Resilience as main part of protection of critical infrastructure

Ludek Lukas, Martin Hromada

***Abstract*—** Protection of critical infrastructure is a relatively new branch of application of management functions by state. The amendment of Act No. 240/2000 Coll. on crisis management has established the duty of Czech republic state's and private's owners of selected objects and systems to ensure the protection of elements of critical infrastructure. Implementation of the taken measures is done in the present time. Quantitative evaluation of taken security and other measures to should be part of this process in the future. This paper will talk basic problems and approaches of resilience of elements and system of critical infrastructure elements. The current approach of the Czech Republic to protect critical infrastructure is based on the approach of the European Union. Its aim is to provide for the elements of critical infrastructure protection.

***Keywords* —** critical infrastructure, sector, protection, resilience, evaluation, management, control.

I. Introduction

Contemporary modern democratic society provides its citizens optimal conditions for their life and development. The latest technology are using significantly in several key areas like health care, food, transportation, information and communication technologies, etc. We can not already imagine our life without these technologies. Limitation of functionality of technology would cause substantial difficulties both for the functioning of the state and life of citizens also.

Based on political developments in nineties the concept of critical infrastructure was formulated as one of the security pillars. Infrastructure sectors are elements that support state by essential support functions. Energy, telecommunications, health care, foods are such infrastructure sectors from the perspective of the state. The states have been aware of their dependence on the operation of infrastructure sectors and began to be actively in this area. States define critical infrastructure and its elements gradually. Selection of individual elements of critical infrastructure is made on the basis of sectoral criteria. The Czech Republic has defined the critical infrastructure legislatively by amendment to the Act No. 240/2000 Coll. on crisis management.

Manuscript received March 29, 2011: Revised version received July 8, 2011. This work was supported by the Ministry of Interior of the Czech Republic under the Research Project No. VG20112014067 and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

L. Lukas. Author was with University of Defence in Brno, Czech Republic. He is now associate professor with Faculty of applied informatics, Tomas Bata University in Zlin, Czech Republic. (corresponding author to provide phone: +420-576035248, e-mail: lukas@fai.utb.cz).

M. Hromada. He is with Faculty of applied informatics, Tomas Bata University in Zlin, Czech Republic. (e-mail: hromada@fai.utb.cz).

II. Protection of Critical Infrastructure as Part of Crisis Management

A. Crisis Situation

A technical accidents, natural disaster and terrorist attacks are main threats for nowadays society. These crisis situations have joint marks as:

- unpredictable occur time,
- broad range of coverage,
- large material damage,
- life or health injury.

To eliminate these damages a crisis management is established in Czech Republic. Crisis management under conditions of safety policy of the Czech Republic is considered as a complex of procedures and provisions managing actions of relevant bodies of public administration and of other relevant authorities, to overcome unfavorable evolvement in society. At the same time it is discerned whether there are situations connected with providing of defence of the Czech Republic against external attack (external safety) or there are situations unconnected with this (internal safety).

Crisis management elements are codified in the Law No. 240/2000 on crisis management and on modification of certain codes (Crisis Code), in latter wording. Based on this law, state of danger can be proclaimed to overcome unfavorable trends of development.

Applied with other laws, this allows proclaiming even state of emergency, state of country jeopardy or belligerency. Crisis management is considered not only as a configuration of tasks for preparedness to crisis situations and for their solution, but also as complex of activities for prevention of unfavorable trends and for recovery of vital infrastructure in disaster area.

Crisis preparedness is provided by different means - organizational (creating of organizational structures, emergency planning, crisis planning), technical (system facilities – equipment etc.), and special abilities (training and education).

Solution of crisis situation is connected with providing rescue and clean-up operations, implementation of measures

for population protection in disaster, emergency survival, measures to ensure functional public administration etc.

Prevention of crisis situations is mainly applied to protect critical infrastructure. All production systems, non-production systems, and services which - when unorganized – could have serious impact to the state safety, economy, state administration, to providing all necessaries of life to citizens, or to fulfilling of international obligations, are considered as critical infrastructure.

B. Critical Infrastructure as Part of Crisis Management

Protection of critical infrastructure is a relatively new branch of application of management functions by state. Due to the results of the analysis of security threats the technological development and society's dependence on energy, products, networks, commodities leads to formulation of the required degree of protection. Modern states solve those problems by multi-level solution. The defining of national critical infrastructure program is usually first step. The legislative pillar is cornerstone of critical infrastructure defining, its components and how to ensure its protection. The organization of critical infrastructure protection is basic part of these programs. Functionality of critical infrastructure determines the effectiveness of state security system. Functionality creates conditions for providing external and internal security measures and protection of population.

It is necessary to protect the critical infrastructure elements especially against physical destructive threats, technological accidents, and cyber attacks natural disasters. The adopted measures are very costly in many cases. The problem lies with critical infrastructure elements that are owned by private enterprise. Protection costs do not related directly with the object of their business and thus increase the overall cost of services. Private organizations are competitive and decrease its cost but there are costs of preventing associated with increased resistance of the element of critical infrastructure. This problem is currently looking to identify a path to its solution, especially in legislative and economic level.

The current problem of critical infrastructure protection is interdependence between critical infrastructure sectors. Internal dependence occurs at several levels, mainly physical, cyber and organization levels. It arises due to financial flows, energy flows, information flows. Countries and people need a systematic solution.

III. Main Threats And Risks Of Critical Infrastructure

Critical infrastructure is key state asset that will provide the main functions needed for state operation. Security analysis provides what should be protected and which threaten the assets. The risk of execution of threats is determined in the security analysis. Risk is the probability that the threat has become. At present, based on safety analysis, fundamental threats to critical infrastructure are:

- natural disasters,
- technological accidents,
- cyber attacks,
- criminal activities,
- terrorist attacks.

A. Natural Disasters

Natural disasters are strong effects of natural phenomena that act negatively on the functionality, structure and integrity of the system. The basic natural disasters are floods, torrential rain, gales and heavy snow in the Czech Republic. Protecting of critical infrastructure elements is the improving of resistance to these threats.

B. Technological Accidents

Technological accidents represent incidents in which there is a negative effect on functionality, structure and integrity of the system due to internal factors (reliability mainly). The internal factors may be faults, failures and other unreliability, causing uncontrolled degradation and destruction of functions. Protection of critical infrastructure element is provided by ensuring of technology reliability. The human factor plays an important role as well.

C. Cyber Attacks

Cyber attack is a targeted activity against information assets of critical infrastructure elements in order to obtain, modify or destroy the data or degrade or destroy the information system. Protecting of critical infrastructure elements is ensured by security technology for information systems. Protection is provided by cryptography and reliable secure communication protocols.

D. Criminal Activities

Criminal activity means the illegal activity in order to illegally obtain or relegating to destroy elements of critical infrastructure. The aim of criminal activities is theft or withdrawal of critical infrastructure elements. Protecting of critical infrastructure elements is a summary of measure of physical security.

E. Terroristic Attacks

A terrorist attack is usually illegal activities leading to the degradation or destruction of critical infrastructure elements to support the enforcement of its policy goals. Protecting critical infrastructure elements is a summary of measure of physical security.

F. Security Measures

Protective measures to ensure the security of critical infrastructure include personnel, technical, structural, technological measures and measures of physical security. The next section will deal only with the implementation of measures in the areas of physical security.

IV. PROCEDURE FOR CRITICAL INFRASTRUCTURE PROTECTION BULDING

A. Protection Aim

The aim of the process of protecting critical infrastructure is to ensure the desired degree of physical security and resilience

for critical infrastructure elements. The aim is also to ensure the recovery process in case of the degradation function of elements. Designated elements must withstand the effects of all threats. This is the principle All Risk.

The basic standards and rules for the protection of critical infrastructure are included in content of the process of creating a security framework for the system of protection of critical infrastructure. There is included:

- establishment of systems and institutions for the protection of critical infrastructure,
- selection of elements for the protection of critical infrastructure, ensuring their protection and recovery functions in case of degradation.

B. Security Framework

Security framework for the protection of critical infrastructure represents the definition of critical infrastructure and its relation to the state and society. The framework defines the position of critical infrastructure in the state security system. There is emphasized the reasons for its protection and risks for the society at time of its disposal.

Creation of juridical environment for critical infrastructure protection includes the development and adoption of the law and other standards activities in this area. The laws and standards should have set objectives of the process, elements and areas of critical infrastructure, institutions for the protection of critical infrastructure and their actions towards the protection and restoration functions. Protection of critical infrastructure is related to crisis management and the efforts of rescue and protection of the population.

C. Standards for Critical Infrastructure Protection

The basic standards and rules should specify criteria for the selection of the objects of critical infrastructure. Standards should to emphasis its importance in critical infrastructure and the requirements for physical protection. Standards should be based on the specifications of classes of elements of critical infrastructure. There are 3-5 classes of protection usually. Classification into classes is based on measurements of the impact of the disable of element for function of critical infrastructure on state and citizens. Degrees of influence are the following levels of assessment:

- degraded but does not threaten the basic functions,
- degraded and threatens the basic functions,
- excludes the basic functions.

D. Identification of Critical Infrastructure Elements

System and critical infrastructure protection authorities creates a management system for the management of critical infrastructure. The structure of the authorities is created by the obligation of authorities and identification of work rules and processes. The juridical relationship is created between critical infrastructure protection authorities and operators of critical infrastructure. Fire Rescue Corps is a state body responsible for protecting of critical infrastructure in the Czech Republic.

Determination of critical infrastructure element is based on usage of statutory criteria. Cross-cutting and sectoral statutory criteria are used currently. Impact of degradation functions in the area of critical infrastructure, state and society is the basis for determining the critical infrastructure element. Power plants, critical substations and airports are included among such elements.

E. Protection Measure

Ensuring the protection, resilience and recovery infrastructure includes security analysis of critical infrastructure elements, the specification of security, safety and operational measures to ensure the required level of security and reconstruction functions. The Operator Security Plan is basis for the protection and restoration functions. Security Liaison Officer must be designated in each element of critical infrastructure.

The system of Critical Infrastructure Protection is created in the Czech Republic currently. The crisis management law is the foundation for the protection of critical infrastructure. Critical infrastructure protection authorities place emphasis on:

- selection of critical infrastructure elements,
- protection and recovery plan (Operator Security Plan) for protecting and restoring of critical infrastructure elements,
- ensure the protection and recovery of critical infrastructure elements.

The whole process is aimed at both the national critical infrastructure elements and the elements of European Critical Infrastructure. The basic problem is to apply the principle of the simplest approach to the protection of critical infrastructure. Building of system is reason for that. Critical infrastructure protection system is currently being created in the basic version. Main reason is due to contradictory requirements of security measures to ensure the function of individual elements. For example on airport the deep security inspection is required and check-in a large number of people in a short time is needed too.

F. Problems and Solutions

The main current problems of the process of critical infrastructure in the Czech Republic include:

- simplifying of access to critical infrastructure protection, protecting only the most important objects,
- system of critical infrastructure protection and security class of elements (objects) is not determined,
- standards are not developed for each class of objects of critical infrastructure,
- there is no system of control and certification of critical infrastructure protection.

Solution of individual problems will be gradual and will be based on both the national analysis and knowledge of the European approach too. Improved protection of critical infrastructure should focus on addressing the following issues:

- specification of critical infrastructure protection system,
- specification of the class of objects of critical infrastructure in terms of impact on the state and citizens' lives,
- specification of standards to ensure protection of critical infrastructure elements,
- specification and optimization of standardized ways of ensuring the protection of critical infrastructure elements,

- evaluation of the protection of critical infrastructure facilities,
- certification of critical infrastructure elements.

V. Possibility of resilience evaluationf of critical infrastrucutre

A. Resilience of Critical Infrastructure

The goal of the protection of critical infrastructure is to ensure its functionality for the needs of functioning of the state and ensuring the good living condition for population. A number of factors or threats have impact on critical infrastructure. This impact may degrade functionality of critical infrastructure, or it completely out of operation. Measures limiting the influence of these factors improving its ability to withstand exposure these factors. Resilience reflects the ability of an element or system to ensure its function in conditions of effects of external and internal factors.

Resilience of critical infrastructure is an indicator which quantifies its ability to ensure the operation in conditions of effects of external and internal factors. Durable element ensures its goal function in conditions which degrade function of this element. Resilience can be understood as the ability to return to good health. Resilience is the ability to resist effect of threats to ensure the basic functionality of the system.

When evaluating resilience there must determined level when the system is still functional. It is obvious that the degradation of system performance may gradually decrease the capacity of services, but the basic functionality in favor of the state is assured. It is difficult to determine the level of degradation of service in which the desired function is still guaranteed. Setting levels (limits) is usually the result of extensive research based on defined needs of public administration. Such studies were carried out in the past for defense needs.

B. Internal and External Factors

Identified major threats are considered as factors that limit the functionality of the system. These factors can be both external and internal. External factors are those that are independent of the critical infrastructure system. The system can not in any way limit their influence and resists of its impact by the repressive action. There is usually a disaster, the effect of criminals, etc. The internal factors are those that are directly influenced by the system. The system can reduce their impact both preventive and repressive measures. These factors include reliability of technical character, system design, etc.

C. Evaluation Approaches

For evaluation of resilience of critical infrastructures there is essential to define the basic approaches that allows evaluation. These approaches are based on abstractions and model depiction of areas of critical infrastructure sectors. Czech Republic adopted an amendment to “Act No. 240/2000 Coll. on crisis management” and at same time adopted of “Regulation No. 432/2010 Coll. on the criteria for determining the element of critical infrastructure”. The Regulation defines both cross-cutting and sectoral criteria. Specific areas and elements defined in the sectoral criteria, which can be regarded as an element of critical infrastructure. Individual areas within the sector are an integrated into system that provides the necessary functionality.

Here is for example in the Energy sector included A.1 Electricity area. Electricity area includes elements of "electricity production, transmission and distribution system." Each element is involved in supplying electricity to its work or its functionality. Evaluation of resilience is possible both for the individual elements, so for the entire area. There seems to be more effective evaluation of the whole area. This approach will clearly determine the proportion of individual elements to ensure the target function. Evaluation of the resilience of elements would be narrow and did not provide an integral view.

Table 1 Model depiction of individual sectors of critical infrastructure

Critical Infrastructure Sector	Model Depiction	Suggested Method of Evaluation
Energy	Controlled Network System	Network Theory
Water Supply	Controlled Network System	Network Theory
Food and Agriculture	System of Processes	Multi-criteria Evaluation
Health	Multi-element Controlled Object	Multi-criteria Evaluation
Transportation	Network	Network Theory
Communication and Information System	Controlled Network System	Network Theory
Financial Market and Currency	System of Processes	Multi-criteria Evaluation
Emergency Services	Controlled Network System	Network Theory
Public Administration	System of Processes	Multi-criteria Evaluation

D. Model Depictions

In order to define approaches and methods for evaluation of resistance of individual areas of critical infrastructure is needed the suggesting of their model depiction. This model depiction (simplification, abstraction) is the basis for determining the evaluation of resilience. Table 1 shows the outline of possible model depictions the individual areas of critical infrastructure. Model depiction allows formalizing specific methods for resilience evaluation.

General abstraction of individual areas of critical infrastructure is the underlying premise for using a suitable theoretical apparatus for evaluating the resilience of element and the system of elements of critical infrastructure. Necessary model depiction is created with using of the theoretical apparatus. This depiction is a tool for this evaluation. We are able to use this model to quantify the level of resilience of evaluated critical infrastructure.

E. Sector Models

The basic model depiction of different sectors of critical infrastructure made on the basis of analysis:

- Multi-element Controlled Object,
- Controlled Network System,
- Network,
- System of Processes.

F. Multi-element Controlled Object

Multi-element Controlled Object represents a group of several elements of the same category that are merged into one unit (the object). Individual elements are distributed on the territory and provide the same functionality. Elements of the object are not mutually follow-up. They are usually mutually substitutable, so they can replace the loss of activity of another element of the same category. Quantification of resilience is possible by using multi-criteria evaluation methods.

G. Controlled Network System

Controlled Network System (CNS) is system of follow-up distributed components with different functionality that together form a complex. This complex performs its target function usually as a service. Each category of elements fulfils its sub-function and result of this sub-function passes to follow-up element. Controlled Network System provides for the state and population desired target function, energy supply, water supply, communication services, etc. The network management subsystem plays an important role in the Controlled Network System. The network management system provides control of system and necessary flexibility of CNS. Quantification of resilience is possible by using the methods of network theory (network graph).

H. Network

The network can be understood as a system of interconnected elements of the same category that provide the desired functionality as a complex. It consists of individual sections (lines, compartments) that are interconnected at nodes. The network can provide the desired functionality on the direct routes or the backup routes. Quantification of resilience is possible by using of the methods of network theory (network graph).

I. System of Processes

The System of Processes characterizes the work of organizations (ministry, offices, company) that are identified as elements of the critical infrastructure. The goal of such a system of processes is to provide a production, control and information functions within the specified range. Result of system of processes can be agricultural production, ensuring the banking and insurance services. Individual processes are interconnected, so that together constitute a logical complex. Network is not part of the complex unlike the Controlled Network System. Individual processes are performed separately, but may be a mutual substitutability between processes. Quantification of resilience is possible by using of multi-criteria evaluation methods.

The individual model depiction is characterized by an emphasis on a particular aspect or single-sort, multi-sort object, network depiction, process expression functions, or the complexity and multi-dimension evaluation.

VI. The Methods and Measures to Ensure the Physical Security of Critical Infrastructure

A. Security Measures

Ensuring the protection of critical infrastructure element contains the set of conceptual, organizational, technological and technical measures to ensure required level of protection of critical infrastructure element. Specification has size of projection, setup and operation. The result of this process is a system of critical infrastructure element protection. The basic pillars of critical infrastructure protection are:

- physical protection system,
- information support,
- system of personnel training,
- recovery system of critical infrastructure elements.

B. Physical Protection System

Physical protection system is a summary of regime measure in the element of critical infrastructure, operation of security guard and technical equipments of mechanical and electronic security systems. The quality of the physical protection depends on the preparation and implementation of a particular operation. Task for the physical protection system is based on an analysis of threats and risks. The analysis is usually done by using software tools. RISKAN is example of such software system. We can also use the methods of modeling and simulation to verify the effectiveness of physical protection measures.

C. Security Guard

Security guard ensures the security oversight of critical infrastructure element. Guard provides patrol of element. In case of violation the guard arrests the perpetrators and ensures its delivery to police. There are used mechanical systems, such as fences, gates, bars, etc to support the implementation of security measures. Sensory and guarding part of physical protection system is created by electronic security and alarm systems, motion detectors and camera systems. Technical equipment significantly promotes surveillance activity of security guard.

D. Information Support

Information support of critical infrastructure element protection provides information on individual threats. Information support is essential to synchronize all the activities of protection, such as managerial and executive. Information system for critical infrastructure protection element support includes both classic and especially computer-oriented information system. Computer network forms its foundation.

E. System of Personnel Training

The system of personnel training ensures preparation of security guard to be ready to fulfill his mission. Preparation is designed to educate employees so they know how to proceed in various ways to undermine the protection of critical

infrastructure element. Guard is not only learnt but training and practice also. To prepare staff we can use simulation methods, especially for the coordination of training activities for ensuring the protection of large objects. Preparation of personnel for the protection of critical infrastructure is crucial.

System for recovery of critical infrastructure elements is designed to prepare the system, organizational and technical measures to ensure the recovery function. In the case of degradation function, the element is ready to ensure its renewal and the fulfillment of the objective function. The system of recovery is based on the recovery plan.

Aim of integration of these measures is to improve the preparedness of the element of critical infrastructure to withstand effect both external and internal factors that threaten the function of a critical infrastructure element.

VII. Information Support Of Critical Infrastructure Protection

A. Protection and Information Needs

Critical infrastructure must be protected, particularly against the physical destructive threats, technological accidents, cyber attacks and natural disasters. The adopted measures are usually very expensive. Information support of management and decision making is one of effective measure. Information support of management, decision-making and cognitive activity plays an important role in protecting critical infrastructure.

Quality of processes is determined by using knowledge and information. The realization of any meaningful action can not be imagined without adequate information support. Each job in the organization of the critical infrastructure requires to meet the information needs for the implementation of information activities. Information plays a role not only in terms of individuals but also in terms of the organization. Information sharing has significant synergistic effect within an organization.

B. Information Support Definition

Information support is a process (set of activities) that support management, decision-making and cognitive processes by information. Information retrieval, processing, presentation, archiving, and other information are essential information activities. The level of the activity depends on the capabilities of user, used tools and especially on used information systems and information technology. User - information system interface plays an important role in this area. Information support is an information flow that represents information interaction between user and interface of an information system. The user should know how to find individual items of information, how to operate with the user interface as inserting data into a database, etc. He should have a conceptual idea about the structure of electronic layers, functions and control information user interface. User's activity will be slow and cumbersome without the above knowledge and ideas. User interface should be designed so as to constitute an obstacle but an advantage for the performance of information activities.

Information support emphasizes process of searching, processing and presentation of information. It closely follows on users thought processes. Information and communications support activities of a user is very difficult to distinguish. Communication support is synchronous or asynchronous exchange of information. Synchronous exchange takes place using the telephone (phonic) traffic or instant messaging tools, asynchronous messaging uses particular tools for electronic mail and fax. Optimal information support is ensured by proper identification and provision of information resources, organizing information flows over time and by using of information for learning, decision making and management. These conclusions are fully valid in the field of process control of critical infrastructure protection.

C. Design of Information System for CI Protection

Progressive definition of the critical infrastructure of the Czech Republic needs to solve issues of information support for its protection. There can be assumed that it will be ensured by an information system. Information system for the protection of critical infrastructure should provide information support to the key processes of critical infrastructure. The main processes for information support:

- the determination of sectors and system of elements of critical infrastructure,
- monitoring of performance, or the degree of protection and resilience of critical infrastructure elements,
- critical infrastructure protection planning, monitoring and certification of security status,
- recovery of function of elements and elements of critical infrastructure, including the prediction of the functionality of critical infrastructure in future,
- knowledge support of critical infrastructure.

Information system for the protection of critical infrastructure can be implemented in several ways and it will respect a system of protection of critical infrastructure. The specification of role of region in ensuring of protection or monitor the status of selected areas of critical infrastructure is main problem primarily. Knowledge of state for energy, information systems, water supply and transport situation is crucial for the region in my opinion.

D. Structure of Information System of CI Protection

Designated critical infrastructure elements will generate data that are essential for monitoring of the functionality of the monitoring element of CI. This data will be evaluated for determining of CI functionality. This data will be the transmitted to a designated center of the region and to central level. The following figure (Fig. 1) schematically illustrates the concept of function of information systems of critical infrastructure at the region level. Abbreviation DM indicates database module, KM - Communication module K - Region, E - Energy, IK - Information and Communication Technology, D - Transport. The functionality of the all CI elements of sector will determine its functionality. This information will be forwarded to the region-level information system.

The proposed information system for the protection of critical infrastructure will collect information from the regional

information system domains. This will be achieved with a comprehensive overview of the functionality of KI and CR in different regions, as well as information and communication within the database module. From regional level, the information transmitted to the central level. Status of the remaining areas will be assessed only at the central level. This will be particularly the health sector, food and agriculture, financial market and currency, emergency services and public administration.

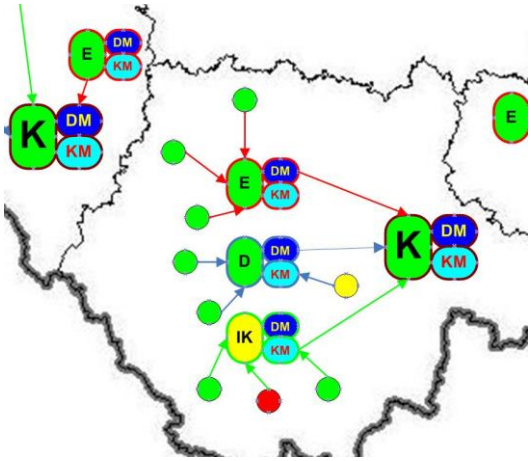

Fig. 1 information system of critical infrastructure protection for region

Information System should be constructed so that the standards CIWIN respected without technological and system barriers. The proposed information system should form one of the segments of the information systems used to support crisis management. A technology should be linked with the system ECC 112/IVS, other IRS information systems and possibly with crisis management information system (if completed). Information outputs of the information system should be on operational information centers FRS and DG Fire Rescue, in my opinion.

Information should support the work of crisis staffs of the different levels simultaneously. Information system for the protection of critical infrastructure should be gradually connected, if practical and desirable, into the European CIWIN.

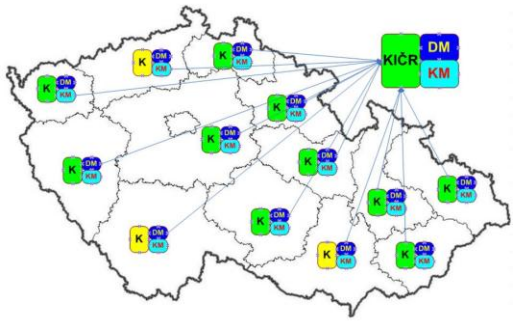

Fig. 2 information system for critical infrastructure protection for central level

E. Concept of CIWIN

The concept of Critical Infrastructure Warning Information Network - CIWIN was developed as part of EPCIP by using of the experience with a similar information system providing information support of critical U.S. infrastructure.

Creation of CIWIN should particularly encourage the exchange of information on shared threats and vulnerabilities and appropriate measures and strategies to reduce risk and promote protection of critical infrastructures. Member States should therefore ensure that relevant information is passed to all relevant government departments and agencies and emergency services. CIWIN should also inform the competent authorities of the industries that would inform the owners and operators of critical infrastructure through a network of contacts established within the Member States.

Critical Infrastructure Warning Information Network should be established by a separate proposal of the Commission. There is needed that within the EU and Member States to avoid duplication warning networks. Network will provide a platform for the secure exchange of best practices on critical infrastructure protection after its completion. CIWIN will provide voice and data services mainly. CIWIN will complement of existing networks and could also provide a platform for the exchange of rapid alerts linked to the Commission (ARGUS). Information Security accreditation of system will be undertaken in accordance with relevant procedures. Security Technologies specified by EU standards will be used to ensure information security.

F. CIWIN Development

The Commission issued a tender for a feasibility study in 2006. The study should include a conceptual design solution of CIWIN. The Belgian branch of Unisys became the winner. The solution proposed to establish a network through the integration of national warning network, with close links to ARGUS. Creating a platform for sharing knowledge, experience and best practices on critical infrastructure protection is an important function of CIWIN. Experts dialog and other stakeholders are important for improving of protection of critical infrastructures in the EU. If specific expertise is needed, the Commission may set up expert groups to protect critical infrastructures at EU level that to address clearly defined issues and to facilitate public-private dialogue on critical infrastructure protection.

Expert groups will support EPCIP by facilitate that exchange of views on issues related to protection of critical infrastructures. These groups constitute a voluntary mechanism, which mixes public and private resources to achieve a goal or set of goals that are considered to be mutually beneficial for both citizens and the private sector. Expert Group on Critical Infrastructure Protection will not replace other existing groups already established or which could be adapted to the needs of EPCIP. Czech Republic expects to use results of CIWIN project for Critical Infrastructure Information Support solution.

VIII. Conclusion

The definition of critical infrastructure is currently one of the most important security measures to ensure the feasibility of the state and its basic functions. Protection of critical infrastructure also significantly affects the lives of citizens. Constitution of critical infrastructure was done mainly because of technological dependency the state functions.

Therefore the technology and systems must be not only rugged, but also protected. Protection of critical infrastructure is significantly dependent on the physical protection measures. The current approach of the Czech Republic to protect critical infrastructure is based on the approach of the European Union. Its aim is to provide for the elements of critical infrastructure protection. Juridical framework and system is formed, but has some shortcomings that require solutions.

References

[1] P. D. Scarlantos, E. I. Kaisar and R. Teegavarapu "Modeling and Simulation of Catastrophic Events Affecting Critical Infrastructure Systems (Mathematical Methods and Applied Computing)" ACCMM1 *Proceedings of the Applied Computing Conference* , Vouliagmeni, Athens, Greece, 28-30 September, pp. 334 – 346 ISBN: 978-960-474-124-3.

[2] M. Hromada, L. Lukas "Utilization of the EASI model in the matters of critical infrastructure protection and its verification via the OTB SAF simulation tool (Recent Researches in Automatic Control)" presented at the *13 th WSEAS International Conference on Automatic Control, Modeling & Simulation (ACMOS 11)*, Lanzarote, Canary Islands, Spain, May 27 – 29, 2011, pp. 131 – 136, ISBN: 978-1-61804-004-6

[3] L. Necesal, L. Lukas "Entities of critical infrastructure protection in the Czech Republic" presented at *the 13th WSEAS International Conference on Automatic Control, Modeling & Simulation (ACMOS 11)*, Lanzarote, Canary Islands, Spain, May 27 – 29, 2011, pp. 383 – 386 ISBN: 978-1-61804-004-6.

[4] L. Lukas, M. Hromada "Management of Protection of Czech Republic Critical Infrastructure Elements" presented at the *13 th WSEAS International Conference on Automatic Control, Modeling & Simulation (ACMOS 11)*, Lanzarote, Canary Islands, Spain, May 27 – 29, 2011, pp. 306 – 309, ISBN: 978-1-61804-004-6.

[5] S. Costinas, B. Otomega, T. Chereches, C. A. Sava and E. Ionita "Management of Emergency Situations Resulting from Technological Hazard, Natural Catastrophes and Terrorist Attacks" presented at *Proceedings of the 11th WSEAS International Conference on Sustainability in Science Engineering* pp. 320 – 324, ISBN: 978-960-474-080-2

[6] I. V. Paputuangan, A. Abdullah and L. T. Juang "Critical Service Recovery Model for System Survivability" presented on *9th WSEAS International Conference on Mathematical and Computational Methods in Science and Engineering*, Trinidad and Tobago, November 5-7, 2007 pp. 21 – 28.

[7] M. Hromada, Critical Infrastructure Protection and Its Technological Aspects, *Security Magazín, vol. XVII. No.1,2010, pp. 21-24*

[8] L. Lukas, *Panorama of global security environment 2009*, Bratislava: CENAA, 2009, ch. 48.

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.

Martin Hromada - was born in 1983. In 2008 completed a master's degree in security technologies, systems and management at the Tomas Bata University in Zlin, where he currently serves as an internal PhD student. The object of his interest is in the protection of critical infrastructure in terms of technological aspects, modelling and simulation.