Physical Protection and Critical Infrastructure Protection in the Czech Republic

L. Necesal, L. Lukas

***Abstract*—** Approaches of Physical Protection are used beside the protection of commercial buildings to protect objects and systems with national and international significance, therefore to Critical Infrastructure Protection. In the introduction of this paper are presented threats that are perceived as important and which should be reduced mainly through critical infrastructure protection. Main point of paper is to present systems that belong to the physical protection area and that are used in the protection of critical infrastructure element. The most commonly used systems, their brief definition and delimitation of their contribution to the protection of critical infrastructure are introduced. The end of paper summarizes other measures that can be used in combination with physical protection systems to protect critical infrastructure.

***Keywords*—** physical protection system, critical infrastructure, protection, alarm system.

I. Introduction

THE issue of critical infrastructure protection is the science theme for several decades, at least since the 70 the last century. This issue is more strongly emphasized in the context of the integration of the Czech Republic into the transatlantic structures (NATO) and the process of European integration primarily to the late 90 years in the Czech Republic. That term critical infrastructure is nowadays a phenomenon that penetrates through the whole range of industries horizontally.

Critical infrastructure could be viewed as a central nervous system of modern society. Services covering not just basic needs but also providing national security and economic development are provided its citizens through critical infrastructure protection. Not only for this reason, it is important to ensure its functionality in any situation. The importance of critical infrastructure is growing at the time of extensive emergency when the large number of people and significant areas are affected. In a crisis, among others, extending the necessary support for folders and create the conditions indispensable for the survival of the affected population.

This paper was supported by the Ministry of Interior of the Czech Republic under the Research Plan No. VG20112014067 and by the Ministry of Education, Youth and Sports of the Czech Republic under the Research Plan No. MSM 7088352102 and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/ 03.0089 and by the Internal Grant Agency of Thomas Bata University in Zlín No. IGA/FAI/2012/010.

The obligatory legislative document regulating the matters of critical infrastructure protection is a EU directive 2008/114ES "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (hereafter "directive") passed on December 8, 2008. This directive represents the first stage of the European programme for Critical Infrastructure Protection (EPCIP).

The Czech Republic, as a member state of the EU, implemented this directive in its legislation in December, 2010 by creating the amendment 430/2010 Coll. of the act 240/2000 Coll. (Critical Act) and determines new obligations when dealing with critical infrastructure protection (CIP).

Currently, in the context of this amendment, the process of identification and designation elements of critical infrastructure is completed. The provisions that the protection of critical infrastructure owner/operator should accept (even for European Critical Infrastructure - ECI, even for National Critical Infrastructure - NCI) are not regulated/defined by the existing legislation (whether European or national). This paper presents a system of physical protection which uses both private and public sector for protection of critical infrastructure elements.

Critical infrastructure protection as a priority to ensure the society operational continuity from the economic and social terms is considered. The essential elements, links and streams of the state system which are the basis ability of state to achieve stability in every situation and start further development under normal, abnormal and critical conditions in operation have to ensure an observance of these functions. The specific interests in protecting critical infrastructures are as follows:

- reduce vulnerability,
- to protect people and critical resources and systems on which the existence of society is depended,
- creating conditions for prevention and ensuring preparedness to manage disruption of critical infrastructure as part of the development program,
- the security of citizens' rights to fair assistance in case of disruption of critical infrastructure and ensure their awareness of the proposed provisions to solve crisis situations, their responsibilities and how they could help in the prevention and how they should react to the situation.

To ensure all of these interests, the deployment of elements and system of physical protection could be used. The specification of these systems in the next chapters is presented.

II. Threats for the basic needs of human society

Critical infrastructure elements could also be viewed as objects of special importance implying the need to address safety issues of these elements from a wide range of threats. These could be caused not only by adverse natural phenomena and technical defects but also by security threats that could be perceived as illegal activity which is motivated by diverse motives (eg, revenge disgruntled employee or customer, movable gain the visibility).

As a result of the existence of international dependence and linking different areas of critical infrastructure, disruption of critical infrastructure of one area could have influence on other areas and may have international impacts. As an example, could be present disruption of electricity, gas, fuel or failure of telecommunication networks. Therefore, the critical infrastructure protection requires public authorities to share responsibility with the private sector and exchange of information between public authorities and other relevant organizations and international cooperation.

There are a number of threats, which may lead to disruption of critical infrastructure (CI) in the Czech Republic. These include the following:

1) Internal problems on objects and in CI systems, whereas the causes of disruption of functions may not be directly affected by the competent subject or objects:
- technological accidents,
- technical failure, lack of spare parts,
- shortages of energy (electricity, gas, heat, fuels),
- disruption of water supplies,
- shortages of raw materials (components) for the production or provision of services,
- collapse of computer networks.

2) Internal problems with subjects and in CI systems, whereas the causes of disruption of functions are directly or indirectly affected by a competent object or objects:
- Temporary change in orientation (priority) to provide goods and services in order to deal with emergencies (non-military crisis management and military).
- Long-time or permanent change in orientation (priority) to provide goods and services due to management's decision to subject of CI (can also be influenced by involving of organized crime into companies).
- "Collapse" of the company from economic or other reasons (strike).

3) External reasons:
- Disruption of object of CI due to natural disasters or industrial accidents in a "neighboring object".
- Disruption of object of CI cause by human (terrorist attacks, criminal acts, the consequences of war).
- Deficiency (decrease) in the workforce, including increased morbidity (pandemics, infectious diseases), such as refusal to work for example by solving their problems related to the creation of extraordinary events.

III. Physical Protection

Physical protection in the CIP area is mostly provided by organization from commercial security industry – CSI (in some cases, the physical protection by the owner/operator separately is provided). The physical protection of any property (buildings, equipment, object, etc.) is created by combining and mutual of these three basic components: Physical Protection Systems (PPS), respons team, regime protection.

1. Physical protection systems – are divided into two basic areas of mechanical barrier systems and technical protection systems.
   a. Mechanical barrier systems are: safe doors, interlocking systems, fence, safe box, etc.
   b. Technical protection systems are: Intruder and / or Hold-up Alarm System (I&/orHAS); Video Surveillance System; Fire Alarm System (FAS); Access Control System (ACS); Mechatronics System.

In connection with the use of a complex system of physical protection three main functions of these parameters and its subsystems are considered:
- Detection - primary we detect intruder using technical protection devices (AIR, PIR, MW Bistatic, Monostatic MW, dual sensor ... etc.) and verify the alarm information using a Video Surveillance System.
- Delay - secondly we need to slow intruder. For this function we use mechanical barrier systems (fences, gates, grilles, security doors, windows and other)
- Response - finally we interrupt or arrest the intruder by the response team.

These basic functions are useful consequently and formulate the structure of the physical protection of elements of CI significantly.

2. Response team/activity - can be carried out by own resources, security, private security service employees or by police or army. This type of protection is expensive but very active and effective. Core is a response of a human element to impulses related to danger / security disruption / object protection such as: breaking in, technological breakdown etc. Impulses for a response team reaction are carried out by an alarm system.

3. Regime protection/measure – consists of a compilation of administrative and organization measures for securing protected interests and values. Generally considered the most important are:

a. Input and output mode of persons and vehicles that the access control of employees, clients, visitors and foreigners to the building and its parts, control of persons and vehicles leaving the building, the eligibility of objects and materials exporting is included. Mode movement of employees in the building that the designation of part of the building with restricted accessibility for employees to designation membership of a particular premises, workplaces, etc. is included.
b. The procedure for receipt, storage, moving expenses materials according to the material and shipping arrangements is determined. The property against theft, damage and degradation is protected by this procedure.
c. Operating mode by which the smooth and safe operation and activities in emergencies is ensured.
d. Key operation mode by which the marking, assignment, transfer keys, their mode of application, production of spare keys, replacement locks in important parts of the building, etc. is determined.
e. The operating mode that with the operation of technical protection systems is connected.

A. Mechanical Barrier Systems (MBS)

The term MBS mean all the mechanical elements and components that make violent intrusion difficult for perpetrators into the protected space. Mechanical protection is a set of mechanical and technical equipment, facilities and components that by their structure or mechanical strength prevents intruders their easy overcoming. Each barrier system is beatable, however it differs in time that the offender has to spend in overcoming it, especially the amount of spent energy, time and technical level of tools or instruments for overcoming them. MBS are the basic structural element of building security from which other concept of protection is further depended. MBS is divided into three categories according to the subject, object or a perimeter.

The concrete MBS can be follows: safety locks, grilles, security film, security and toughened laminated glass, safe, safety deposit boxes.

B. Intruder and / or Hold-up Alarm System (I&HAS)

I&/orHAS in the terminology of the Czech Republic earlier referred as an Electric Security System (ESS). I &/or HAS is a "combined system designed to detect intrusion alarm and panic alarm" [2]. Alarm system can have a function as an Intruder Alarm System (IAS) or Hold-up Alarm System (HAS). Mostly it combines both these features together so that we talk about Intruder and Hold-up Alarm System. Intruder Alarm System is an alarm system designed to detect and indicate the presence, entry or trial of entry of an intruder into guarded areas. Hold-up Alarm System is an alarm system that allows purposeful creation of alarm situation if attack comes.

Another part of this paper deals with the I&HAS. However, the vast majority of today's systems allow both mentioned functions ("security" and "emergency"), in consequence the following text, it is possible to perceive as generally valid for I&HAS.

The purpose of I&HAS is to increase the safety / protection of guarded objects / items against theft, damage, attack, etc. It should be noted that I&HAS only "detects indicates signals and transmits the information". The system is not able to implement action against perpetrators of this crime, it means for example the detention of the offender. Here we encounter not only the legislative obstaclesTherefore, it is necessary to establish on the I&HAS components of physical protection to implement a robust.

By combining I&HAS with classical protection (mechanical barriers systems) it is possible to push the limits of intrusion detection of the protected area / object etc., to the level of the pre-alarm. Namely the state where it could be highlight on physical protection component of non-standard situation and thus to prepare it for possible intervention even before the perpetrator for example enters the building. This option is significant by I&HAS higher security levels.

The level of security system of I&HAS depends on the desired level of security provided for in safety assessment of the building. The degree of security system / subsystem component corresponds to the I&HAS with the lowest level of security contained therein. EN 50131-1 standard defines four security levels: low risk, low to medium risk, medium to high risk, high risk.

I&HAS is usually composed of at least the following components: main board (with backup power supply), detectors, signal elements (equipment) and elements for the transmission of alarm information. The current systems manage well the problems of false alarms and allow the remote management and integration with other systems of technical protection.

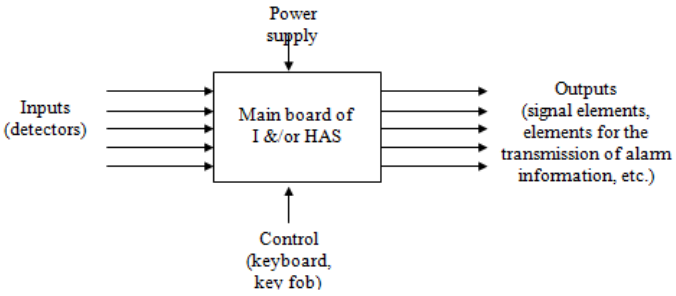

Fig. 1 Scheme of I&HAS

Between the signaling elements belong an outdoor siren, internal siren, strobes, as well as a GSM phone, pager, etc. The elements for transferring alarm information are now often integrated into central panel board (eg, GSM module, a module for communication on telephone network). But even today it is possible to find on the market these elements to transfer alarm information as a separate device. This basic configuration is commonly accompanied by extension elements that allow interconnecting with other systems or

extend their functionality (printers, remote message via LAN/ WAN, wireless communication, etc.).

In the field element protection of CI it is possible to use I&HAS mainly in property crime prevention and protection against terrorism. In these areas risk of critical infrastructure facility could be minimized to a minimum by appropriate combination with other alarm systems. By deployment of I&HAS could be eliminated internal and external risks disruption of CI associated with human influences.

The Centre of I&HAS performs the following functions:

- receives and evaluates the output signals from the detectors,
- allows control of I&HAS by controls elements (keyboard, wireless keyfobs, etc.)
- control signaling, transmission, recording and other devices that indicate the status of I&HAS,
- powered detectors and other elements by electricity,
- allows diagnostics of I&HAS system.

C. Video Surveillance System (VSS)

There is still used the old name "CCTV system" or "CCTV surveillance system in the Czech Republic. Abbreviation CCTV means Closed-circuit television. This technology has almost not been used yet. VSS underwent huge development in recent years - in the acquisition, processing, transmission as well as store visual information. The main contribution to this has the IT branch with which are the VSS more and more interconnected in recent years.

VSS includes a minimum: cameras, imaging and other additional equipment needed for signal transmission and in monitoring the operation defined zone, scene, space. Today VSS for example is able to detect the offender, deferred object, etc.; alert service, store and transmit information to other alarm systems, etc.

VSS can significantly contribute to the protection of critical infrastructure against property crime, terrorism, technological accidents and also natural disasters. VSS are deployed ideally in combination with other alarm systems, especially with I&HAS and ACS which can compensate some of their weaknesses and extend their capabilities appropriately. By deploying camera systems it is possible to eliminate the risk of security breaches associated with both CI human influences and technological accidents or natural disasters.

D. Fire Alarm System (FAS)

The basic task of FAS is early detection of the primary symptom of fire, reporting the event operation of the system, warning of the risk incurred and the activation of other fire safety devices that prevent the spread of fire, making it easier to dispose of or carry out the self-destruction. Another task of FAS is the detection of alarms / forwarding information on the fire people who may be in the building threatened by fire. FAS is the only system of technical protection which reports directly to national supervision under the Law on fire protection.

The usage of FAS is in the field of protection of element CI against the risks associated with technological and industrial accidents and terrorist attack. Therefore, they can provide some protection both from some internal and external risks.

E. Access Control System (ACS)

The main aim of ACS is management, control and protection of access to sections, objects and their individual parts. Each person is allowed or denied access to such guarded areas on the basis of various identification signs. The identification of the most commonly used access cards, chips, tokens or biometric data. ACS decided on the basis of access rights which are assigned to the person. These rights allow it, or not allow transit through the access interface (doors, turnstiles, gates, barriers, etc.). Such a passage, but his attempt is recorded in the ACS software. ACS collaborates with other technical systems of protection.

By using the ACS it is possible to protect persons, property both inside and outside of the protected area, information, and it especially against property or other crime, terrorism and other acts of violence. ACS thus reduce the risks associated with both some internal and external challenges of CI elements and systems.

F. Mechatronics System

Mechatronics is the combination of mechanical engineering, electronic engineering, computer engineering, control engineering, systems design and engineering to create useful products.

Mechatronics system (in the commercial security industry) uses a combination of mechanical barrier system and alarm systems as an integrated complex. Among the mechatronics systems belong especially electronic locking doors, barriers, turnstiles, combined electromechanical (electromotive) locks and lock systems, electronic door openers, and a combination of sophisticated extensions using IT and other technical systems of protection.

As already mentioned, mechatronic systems, in combination with alarm systems (I&HAS and for example, ACS) or as separate elements, systems of technical protection are used. It means that the usage in the field of protection of elements CI depends on the system with that are used or other similar alarm systems.

IV. Other Measures for Critical Infrastructure Protection

It is necessary to deal with the CIP issues as a complex system because with critical infrastructure protection (as well as with security in general) it applies that a system is as strong as its weakest link. This means that the individual measures for CIP (the ways of protecting the CI) must be balanced, intertwined and complementary. Other measures which are used (and can be used) for protection of the CI are described in the following chapters.

A. *Risk and crisis management*

The strategy for risk and crisis management constitutes a systematic process and consists of five phases representing the necessary scope of process-based risk and crisis management in a private enterprise or a government authority. The five phases are as follows: 1. preliminary planning to establish a system of risk and crisis management; 2. risk analysis; 3. specification of preventive measures; 4. implementation of a system of crisis management; and 5. regular evaluation of phases 1 through 4. The Fig. 2, illustrates this strategy and shows the process in the form of a chart [15].

As described in A guide of Ministry of the Interior of Federal Republic of Germany: Protecting Critical infrastructures – Risk and Crisis Management [15], risk and crisis management is based on a general "plan – do – check – act" (PDCA) management cycle. This allows it to be incorporated into existing management structures such as quality management, existing risk and crisis management, or process management. The term "organization" refers in this paper to private enterprises or government authorities which operate critical infrastructures as defined above [15].

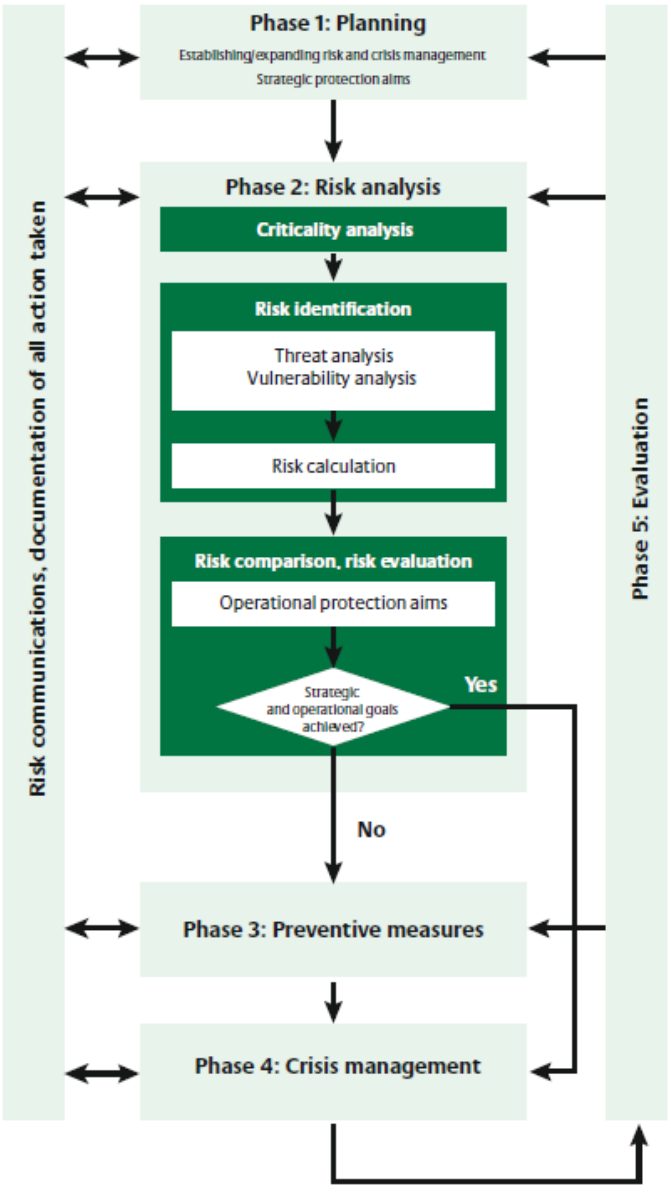

Fig. 2 The five phases of risk and crisis management [15]

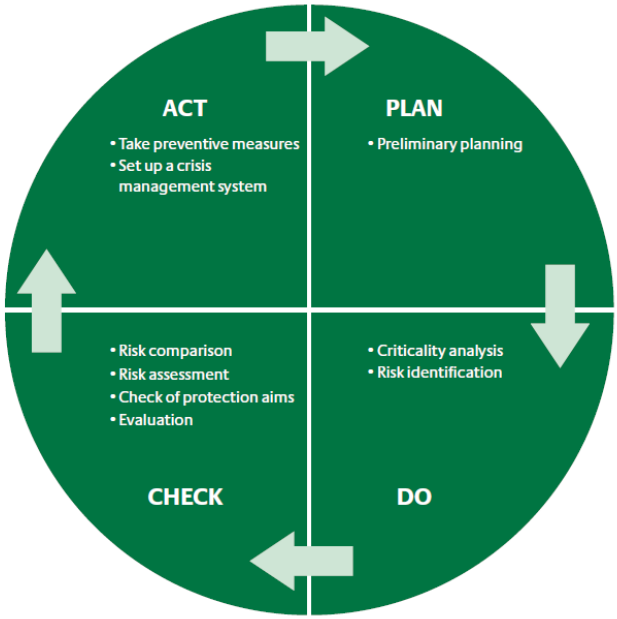

Fig. 3 The process of risk and crisis management based on PDCA [15]

B. *Business continuity planning*

Nowadays, every society is exposed to a great amount of a variety of risks and possible threats whose effects can completely annihilate its hard-gained state. This risk is even bigger with companies which are the owners or keepers of critical infrastructure.

Modernly-run organizations pay still more attention to Business continuity planning (BCP). The ability of an organization to renew its key processes is dependent on the advancement of its BCP program. Organizations which do not have BCP have only a very little chance of full recovery after a exceptional event. One of the main outputs of the BCP is a Business continuity plan – an essential document defining strategy of solving critical and exceptional situations.

BCP may be defined as a compilation of activities (Fig. 4) focused on decreasing the risk of collision emergence and restricting impacts on critical company processes. It is important to realize that the continuity planning is not only a plan of a response to a critical event but also includes an important precautionary aspect. One of the main outputs from this process is Business Continuity Plan. Good quality continuity plans are capable of minimizing the consequences of exceptional events and at the same time enable and accelerate the actuation of operation into a standard condition.

Good quality of the continuity plans should be a strategic aim of any organization – from big multinational organizations to small or middle businesses. Although the measure of employing specific technologies will be different in different types of organizations, it is necessary to keep the main principles of a life cycle of continuity management when designing the continuity plans. Among them are namely a good quality analysis, testing and regular maintenance. All individual measures must be intertwined but with BCP and Risk and crisis management it applies doubly.

Fig. 4 BCP & IT Security [16]

C. IT security

Dealing with IT security is a cross-cutting discipline that impacts all parts of information system. The aim of the solution is to determine rules and subsequently ensuring their observance, eventually enforce them. The reason for a proactive approach to the IT security is namely the fact that the expenses spent for precaution of security incidents are significantly lower than expenses related to eliminating their impacts.

The main elements/parts of IT security are intertwined with other measures for critical infrastructure protection. Therefore it may seem that the individual elements/parts of IT security repeat in other measures. But even that is an incorrect understanding of this problem. As it has been mentioned before, the measures for critical infrastructure protection are based on a complex approach to security. That means that there is created for example one security policy within the company which, however, includes all measures from Risk and crisis management to Physical protection. The main elements/parts of the IT security are:

- Security policy - defines the basic rules and requirements with the aim to ensure the protection and security of information in an organization. After approval of the management serves as a binding regulation for employees.
- Management of a physical access - ensuring of the physical access to key components of the IS for personell only, including the option of supervision. This area is intertwined with Physical protection systems.
- Folder services, authentization and authorization - central database of users, enabling the management of their identification and access data, including logging in and access monitoring. A potential expansion can be systems for identity management, single sign-on or systems for multi-factor authentization.
- Security supervision and management system – an important element of security which enables gathering information about events from various systems, unifying them into one place and subsequently evaluating them.
- Invasion checking – all operational activity or measures within security must be checked from the perspective of keeping the defined security policy or the occurrence of vulnerability - compliance monitoring, vulnerability scanning and penetration tests.
- Antivirus protection – often makes up the base of IS security. It is important to build one or more barriers into the potential route of a dangerous code in a direction of the organization's information system – so called multi-layer antivirus protection. The essential element is central management and monitoring of antivirus solution and further protection against new kinds of attacks (combined attacks, phishing, spyware, installers, rootkits etc.)
- Protection for the web's perimeter – used for the web's separation from web's of other subjects and public webs. Often composed of firewall, IDS/IPS sensor, content filters, antispam and antivirus protection.
- Content check - namely filtering the content on the web's perimeter with the aim to eliminate unwanted content when transfering into the organization's web or the other direction.
- Data encryption - a system to prevent tampering with data, their possible theft or modification. It is used to protect data stored on disk storage, removable media and communication through untrusted networks. In particular, these are systems for online disk encryption, file systems, parts, electronic mail, symmetric and asymmetric encryption of data streams.
- Protecting mobile devices - the use of portable equipment requires special emphasis on security, because these devices beyond the standard understanding of perimeter protection in computer networks. Their mean antivirus protection, personal firewall, an IDS sensor, anti-spyware, encryption of locally stored data, multiple factor authentication, secure remote access, protection of insertion into the LAN, backing up data stored locally.

D. Personal and administrative security

In this area which observes the "life cycle of an employee", the security measures can be divided into those that are made before the employment relation emergence, during the employment relation and after the employment relation's termination or alternation.

The basis of personal and administrative security is determination and subsequent documentation of security roles and responsibilities according to requirements of the company security policy. In order to ensure an adequate level of security, it is necessary to carry out inspections with the new employees. That includes simple techniques such as identity verification according to documents, verification of education or training documents, etc. A higher level can be carrying out of a personal profile analysis, reference verifying or business register check or insolvency register. The highest form can be proving integrity on the basis of the extract from the crime register or other special methods. Herein, when verifying, it is necessary to pay attention to the fact that all activities are carried out thoroughly in accordance to the effective laws. The last stage of accepting an employee is negotiating exact conditions for work, which should also include a specification of an employee's responsibilities and duties in regard to maintaining security.

For the development of personal security during the employees' activity in an organization, three safety measures are important:

1. Senior employees' responsibility – including acquainting subordinates with safety rules and their motivation to following these rules.
2. Broadening the security consciousness – realized via schoolings, seminars, trainings and other educational activities. The aim is to project the designated rules into actual behavior of all employees, which is a very difficult and everlasting task.
3. Disciplinary proceeding – meant for situations when the designated rules have been broken. The aim is to discipline and draw attention to detected misconduct. With subtle misconduct, oral reprehension is enough. More serious issues could result in financial sanction, change of position and in extreme cases even in termination of the employment relation or lawsuit.

The last stage of the employee's stay in the organization is the termination of his/her employment relation. Procedures connected with a change of position should be designed in a similar way but they are usually not so strictly regulated and watched. The main security measure is a clear and unequivocal determination of responsibilities related to the termination of the employment relation. The primary issue is to co-ordinate relations between human resources and line managers. In relation to the leaving employee it is important to draw attention to the fact that his obligation of reticence continues even after his employment relation termination. Another measure is returning of all borrowed devices. The most difficult issue here is data deletion on private devices of the employee. The basic task of employees involved in the working of information and communication technologies is locking and deletion of access accounts and closing of all access routes into the organization for the leaving employee. That includes the area of physical protection.

V. Conclusion

This paper presents an overview of physical protection systems which fall into the commercial security industry. The commercial sphere is mentioned. However, many of these systems to the highest degree of risk are certified. Systems that fulfill the highest safety category levels in banks, military bases, government institutions, etc. are commonly used. Therefore, there is no problem in using these systems in the CIP area on the specific elements of critical infrastructure, for example power plant, transportation system, etc.

They could be on many of these elements commonly use, the protection of buildings or facilities involved in the functioning protection of CI is mentioned. The risks associated with internal problems of CI objects (failures, accidents) and risks associated with external reasons (terrorism, natural disasters) are eliminated by PPS.

However, the requirements for such systems deployed to protect critical infrastructure element CI is not regulated by the current legislation (or technical standards used as guidelines). In practice, each CI subject solves its own security standards. In the Czech Republic subjects of energy area try to reach consensus in cooperation with the Ministry of Industry and Trade at least. The mentioned consensus is in the standards of safety of CI subjects. Approaches presented in this paper are identic with the standards of individual subjects.

In subsequent phases of the CIP the harmonization of standards, norms and legislation in this area should be taken into account by not only national but also international entity.

References

[1] *Green Paper on a European Programme for Critical Infrastructure Protection*, The Official Journal of EU, November 2005.

[2] ČSN EN 50131-1 ed. 2. *Poplachové systémy- Poplachové zabezpečovací a tísňové systémy- Část 1: Systémové požadavky.* Praha: Český normalizační institut, 2007. 40 s.

[3] *Communication from the Commission COM (2006)786 on a European Programme for Critical Infrastructure Protection*, The Official Journal of EU, December 2006.

[4] *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, The Official Journal of EU, December 2008

[5] *Law 430/2010*, The Collection of Laws of the Czech Republic, Vol. 2010, December 2010

[6] *Government Regulation 431/2010*, The Collection of Laws of the Czech Republic, Vol. 2010, December 2010

[7] *Government Regulation 432/2010*, The Collection of Laws of the Czech Republic, Vol. 2010, December 2010

[8] M. L. Garcia., *The Design and Evaluation of Physical Protection Systems*, Second edition, Sandia National Laboratories, 2007.

[9] I. Beneš, "Critical infrastructure," *Vesmír*, vol. 85, no. 12, p. 719, December 2006.

[10] I. Lauberte, E. Ginters, " Agent-Based TemPerMod Simulator Cell Architecture," 13th WSEAS Internationa Conference on Automatic Control, Modelling & Simulation (ACMOS´11), Recent Rechearches in

Automatic Control, Lanzarote, Canary Islands, Spain, pp. 75-79, May 2011.

[11] L. Lukas, M. Hromada, "Utilization of the EASI model in the matters of critical infrastructure protection and its verification via the OTB SAF simulation tool," *13th WSEAS International Conference on Automatic Control, Modelling & Simulation (ACMOS´11)*, Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, pp. 131-136, May 2011.

[12] L. Lukas, M. Hromada, "Management of Protection of Czech Republic Critical Infrastructure Elements," *13th WSEAS International Conference on Automatic Control, Modelling & Simulation (ACMOS´11)*, Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, pp. 306-309, May 2011.

[13] L. Necesal, L. Lukas, "Entities of critical infrastructure protection," *13th WSEAS International Conference on Automatic Control, Modelling & Simulation (ACMOS´11)*, Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, pp. 383-386, May 2011.

[14] L. Necesal, L. Lukas, " Critical infrastructure protection and role of infrastructure owners/operators," Annals of DAAAM & Proceedings 2010, The 21st DAAAM WORLD SYMPOSIUM, Zadar, Croatia, pp. 1323-1324, October 2010.

[15] A guide risk and crisis management CIP,Ministry of the Interior of the Federal Republic of Germany, 2007. Available : http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.html?nn=106228

[16] eSecurity. (2012, July 15). Business Continuity, Disaster Recovery Planning [Online]. Available: http://www.esecuritytogo.com/ccpage.aspx?pageid=6&name=Planning&lid=10&lgid=1

[17] L. Necesal, M. Hromada, "Physical Protection Systems and Critical Infrastructure Protection in the Czech Republic" *1st International Conference on Automatic Control, Soft Computingand Human-Machine Interaction (ASME´12)*, Porto, Portugal, July 2012.

Ludek Lukas - (LTC ret.) was born in 1958. He graduated university studies in 1981 at Military Technical University in Liptovsky Mikulas (Slovakia) and doctoral studies in 1993 at Military Academy in Brno (Czech Republic).
During his working at the Military Academy in Brno (1991 - 2005) he held the function of lecturer, group leader, head of department and vice rector for study affairs. He currently works at the Tomas Bata University in Zlín as associate professor. His scientific research, publishing and educational activities are focused into area of C2 communication and information support, information management, physical security and critical infrastructure protection.

Lubos Necesal - was born in 1985. In 2009 completed a master's degree in security technologies, systems and management at the University of Tomas Bata in Zlin, where he currently serves as an internal PhD student. The objects of his interest in the critical infrastructure protection are Physical Protection Systems.