Prof. Ing. Tomáš Loveček, PhD. [1]

VULNERABILITY ASSESSMENT OF PHYSICAL PROTECTION SYSTEMS

Abstract: If property protection is process of creating a secure state using protection measures with the purpose of disrupting or stopping any activities or events which are contrary to the interests of this property owner, then physical protection system is a tool used to achieve this state. The states strategic objects can be for example: the elements of critical infrastructure, key assets, and other important objects, nuclear stations, objects for storing and manipulating classified information, Seveso companies, etc.), no matter if they are owned by or managed by physical or legal persons. Requirements for their protection against intentional acting by unauthorized persons (i.e. anthropogenic attack vector), whatever is their aim (to damage, to destroy or to alienate protected assets located in that object); are given primarily by EU directives, generally binding legal regulations of EU Member States, national and international technical standards or various requirements of third parties (e.g. insurance companies). Existing approaches to assessing the level of strategic objects, have qualitative or quantitative nature.

Key words: Physical Protection System, Critical Infrastructure, Risk Assessment, Intruder, Vulnerability Assessment

[1] Prof. Ing. Tomáš Loveček, PhD., University of Žilina, Faculty of Security Engineering, Univerzitná 8215/1, 010 26 Žilina, Slovakia, Tomas.Lovecek@fbi.uniza.sk

1. INTRODUCTION

The subject of protection may assume different forms depending on the issue being discussed. In the broadest sense, we may be talking about protection of material or immaterial property, which can represent an object or information owned or managed by a natural or a legal person. Literature also use terms such as "protected asset". The subject of protection can also be defined from the aspect of a field which is governed by a generally binding legal regulation or standard, the subject of protection being e.g. personal data, classified information, object, system, process, technology or a delimited area. If the subject of protection in not determined by a binding regulation or norm, it must be determined on the basis of nature of the activity by the owner or operator himself, which can generally be the case with protection of the (main) production process or service provision. In most cases, the subject of protection (e.g. information on a data carrier, information system, service, technology, object, construction, substance etc.) is bound to a specific area with clearly defined borderline (perimeter). This type of area, in which the subject of protection is located, can be a territory, location, estate, zone, object or a room within an object.

2. PROTECTION SYSTEM

Requirements of generally binding legal regulations, technical standards, insurance conditions and requirements of internal company regulations for object protection result in the need to take certain security/protection measures, which should be applied in a manner ensuring protection of property of their owner or operator.

If property protection is the process of instituting a status of security by using protection measures which aim to thwart or stop any unwanted activities or events (e.g. short circuit and subsequent fire), which are inconsistent with the interest of the owner or administrator of this property, then the protection system is a tool used to achieve this status.

The Act on Private Security defines the security system, consisting of a scheme of electric, electronic, mechanic or other parts constituting a fixed built-in barrier preventing a person or an animal from accessing or exiting or driving out of the protected object or protected place, which cannot be overcome without expert knowledge or without using force [23].

In Anglo-Saxon countries, there are two most common terms describing the property protection system. These are physical protection system: [1] and security system. In 1970s, Physical Protection System was the first term which found global usage in relation to complex protection of nuclear and military facilities from intentional

anthropogenic threats (e.g. vandalism, theft, burglary, sabotage, terror attack). The term Security System is related rather only to alarm systems.

A common requirement of the above-mentioned definitions is to create a protection system, which, as an efficient way of applying protection measures, enables preventing an intentionally acting unauthorised person to achieve their goal, which can be theft, damage or destruction of a protected asset.

Such a protection system can be understood as a system consisting of mechanic, technical, personnel and regime protection measures/elements which can be divided into:

- passive protection measures,
- active protection measures,
- manned guarding measures,
- regime measures.

Passive protection measures aim to dissuade, slow down or stop an unauthorised person or intruder, while active protection measures serve for their subsequent detection and initiation of alarm status. In special cases, active protection measures are able to substitute passive protection measures (e.g. security fog devices/systems). Physical protection measures ensuring timely intervention and detention of the intruder are an integral part of the protection system. Regime protection measures ensure correct and efficient functioning of all mentioned protection measures [3].

2.1. Active protection measures

Technical standard [14] defines the Alarm System as electric installation element reacting to manual or automatic detection of presence of danger. A similar definition of the alarm system can be also found in [16], which describes alarm system as an electric device reacting to manual stimulus or automatic detection of presence of danger. However, this standard introduces the term Alarm Application, meaning an application used for protection of life, property or environment. Such an application can represent:

- intrusion and hold up system,
- social alarm system,
- lift alarm system,
- environmental impact alarm system,
- CCTV surveillance system,
- access control system,
- fire alarm system.

In case of definition of alarm application, its purpose is to be understood in a broader sense than solely detection of presence of danger in form of an intruder. One

of the examples is CCTV, whose purpose according to [12], can be also monitoring, surveillance, recognition, identification or investigation [3].

Non-alarm Applications are systems used only for control (e.g. heating, air conditioning, lighting, control of energy systems, building management), their primary function not being protection of life, property or environment [16].

Integrated Alarm System integrates multiple systems/applications, with at least one of them being an alarm system [16]. The standard [10] defines three types of alarm systems:

- intruder alarm system, alarm system designed to detect and signal presence, breaching or the intruder's attempt at breaching the guarded premises,
- hold-up alarm system, system enabling the user to intentionally initiate an alarm status,
- social alarm system, is a system providing means to call in help designed for persons whose life is considered to be in danger.

Alarm systems are connected to a whole set of technical standards which divide alarm systems into:

- intrusion and hold up systems [9],
- CCTV surveillance systems [12]/video surveillance systems **Error! Reference source not found.**,
- access control system [11],
- social alarm system [15],
- alarm transmission systems and equipment [14].

The standard [18] defines alarm systems separately as an access system, security device (understood as electric security system) and CCTV surveillance systems without common denomination.

From the aspect of technical standards, the used terminology is rather consistent and its definitions compatible, as in all cases we come across the term alarm/non-alarm system, which can be specified in more detail regarding its purpose or application (e.g. intruder alarm system).

The Act on Private Security [23] uses an equally frequent term alarm system, meaning a scheme of electric, electronic mechanic or other parts constituting a fixture attached to/on a protected object, which initiates a luminous, sonic or other type of signal after unauthorised intrusion into the protected object. This term is also used in the Act on Banks [24], which stipulates that banks secure certain areas by means of a functional and active security and alarm system.

2.2. Passive protection measures

In comparison with the active protection measures, passive protection measures are not based on technical standards, in which we may find definitions of various specific representatives, even though there is no definition of the whole group of elements ensuring detaining or slowing down the intruder.

Generally binding legal regulations as well as literature describe passive protection measures as mechanical barriers.

According to literature [5], the core of classic protection is using all mechanic and barrier means, which make it difficult or prevent the intruder (unauthorised person) from entering the protected area or manipulating with protected objects. Application of mechanical barriers lies in their mechanic solidness, resilient materials in combination with the other types of protection. A barrier system may include e.g. fencing around the object and its significant parts, barred entrances to the object, reliable closing and locking.

2.3. Physical protection measures

An integral part of every protection system are physical protection measures which ensure timely intervention and detention of the intruder. Literature and legal regulations define physical protection as protection performed by means of physical presence of persons in the protected area or its proximity [3]. According to [23], physical protection means patrol, guarding, operation of the alarm system and direct control over these activities. Persons performing physical protection are most commonly member of security services or units, armed forces or guards. Generally speaking, these can be members of police and security services. Police and security services can be divided into groups on the basis of multiple criteria:

- relation to national authorities,
- type of administrator/operator,
- nature of legal regulation of specific security services,
- area and type of activity of security services (organisational and tactical forms),
- scope of authority related to territory and matter,
- level of management of security services [6].

The basic terminology of security service providers is governed by technical standard, which defines security services as services provided by a security service company aimed at protection of persons, property and other assets. In terms of these services, the standard describes various positions such as Security supervisor, licensed security officer/security guard, alarm response officer, guard dog handler, city patrolling, door supervisor, monitoring and alarm receiving centre operator, mobile area/site patrolling, Reaction time, static guarding, armed security officer/guard. The area of airport

security service providers is governed by technical standard [8] which, except of the basic terminology, also describes extent of trainings and the method of employee selection. The area of marine and port security services is governed by the technical standard.

3. DETERMINING LEVEL OF PROTECTION

In the stage of planning, projecting, executing and operating object protection systems, we can evaluate them based on their functionality, efficiency, reliability and quality [4].

From the economic aspect, system efficiency can be defined as return on finance invested in the system and evaluated based on its results. Economic efficiency of the object protection system can be defined as the relationship which, by means of economic indicators, expresses interdependency between economic benefits of the system's influence on decreasing economical losses due to criminal activity and economic costs for its design [4].

System reliability is characterised by its complex ability to keep its functional characteristics in a given time and conditions. Reliability is a factor which is often expressed as probability that the system (e.g. electric security system, video camera surveillance system) or its element (e.g. detector, central office, communicators) will perform the required task for the specified period under pre-defined circumstances. In practice, reliability is expressed by the number of malfunctions per time unit during a monitored period. In many cases, reliability of the protection system also depends on reliability of the human agent (e.g. security service officer, operator of the surveillance central office) [4].

Quality of the protection system represents a set of features of the entire system which make it able to satisfy legitimate and anticipated needs of a specific subject (e.g. owner, operator, administrator) and thus ensure security of a given environment, in a given time and for a specific purpose [4].

Searching for an optimal protection means looking for a solution which is reliable, economically efficient and which, at the same time, meets the requirements of a functional object protection system.

A functional object protection system is a system which meets the basic requirement: from the moment of detection, the time of attack is longer (including the time of breaching passive protection measures and time of intruder's movements) than the reaction time of the task force. This means that the system is efficient, if the ratio of times is bigger than one.

Due to influence of various outer factors, fulfilment of the above mentioned requirement is not necessarily sufficient, however, it is an essential condition if the system is to be functional.

If the intruder aims to steal a protected asset with the intent of subsequent encashment, it is sufficient to detain them in the time of escape at latest, which prolongs the overall disposition time of the task force.

If the intruder aims to damage or destroy the protected asset with the intent of sabotage or terror attack, it is necessary to detain them before achieving their goal, e.g. before damaging or destroying the protected asset. In this case we cannot count in the time of their escape [3].

Proving the fulfilment of this basic and seemingly elementary condition of the system functionality in a credible way is often hardly possible in practice. The existing procedures (standards, methodology, directives etc.) related to object protection use one of the two basic approaches:

- qualitative approach,
- quantitative approach.

Procedures requiring qualitative approach are based on expert assessment of assessors in cases when it is not possible to verify sufficiency of the suggested protection level in a precise manner, making it necessary to rely on expertness of creators of these procedures. In this case, it is impossible to verify whether the protection system is not underestimated or, on the contrary, overestimated.

Procedures based on quantitative approach make it possible to exactly prove adequacy of suggested protection measures by means of measurable input and output parameters [3]. In this case it is possible to verify whether the protection system is underestimated or overestimated in relation to suggested protection measures.

Currently, there are several tools (software) using one of the mentioned approaches to assess functionality of the protection system [3]:

- Qualitative approach: RiskWatch (USA), CRAMM (United Kingdom),
- Quantitative approach: SAVI, ASSESS (Sandia National Laboratories, USA), Sprut (Scientific and Production Enterprise ISTA SYSTEMS JS Co., Russia), SAPE (Korea Institute of Nuclear Non-proliferation and Control, South Korea), SATANO (University of Zilina, Faculty of Security Engineering, Slovak Republic).

The least subjective but also the least frequently used approach is the quantitative approach. The reason is that the existing tools were created to assess protection of specific

non-commercial facilities and they are not freely available. However, the main reason is the fact that in practice real values of input parameters are often lacking, such as:

- breach resistance of passive protection measures which changes depending on the type of tools used to breach them,
- probability of detection of active protection measures which changes depending on intruder's knowledge of used technology (e.g. method of evaluating change of physical parameter due to breach of protected area),
- reliability of active protection measures,
- human agent reliability.

For these reasons, the above mentioned tools are used in practice only in a specific area (e.g. protection of nuclear facilities), or rather they are still being developed by various research institutes (e.g. The Nuclear Regulatory Authority of the Slovak Republic; University of Zilina, Slovakia; University of Defence, Czech Republic). In practice, procedures based on qualitative approach are much more commonly used. These can be divided into [3]:

- (qualitative) directive approach, with specifically defined protection measures regardless of the facility's characteristics and the environment in which the object is located,
- (qualitative) variant approach, with the option of choice of a finite number of proposed solutions combining various protection measures, which can, to a certain extent, take into consideration not only characteristics of the facility and the environment, but also financial, technical or personnel conditions and capacity of the owner of administrator of the object.

The first and the most important step in the process of planning and projecting an object protection system is determining the minimal protection level, which subsequently determines the selection of technology of active and passive protection measures, dislocation, parameters and functionalities. The minimal protection level determines what protection measures are to be implemented, in what ratio and with what kind of features (e.g. security level/class, purpose and usage, key parameters of system elements, dislocation).

Minimal protection level can be deduced from so called security requirements, which can be determined by:

- basic condition of protection system functionality,
- third party:
    - national authorities, by means of generally binding legal requirements,
    - standards institute, by means of standardisation norm,
    - insurance company, by means of contractual terms,
    - customer, by means of contractual terms or recommendations,

- parent company, by means of internal organisational regulations,
- another third party, by means of a directive, regulation, contract, standard etc.

If the minimal protection level is determined based on fulfilling the basic condition of protection system functionality, the quantitative approach is applied, using temporal and probability base values of input and output parameters (e.g. times of breach resistance, times of movement and reaction times, probability of detection etc.).

If the minimal protection level is determined based on fulfilling security requirements of third parties, the qualitative approach is used in most cases - directive or variant approach.

If the above mentioned breach resistance values are known, it is possible to apply quantitative approach when determining the minimal protection level, which is based on the philosophy that it is necessary to use as many passive and active protection measures to ensure that the intruder is detained by the task force before achieving their goal. In this case, minimal protection level could be based, for example, on minimal parameter values:

- measures efficiency coefficient: >2,5
- probability of interruption: > 0,85
- cumulative probability of intruder detection: > 0,95

These minimal values suggest the number of mechanical barrier measures with respective breach resistance which should be implemented in a given reaction time of the task force. Furthermore, minimal parameter values determine the primary moment of detection and what the probability of intruder detection by individual elements of alarm system should be.

As today we do not have access to a complex base of values of input parameters, it is necessary to determine the required minimal protection level on the basis of security requirements of one of the relevant third parties. These can be the national authorities (e.g. ministries, National Security Authority, Nuclear Regular Authority etc.). standardisation institute (e.g. ISO, CEN/CENELEC, BS, DIN etc.), insurance company, parent company, investor or customer.

4. RISK MANAGEMENT IN THE DESIGNING AND EVALUATING OF PPS

In many cases, the establishment of a minimum level of protection is linked to the risk management process, where the requirements for protective measures increase

both in scope and are also made tighter with an increasing risk level (e.g. increasing the security class for alarm systems). If the risk management process does not impact on the resulting minimal level of protection (i.e. it is determined by directive), it has a significant impact on the determination of the placement of protective measure elements (e.g. cameras, detectors, mechanical barriers, etc.)

The requirement for the risk assessment process related to the protection of premises against intentional anthropogenic threats is given by international and national acts of general application, and standards for a particular area of application (e.g. classified information, protection of critical infrastructure, protection of banking subjects, protection of commercial and administrative premises or protection of residential premises, etc.).

The general principles and guidance on how to approach the risk management process are defined in [20]. Principles and instructions. Many of the above regulations do not conform with the standard, either from a terminological or a procedural point of view. Even where the relevant regulation directly refers to this standard (e.g. [19], [13]).

Whilst it is necessary to use the existing legal framework (both in terminological and procedural terms), it is also necessary to honour and apply the generally applicable principles that apply to risk management to the maximum extent.

According to [20], risk management is a structured and coordinated set of activities and methods to guide and manage the organisation in relation to risks2, which may affect its ability to achieve set goals. The concept of risk management refers to the architecture of effective risk management that includes (Figure 1):

- principles of risk management,
- structure of risk management (framework),
- process of risk management.

The standard can be used by any public, private or social organisation, association, group or individual. Therefore, this standard is not specific to any type or branch of industry, for ease of reference the various users of the standard refer to the generic term organisation.

[2] The risk is characterised by reference to a potential event and its consequences

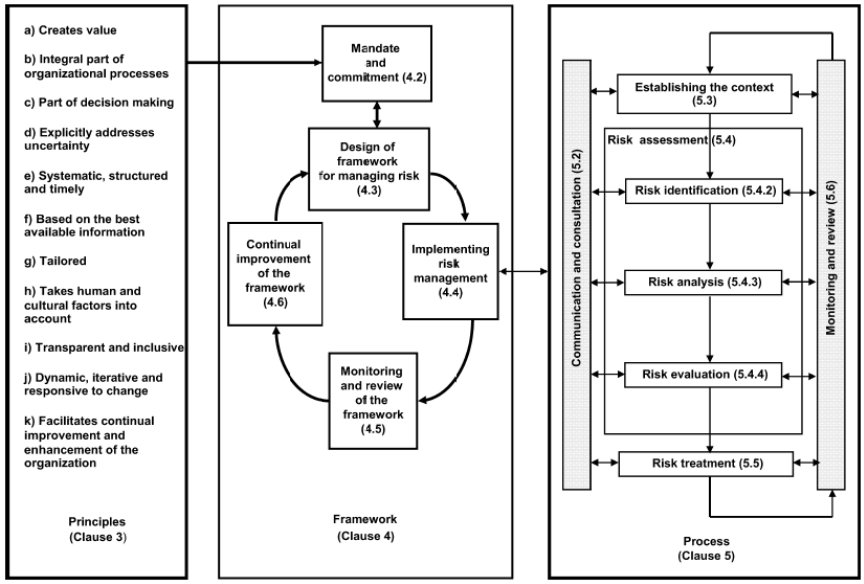

Figure 1 Relationships between the principles, structure and process of risk management [20]

The standard can be used during the existence of any public or private organisation, in associations and for individuals in a wide range of activities and processes related to strategy/decision making, operations (production, service), project preparation and, last but not least, property protection. It can be applied to any type of risk of any nature, regardless of whether it has positive or negative It can also be applied at different levels

An example of the use of the risk assessment process at different levels is the Critical Infrastructure Act, which requires the central authority to develop sector risk analysis and update it on a given critical infrastructure segment. At the same time, the Act imposes an obligation on the operator of a critical infrastructure element to assess the risk of the threat of disturbance or destruction of each item of equipment, their vulnerable sites, the foreseeable consequences of disruption or destruction of the functionality, integrity and continuity of the element. In both cases, the procedures set out in the aforementioned [20] may be applied, but in both cases other contexts influencing the resulting magnitude of the risk and the subsequent method of handling unacceptable risks will be taken into account.

From the point of view of designing security systems, the risk assessment process may be used at different levels, namely:

- the establishment of a minimum level of protection for the entire protection system for the premises (e.g. in the case of protection of classified information where

the risk assessment process affects the required overall minimum point value that may be achieved by a combination of different protective measures),

- the establishment of a minimum level of protection of the chosen security measure (e.g. when determining the security level of the CCTV system, from which the requirements for its functionality and the parameters of the individual components are derived),
- placement of systems and their protective measure elements (e.g. when placing cameras on premises),
- identification of the risk of failure to prepare and implement a protection system project on a given premises (e.g. in the case of risk assessment related to project management).

In the case of a requirement to take risk into account when determining the minimum level of protection, whether the whole system or part thereof (e.g. a CCTV system), in most cases a methodological instruction is handled by a competent authority (e.g. the National Security Agency, National Standardisation Organisation). In the case of decisions on the placement of individual system components (e.g. detectors, cameras, APASs, etc.), in addition to the instructions issued by manufacturers and technical standards defining the general guidelines for the use of such systems in practice (e.g. EN 50131-7, EN 50132-7, STN EN 60839-11-2), the already mentioned risk assessment process plays an important role, consisting of the sub-processes identification, analysis and risk assessment.

According to [20], the risk assessment process forms a part of the risk management process and consists of the identification, analysis, and risk assessment sub-processes.

Risk identification involves the identification of sources of risks, events, and potential consequences.

Risk analysis is the process of determining the level of risk where this level is expressed as a combination of consequences and their probability of occurrence.

Risk assessment is the process of comparing the results of risk analysis with risk criteria to determine whether the risk or its achieved level is acceptable. In the event that such level is unacceptable, the risk must be addressed, which is the process of risk modification.

As already mentioned in the example in Table 1, the risk assessment process may also be applied at a micro level where the aim is to decide on the location of safeguards, primarily on the basis of an assessment of the likelihood of possible risks. The consequence is the same in the given case, namely loss or damage to the asset. In the given case, the risks are represented in possible scenarios; in what way, or how, the intruder is able to achieve their goal. If we assess risks whose consequences are

constant, i.e. the protected asset does not change (e.g. a safe in a family home) and the level of this risk is only affected by the probability of the occurrence of a given negative event (security incident), we can also refer to vulnerability analysis, which does not change the fact that the same principles are used as those used in the risk analysis process (a combination of consequences and their likelihood of occurrence).

Table 1 An example of risk analysis (vulnerability analysis) in selected premises (Source: authors)

Risk		**Possibility of occurrence <1-5>**	**Consequence <1-5>**	**Risk level**
Event	**Consequence**			
Theft of material from warehouse C2 outside working hours by climbing over the fence and breaking through the entrance door into the warehouse	Interruption of delivery of construction material to the production unit	**4**	**5**	**20**
Theft of material from warehouse C2 outside working hours by climbing over the fence and breaking through the window into the warehouse		**4**	**5**	**20**
Theft of material from warehouse C2 outside working hours by using a paraglider by entering via the roof ventilation system		**1**	**5**	**5**
Theft of material from warehouse C2 outside working hours by breaking through the perimeter wall that forms a part of the perimeter of the protected area		**2**	**5**	**10**

From the example in table 1 we can see that the different scenarios have different possibilities of occurrence (expressed for example by probability), which should ultimately be used in the placement of protective measures. It follows from the aforementioned example that when placing alarm system components designed to detect an intruder, emphasis should be placed on door and window apertures.

5. SOFTWARE SUPPORT FOR DESIGNING OBJECT PROTECTION SYSTEMS

A designer (a project team) should have a clear idea in which stage/process of the project will they use software support.

In the various project phases, a designer will encounter standard office packages, budget tools, project management (planning) tools, and, last but not least, specialized tools

created for the designer's needs. In the case of designing protection systems, it is also advisable to use graphic programs for better quality presentation of design results.

Software tools to support object protection systems design can be divided into several groups:

- software tools that enable to model dislocation of areas, objects and protection measures in 2D and 3D environment (particularly CAD tools),
- software tools that enable comprehensive assessment of the effectiveness of the object protection system (e.g. SAVI, SPRUT, SATANO).

5.1. Software tools that enable to model dislocation of areas, objects and protection measures

For dislocation of active and passive protection measures and subsequent determination of their parameters and operating conditions, a range of software CAD tools can be used. Computer-aided design means using computer to support design and design documentation. This is a substantial area of information technology, in which program environment is used instead of a drawing board. CAD applications always include graphical, geometric, mathematical and engineering tools for 2D drawing and object modelling. More advanced CAD tools can handle calculations, analyses and management of systems, e.g. production. A closely related area is 3D visualization of a drawn model, which is mainly used for visualization purposes. There are standard and specialized CAD tools in 2D and 3D environment available. Most commonly used CAD tools include particularly AutoCAD, ArchiCAD, IntelliCAD, Allplan, and currently popular SketchUP. Specialized CAD tools include other programs and their components that can be categorised in relation to their area of application. In the field of engineering, SolidWorks, CATIA, Inventor etc. are particularly popular. Tools for the fields of construction, architecture, electrical engineering and others are also to be found. Some of the programs are used in various fields. In principle, CAD tools are used during designing and modifying protection system for:

- designation of protection measures including cable distributions (e.g. AutoCAD),
- coverage of protected area by alarm systems (e.g. VideoCAD, IP Video Design Tool),
- modelling of 3D design (eg SketchUP).

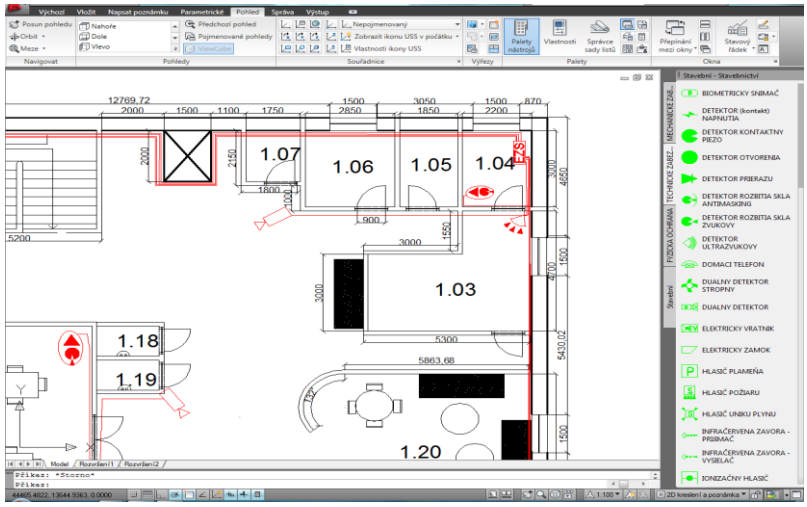

Figure 2 Part of the floor plan of a bank building and a security system design using an AutoCAD security tools palette (Source: authors)

Axis Camera for Autodesk® Revit®

Autodesk is developing several other CAD tools. Autodesk Revit is a BIM (Building Information Modelling) application which can be used to install an Axis extension for CCTV systems. Traditional CAD applications are based on tools for developing 2D drawings or creating geometric 3D models. BIM offers a new way of working that uses intelligent elements of the information model. Any changes and modifications to the model will be immediately reflected in all project aspects. The data remains consistent, coordinated and accurately describes the project properties for all members of the project team. The Axis Camera extension provides camera system designers with a useful tool for modelling CCTV solutions in a specific object.

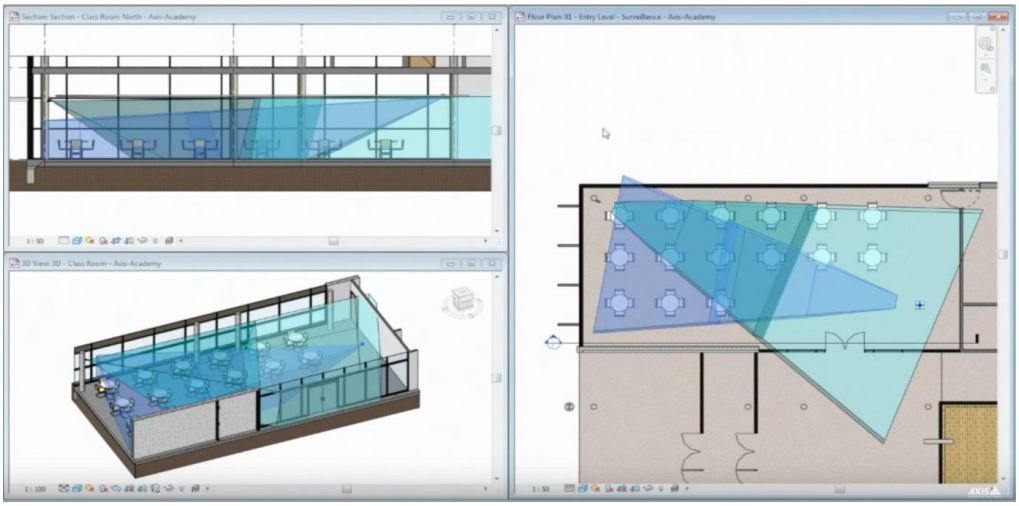

Figure 3Use of the Axis Camera library extension in the program Autodesk Revit [4]

Axis for SketchUp

Software tool SketchUP is a 3D modelling computer program designed especially for the fields of architecture, interior design, construction and engineering. Its benefit is program extension in a set of tools for modelling of camera systems and/or scanned zones. The extension has been developed by Axis Communications (a manufacturer of security cameras). A user can view the scanned area from various viewpoints, as well as the image taken by the selected camera. The following figures show examples of its use.

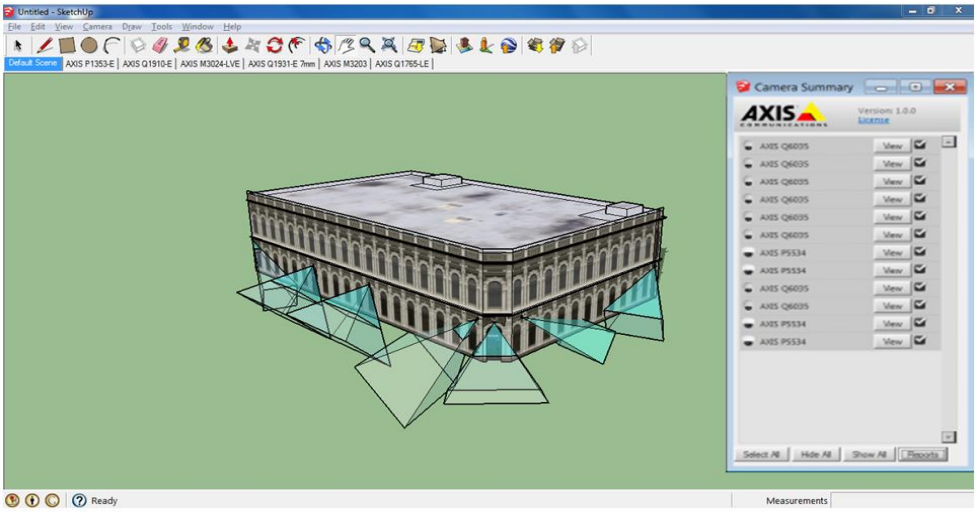

Figure 4 A bank building model and a camera system design in the SketchUP using Axis extension [4]

VideoCAD and IP Video Design Tool

Visualization of protected area coverage by alarm systems enable, among others, specialized software programs such as VideoCAD or IP Video Design Tool. These programs are considered as CAD programs, developed specifically for designing CCTV systems. The programs enable designing objects (premises, buildings, objects) in 2D environment and design location of cameras in these objects. They also enable to set up the spatial parameters of camera installation (height above the floor, angle of inclination, camera rotation - tilting). Furthermore, they enable to set up camera parameters depending on the situation and intended purpose of using the camera (monitoring, detection, observation, recognition, identification).

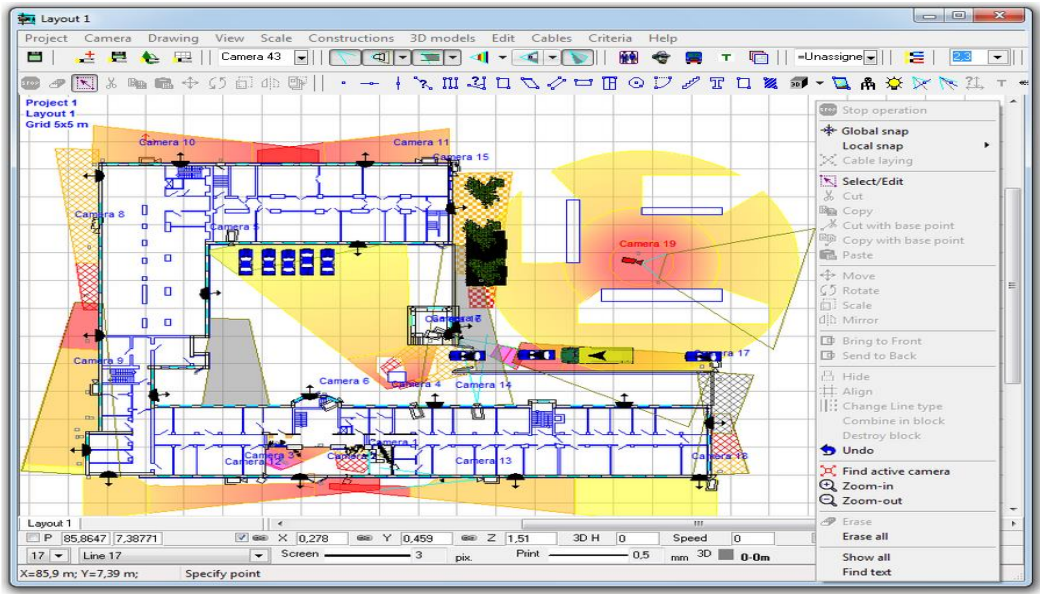

Figure 5The VideoCAD and an example of camera system design [4]

There are also other program tools available, such as programs to calculate length of a supply cable or data storage on a data server, program extensions, programs from alarm system manufacturers, and others that enable to improve the design of object protection systems (e.g. J-Link 1.5.1, IP Camera CCTV Calculator, CCTVCAD Lab Toolkit and other software).

5.2. Software to Assess Effectiveness of Object Protection System

Various tools can be used to assess effectiveness of the object protection system or to analyse vulnerability, for example: SAVI (Sandia National Laboratories, USA) Sprut (ISTA, Russia), SAPE (Korea Institute of Nuclear Non-proliferation and Control, South Korea); and SATANO (Czech Republic, Slovakia).

EASI, ASD, SAVI (Sandia National Laboratories, USA)

These three closely interconnected methods are based on searching for a path with the lowest cumulative detection probability to the critical detection point, and they are intended to evaluate effectiveness of nuclear facilities protection. They use central partition of security areas with a single area of protected interest in the centre of the system, and they are based on knowledge of the security system by the intruder.

According to the terminology used in these methods, a path with the lowest cumulative detection probability to the critical detection point is called the critical path or the path with the lowest cumulative probability of interruption. Detection before the critical point of detection is called timely detection. **EASI** method (Estimation of Adversary Sequence Interruption) enables to calculate the probability of interruption only in one (predefined) path. **ASD** method (Adversary Sequence Diagram) is a method for graphical representation of possible attack paths in the protection system. ASD depicts the object and its protection system as layers separating the external attacker from the target inside the object. Individual physical areas are separated by the protective barrier which includes everything that delays or detects the intruder (Physical Protection of Nuclear Facilities and Materials, USA).

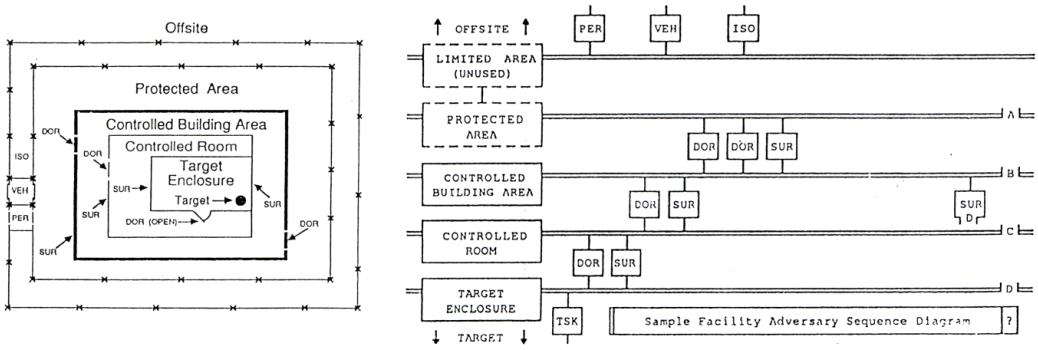

Figure 6Protected area (on the left) modelled by the ASD method (on the right) [22]

Software program **SAVI** (Systematic Analysis of Vulnerability to Intrusion) combines the EASI and ASD methods and evaluates all possible paths to the central area in terms of the probability of interruption (P_I) and creates a list of the ten most vulnerable paths in terms of the probability of interruption (Physical Protection of Nuclear Facilities and Materials, USA). If the interruption probability values are equal, it will sort the paths by the total attack time. SAVI is supplemented with an extensive database of delay and detection parameters of the most frequently used protection measures [21].

SAVI also implements sensitivity analysis. In regard of the most critical parameter being the time needed for the intervention, it is different values of intervention time that SAVI uses as input in sensitivity analysis.

***SAPE** (Korea Institute of Nuclear Non-proliferation and Control, South Korea)*

SAPE (Systematic Analysis Of Physical Protection Effectiveness) is a software program to evaluate effectiveness of protection systems that is based on SAVI and ASSESS methods, but improves them significantly. Instead of the simple ASD, the method uses a new 2D model of a guarded area, as well as a new heuristic algorithm that significantly enhances sensitivity analysis [2].

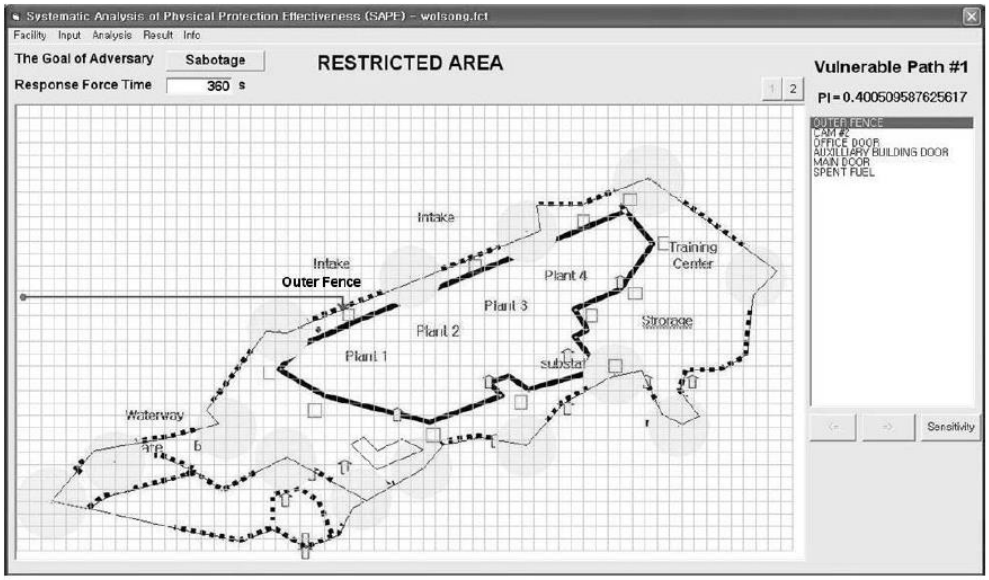

Figure 7 Benefits of 2D maps compared to the ASD are particularly obvious when modelling extensive protection systems [2]

SAPE replaces the ASD method with a two-dimensional map, as the ASD diagram is confusing, complicated to use and gives inaccurate calculations. During transfer through individual areas, a constant value is always added to the total time, regardless of the specific route the intruder chooses (e.g. regardless of the actual point of crossing the fence by the intruder etc.). Compared to SAVI and ASSESS, SAPE significantly extends the sensitivity analysis by analysing all protection measures for the most vulnerable path. The resulting values will then represent the relative effectiveness of updating individual protection measures.

SPRUT (ISTA, Russia)

SPRUT is a software tool developed by ISTA and intended to evaluate efficiency of physical protection of nuclear facilities. The software is used to model a combat encounter of intruders with man guards. A newer version of SPRUT-IM uses stimulation modelling of intruders' penetration into an object to calculate the most effective scheme of resisting an attack. 10SPRUT consists of three parts [7]:

- calculating quantitative parameters of the protection system's efficiency,
- finding the weakest protection spots (analysis),
- determining optimal pathways for intervention (synthesis) [8].

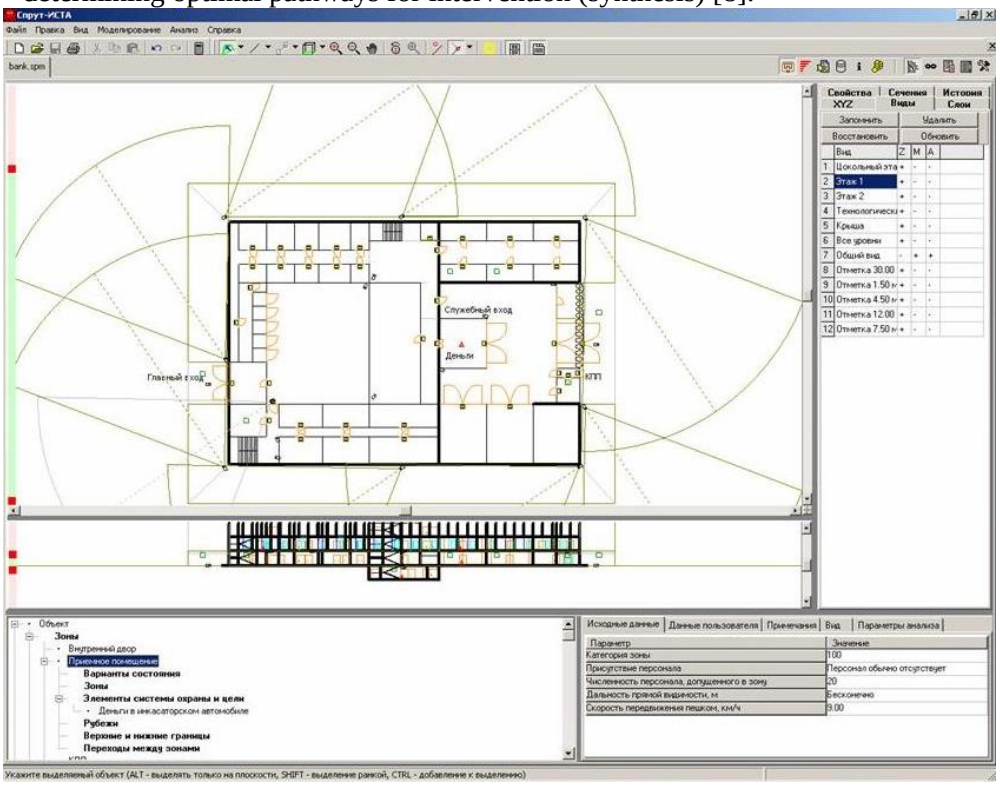

Figure 8 Graphical user interface of SPRUT software [7]

SATANO (TLP spol. s r.o., Czech Republic, The University of Žilina in Žilina, Slovakia)

SATANO (Security Assessment of Terrorist Attack in a Network of Objects) software tool is a simulation tool that enables to quantitatively evaluate level of object protection systems on various 2D map bases.

Figure 9 GUI of the SATANO software tool: Security Assessment of Terrorist Attack in a Network of Objects (Source: authors)

This tool can be used to model physical protection system over any map basis on the relevant scale and thus is, unlike other software tools (such as SAVI), is suitable for any one-storey or multi-storey nodal or linear objects (e.g. airports, administrative buildings).

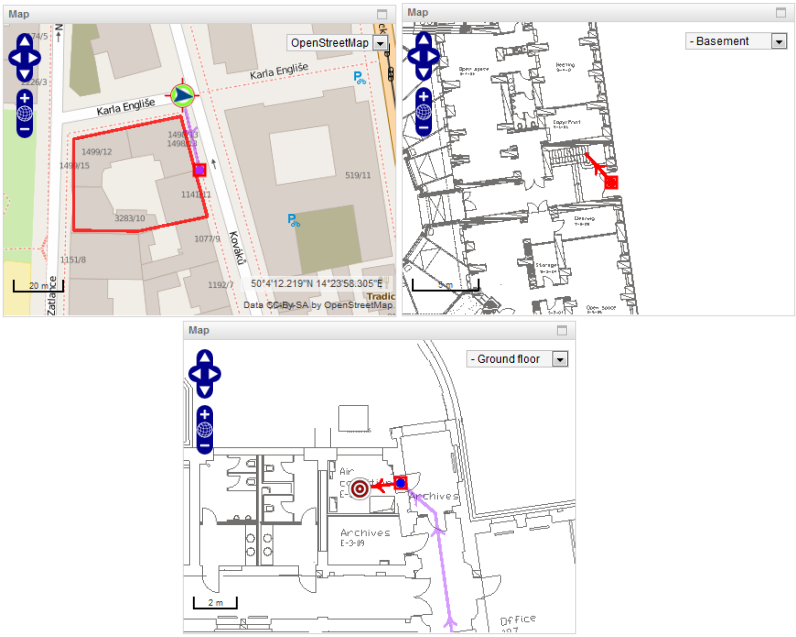

Figure 10 Modelling physical protection system (Source: authors)

Another benefit of the newly created software simulation tool is the option to model detection areas, depending on the alarm system parameters (e.g. I&HAS, CCTV systems) that affect their detection characteristics. Based on relevant parameters of alarm system detection measures, the SATANO enables to model detection characteristics of "2D" (linear detectors) as well as "3D" (CCTV systems, standard PIR detectors, 360° detectors). When needed, it is possible to create a custom detection characteristic.

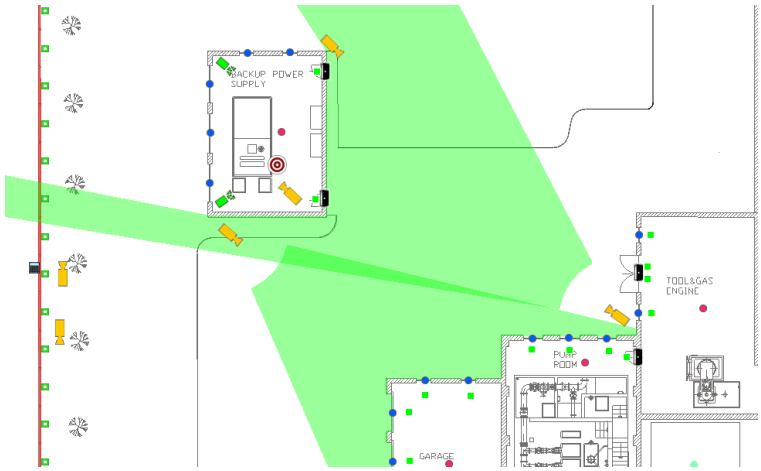

Figure 11 Protected area coverage by detection characteristics of the CCTV system

(Source: authors)

The above mentioned software tools, intended to assess effectiveness of the object protection system or for vulnerability analysis (e.g. SAVI, SAPE, SPRUT, SATANO), differ mainly in the following:

- output parameters interpretation (probabilities, ratios, time data),
- method of inserting input values (predefined input values, input values entered by the evaluator),
- approach to considering accidental effects (deterministic or stochastic),
- intruder's way of making decisions (for certainty or uncertainty),
- method of tracing a path during transfer of the intruder (e.g. ASD diagram and exact trajectory),
- the expected type of attack (destruction/damage or theft),
- method of the guarded area modelling (2D or 3D visualization, input matrix),
- method of using sensitivity analysis.

6. REFERENCES

[1] GARCIA, M. L. 2001. The Design and Evaluation of Physical Protection Systems. USA: Elsevier.2001. ISBN 0-7506-7367-2.

[2] JANGS, S., 2009, Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection (SAPE). IN : Nuclear Engineering and Technology, VOL.41 NO.

[3] LOVEČEK, T. – REITŠPÍS, J. 2011. Projektovanie a hodnotenie systémov ochrany objektov/Design and evaluation of object protection systems. Žilina : Žilinská univerzita v Žiline, 2011. 281 s. ISBN 978-80-554-0457-8.

[4] LOVEČEK, T. – MARIŠ, L. 2015. Efektívnosť systémov ochrany objektov/ Effectiveness of object protection systems. In: Bezpečnostní technologie, systémy a management V. - Zlín: Radim Bačuvčík – VeRBuM, ISBN 978-80-87500-67-5. - S. 64-79.

[5] MACH, V. 2010. BEZPEČNOSTNÉ SYSTÉMY: Mechanické zábranné prostriedky/ SECURITY SYSTEMS: Mechanical barriers. Žilina : Žilinská univerzita v Žiline, 2010. 199 s. ISBN 978-80-970410-6-9.

[6] SELINGER, P, UHRÍN, S. 2003. Bezpečnostné služby/Security services. Žilina: EDIS. 2003. ISBN 80-8070-065-6.

[7] Тарасов Ю. : Специализированные программные комплексы, IN: безопасность • достоверность • информация, № 3 [78] • май— июнь 2008

[8] Николай Р. : Методические аспекты задания требований к антитеррористической защищенности объектов и оценки достаточности осуществляемых мероприятий защиты, IN: безопасность • достоверность • информация, № 3 [78] • май— июнь 2008

[9] DIN EN 16763 Services for fire safety systems and security systems.

[10] STN EN 50130-4 Poplachové systémy. Časť 4: Elektromagnetická kompatibilita. Norma na skupinu výrobkov: Požiadavky na odolnosť súčastí požiarnych, zabezpečovacích a tiesňových systémov, systémov CCTV, systémov kontroly vstupu a systémov privolania pomoci/Alarm systems.Part 4:Electromagnetic compatibility.Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems

[11] STN EN 50133-1 (33 4593) Poplachové systémy. Systémy kontroly vstupov na používanie v bezpečnostných aplikáciách. Časť 1: Požiadavky na system/Alarm systems. Access control systems for use in security applications. Part 1: System requirements.

[12] STN EN 50132-1 (33 4592) Poplachové systémy. Sledovacie systémy CCTV na používanie v bezpečnostných aplikáciách. Časť 1: Požiadavky na system/Alarm systems.CCTV surveillance systems for use in security applications.Part 1:System requirements.

[13] STN EN 50132-7 (33 4592) Poplachové systémy. Sledovacie systémy CCTV na používanie v bezpečnostných aplikáciách. Časť 7: Pokyny na používanie/Alarm systems - CCTV surveillance systems for use in security applications -- Part 7: Application guidelines.

[14] STN EN 50136-1-1 (33 4596) Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 1-1: Všeobecné požiadavky na poplachové prenosové systémy/ Alarm systems. Alarm transmission systems and equipment. Part 1-1: General requirements for alarm transmission systems.

[15] STN EN 50134-1 (33 4594) Poplachové systémy. Systémy privolania pomoci. Časť 1: Požiadavky na system/Alarm systems. Social alarm systems. Part 1: System requirements.

[16] STN P CLC/TS 50398 (33 4597) Poplachové systémy. Kombinované a integrované poplachové systémy. Všeobecné požiadavky/Alarm systems. Combined and integrated alarm systems. General requirements.

[17] STN EN 62676-4 (334592) Obrazové sledovacie systémy na používanie v bezpečnostných aplikáciách. Časť 4: Pokyny na /Video surveillance systems for use in security applications - Part 4: Application guidelines

[18] STN EN 14383-1 Predchádzanie zločinnosti. Územné plánovanie a navrhovanie. Časť 1: Definície špecifických termínov/Prevention of crime. Urban planning and building design. Part 1: Definition of specific term.

[19] STN ISO/IEC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti/Information technology.Security techniques.Information security risk management.

[20] STN ISO 31000 Manažérstvo rizika. Zásady a návod/Risk management. Principles and guidelines.

[21] Analýza účinnosti systému bezpečnostní ochrany jaderných zařízení a jadrných material, 1991, Ústav jaderných informácí/ Analysis of the efficiency of the system for the security protection of nuclear installations and nuclear materials.

[22] Physical Protection of Nuclear Facilities and Materials, Albuquerque, New Mexico, USA

[23] Zákon č. 473/2005 Z.z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene
a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti) / Act No.473/2005 Provision of services in the field of private security.

[24] Zákon č. 483/2001 Z.z. o bankách a o zmene a doplnení niektorých zákonov / Act No. 483/2001 Banks.