Measures for Critical infrastructure protection

Ludek Lukas, Lubos Necesal

***Abstract*—** Methematical models and methods are applied across different scientific fields. Including the issues of critical infrastructure protection (CIP) which has come forward in the interest of EU in the last decade. In order to understand the broader connections and the present state of CIP, the article speaks of the contemporary process of marking and identification ECI and entities which are (or should be) included in this process – specifically in Czech Republic. The main aim of the article is to introduce the measures for the critical infrastructure protection. These measures often use a mathematical apparatus, namely in the field of determining threats, evaluation of risks and forming of exceptional events etc. The purpose of the article is not only to list the mathematical models, tools or methods used but to introduce the issues of critical infrastructure protection and open areas, in which these models, tools and methods can be used.

***Keywords*—** Critical infrastructure protection, measures, physical protection, risk and crisis management, identification and designation of ECI.

I. Introduction

IN every society/country, several infrastructures (at least the state's infrastructure itself) can be defined. These infrastructures have a different meaning to the functioning of a state – known as criticality of infrastructure. In an ideal world, the country would guarantee trouble-free function of its infrastructures. Nevertheless, it is impossible to reach such state in real world. The main reason of this is the change of human society in the last few centuries. In the past, the society was significant with its reserve behaviour (city walls, gates, etc.) and its resistance (self-sufficient infrastructure – source of water, own services, stores of food etc.). Today's metropolises are different – open, not limited by walls and/or borders and interconnected with centralized systems of infrastructure and trade links of the globalized world. This applies not only for European cities but for the whole European community – the European Union. The interconnection of particular technologies, infrastructures and countries brings not only advantages but also disadvantages, such as dependence and vulnerability. Recently we have seen the possible threats endangering present countries e.g. terrorism, natural disasters, negligence, accidents, hacking or felony. These threats are not limited by international borders which was demonstrated during terrorist attacks in the USA (September 2001, New York), Indonesia (October 2002, Bali), Spain (March 2004, Madrid) and in the United Kingdom (June 2005, London) [13].

It is because of these reasons why it is important to distinguish the significance (criticality) of particular infrastructures for society and secure their functions according to their significance and protection not only on a regional basis. Effective protection needs communication, coordination and cooperation on national, European and (in a case of need) worldwide level among all involved subjects. The European Union has been dealing with problems of current critical infrastructure (CI) and critical infrastructure protection (CIP) since the beginning of the third millennium. The Council of EU requested the preparation of overall strategy for enhancing protection of critical infrastructures on a meeting in June 2004. In response, on 20 October 2004 the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures [3].

The Council's conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" adopted by Council in December 2004 endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP).

The matters concerning critical infrastructure have been dealt with on European level since the beginning of the second millennium. The obligatory legislative document regulating the matters of critical infrastructure protection is a directive EU 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).

On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection which provided policy options on the establishment of the programme [3]. In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a EPCIP; in April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders [3].

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.

Directive of the Council 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection was adopted on 8th December 2008. This directive presents the first step of chosen admission (step by step) whose aim is to determine and indicate ECI and to assess the need to increase their protection. This also establishes duties of an owner/operator of ECI [13].

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. In terms of this amendment, a procedure of identification and designation of critical infrastructure is in progress at the moment. The procedure of identification and designation of critical infrastructure and entities taking part in this procedure are described in the following chapter. However, further entities which are not presently engaged in this procedure, but could influence the system of CIP, can be defined.

II. Entities of the Current Procedure of Identification and Designation of CI

The amendment 430/2010 creates conditions for dealing with the CIP matters on national level. Defining CI on the national level is a precondition for specifying the European critical infrastructure (ECI) and hence even for satisfying the requirements following from the directive. In the legal code of Czech Republic, the matters of critical infrastructure had not been in any way regulated until December 2010.

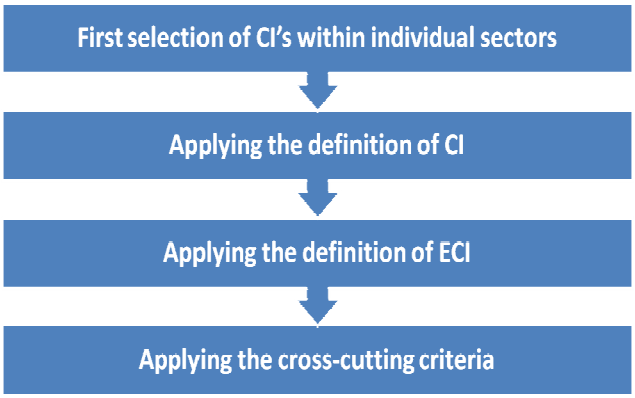

Fig. 1 the procedure of identification and designation of ECI

A procedure of identification and designation of CI is in process in Czech Republic at the moment. Based on this procedure, active CIP system entities in CZ can by defined. As shown in Fig. 1, the procedure proceeds from the already mentioned legislation and consists of four steps.

A. First selection of critical infrastructures within individual sectors

This step is in process in the Czech Republic at the moment. Entities which are implementing this step are gestors for the individual sectors (respective Ministries and other central administrative authorities, into whose sphere the CI sectors fall) and CI subjects (individual owners or operators of the CI). The selection is carried out on the basis of a consensus between the gestors and the CI subjects and when applying the sector criteria defined by the legislative.

B. Applying the definition of critical infrastructure

This step is directly intertwined with the previous one. The core of this step is that the potential CI has to comply with the CI definition which is given by legislation (directive). This step is carried out by the same entities as in the previous step.

C. Applying the definition of European critical infrastructure

The ECI definition will be applied to CI defined by the sector criteria and complying with the CI definition. The CI's which satisfy the transboundary element definition of ECI, will follow the next step of the procedure. The CI's which do not satisfy the transboundary element of the definition of ECI can be designated as national CI's of the Czech Republic. This step is carried out by the same entities as in the previous two steps.

D. Applying the cross-cutting criteria

Each Member State shall apply the cross-cutting criteria to the remaining potential ECI's. The cross-cutting criteria shall take into account the severity of impact and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI. This step is arranged by the Ministry of Internal Affairs – Firebrigade Directorate General as the highest CIP gestor and a contact point in Czech Republic in terms of ECI.
The CI's that have passed through all the steps of this procedure are considered to be potential ECI. These potential ECI will be announced by the Ministry of Internal Affairs to a respective EU authority – European committee and to those Member States which they may have a severe impact on. The subsequent steps of this procedure will be carried out on the EU level.

As it follows from the procedure of the CI elements identification and designation, the active CIP entities in Czech Republic at this time are Ministries and other central administrative authorities, into whose sphere fall some sectors of the CI and individual owners or operators of the CI. In terms of EU, the EU sheltering authority for EPCIP is the European Committee. However, there are other entities which influence or may influence the arising the system of critical infrastructure protection. These entities and their concise characteristics are the content of the following chapter.

III. Entities of Critical Infrastructure Protection in Czech Republic

In the Czech Republic, multiple primary entities which influence the system of critical infrastructure protection can be defined. These entities range by the level of activity from European, through national to regional level. A possibility to

influence the CIP system is related to it, among other things. This chapter represents a basic listing of entities which take part in the current procedure of the CI elements identification and designation in the Czech Republic, as well as entities which have the potential to join this procedure and take part and influence the CIP system in the future.

Mainly potential CI subjects, individual gestors and co-gestors are engaged in the current procedure of the CI elements identification and designation in CZ. The initiative for this procedure came from the European Union entities in terms of the European programme for Critical Infrastructure Protection. It is possible to say that other entity groups will take part in this procedure (experts from the CIP sector, research institutions, consulting companies, etc.) but question is if this part is sufficiently. Considering that the CIP system is outlined for public protection and security increase, they should participate in this system more. The state should arrange a higher level of public education as far as these matters are concerned. The CIP system is going to affect the life of each citizen of a Member State. Thus everyone should take the opportunity to influence the future and direction of security environment in their state and European Union as a whole accordingly.

A. European Union entities

The main entity which shelters EPCIP is the European Committee. The European Committee is an authority which has the right of initiative, implementation, direction and legislation inspection. The Committee acts as the contract keeper (its fulfilment) and embodies the interests of the Community. Another entity on the European level which directly impacts the CIP is European Council. Its goal is to give the European Union prompts for further development and determine its general direction.

B. Ministries and other central administrative authorities of CZ

Ministries and other central administrative authorities are gestors or co-gestors for the individual CI sectors and their main task is coordination and consensus finding with CI subjects when implementing CIP. The ministries these are: Ministry of Foreign Affairs, Ministry of Defence, Ministry of Finance, Ministry of Labour and Social Affairs, Ministry of Internal Affairs, Ministry of Environment, Ministry of Industry and Trade, Ministry of Transport, Ministry of Agriculture, Ministry of Health, Ministry of Justice. The Ministry of Internal Affairs is a contact point for the ECI matters and performs tasks in the CIP sector following from Czech Republic's membership in European Union (proposes cross-cutting criteria; processes a list that is a base for CI elements and ECI elements determination; communicates and informs the European Committee about ECI; etc.).

Central administrative offices acting as gestors or co-gestors for the individual CI sectors are: Energy regulatory office, Administration of State Material Reserves, Czech Telecommunication Office, Czech National Bank, State Office for Nuclear Safety, Czech Mining Office, National Security Authority, Czech Statistical Office, Security Information Service.

At this time, mainly gestors and co-gestors from sectors which the procedure of CI identification and designation (power-industry and transport) is being implemented in, are engaged.

C. CI subjects – owners/operators of the CI

According to legislation, the CI subjects are the individual owners or operators of the CI element. At this time, the procedure of CI elements identification and designation is not yet finished, so the individual subjects have not yet been informed about being the ECI owners/operators and about the rights and duties they have in connection with this designation. However, it is in the interest of these subjects to be a part of the CIP procedure from its beginning. Most subjects which the present procedure of CI elements identification and designation concerns are actively participating in this procedure. According to the legislation, the primary and ultimate responsibility for the ECI protection rests with the Member States and owners/operators of these infrastructures. So if the potential subjects of this procedure take part in it, they may (among other things) also influence which and how many ECI elements are designated and later on also the financial demandingness (effectivity) of the measures that will be executed in terms of CIP. Financial responsibility related to measures increasing the ECI element security rests with the ECI element owner/operator.

D. Economical subjects

By economical subjects, persons (physical, juridical) or aggregated categories of persons are meant. Economical subjects do not fall into the first three entity groups described but they are economically interested in the potential CI sector. With it are connected economical impacts on these subjects following from CIP implementation. It is the active participation of the economical subjects in the CIP system that allows them to influence the economical impact of the taken steps following from the CIP system. By that, mainly requirements on financial activity of the taken steps, prevention and removal of the duplicities in the system, rightfulness of the measures etc. are meant.

E. Public

The previous category may be subsequently understood also as a public entity. Furthermore, the public interests are primarily represented by central administrative authorities of CZ. Nevertheless, despite these relevant circumstances we introduce the public entity individually. The reason is the emergence of the CIP as a system for citizen - public security increase. Hence the public entity should be considered individually. The ways the CIP system may influence the public are multiple. The primary, indirect way, is via state structures - central administrative authorities of the given member state. These authorities are lead by an elected public representation or this elected representation chooses the

leadership of the given central administrative authorities. Another way is via civil association whose purpose will be defending specific interests of a certain part of public in the CIP system. The public interests may be influenced also by an individual. For example, the Ministry of Internal Affairs in CZ established a database of experts in the security research sector which, among other things, deals with the research sectors concerning the CIP matters. However, a certain level of expert qualification is required for this activity.

F. Other entities

The last entity group is represented by institutions and organizations which are concerned with the CIP matters on an expert level. That includes services both paid (auditorial, consultant and counselling companies) or in terms of research (universities, research institutes, etc.). These entities have a high potential for influencing the CIP system, mainly as far as the professional aspect is concerned.

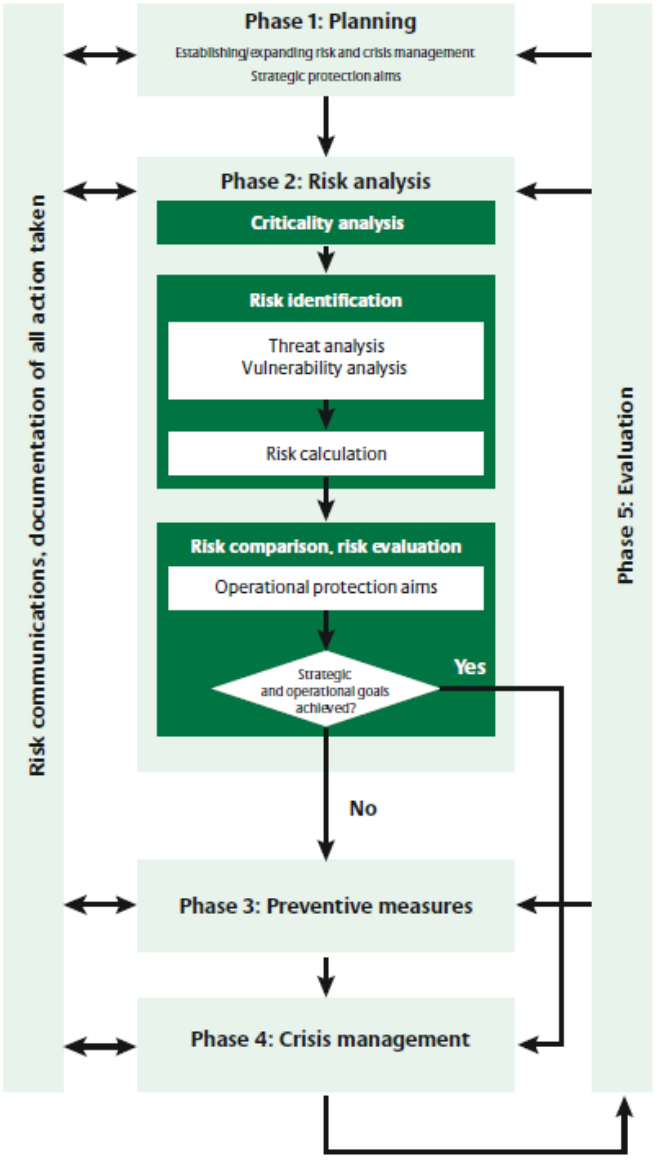

Fig. 2 the five phases of risk and crisis management [14]

IV. 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. 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 [14].

As described in A guide of Ministry of the Interior of Federal Republic of Germany: Protecting Critical infrastructures – Risk and Crisis Management [14], 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 [14].

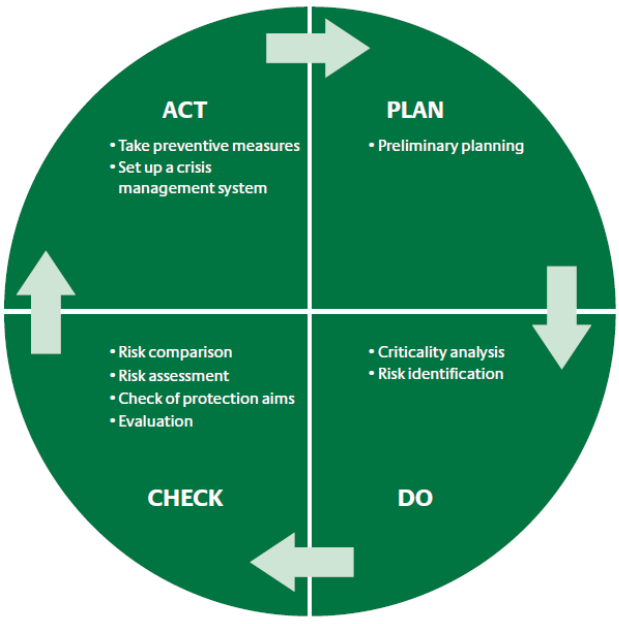

Fig. 3 the process of risk and crisis management based on PDCA [14]

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.

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.

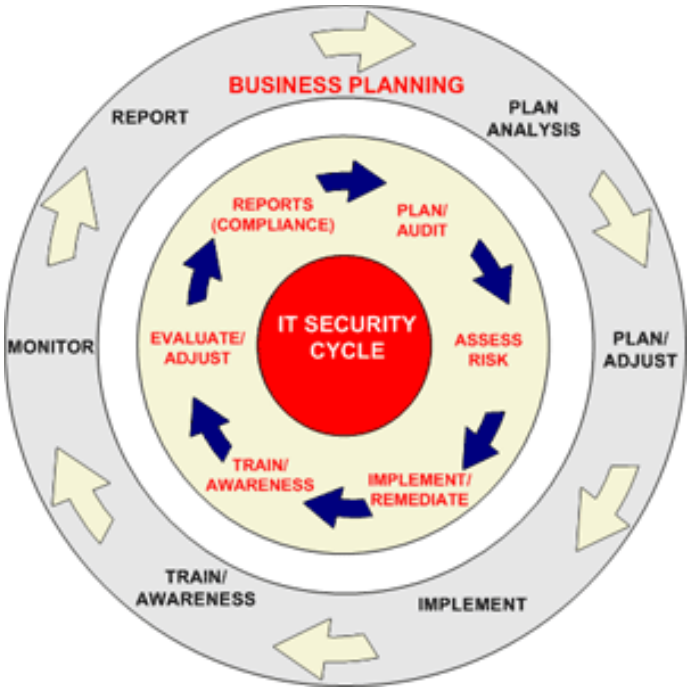

Fig. 4 BCP & IT Security [15]

- 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 - VPN.

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. Physical protection

Physical protection in the area of CI is secured by companies in the commercial security industry (CSI). In CSI, the physical protection of any object (building, appliance, object etc.) is achieved by combining and intertwining of three basic elements: physical protection systems, response team/activity, regime protection.

1. Physical protection systems – is divided into two basic areas of mechanical barrier systems and technical protection systems.
   a. Mechanical barrier systems in object concepts as the building are walls, roofs, floors, doors and windows objects. Generally these are for example: safety locks, grilles, security film, security and toughened laminated glass, safe, safety deposit boxes.
   b. Technical protection systems are: Intruder and / or Hold-up Alarm System (I&/orHAS); Security Camera System (CCTV system, CCTV surveillance system); Fire alarm system (FAS); Access Control System (ACS); Mechatronics System.

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. The 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 means of transport which includes namely checking the entrance of employees, clients, visitors and foreigners into the object and its parts, checking the leaving of persons and vehicles from the object, a right to take out objects and materials.
   b. Mode of the employee's movement in the object which also includes a determination of a part of an object with limited accessibility for employees and designation of their affiliation to certain transports, working places etc.
   c. Material and expedition mode sets the procedure when receiving, storing, exporting and movement of material. This way the property is protected against theft, damage and devaluation
   d. Operational mode which secures continuity and security of operation and working when an exceptional event occurs
   e. The key mode of operation which serves to determinate the marking, assignment, handing over of keys, the way they are used, the making of spare keys, changing of locks in important parts of the object etc.
   f. Operational mode related to the working of technical protection systems.

E. 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

A process of identification and designation of CI is in progress in Czech Republic at the moment. In this process, several basic entities can be defined. These entities range by the level of activity from European, through national to regional level. A possibility to influence the CIP system is related to it, among other things. This article represents a basic listing of entities which take part in the current procedure of the CI elements identification and designation in the Czech Republic, as well as entities which have the potential to join this procedure and take part and influence the CIP system in the future. The main role in this process is played by potential CI subjects, individual gestors and co-gestors.

The basic measures for CI protection introduced by the article are Risk and crisis management, Business continuity planning IT Security, Personal and administrative security and Physical protection. Mathematical models, tools and methods are used across these measures, namely in areas of determining threats and evaluation of risks, forming exceptional events, intrusions [10] into the secured object, simulation and forming of technological breakdowns, their spreading and impact etc.

Possibilities of further utilization of mathematical models, tools and methods lie in further improvement of present utilization but mainly in expansion into other measures for critical infrastructure protection. That means application of current/improved mathematical tools for new issues which have not been solved in this way so far. A current problem that is a typical example of this state is the evaluation of critical infrastructure resistance, specifically of the elements of critical infrastructure.

References

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

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

[3] *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

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

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

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

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

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

[9] 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.

[10] 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 Internationa Conference on Automatic Control, Modelling & Simulation (ACMOS´11)*, Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, pp. 131-136, May 2011.

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

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

[13] 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.

[14] 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

[15] eSecurity. (2011, June 15). Business Continuity, Disaster Recovery Planning [Online]. Available: http://www.esecuritytogo.com/ccpage.aspx?pageid=6&name=Planning&lid=10&lgid=1