International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:8, No:11, 2014

The Use of Crisis Workplace Technology to Protect Communication Processes of Critical Infrastructure

Jiri Barta, Jiri F. Urbanek

***Abstract*—**This paper deals with a protection of the national and European infrastructure. It is issue nowadays. The paper deals with the perspectives and possibilities of "smart solutions" to critical infrastructure protection. The research project deals with computers aided technologies are used from the perspective of new, better protection of selected infrastructure objects. Protection is focused on communication and information channels. These communication and information channels are very important for the functioning of the system of protection of critical infrastructure elements.

***Keywords*—**Interoperability, Communication systems, Controlling Process, Critical Infrastructure, Crisis Workplaces. Continuity.

I. Introduction

THE risk of various extremist and terrorist actions is serious in the present time. This topic became a much discussed subject in professional community. Awareness, education and protection of organizational information secure environments are currently highly serious and relevant topics. Here, particular areas, technologies or states, that could be the next terrorist targets, are controversial and often fuzzy. Terrorist attacks represent the events, which are not only well planned but also very well procured with material assets by their perpetrators. To ensure the defence against these attacks on time, various instruments of security, crisis, and emergency management are used. Their basic parts consist of the activities covered by contingency and emergency planning which are based on the analysis and assessment of risks and threats. It is an expert analysis of the required goals which identifies the appropriate ways of goals achievement, and person-oriented leadership that supports the creative work and cooperation [7], [8].

Along with the extremist and terrorist actions act the negative events, such as natural disasters. In case of natural disasters, outcomes from scientific and technical progress are threatened. The risk of anthropogenic extraordinary events, that cause deaths and damage to the human property and the environment, is increased by the development of new sources for meeting demand and innovations of production capacity technologies. Assets designed for meeting demand belongs to the elements of critical infrastructure are mostly endangered by industrial accidents and environmental disasters [2], [6].

Managing the emergency situations at the Emergency Staff requires a high co-operation between its members and their fast decision making. For these purpose it is necessary to prepare Emergency Staff members adequately. The information support is based on the principles of process management, and Process Framework for Emergency Management was used during the design of crisis workplace to support decision-making processes of crisis management [5], [8].

II. Motivation

The assessment of identified threats and opportunities is a significant phase of SWOT analysis, which may fundamentally affect security of information and communication systems of the critical infrastructure workplace. This implies that the importance of infrastructure, especially the critical one, together with the European critical infrastructure is emphasises sufficiently and understood to be a serious threat to the state and its inhabitants from the perspective of possible terrorist attacks [8].

Preventive measures protect critical infrastructure elements are the most effective but they require the availability of necessary technologies, economic resources and personal qualities. In developed states, instruments for security management are used that help to ensure the high security of critical infrastructure elements.

The technology is a key factor in protecting critical infrastructure elements [3]-[5]. It is not necessary to invent and develop new technologies for the protection and security of individual subjects. It is possible, and for economic reasons often necessary, to use common technologies with a slight modifications or in a new way. These procedures create opportunities to secure the selected infrastructure objects at relatively low costs.

To ensure the defence against these attacks on time, various instruments of security, crisis, and emergency management are used. Their basic parts consist from the activities, covered by contingency and emergency planning, which are based on the analysis and assessment of risks and threats. It is an expert analysis of the required goals, which identifies the appropriate ways of goals achievement, and person-oriented leadership that supports the creative work and mutual collaboration [10], [11].

Preventive measures for protecting communication and information processes to infrastructure elements are the most effective but they require the availability of necessary

J. Barta works as a lecturer at The Department of Crisis Management of University of Defence and he is studying a doctorate in the field of protection of troops and the population at the University of Defence in Brno, K106, Kounicova165/65,662 10 Brno, Czech Republic (e-mail: jiri.barta@unob.cz).

J. F. Urbanek is Professor at the Department of Civil Protection, University of Defence, Kounicova 65, 66210 Brno, Czech Republic (phone: +420603326355; e-mail: jiri.urbanek@unob.cz).

technologies, economic resources and personal qualities. In developed states, instruments for security management are used that help to ensure the high security of communication and information infrastructure elements. The technology is a key factor in protecting information infrastructure elements.

It is not necessary to invent and develop new technologies for the protection and security of individual subjects. It is possible, and for economic reasons often necessary, to use common technologies with a slight modifications or in a new use cases. These procedures create opportunities to secure the selected infrastructure objects at relatively low costs [1].

The researchers the University of Defence are working on various scientific research projects of military and security character. The basic issue of this article is to protect the critical infrastructure. Therefore, the focus is put only on research in security for the protection of these elements. The Department of Crisis Management at the University of Defence solves many projects within its research activities in the field of safety. One of these projects addresses the uses the interoperability of workplaces to support managing of security management in a computer network.

University of Defence operates under the auspices of the Ministry of Defence. This project focuses on the communication and information channels of selected infrastructure elements and other objects.

III. Approaches and Methods

In this part of the paper presents approaches and methods that were used in the framework of the research project and processing paper. In the subchapters are defined only the most important methods and procedures to the research project specific application.

A. COTS

The basic requirement for recommended tools used to protect communication processes of critical infrastructure their applicability. The tools and technology must be freely available and widely spread. They toy with the question of the use of common security technologies and other security options that use the principle of COTS (Commercial Off The Shelf) as much as possible. That means the maximal utilization of commercial products and services to create a specific system or technology [9], [11].

B. DYVELOP

The task of DYVELOP method is to formulate, express, qualify and evaluate any problems and suggest its solution. Then is necessary take a think and gather all the information. This information must be analyzed and organized in logical entities. But for good scenario, they have to be expressed in sophisticated relations among them. Common heuristics, brainstorming and other methods of qualitative research are not useful and sufficient for it. They are able to give just simple record of different thinking and ideas. If only the ´Mind Maps´ are good for it [11] that are able register also information mutual relations in simple manual record.

The DYVELOP method is the lots more useful, because it is able to make informational, situational, events and entities surveys, analyses, orders, rules, arrangements, systems, records and archives, using common and well known computer software (MS Word, MS PowerPoint, …). Operational environment apparatus just the Microsoft Word can be advantageously used for DYVELOP modelling and simulations [10].

An using of DYVELOP method gives possible to gather, collect, classify, treat, computerize, evaluate, develop, progress, evolve, repeat and replicate any information, entities, processes, relationships, communication interface, procedures and steps on a scene. Even, it is capable retroactively formulate and sustainable put the inter results and results, depending on domains: real-time, space and participants. The DYVELOP creatively use computer simulation and modelling by means of simple graphically - mathematical formularization in chronological, sequential, logical and environmental relations changes.

IV. Use of Crisis Workplace Technology

Each subject of critical infrastructure should assure security of its communication and information system by reason of data loss (or theft) possibility. Comprehensive identification of security policy is integral part of the protection securing. Comprehensive identification of security policy is integral part of the protection securing. The identification consists in compiling a list of organization communication and information system and access points to the information system. Other part of the identification process is represented by determination of assets vulnerability within the system realized by application of methods intended for data gathering. The aim of this step is to create the register of assets and system vulnerability (weak points) for the reason that the vulnerability may be the potential target of threats.

The active and passive prevention is essential for the network and communication interface security. The purpose of active prevention (or just prevention) is to reduce the threat (before its activation as the peril) and potential damage. It includes:

- Threat elimination or reduction,
- Asset resistant strengthening.

Building up the preparedness results from the vulnerability determination, because the preparedness can be defined as an ability of communication systems to manage any emergency event or crisis. The preparedness of critical infrastructure subject should cover the protection of all assets and it manages all consequences of any emergency/disruptive events. Therefore, it means that any subject of critical infrastructure has to design such organizational structure of all resources in order to ensure efficient mobilization at the appointed time and place. Although, the preparedness means creation of certain safety measures because it is impossible to be prepared for every threats.

The subject of critical infrastructure should make its own security policy that should contain base rules for ensuring the security of its assets with the help of organizational, personal and technological measures. The important factor is approach

of organization management for influencing the efficiency of security policy. It must be exemplary in compliance with the rules and regulations of security policy in order to be effectively applied to all the structures elements of critical infrastructure. The security policy helps to manage difficulties, connected with intense utilization of information systems that are perceived as essential resources for any organization and its performance.

V. Implementation of the External Systems Outputs

The important factor for effective crisis response is implementing the outcomes of external systems into decision-making processes. Corresponding group are Environmental Information Systems to Support Decision-making Processes of the Crisis Workplace [1], [8]. The accuracy and up-to-datedness of information is essential for rapid and effective decision-making dealing with emergencies and crisis situations. Within the publicly provided information are provided data from various monitoring and information tools. Data are provided in the expanded form of various influences such as fires, rainfall, floods, winds, droughts, etc. Analysis of the various national systems providing publicly available information crucial for the integrated rescue system in emergency or crisis situations is an important step to improve interoperability between the different subsystems and extend the usability of the developed work and communication platform within the communication and information systems of critical infrastructure subject.

Next section deals with perspectives and possibilities of implementation of information about the origin or threat of natural hazards in the system that is being developed for the communication of the emergency staffs and putting on institutions interoperability working in the network to support decision-making processes of security management of critical infrastructure subject [10], [11].

The subject of critical infrastructure should be based on hazard (threat) of critical energy infrastructure individual elements in the creation of scenarios. Analytical group creates a risk register on the basis of risk analysis for a particular element and sets out the effects that will be simulated. For risk analysis can be used qualitative, semi-quantitative or quantitative methods (What-if method, FTA, ETA, FMEA, HAZOP, HRA, etc.) In the area of critical infrastructure was developed a special method RAMCAP Plus All Hazards Risk and Resilience Prioritizing Critical Infrastructures using RAMCAP Pluss Approach, Software applications eg. Security Risk Scorecard, Property Security Risk Survey, SFÉRA-ENERGY facilitate risk analysis. In the context of the publicly provided information are provided data about climate, soil and hydrological drought, which are crucial for the energy sector.

The most usable information basis is presented by the Czech Hydrometeorological Institute with its Integrated Warning System services dealing with dangerous meteorological and hydrological elements and phenomena in a particular territory. System of integrated warning service issue warning information for 32 dangerous phenomena, that are divided into 8 groups (temperature, wind, snow, frost, storm, rain, floods and fires). Alerts of storms, rains and floods are issued in cooperation with the flood forecasting and warning service. To the danger of flooding are attached other key sources of information - VODA portal provides information about water conditions and flow rates in rivers, water levels in reservoirs, rainfall and water quality. VODA portal information is also provided by river basin authorities. Information system POVIS (Flood Information System) is designed for flood protection and flood authorities, there are contained digital flood plans and books. Hydroecological Information System VÚV TGM (HEIS VÚV) completes the whole flood issue. Fig. 1 shows the communication interface. This allows you to transfer information between computer systems.

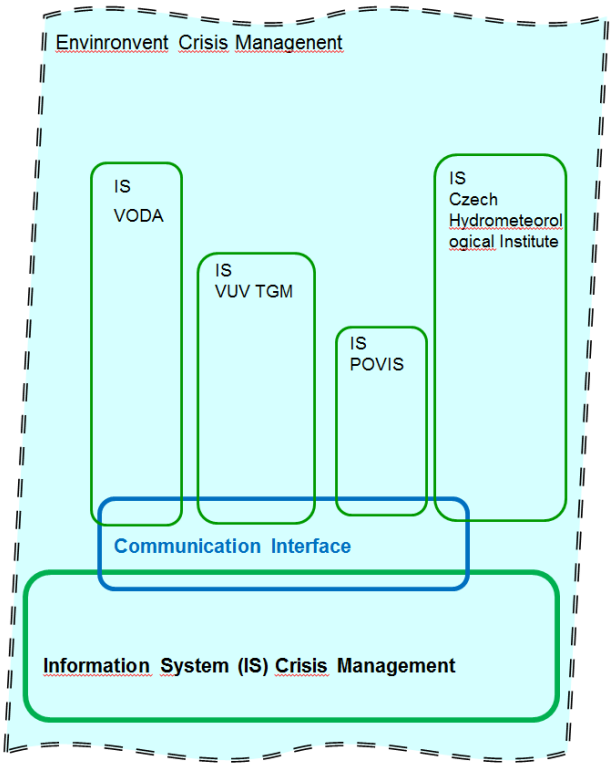

Fig. 1 The basic information systems with communication interface

The National Information systems are connected to the foreign systems, especially the neighboring countries for the danger of flooding, the European Union (MeteoAlarm, Floods Portal EFAS,) and international organizations, in which the Czech Republic is a member. These systems can be used in phase of preparation and solution to emergency or crisis situations and important information from these systems that are integrated in one place make much easier decision making in dealing with these events.

Using of the outputs from the individual information systems on one communications interface of information system for communication of the crisis staffs, and deployment sites interoperability in the network will save time in decision

making process in solving emergency and crisis situations. This allows make more important decisions with relevant and verified information in the same time. Faster mastering of crisis situation will have a positive effect of the course emergency solutions and it will minimize the negative effects on the environment. Verification of the usability of this interface was the practical exercises students of the University of Defence. Students solve real situation in the role of the crisis staff and compared with previous exercises had better results.

VI. Conclusion

The identical information is important for critical infrastructure entities to ensure the security of critical infrastructure elements and their preparedness of employees to manage and minimize damage of communication and information systems. The designed protection system will also have to use this information in order to create a critical and catastrophic environment that is close to the reality. This will provide practical training in an environment very similar to the reality. It ensures better training of critical infrastructure emergency staffs. Faster mastering of emergency or crisis situation will have a positive effect of the course event solutions and it will minimize the impact of negative effects on the environment. The result of the implementation of this technology will be validated in the practical test simulator real subject of critical infrastructure and their communication processes [6].

The result shows that this technology to protect communications systems using freely available tools and compliance with the rules is suitable for use in critical infrastructure entities. Of course, the availability of these technologies and their prices could be prohibiting in some cases. This is the most important advantage of the above described technology. It can be used to protect a variety of subjects or activities. Options of implementation will depend on the needs of individual cases and limits of technology. This technique is already known, affordable and therefore nothing prevents its using it for the protection of selected critical infrastructure objects.

References

[1] Barta, J., Sadovska, V., Srnik, A., Urbanek, J. F. Protection of Information and Communication Systems. Environmental Software Systems. Fostering Information Sharing., 2013, vol. 2013, no. 413, p. 302-310. ISSN 1868-4238.

[2] Bozek, F., Jesonkova, L., Dvorak, J., Bozek, A. General Procedure of Risk Management. *Ekonomika a management*, no. 3, 2012. p. 15-24. ISSN 1802-3975.

[3] Czech Republic, Act No. 239/2000 Coll., on the Integrated Rescue System and on amendment of certain codes, in latter wording", In Czech Republic Statute Book, 2000.

[4] Ludik, T., Navratil, J., Langerova, A., Process Oriented Architecture for Emergency Scenarios in the Czech Republic", In International Conference on Business Process Management. Venice: World Academy of Science, Engineering and Technology, 2011.

[5] Ludik, T., Racek, J. Process Methodology for Emergency Management. *IFIP Advances in Information and Communication Technology*, Heidelberg: Springer, 2011, 359, od s. 302-309, 8 s. ISSN 1868-4238. 2011. od s. 302-309, 8 s.

[6] Mitnick, K. D., Simon W. L. *The art of deception: controlling the human element of security*. Indianapolis, Ind.: Wiley, xvi, 2002. 352 pp. ISBN 07-645-4280-X

[7] Prochazkova, D. et al. *Bezpecnost a krizoverizeni.* 1. vyd. Praha: Police history, 2006. 255 s. ISBN 80-86477-35-5.

[8] Rehak D, Grasseova M. *The ways of assessing the security of organization information systems through SWOT analysis*, pp. 162-184. DOI: 10.4018/978-1-61350-311-9.ch007. In ALSHAWI, Mustafa, ARIF, Mohammed (eds.). *Cases on E-Readiness and Information Systems Management in Organizations: Tools for Maximizing Strategic Alignment*. 1st edition. Hershey, PA, USA: IGI Global, 2011. 318 p. ISBN 978-1-61350-311-9. DOI: 10.4018/978-1-61350-311-9

[9] Urbanek J. F., Barta, J.,Heretik, J., Navratil, J., Prucha, J. Cybernetic Camouflage on Human Recipient - Visual Illusion INTERFACE. In: The 9th WSEAS International Conference on Circuits, Systems, Electronic, Control & Signal Processing (CSECS´10). Řecko: WSEAS, 2010, p. 22-33. ISBN 978-960-474-262-2.

[10] Urbánek, J. F. et al. *Scénářeadaptivníkamufláže,* Brno: Tribun EU, 2012.130 pp. ISBN: 978-80-263-0211-7.

[11] Urbanek J. F. et al.*Crisis Scenarios.* Brno: University of Defence, 2013, 240 p. ISBN 978-80-7231-934-3.

Professor Jiri F. Urbanek, Ph.D. was born 29th March, 1949 in Pelhrimov, Czech Republic. He was graduated 1972 at Brno University of Technology, Faculty of Mechanical Engineering. 14 years he operated in Czech industrial and mining enterprises, including technical help for mining rescue services. Parallel he was graduated Ph.D. with thesis Mathematical Methods in Industrial Processes. Then he gave the lectures on technological, managerial and military universities in the branches Automation, Cybernetics, Management, Logistics and Non-conventional Technologies. On Brno University of Technology he habilitated in branch Mechanical Technology and later in branch Management and Battle Employment of Ground Forces in Vyskov Military University.

Now, he gives professor's lectures at University of Defence, Faculty of Economics and Management in Brno, Czech Republic. His research branches are Safety, Civil Protection, Interoperability, Security Management, Crisis Scenarios and Civil Emergency Planning. He is European Commission expert for Security Research and for the Development of Small and Middle Enterprises. He solves many national and international research and development projects. Now is in the solution of EC 7FP Security Research project CAST. He is not WASET member to this date.

Jiri Barta was born 16th June 1977 in Vyskov, Czech Republic. He was graduated 2001 at Military University of Ground Forces in Vyskov, Faculty of Economic and Management. From 2003 to 2004 he worked as a lecturer at the Civil Protection Department of Military University of Ground Forces in Vyskov. He gave the lectures on Crisis Scenarios, Civil Emergency Planning and Information Systems for Crisis Management. Parallel he 11 years operated in the private sector in the field of insurance and family finances.

Since 2004 he gives lectures at University of Defence, Faculty of Economics and Management in Brno, Czech Republic. His research branches are Safety, Civil Protection, Interoperability, Security Management, Crisis Scenarios and Civil Emergency Planning. He solves many national research and development projects. He is the author of more than 50 scientific articles, patent and co-author of two monographs collective expertise.

Now he is studying at the University of Defence in Brno too. He is study the field of protection of the population at the Faculty of Economics and Management. is focused on the implementation of the project output ADAPTIV to use military structures and critical infrastructure protection.His supervisor is a university professor Jiří F. Urbánek.