles, bats, various spray guns, stun guns, gas guns, and even real firearms, especially handguns. There are also syringes filled with red liquid threatening the victim that it is blood infected with HIV. As a rule, facilities with a smaller number of employees, without technical and physical protection with relatively high turnover are selected. The time of attack varies, but these are generally evening hours before closing of the facility. They attack suddenly, grab the prey and run.

The concept of protection of facilities where money is kept or collected or other values against criminal activities of individuals and groups is certainly one of the most demanding jobs of all the subjects both of public and private security. This refers first of all to armed robbery attacks in closed premises such as banks, post offices, exchange offices, betting and other similar facilities. In these critical moments the employees, clients, customers, security guards and all other persons who happen to be at the place of occurrence are threatened. In such crimes material damage is not only direct monetary loss or damage to equipment which is clearly identifiable and measurable but rather also the indirect damage (lost working days, lost connections with clients, customers, and buyers, psychological problems of employees with resulting lawsuits, loss of business reputation, etc.) which often reach a level equal or even greater than the direct damage.

Such a situation clearly requires extensive and continuous undertaking of preventive security measures in order to timely identify and eliminate possible factors of threat. The organization of prevention should be primarily aimed at deterring and slowing down the potential perpetrator from carrying out the offense, then its early detection and alarming, timely reporting to the police, preventing possible hostage situation, narrowing the space for escape and their identification and arrest. This requires good security assessment of the concrete object with the plan of protection measures. In implementing such measures the private protection which is practically unavoidable in this chain plays a huge role. This is also

where expertise and training of the security guards come to the fore, as well as their good judgement in predicting and identifying possible suspicious circumstances, and the ability to quickly adapt to a new situation. Moreover, here is the unavoidable incentive and development of the security culture of the employees along with the education regarding their behaviour before, during and after the crime.

Table 1 contains data about the number of registered robberies in Croatia for the period from 2007 to 2011.

Apart from monetary institutions the table contains also as object of attack other facilities (homes, shops, gas stations, kiosks, outdoor areas, etc.). In the observed period a total of 4.482 robbery crimes were committed. Figure 1 show that in the time period from 2007 to 2011 on the Croatian territory a total of 373.072 crimes were committed. Figure 2 show the total number of committed crime robberies in Croatia from 2007 to 2011.

Specific Characteristics of Private Security

When speaking about the private security system, it is emphasised that private protection has no special authorities, and the basic difference compared to police lies in special authorities. The authorities of private security are equal to the authorities of any individual, i.e. one of the essential differences would be in the source of private protection authority, with the right of individual for self-protection being the fundamental right and need whereas the authority of public security is reflected in the legal obligation to protection of certain social values i.e. that no one can transfer to someone else more rights than they are entitled to.

As indicated above, the Private Security Law forbids legal entities and tradesmen, involved in the activities of private security, the implementation of operational methods and means which are applied based on special regulations by the police, and this also yields one of the specific characteristics i.e. differences between the public and private security. On the other hand, when it comes to fighting and preventing crime, one of the essential differences lies in the object of protection. To the public system the primary object of protection is to serve the interests of the society. However, in case of private security, the goal is to serve the interests of the organization or individual persons, and not the society as a whole. Thus in the private security the interest for the prosecution of perpetrators is not the primary interest, even less their conviction, but rather the priority lies in serving the in-

TABLE 1
ROBBERIES COMMITTED ON THE TERRITORY OF THE REPUBLIC OF CROATIA REGARDING PLACE OF OFFENCE FROM 2007 TO 2011.
Source: MUP RH

Robberies	2007	2008	2009	2010	2011
Post offices	14	19	18	30	19
Banks	1		24	42	30
Exchange offices	8	8	6	29	24
Houses and apartments	22	30	30	43	39
Shops	136	121	101	249	272
Gas stations	52	33	41	54	62
Kiosks	37	39	27	92	65
Residential buildings	10	8	10	169	29
Outdoor areas	132	84	91	331	284
Betting shops	77	106	58	195	317
Other	136	106	112	207	203
TOTAL	625	554	518	1,441	1,344

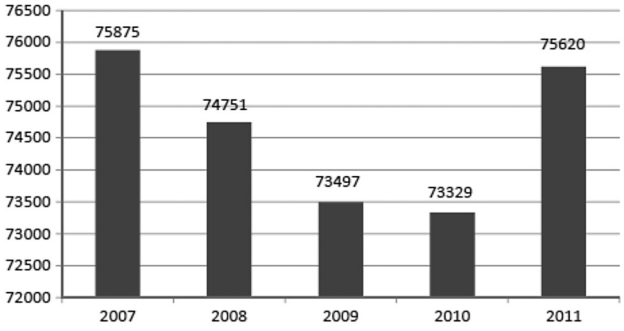

Fig. 1. Total number of committed crimes on the Croatian territory from 2007 to 2011.

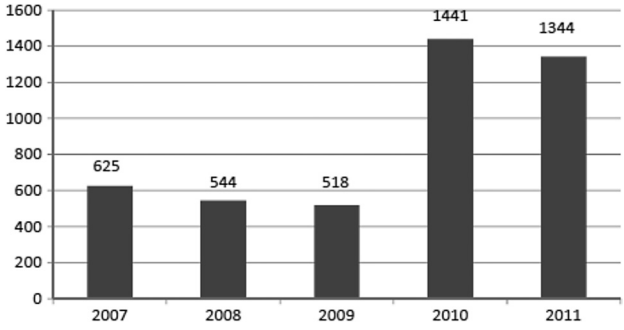

Fig. 2. The total number of committed crime robberies in Croatia from 2007 to 2011.

terests of the private client which do not have to coincide with public interests and security.

Such an attitude can come into conflict with public interest, if there is an obligation for everyone to undertake certain activities, i.e. inform the government bodies; however, considering that there is no regulation which would protect private interest in such cases, the conflict does not exist.

Processes of Operational Private Security Jobs

Private security is an area which is not provided by the government. However, the major part of these relations is the interference field which means that there is no clear border line between the area under the authority of the government and the one under the authority of private security. The very fact of the existence of private security does not exclude the obligation of the government to protect the assets of individuals which are also protected by private security.

The goal of private security is to ensure high-quality provision of services of physical and technical protection of persons, facilities, premises and assets. Operating activities of private security regulate the method of performing the process of physical protection, surveillance, and overview of the activities and performing of all accompanying activities to upgrade the system, which is the prerequisite for high-quality service provision.

Physical protection involves maintaining of a favourable security situation within the protected area, maintaining of the regulated order and peace, restriction of access to unauthorised persons, timely detection of harmful phenomena and illegal acts that could endanger persons, facility, premises and assets, provision of intervention upon alarm messages and other interventions in compliance with the contractual obligations.

The activities of physical protection, permitted means for work, and the method of their usage have been regulated in the Republic of Croatia in the Private Security Law, by means of regulations on the conditions and method of physical protection implementation, other legal regulations and by laws. The usage of additional means for performing the activities has been regulated by internal regulations, instructions and handling procedures depending on the requirements of the clients (short firearms, radios, hand-held metal detectors, flashlights, etc.)[8].

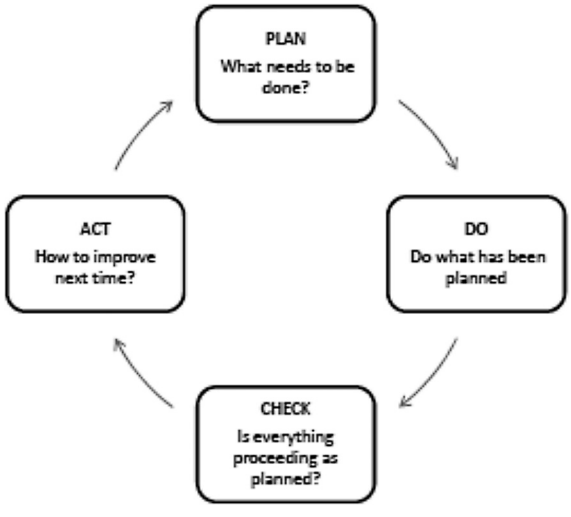

Fig. 3. Implementation of Deming PDCA methodology in private security system.

The means used to perform physical protection must be of a certain quality which has been regulated by international standards, i.e. the accepted rules of technical profession when there are no standards. Figure 3 show implementation of Deming PDCA methodology in private security system.

In General about Risk Assessment of Assets

Risk assessments of facilities of special significance for the defence are made by using the methodologies of the relevant ministries depending on the purpose of the facility declared by the Croatian government as especially significant for the defence of the country.

When making the risk assessment, among other things, the Law on the Secrecy of Data is also applied, and in this case the Risk Assessment becomes a classified document labelled »Secret«.

Furthermore, according to the Regulations about the conditions and method of implementing the technical protection, the implementation of technical protection means, among other things, also the development of risk assessment[9]. Risk assessment is the basic document which defines with which means and according to which concept of security the observed facility, production or some other processes and persons included in the mentioned process, are to be protected.

Risk assessment determines the critical points of the protected facility, from construction, transportation, electrical, fire protection and other defects or omissions that, from the aspect of security may be the source of endangering the security of a facility regarding any basis – larceny, burglary, aggravated larceny, robbery, terrorist attack, fire, explosion.

Risk assessment is produced on the basis of data about:

1. Type, purpose, size, and design of the building, location, and environment as well as construction and other properties of the building;
2. type and number of permanent and occasional users;
3. working regime and manner of using the facilities;
4. equipment, objects and documents that will be kept at the facility or are already kept, and the level of risk of their damage, misappropriations or destruction.

The recording of the existing condition of the protected facility and the analysis of the problem with rating, risk assessment, safety study and project task form an integral part of the technical security system project. Based on the risk assessment the security study is made.

The security study determines the optimal level of technical security and integral protection as well as connection with other technological systems on the facility.

Risk assessments are made for all objects and areas that the government, with the existing measures of protection protects insufficiently or not sufficiently well or not at all. The special category are the facilities of special significance for the defence, that have been declared as such by the Decision of the Croatian Government[10].

Legal or natural person who has made the Risk assessment document is responsible for all the regulated (suggested) measures of facility protection, whereas the owner or user of the facility is responsible for the implementation of all the measures of physical and technical protection. The owner or the user of the facility may hire a company (security company) that will carry out for them the security measure proposed in the Facility protection plan (Figure 4).

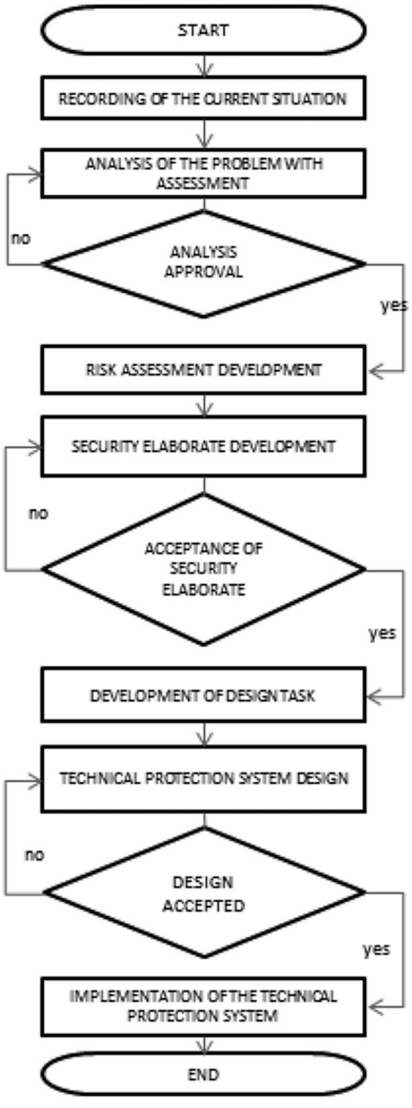

Fig. 4. Flowchart of technical security system design. Source: authors.

Advantages of Designing the Assets Risk Assessment

The benefit of developing risk assessment is the fact that first of all the existing condition has to be realistically recorded and it often destroys numerous illusions about somebody's security. However, developing risk assessment also helps to make us face already at the start realistically the fact that during the risk analysis and establishing the security system there is no 100% security or absolute safety. However, risk assessment verifies its justification immediately, since it emphasises the fact that there are modern methods and technologies of protection that may reduce threats to an acceptable or minimal measure. Such threats and damages as consequence of threat can never be reduced to absolute zero.

Risk assessment, as the basic document during the design of the security system, has multiple benefits:

- risk assessment contains the recording of the existing security condition based on which the responsible persons who make decisions about the security of the employees and company assets (administration and top management) obtain very fast a picture about the security condition at the company made by the independent external company, which has to be registered for the activities of technical protection and development of project documentation for the security systems;
- risk assessment emphasises good and bad sides of the currently implemented security concept at a company and enables decision-making about where and to what extent it is necessary to intensify or reduce the current security measures;
- the very process of developing the risk assessment for a certain institution or company has to include all the organizational structures from the lowest operative to the highest managerial people who make strategic decisions for a company, at the same time intensifying the responsibility and awareness of every individual about their role in the company from the aspect of security and safety, since the final report is made on the basis of every individual and their workplace, in which every person plays an important role and feels that their work contributes to and affects in the process organization the success of the work as a whole.

Analysis of the Existing Protection System of Facilities and Premises

Regarding the significance and status of the facility of special significance for country defence, only the measures of technical and physical protection have to be performed on the facility in order to protect the facility, persons and assets.

The protection measures include: physical protection, fences and natural barriers, lighting, entry control – identification, video surveillance, protection of secrecy as well as other safety measures (»Special security mea-

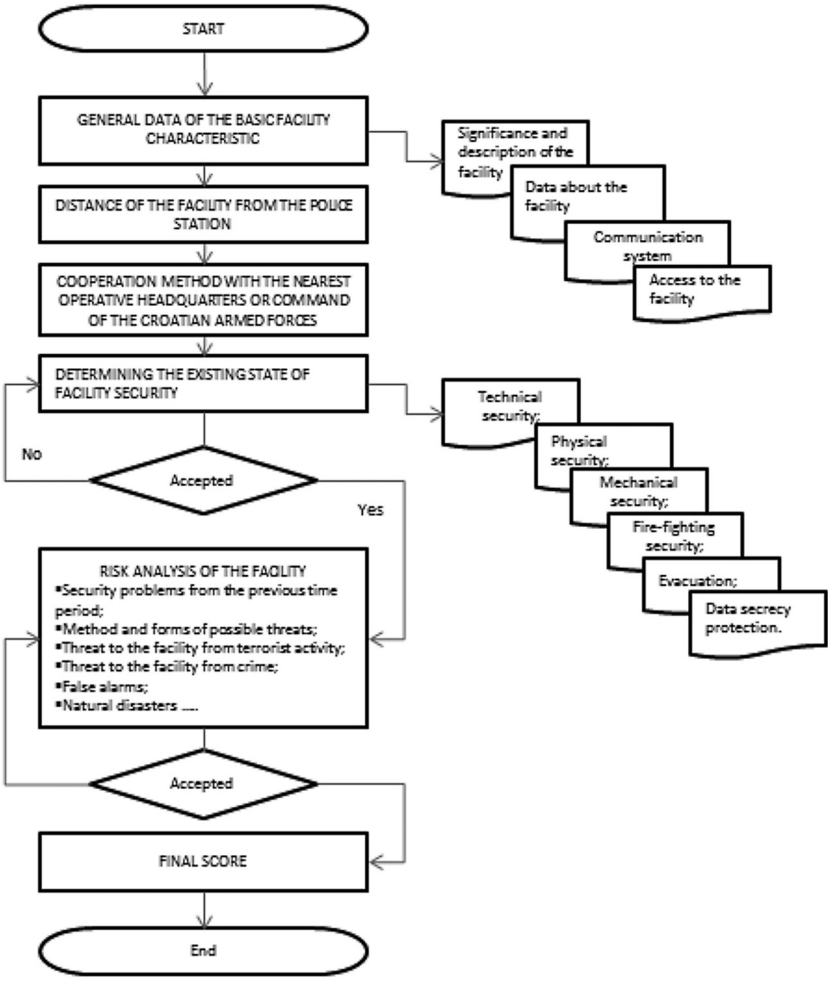

Fig. 5. Flowchart of developing risk assessment of facilities of special significance for the defence. Source: authors.

sures include: continuous presence of the physical security service, electronic security, which apart from basic functions provides audio-visual surveillance, surveillance and action in order to prevent disruption of security-information zone, electronic masking and protection against data disclosure; security check of all employees; counterintelligence protection«).

The consequences of an attack on the facility can be multiple, almost disastrous on the national and even on the regional level. Ranging from material and human losses, through ecological disasters to many years of negative impact on tourism which is a significant source of income at the government level. Damages that may occur as a consequence of unintentional accident or intentional attack on the facility would be multiple and they would have negative impact on the operation of the facility and the very company which comprises the facility (Figure 5).

Implementation of Risk Assessment in Case of Private Security

The concept of risk has been extremely often used lately, although the problems related to risk have always been present, ever since the existence of humans. It is, namely, from ancient times that humans have always lived in conditions of insecurity of various forms. Thus, e.g. there was no security in food, moving through area was insecure, hunting, construction of houses and settlements, etc. In all those ancient times various security measures were applied, and using them people tried to increase security. Thus, e.g. they moved through the areas in groups, avoided moving at night due to poor visibility, constructed their houses on places where defence was easier, settlements were girded by fences and walls, etc.

Since risk is in a way a measure of insecurity, i.e. there is sense that greater risk denotes also greater insecurity, it is obvious that risks have always been present. If so, why is it that they started to be discussed so often now, when they have always been present in the human lives and all the activities involving people? The reason lies in the fact that the organizational and technical-technological systems have developed so much that it has become a necessity to deal also formally with the issues of risk in order to reduce the loss and damage of assets, as well as the issue of rational investment into the security systems.

There are many definitions of the concept of risk. Almost in every area the concept of risk is defined in a different way. However, all the definitions eventually speak about the same thing in a slightly different manner and can cause confusion in those who are less familiar with it, in understanding what risk is. Thus e.g. in the Rječnik stranih riječi (Dictionary of Foreign Words) by Klaić, B it says: risk is a daring venture, putting at risk, danger (especially the loss in monetary affairs), peril, exposure to accidents, incidents, destruction, loss[11]. Anić and Goldstein[12] define risk as a danger that is predictable to a certain extent, whose intensity can be determined i.e. possible loss or damage for which insurance premium is paid. Apart from these definitions there are a number of others. Not one of them is mandatory for anyone. Each user can use the one that in their opinion best fits their vision of the concept of risk.

In the meantime, more precisely in 2009, the international ISO 31000 standards were published for risk management[13] and a glossary ISO Guide 73 which, among other things, defines as follows: risk is the effect of uncertainty for goals. The effect here may be considered to be positive or negative[14].

If the effect is negative then it is called loss or expenditure. The goals may be various, such as e.g.: finances, health and safety of people, ecological goals of the environment, security of facilities, etc.

In this context risk is often characterized by potential event and consequences, i.e. the combination thereof. Potential event is usually characterized by the probability of its occurrence, such as e.g. what is the probability of occurrence of a burglary, or what is the probability for someone to injure another person, etc.

In this context risk is considered as the combination of the probability and consequence. This means that the following can be claimed: if there is no consequence (losses, damage) then there is no risk regardless of the probability of a certain event. On the other hand, if there is no probability of a certain event there is no risk either.

Consequently, it may be said that being familiar with risk, i.e. its dimension are important in order to be able to even discuss the level of uncertainty. Generally, there are many ways in which the dimension of risk, i.e. uncertainty may be determined. Certain ways are appropriate for certain needs, whereas some others are appropriate for other needs. In the area of personal security usually the method is used which is based on the assessment of the probability of a certain event and consequence that this event can cause. In this sense usually the following expression is used: Risk = Probability × Consequence

Such approach in determining the dimension of risk belongs to the group of the so-called qualitative methodology. The main characteristic of this methodology is that neither probability nor consequence are known precisely, but rather these are estimated based on the experience and some more or less unreliable indicators. Therefore, one cannot speak about risk calculation but rather about risk assessment.

The parameters used in risk assessment and the consequence are estimated in the qualitative method based on the tables that are defined in advance as a rule. The examples of tables for the assessment of the dimension of parameters are presented below.

Table 2 shows that probability is defined at three levels: low, moderate and high. This, however, is neither a rule nor a regulation.

This is exclusively the choice of those who are working on risk assessment. The table may have more levels: 5, 7, 9, etc. However, the problem in case of a larger number of levels is the description in remarks so as to be able to unambiguously select the order of probability. If there are indicators so that more than three levels can be defined, then it is better to define the table with more levels. The text of the description and the remarks presented in Table 1 are an illustration and the users may adapt them to their needs. It should be noted that the table of probability is used for all risks in the assessment of a facility. Only different frequencies for different types of events can be entered into the column of remarks. Thus, e.g. for burglary it may remain as presented, and for the assault some other value for the number of assaults within a certain period of time may be taken.

Table 3 shows the values of the selected amounts for certain levels of consequences. Since every consequence is in fact a loss, then this consequence is expressed in the financial value, and has significance: if the event occurs (e.g. theft) what damage is expected. Here the table of consequences is shown with five levels. Obviously it is far simpler and more precise to define the levels of the table in comparison with the probability. However, not more than five levels are necessary; maybe seven.

If the abovementioned expression for risk assessment is applied, this may yield the following:

$$\text{Risk}_{\min} = \text{Probability}_{\min} \times \text{Consequence}_{\min} = 1 \times 1 = 1$$

$$\text{Risk}_{\max} = \text{Probability}_{\max} \times \text{Consequence}_{\max} = 3 \times 5 = 15$$

It can be seen that the risks for the above tables are in the range from 1 to 15. The lower the risk the more fa-

TABLE 2
SCALE OF EVENT PROBABILITY

Ord.	Rank	Description	Remark
1	Low	Low probability or very rare occurrence of the event	e.g. once annually
2	Moderate	The event occurs periodically	e.g. once in six months
3	High	The event occurs very often	e.g. once monthly

TABLE 3
SCALE OF CONSEQUENCES

Ord.	Rank	Description – value of loss
1	Negligible	Less than 1,000 kn
2	Little	From 1,000 to 5,000 kn
3	Moderate	From 5,000 to 10,000 kn
4	High	From 10,000 to 20,000 kn
5	Extreme	Over 20,000 kn

vourable it is, i.e. the greater the risk the higher the probability that it will come to losses.

According to ISO 31000 standard[13] after having done the risk assessment the risk has to be ranked. For the above example the ranking of the risk may be performed according to Table 4.

The method of ranking risk, i.e. defining the levels is the user's choice, but the example given in Table 4 is adequate for the above method of determining the probability and consequence.

The last column of Table 4 contains the description of the activities that need to be undertaken in dependence on the dimension of the assessed risk.

After having done the risk assessment and ranking, it is necessary for the unacceptable risks, i.e. for all risks that are above the threshold of acceptance to undertake some of the activities to reduce the risk, i.e. the damage. According to ISO 31000 standard[13] there are four possibilities of handling unacceptable risks, i.e. risks that are above the threshold of acceptance. Adequate handling of unacceptable risks according to the standard is called risk processing and there are four types of processing presented in Table 5.

It should be noted that in no case of implementation of any form of risk processing absolute security is achieved, i.e. in no case is it possible to eliminate risk completely. In all forms of risk processing, apart from by acceptance, the risk is more or less reduced. It would be ideal if some of the procedures of risk processing would reduce the risk to the level of acceptance.

For some types of risk several forms of processing can be simultaneously applied, as e.g. for the case of burglary surveillance cameras can be installed, grids on the windows, as methods of reducing risk, and contracting an insurance policy as a form of transferring part of risk to others.

Conclusion

In the paper we have given recommendations to implement risk assessment in the area of private security while making the risk assessment of persons, facilities, and assets as well as the system scheme and the model for the making of risk assessment of persons, facilities and assets.

We have also found that before and during the risk assessment it is necessary to document the risk assessments both because of the decisions in the organization and implementation of the protection activities, as well as because of the possible subsequent forensic requirements.

The key documents for the risk assessment documentation can be regulated by special regulations or acts, as

TABLE 4
RANKING OF RISK

Order	Risk rank	Risk limits	Necessary activities
1	Low	1–4	Risk is acceptable and no activities are necessary.
2	Moderate	5–9	Risk has to be controlled and when possible the risk should be reduced
3	High	10–15	Risk is unacceptable and currently adequate safety measures need to be undertaken.

TABLE 5
TYPES OF RISK PROCESSING

Processing	Description
Acceptance of risk	Formally risk is accepted as it is. The reason for this lies in the fact that because of several reasons there is no real possibility of reducing risk, e.g. due to expenses of reduction. Then the decision is made about accepting the risk regardless of its level.
Transfer of risk	In risk transfer a greater or smaller part of the risk is transferred to someone else, such as e.g. the insurance agency, a company that performs certain activities and they take over a part of the risk, etc.
Avoidance of risk	The situation in which the liability or prohibition are used to avoid the occurrence of risk. An example of risk avoidance is the prohibition of creating an open flame in the vicinity of explosive or flammable substances, prohibition for clients to carry weapons into a bank, etc.
Reduction of risk	With these procedures and/or technical equipment the dimension of risk is reduced. An example of risk reduction is the installation of video cameras, raising of physical barriers (fences), training of security guards, etc.

well as internal regulations of the company performing risk assessment. These should certainly include the following documents:

a) Regulations and criteria of risk assessment. It defines the methodology and scale of assessment. Their example is given in Tables 2, 3, 4 and 5;

b) Document with analysis of types of risk that reduce the security of the protected facility presenting the method in which such risk can be realized;

c) Documented risk assessment for every type of risk that has been determined by analysis to be possible. This assessment is performed using the adopted methodology;

d) Report on the ranked risks based on the assessment and ranking scale;

e) Report on the remaining risks, that will remain even after the risk processing has been performed;

f) Risk processing plan in which for every risk it is indicated which processing procedures are performed for every risk, within which time period this has to be implemented, using what equipment, responsibility for implementation, and price i.e. expenses of implementation.

All these documents need to be produced before the final acceptance of the entire risk assessment.

Acceptance and approval of the entire documentation related to risk assessment lies under the responsibility of the head of the security of facilities and the protection claimer, who are at the same time responsible also to undertake measures in crises.

REFERENCES

1. TATALOVIĆ S, BILANDŽIĆ M, Osnove nacionalne sigurnosti (Ministarstvo unutarnjih poslova, Zagreb, 2005). — 2. GRIZOLD A, Međunarodna sigurnost, Teorijsko-institucionalni okvir (Sveučilište u Zagrebu, Fakultet političkih znanosti, Zagreb, 1998) 28. — 3. Introduction to Security Risk Analysis, accessed 12.03.2013, Available from: URL: http://www.security-risk-analysis.com. — 4. JURAK F, Sigurnost i razvoj – osnove teorijskog pristupa (Zbornik radova nastavnika i suradnika Više škole za UP-e, MUP RH, Zagreb, 1991) 71. — 5. SINGER M, Kriminologija (Nakladni zavod Globus, Zagreb, 1994). — 6. KOVČO-VUKADIN I, Hrvatski ljetopis za kazneno pravo i praksu, 12 (2005). — 7. DUJMOVIĆ Z, Pristupi u otkrivanju i razrješavanju razbojništva (Policija i sigurnost, MUP RH, Zagreb, 1994). — 8. VEIĆ P, NAĐ I, Zakon o privatnoj zaštiti s komentarom (Žagar, Rijeka, 2005). — 9. Pravilnik o uvjetima i načinu tehničke zaštite, Narodne novine br. 198/03, accessed 03.05.2013, Available from: URL: http://www.nn.hr/Default.aspx. — 10. Uredbu o kriterijima za odabir, mjerama za zaštitu te načinu označavanja vojnih i drugih objekata posebno važnih za obranu, Narodne novine, br.63/11, accessed 03.05.2012, Available from: URL: http://www.nn.hr/Default.aspx. — 11. KLAIĆ B, Rječnik stranih riječi, (Nakladni zavod Matice Hrvatske, Zagreb, 1984) 1171. — 12. ANIĆ V, GOLDSTEIN I, Rječnik stranih riječi, (Nakladni zavod Matice Hrvatske, Zagreb, 1999) 1111. — 13. ISO 31000: 2009, Riskmanagement – Principles and guidelines, accessed 20.02.2013. Available from: URL: http://www.iso.org/iso/catalogue_detail?csnumber=41933. — 14. Guide 73:2009, Riskmanagement – Vocabulary, ISO, 2009, accessed 19.02.2013. Available from: URL: http://www.iso.org/iso/catalogue_detail?csnumber=41933.

I. Nađ

University of Applied Sciences Velika Gorica, Zagrebačka cesta 5, 10410 Velika Gorica, Croatia
e-mail: ivan.nadj@vvg.hr

ZAŠTITA OBJEKATA I PRIMJENA PROCJENE RIZIKA

SAŽETAK

Stanje sigurnosti na određenom području nameće potrebu stalnog propitivanja postojećeg sustava zaštite kapitalnih objekata u državi, a osobito objekata od posebnog značaja za obranu. Objekti od posebnog značaja za obranu bitni su dio svakodnevnog života, koji omogućuju neometano funkcioniranje gospodarstva i svih drugih djelatnosti države. Pod zaštitom objekata kritične infrastrukture razumijeva se sustav obveznih mjera kojima se sprečava uništenje ili oštećenje objekata, odnosno zaštita otkrivanja tajnih podataka o objektima i djelatnostima u njima. Za svaki oblik ugrožavanja, potrebno je poduzimati adekvatne preventivne mjere zaštite. Osnovni oblici mogućih ugrožavanja objekata koji mogu izazvati veće ili manje štete, a koji su u neposrednoj domeni tjelesne i tehničke zaštite su različiti oblici terorističkih djelovanja, sabotaže, diverzije, eksplozije, veći požari, prirodne katastrofe, provalne krađe i krađe, razbojništva i sl. Cilj ovog rada je prikazati odgovornost kriznog menadžmenta za objekte kritične infrastrukture, tijekom izrade prosudbe ugroženosti i planova zaštite uz primjenu procjene rizika.