Petr Selinger

Technical protection of objects

Security Dimensions and Socio-Legal Studies nr 7, 62-69

2012

Ing. Petr Selinger, PhD.
Department of Security Management, Faculty of Special Engineering, University of Zilina

TECHNICAL PROTECTION OF OBJECTS

Abstract:
The paper examines the issue of technical protection of objects. It deals with outsourcing of various types of electronic means as entry control system, electric fire signaling, camera systems and alarm security systems.

Keywords**:** *Security, protection, property, monitoring, detectors, violator.*

1. Introduction

Technical security systems play a significant role in securing the protection of properties. Their purpose is a permanent monitoring of the protected area and in case of an intrusion of a violator provision of a warning. As they are able to monitor the area permanently, they significantly strengthen the function of human senses. Unlike humans, their ability to capture masking attempts of a violator is permanent. Simply said "an alarm security system is as perfect as perfect its violation detectors are" [1].

In cooperation with physical protection technical means represent the basic security measures for protection of objects. Their aim is to support the implementation of regime measures, improvement of the physical protection, discouraging a violator from his action, prevention of his action and prolonging the time taken up by his attempts to enter the protected object. The protection of critical infrastructure objects involves the same task.

2. Technical systems used in the protection of objects

Generally, the security system involves a purposeful arrangement, use of mechanical and technical means, organization and regime measures and available human resources.

A complex securing of object is achieved by interlinking the elements of:

- classical protection;
- technical protection;
- regime protection;
- physical protection.

The elements of classical and technical protection slow down and subsequently detect the violator and that is why the physical protection is an inevitable component of a complex protection of critical infrastructure objects, ensuring an on time physical intervention and detention of the violator.

a) Means of a mechanical barrier

Means of a mechanical barrier are basic security components of complex protection of integrated security systems. They consist of a system of barriers and obstructions whose purpose is a time delay between the initial moment of object violation and the moment of violation completion. The time range is divided into several phases of object violation.

The protected critical infrastructure object is framed by an appropriate type of mechanical protection system defining the protected perimeter. In this area the security service providing physical protection is usually responsible for tasks which follow priorities and interests associated with the protected object and which are supported by technical means [2].

b) Electronic security systems

Alarm systems signaling violation /PSN/

The range of protected objects is rather large, starting with critical infrastructure objects, common sale, office and stock objects up to bank offices and museum objects. The violation signals are transmitted to the Centre of

registered alarms and by means of a motorized patrol it is possible to make a qualified intervention against a criminal/s/ and in this way to provide the clients with significant property protection [3].

Systems of access monitoring and attendance recording /SKV/

This category embraces various transition tourniquets, transition barriers, electromagnetic locks, gates, railings, electronic readers of chip cards, contactless or magnetic cards, biometrical sensors, etc. These systems are the components of protection of objects concerning their access regimes. Integrated systems of security signaling and access monitoring are increasingly applied as a complex system of object security, where sensors, detectors, keypads, readers, attendance terminals are interconnected in one integrated electronic evaluating and directing module, the central office PSN/SKV.

Systems of electronic fire signaling (EPS)

These systems are focused on early fire warning in the protected area. The signal "fire" and failure signals from these systems can be repeatedly transmitted to the Centre of registered alarms which can immediately take effective measures for property protection [3].

Boards of centralized protection, canters of alarm registrations (PCO, SRP)

The application of these systems enables remote or local monitoring of critical infrastructure objects by means of a telephone line, wireless or radiophone transmission of messages or via a GSM/GPRS network [3].

Systems of industrial television /CCTV/ [4]

Closed television circuits serve mainly as a functional component and a complement to security systems and they represent significant and effective support of physical protection of a object, that is of classical security service. Generally preferred are the applications of digital multiplex proceeding and an automatic non service camera recording with the possibility of remote client access to the camera pictures and recorded files.

The application of camera systems in practice

The camera systems belong to those elements of security systems, purpose of which is first of all to visually verify the information from alarm systems,

subsequently monitor the situation in the protected object and finally to record it if necessary. In certain cases camera systems can be equipped with video detection. It detects the presence of a violator in the protected area and thus supplements the camera system. In practice a combination of camera systems and further active elements is applied. (e.g. PSN, EPS or SKV).

Camera systems combined with PSN

The possibility to interconnect a camera system with an alarm system reporting violation is mainly used for protection of important objects. The use of a camera system as a complement to PSN brings following complementary functions of protection:

- **verification of alarm information** about a violation of the protected object obtained from the alarm system, which enables to minimize false alerts and to check whether the signal from the PSN is caused by a real violator or it is a false alert caused by disturbing influences on the components of PSN;
- **monitoring of the protected object**, which improves global protection because it supplies the employees of physical protection with visual information about the protected object;
- **recording of emergency situations**, which can be later used as a proof material in the decision making process about guilt of the arrested violator. Furthermore, the obtained records can be used in the analysis of activities of people in the protected critical infrastructure object, in the analysis of proceedings of the physical protection during the intervention against the violator or for other purposes.

The combination of alarm systems with CCTV is applied in e.g. in financial institutions, where the camera recording of dispenser sites is interconnected with emergency alerts located in the cash desks. The so called dotation ways and the access to deposit sites are also monitored by cameras. The monitoring has a twofold purpose: on one hand it enables identification of the violator, on the other observing the activity of bank employees. In case of an emergency event it is possible to retrospectively analyze suspicious behaviour of the employees and the process of violation.

Another possibility is the use of the camera system in combination with perimetric protection of the object. In this case, the most important is the information about the situation in the object at the moment of the alert. It concerns most of all moments of alerts possibly activated by animals or weather circumstances. The camera systems are supposed to be equipped with proper direct inputs and in case of PSN with contactless outputs. The connection through a proper communication range is more progressive, typical is the application of the serial collective RS 232. In a practical model of such a combined system it is necessary to design such a constellation of PSN elements and cameras as to have the chosen protected areas secured with the PSN detectors connected with the focus range of the responsible camera.

Camera systems combined with access monitoring system

The simplest example of such a system is the so called videotelephone. The videotelephone is a device consisting of a home telephone with an electronic porter that is complemented with a visual information transmission. The system is usually equipped with a miniature camera with a widescreen lens and lightning in the visible or infrared spectrum. The devices use transmission of the video signal through a common twisted pair of alerting cables. The internal station is provided in twofold variants. The first one uses a 5" diagonal vacuum screen and the picture obtained from it is of relatively high quality but of relatively big dimensions, which causes problems with installation /it has to be either built into the wall or used in a table variant/.

The second possibility is the use of a small screen (approx. 1") complemented with optic for angle projection of the picture to a deflector with a parabolic screen and a B" diagonal. This way the internal station can be relatively flat, it can be installed on the wall similarly to a home telephone. The lifespan of such entrance video porters is relatively short because they are often exposed to damage or theft. A more resistant and also a cheaper way of securing the object entrance is to locate the camera itself outside the reach of the entering person. However, the video porter can bear advantages in some cases, e.g. if a camera sight approximately on the level of eyes is required.

A more complicated variant is the one connecting the camera system with the system of control and management of the entrance of the critical infrastructure objects. It involves connecting the outputs of the access terminal /or terminals/ with alarm input equipment designed for processing and distribution of video signals (camera switcher, quadrant selector, multiplex or cross switcher).

The entry points equipped with access terminal systems will thus be within sight and supervision of the adequate camera during the terminal service. The need of constant watching of the monitor is very exhausting for employees of the security service and with time passing their attention decreases. Therefore it is essential to reduce the reaction of the system only to certain security incidents:

- trespassing of a person without valid permission (the identification element depends on time or place restricted, can be stolen or lent);
- a sabotage of identification terminal (a sabotage of a magnetic card reader, etc.);
- a violent entrance door opening (without using the terminal);
- the entrance door not closing after trespassing of a person;
- the pre-defined time limit for door opening for trespassing of a person was violated, etc.

In case of very important movements it is essential to monitor every (also the authorized) entry of people and to record them [4].

A further variant of securing the entrance of the utmost important objects is a two door entrance. In this case it is also possible to use the camera system for monitoring and possibly also recording trespassing. Via connection to directing elements of the entrance control system with the camera system it is possible to get a live record of a person trespassing. During the rest time the capacity of the recording media is saved by switching back to the chosen sampling regime. In the locations where the entry of authorized people as well as monitored entrance of unauthorized people (visitors) is assumed it is possible to complement the standard entrance monitoring system with remote operation from the security staff location [4].

Other instrumental systems

This category embraces most of all the detection and signalling of gas outflow, user PC systems concerning security applications, paging systems, implementation of telephone lines, home audio and video phones, etc. [3].

3. Conclusion

The protection of objects contributes to development and to elimination of failure points and areas, it improves consistent cooperation between owners, administrators, the state and municipal authorities, supports cooperation between individual systems and subsystems and the existence of reserve and supplement elements of the critical infrastructure. The protection measures are differentiated and adequate for the level of potential danger.

The following devices belong to the basic devices of protection system designed for protection of critical infrastructure elements:

– devices for prevention of threat, legal norms and technical requirements, system of securing and security documentation, regime measures for the element, alert system of authorities and population, autonomy of the element, etc;

– devices for reduction of the risks for the existence and stability of the element, technical means of protection, physical protection, protection plans, media activity, activity of public authorities including prosecution and courts;

– devices for averting an attack on the element or its protection system, intervention of security service, intervention of armed security authorities, intervention of armed forces, intervention of the allies of armed forces, etc.;

– devices for elimination of attack consequences, outsourcing of reserve equipment, connection to functional systems, renewal or replacement of the damaged elements, application of directive state force devices, establishment of health care plan, feedback to ZHN, etc. [5].

Bibliography

1. Zakon c. 45/2011 Z. z.: O ochrane kritickej infrastruktury (in Slovak). [Law no. 45/2011 of Coll. on Critical Infrastructure Protection].
2. Lukas, L. et al.: *Bezpecnostni technologie, systemy a management* I. (in Czech) [Security technology, systems and management I.], VeRBuM, Zlin 2011, ISBN 978-80-87500-05-7.
3. Velas, A.: *Elektricke zabezpecovacie systemy* (in Slovak), [Electric Security Systems], ZU Zilina, 2010, ISBN 978-80-554-0224-6.
4. Lovecek, T.: *Kamerove bezpecnostne systemy* (in Slovak), [Camera Security Systems], ZU Zilina, 2008, ISBN 978-80- 8070-893-1
5. Senowsky, M., Senowsky, V.: *Zakladni otazky kriticke infrastruktury* (in Czech). [Basic Issues of Critical Infrastructure], In. *SPEKTRUM,* No.1, 2007, VSB-TU Ostrava. Priloha: Ochrana kriticke infrastruktury, pp. 2-4. ISSN 1211-6920.