International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:6, No:11, 2012

Analysis and Design of Security Oriented Communication System

Jiří Barta

***Abstract*—**The paper deals with results of a project "Interoperability Workplaces to Support Teaching of Security Management in a Computer Network". This project is focused on the perspectives and possibilities of "new approaches" to education, training and crisis communication of rescue teams in the Czech Republic. It means that common technologies considering new perspectives are used to educate selected members of crisis management. The main part concentrates on possibilities of application of new technology and computer-aided tools to education and training of Integrated Rescue System teams.This project uses the COST principle for the creation of specialized centers and for all communication between these workplaces.

***Keywords*—**Communication of Crisis Management, Information System, Interoperability, specializedcenter, Security Oriented Information System.

I. Introduction

THE education, awareness and protecting in the field of crisis management are currently highly serious and relevant topics.The article deals with the perspectives and possibilities of "new approaches" to education and training of rescue teams in the Czech Republic.Integrated Rescue System teams have indispensable roles with respect of managing crisis situations in all states of the European Union.The risks of various terrorist events and incidents represent currently very serious problem in terms of the critical infrastructure. It is believed that the danger is a very underestimated due to the inclusion of the Czech Republic into the group with low terrorist attack risk. To ensure protection from these emergencies in time, various instruments of security, crisis and emergency management are used (Procházková et al., 2006). Their basic parts are consist of activities covered by the contingency and emergency planning, which are based on specific analysis and assessment of conventional risks and threats. The basic mission of education and training is to prepare members of crisis management to prevent emergency situations (Kyselák et al., 2011).

The issue of critical infrastructure has been greatly discussed in recent years. Critical infrastructure is defined as assets, systems and services important for Member States, which are essential for the maintenance of vital societal functions, health, safety, national security, economic or social well-being of population. Disruption or destruction of any part of the critical infrastructure would have a significant impact on security of Member State as a result of functional failure.

J. Barta works asa lecturer at the Department of Civil Protection,Faculty of Economics and Management, University of Defence,Kounicova 65,662 10 Brno,Czech Republic. (e-mail: jiri.barta@unob.cz)

II. Project Background and Motivation

Used materials were obtained from public sources. Afterwards, throughout the literature search of such documents, an answer to following question was searched for: How to protect critical infrastructure, and especially population from emergencies, e.g. various terrorist attacks, accidents and natural disasters. It was found out, that early prevention is the most effective and meaningful measure. It prevents losses, damages and subsequent costs to restore impaired system to the original state. The question of the critical infrastructure has been recently opened in the European Union. Results of formal talks were published in the Directive Council of the European Union. The Directive refers to the identification and designation of European Critical Infrastructure and the assessment of the needs to improve its protection (Council Directive, 2008).

The basis is to highlight the vulnerability of some critical infrastructure elements or critical infrastructure element systems. Disruption of such elements or whole systems would have a significant impact on national security, security of essential needs of population, human health or economy of the state. The Directive deals with the concept of European Critical Infrastructure and emphasizes the increasing protection of European Critical Infrastructure elements.

Collapse of any infrastructure element could cause a failure of critical infrastructure in another Member State or all Member States. European Critical Infrastructure is defined as critical infrastructure located in Member States, its disruption or destruction would have a substantial impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure (Council Directive, 2008). Figure 1 presents the relationship between European Critical Infrastructure (ECI), Czech Critical Infrastructure (CI) and critical infrastructure planning and security documents of Critical Infrastructure Protection (CPP).

Considering this international proportion, an integrated approach of the whole EU has been chosen to identify weaknesses, vulnerable points and gaps in protective measures. The goal of every EU member state is to protect entities and elements of critical infrastructure, prevent their disruption or their destruction, and minimize the impacts of possible failures of such infrastructures at the national and regional levels (Explanatory Memorandum, 2000).

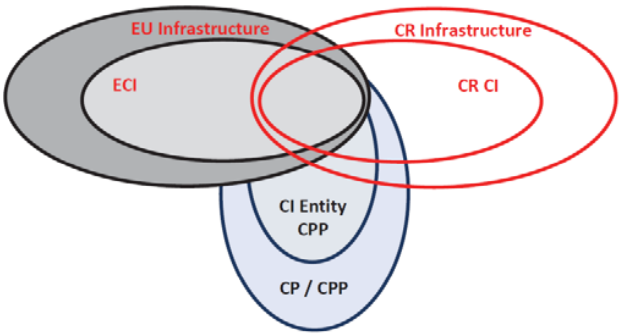

Fig. 1 European and National Critical Infrastructure (Hadáček et al., 2011)

In the Czech Republic, the main task was set by law to crisis management (here in after the Crisis Code). The law integrates the critical infrastructure protection into the system of crisis management. The crisis management is defined as a complex of management activities performed by responsible authorities, who carry out security risks analysis and assessment, planning, organizing, implement and control activities executed in connection with crisis situation solution. (Czech Republic, 2000b) From the previous text, it is evident that the national critical infrastructure protection is primarily included in the competence of Crisis Code. This Law also addresses situation where prevention is not enough and incidents can emerge. These situations are solved by units of the Integrated Rescue System. These units are the First Responders by terrorist actions, incidents and other crisis situations.

III. Approaches and Methods

Throughout the literature search of these documents, an answer to the question of how to train and educate rescue teams and members of crisis management was sought out. The system approach to security from an all-society point of view is based on understanding the protection as a structure of elements with a network of relations among them, that develop in time (Ludík&Ráček, 2011). In order to ensure the system approach, required terminology and defined planning documentation to implement measures to education and training of Integrated Rescue System teams, have to be identified.

Integrated Rescue System teams and executive constituents of crisis management (regional authorities and other authorities with territorial competencies) are educated and trained, but their communication, cooperation and practice are insufficient. They have limited possibilities of mutual cooperation within emergencies. Education and training are needed for the experience of rescue teams. It is shown in Hierarchy of knowledge and Skills of Rescue teams on figure 2.

The Population Protection Department at the Faculty of Economics and Management at the University of Defence solves many of distinct projects in terms of its research activities in the field of security, communication, civil-military cooperation and other. One of these projects aims for a novel perspectives and possibilities of "new approaches" to education and training of selected members of crisis management in the Czech Republic.

This research project of University of Defence called Interoperability Workplaces to Support Teaching of Security Management in a Computer Network (INTROP). The primary goal of the research project is to create new system and technology for education, training and exchange of relevant information with managers of crisis management.

Fig. 2 Hierarchy of knowledge and Skills of Rescue teams

To deal with the question of using common security, communication and information technologies and other computer-aided technologies, is to apply the principle of COTS (Commercial Off The Shelf) as much as possible. That means maximal utilization of commercial products, technologies and services to create a specific system or technology (Urbánek&Průcha, 2009).

IV. Adaptive Camouflage Case Study

In project of Interoperability Workplaces to Support Teaching of Security Management can be applied information technology and systems that were developed in the within the system adaptive camouflage. It is mainly a software tool for management and communication.

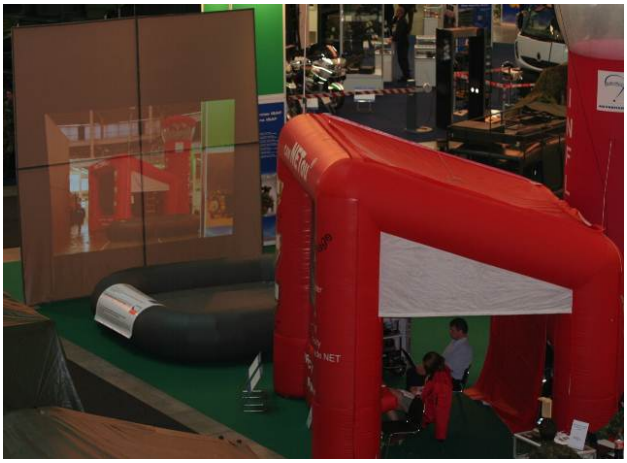

Fig. 3 Mobile Communication Center

On the figure 3 Is mobile center for communication and projected adaptive camouflage. This center has autonomous system and energy infrastructure for crisis situation. This mechanism is very resistant, autonomous electricity source 230V, 10A and mobile projecting system with powerful projector. This set was use when testing usability of system adaptive camouflage.

Its material cannot be published; its composition is in secrecy regime. It overall construction and configuration is a patented process.

Communication interfaces adaptive camouflage isused as a platform to create own system of communication. Communication scheme adaptive camouflage system interface is shown in Figure 4. There is a very good solution link client – server and framework of communication and sharing of data.

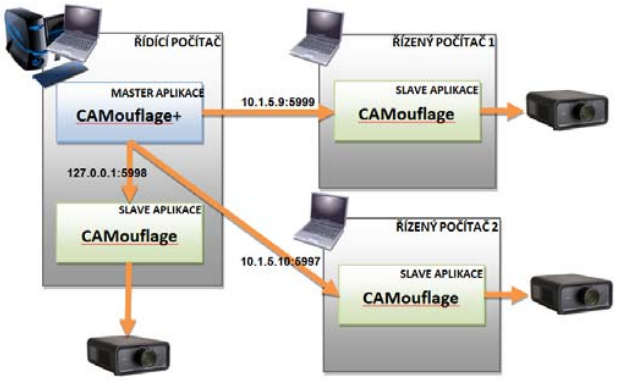

Fig. 4 Scheme of communication network

V. Virtual Simulator Case Study

The project discusses the abilities to create model situations of activities, units and small rescue teams. At selected activities there is described process of generation the specific model situation in order to verify the proposed methodological procedures of solution by real-time simulation using technical education and training means. The paragraph deals with the possibilities of using the verification experiments to replenish and further refinement of the model parameters, where applicable, of the model itself. Model and its parameters are the result of the analysis system. By customization you can synthesize the new system, already with the desired characteristics. Then on the other options can be verified other properties, in particular his openness and sensitivity to changes (Kozůbek&Flasar, 2011).

We have possibilities to get acquainted with practical usage with Virtual Battlespace 2 (VBS2) tactical-level simulator that is installed for and operated by Faculty of Economics and Management, University of Defence.

It is presented the newly built laboratory of Military Management and Tactics Department in University of Defence building intended for student practical training in decision-making and planning process implementation supported to the BMATT group. They assessed the simulator be a very useful tool for supporting team leaders decision making and improving their skills and habits of crisis control, completing missions and find solutions in unexpected crisis situations.VBS2™ - Virtual Battlespace 2 is a fully interactive, three-dimensional training system providing a premium synthetic environment suitable for a wide range of military (or similar) training and experimentation purposes. VBS2™ offers both virtual and constructive interfaces onto high-fidelity worlds of unparalleled realism.

VBS2™ VTK (Virtual Training Kit) is the baseline VBS2 product, a complete package combining the robust and flexible VBS2 virtual environment with scenario editors, a development suite (for terrain and 3D model import) and an integrated HLA/DIS gateway. It is a versatile framework for either employing or customising VBS2, with an emphasis on empowering the end user to both create scenarios and import content (such as new terrain areas or 3D models).

It is a fully-featured training tool including after-action review capability, HLA/DIS compliance, and a comprehensive yet easy-to-use mission editor that allows any imaginable scenario to be created and also modified in real time. VBS2™ has potential applications across the entire training and experimentation spectrum (Bohemia Interactive, 2010).

VI. Conclusion

The paragraph assesses the capabilities of tactical virtual simulator Virtual Battlespace 2 and possibilities of its use in training at the Czech University of Defence. There are possible applications in research of preparation and execution of asymmetrical rescue operations. Virtual simulator Virtual Battlespace 2 may also support the training of crisis staffs and control, small rescue unit. One of the intent is to verify possibilities to use it for the Integrated Rescue System of the Czech Republic for education, preparation and training.

Unfortunately, the project is fairly new, so there is not much information currently being shown in this interesting area. The project was started in April this year. In the first part of research the materials obtained from public sources were used. On basis of the analysis of such documents, an answer to the question of how to train and educate chosen crisis management members was achieved.

At the same time, it should be noted that this solution is a compromise in many aspects and it does not fully meet needs of all stakeholders. In addition, relations among the lines of preparation for solution of civilian crisis management and lines of preparation and training for crisis management staff have to be considered carefully.

The resulting situation can be recognized as an essential qualitative advance, but it has to be developed henceforth. The “Workplace expert of crisis management” belongs among the priority issues and it needs to be contemplated from the national security point of view, as well as the crisis management viewpoint.

The first steps to resolve such issues meet consistently all requirements resulting from the Conception of population protection. It is important to detect system unclarities and gaps when an issue emerges, and to formulate all requirements on education and training in this area to be further developed.

ACKNOWLEDGMENT

The paper has been written as part of the research project of University of Defence with acronym INTROP - Interoperability Workplaces to Support Teaching of Security Management in a Computer Network (SV12-FEM-K106-05-BAR).

REFERENCES

[1] Bohemia Interactive / Virtual Battlespace 2 (VBS2) 2010. [on-line]. c2010. [cit. 2012-6-6]. Dostupné WWW: <http://www.bistudio.com/bohemia-interactive-simulations/virtual-battlespace-2_czech.html>

[2] Explanatory Memorandum 2000. to the Draft Act No. 240/2000 Coll., on crisis management and on amendment to certainActs (theCrisisAct), as amended.

[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 [online]. [cit. 2012-6-6].WWW: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF

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

[5] Czech Republic. 2000b. Act No. 240/2000 Coll., on Emergency Management and on amendment of certain codes (the Crisis Code), in latter wording. In Czech Republic Statute Book.

[6] Hadáček L., Ščurek R., Cígler J. 2011. Projection of the National critical Infrastructure. Transaction of the VŠB - Technical University of Ostrava: Safety Engineering Series. VI, 2, p. 56 - 60. ISSN 1801-1764.

[7] Kyselák, J., Raclavská, J., Šuláková, L. 2011. Smart solution for area of population protection. In Proceedings of the 10th WSEAS International Conference on Computational Intelligence, Man-Machine Systems and Cybernetics (CIMMACS´2011) and the 10th WSEAS International Conference Information Security and Privacy (ISP´11). Jakarta, Island of Java, Indonesia: Published by WSEAS Press. p. 183-188. ISBN 978-1-61804-049-7.

[8] Kozůbek, J. Flasar, Z. 2011. The Modeling ofTacticalActivities in Contemporary and FutureOperations. Economics and Management. Brno: University Press of University of Defence, č. 1/2011, p. 41-49. ISSN 1802-3975.

[9] Lovecek, T., Ristvej, J., Simak, L. 2010. CriticalInfrastructureProtection Systems EffectivenessEvaluation. JournalOfHomelandSecurity And Emergency Management, Volume 7, Issue 1, ArticleNumber 34. ISSN 1547-7355.

[10] Ludík, T., Ráček, J.2011. Process Methodology for Emergency Management. IFIP Advances in Information and Communication Technology, Heidelberg: Springer, 359, p. 302-309, ISSN 1868-4238.Proházková, D. a kol. 2006. Bezpečnost a krizové řízení. 1. vyd. Praha: Police history. 255 pp. ISBN 80-86477-35-5.

[11] Urbánek, J. F. a kolektiv. 2012. Scénářeadaptivníkamufláže, Brno: Tribun EU. 130 pp. ISBN 978-80-263-0211-7.

[12] Urbánek J. F., Průcha J. 2009. A Development of Wireless Interoper-mobile Application for Outdoor Operation Management, In 8th Int. Conf. on Electronics, hardware, wireless and optical communications, EHAC ´09,, Cambridge, UK, WSEAS Press, Feb.p 57-64. ISBN 978-960-474-053-6, ISSN 1790-5117.

[13] Urbánek, J. F.,Urban, R.,Steinhäusler, F. 2010. Preparedness of First Responders and Risk Rating of European Union Terror Threat Life Cycles. Prehospital and Disaster Medicine, 25, p S10-S11 doi:10.1017/S1049023X00021944

[14] Urbánek J. F.,Barta J., Heretik J., Navrátil J. and Průcha J. 2010.Cybernetic Camouflage, on Human Recipient – Visual Illusion Interface. Speaking In The 9th WSEAS International Conference on Computational Intelligence,Man-Machine Systems and Cybernetics (CIMMACS '10), University of Los Andes, Merida, Venezuela, December 14-16, ISBN 978-960-474-257-8, ISSN 1792-6998; Published In WSEAS/Europment/EuroSAM International Conferences; December 29-31, 2010 Vouliagmeni, Athens, Greece; Recent Researches in Circuits, Systems, Electronics, Control & Signal Processing, Proceedings of the 9th WSEAS International Conference on Circuits, Systems, Electronics, Control & Signal Processing (CSECS'10);ISBN: 978-960-474-262-2, ISSN: 1792-7315, p 22 – 27.

[15] Urbánek, J. F., Urban, R., Steinhäusler, F., Lokajová, V. &Zaitseva, L. 2010. First Responders Preparedness and Risk Rating of EU Terror Threats Life Cycles - paper. InBook of AbstractssIPRED - TheFirst Israeli International Conference on Preparedness & Response to Emergencies and Disasters, Tel Aviv, 11-14. 01. Izrael.

[16] Zouhdi, S., Sihvola, A., Vinogradov, A.P. 2008. Metamaterials and Plasmonics: Fundamentals, Modelling, Applications. New York: Springer-Verlag. 316 pp. ISBN9781402094064.

Jiří Barta graduated in 2001 from the Military University of the Ground Forces in Vyškov, Czech Republic, Faculty of Economics and Management. Line of study was"Environmental Protection".Since 2010, he has been studying in thedoctoral study program called "Civil Protection". The topic of her doctoral thesis will be about protection forthe armed, civil and objects.

Since 2003 he taught at the Military University of the Ground Forces in Vyškov as an Assistant Professor. Since September 2004 he has been working as a lecturer at the Civil Protection Departmentat the University of Defence in Brno, Czech Republic.

Mr.Bartasolves many research and development projects. He is author or co-author of 65 papers, 2 books and 3 patents.