Research of Extreme Weather Impact on Critical Infrastructure

Maria Luskova, Bohus Leitner, Eva Sventekova, Zdenek Dvorak, *
* Faculty of Security Engineering, University of Žilina, Slovakia
Maria.Luskova@fbi.uniza.sk, Bohus.Leitner@fbi.uniza.sk, eva.sventekova@fbi.uniza.sk
Zdenek.Dvorak@fbi.uniza.sk

Abstract* — *In recent decades the frequency of different extreme weather events, including heavy rainfall and flash floods, river floods, landslides, windstorms, freezing rain, wildfire and hurricanes, has increased and these have damaged many regions across Europe and worldwide. A lot of centuries old buildings have suddenly been demolished, power delivery has failed and transport has been disrupted. These events have great devastating impacts on critical infrastructure systems. Extreme weather events and their impact on critical infrastructure was a topic of the project RAIN - Risk Analysis of Infrastructure Networks in response to extreme weather solved from May 2014 to April 2017 within the FP7 Framework Programme, Call Fp7-SEC-2013-1. The aim of this paper is to present the scientific results of the RAIN project achieved by the project consortium, characterized by multidisciplinary partners, and led by coordinator from the Trinity College Dublin. The project had a core focus on Critical Land Transport infrastructure and Energy & Telecommunications infrastructures. The Faculty of Security Engineering, University of Zilina participated as leader of work package 3 Land Transport Vulnerability.

Keywords: FP7 project, security, critical infrastructure, research, education.

1 INTRODUCTION

In last years, a variety of extreme weather events, including droughts, extreme temperatures, forest fires, rain induced landslides, river floods, storms, hurricanes, have threatened and damaged many different regions across Europe and worldwide. According to data, collected since 1980 by the insurance industry, the number of weather-related catastrophes recorded worldwide increased from an annual average of 335 events from 1980 to 1989, to 545 events in the 1990s and to 716 events for 2002–2011. Floods, heat waves, droughts and wild fires show the most pronounced upward trend, followed by storms [1].

These events have a severe impact on society. They affect human lives, livelihoods, cause irreversible changes in the environment and have also a devastating impact on infrastructure systems. In this context, in the year 2012, the Faculty of Security Engineering of the Žilina University became a member of consortium that prepared and submitted FP7 project proposal titled Risk Analysis of Infrastructure Networks in response to extreme weather – RAIN. This project was submitted within the call of FP7-SEC-2013-1, topic SEC-2013.2.1-2: Impact of extreme weather on critical infrastructure. The RAIN project was approved by the Research Executive Agency of the European Commission for financial support from May 2014 to April 2017. The main objective of the RAIN was to provide an operational analysis framework that identifies critical infrastructure components impacted by extreme weather events and minimise the impact of these events on the EU infrastructure network.

The aim of this paper is to present the ways of exploitation of the RAIN project results in education of critical infrastructure protection professionals at the Faculty of Security Engineering, University of Žilina within the study programme “Security and Protection of Critical Infrastructure”. This study programme is unique in central Europe, is primarily focused on the fields of energy and transport, is multidisciplinary oriented and focusing on various types of infrastructure networks and based on the needs of practice.

2 FP7 PROJECT “RAIN” - OVERVIEW

The vision of the RAIN project was to provide an operational analysis framework that identifies critical infrastructure components impacted by extreme weather events and minimise the impact of these events on the EU infrastructure network. The project has a core focus on critical land transport infrastructure and Energy & Telecommunications infrastructures [2]. The results of the RAIN project were achieved based on the collaboration between fifteen organizations in eight countries (Ireland, Germany, the Netherlands, Spain, Finland, Italy, Belgium and Greece). The project coordinator Trinity College Dublin (TCD) coordinated the work of the European Sever Storms Laboratory (ESSL), University of Zilina in Zilina (UNIZA), Technische Universiteit Delft (TU-Delft), Gavin and Dehorty Geosolutions Ltd (GDG), Dragados SA (DSA), Freie Universitaet Berlin (FU-Berlin), Roughan & O’Donovan Ltd (ROD), Hellenberg International OY (HI), Instituto di Sociologia Internazionale di Gorizia (ISIG), Prak Security and Judgment (PSJ), the Finnish Meteorological Institute (Ilmatieteen Laitos, FMI), Youris.com (Youris), Independent Power Transmission Operator (IPTO) and Applicaciones En Informatica Avanzada SL (AIA). The RAIN consortium is characterized by multi-disciplinary partners represented by meteorologists (FMI, FU-Berlin), climate researchers (ESSL), economists (TCD), energy specialists (IPTO & AIA), CI owners/operators (DSA), infrastructure risk analysts (TU-Delft &TCD), specialist engineering designers and planners (ROD and GDG), security and strategic response experts (UNIZA, PSJ, HI), social scientists (ISIG) and dissemination experts (YOURIS).

The project research activities were organised according to six technical work packages (WPs). WP2 focused on hazard identification, WP3 on land transport critical infrastructure and WP4 on energy & telecommunications systems. Development of the Risk Analysis framework, quantifying the risks and the benefits of providing resilient critical infrastructure, and developing mitigation strategies were covered in WP5, WP6 and WP7. Management and dissemination activities were realized within WP1 and WP8. Fig.1 indicates the WPs and the interaction and interdependencies between them.

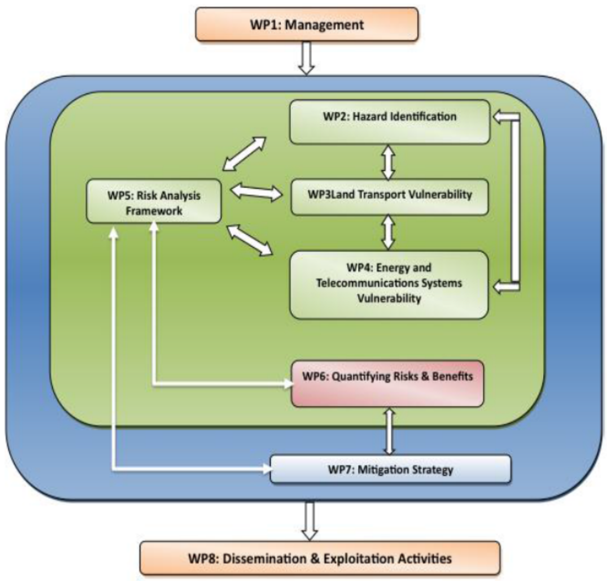

Fig.1: Work Plan Strategy [2]

3 Results of the RAIN Project

The principal objective of the RAIN (Risk Analysis of Infrastructure Networks in response to extreme weather) project, www.rain-project.eu, was to provide an operational analysis framework to minimize the impact of major weather events on land based transportation and energy and telecommunication) critical infrastructure in the EU. A holistic risk-based decision making framework was developed to establish the key components of these infrastructure networks and to assess their sensitivity to extreme weather event as well as to facilitate identification of the impact of alternative mitigation measures [2].

The main results of the project have been broken down into the technical work packages and can be briefly characterized as following chapters.

3.1 The results of the WP2 Hazard Identification

R-2.1 Definition and description of natural hazards. Within the project the following individual hazards were studied: winter weather (e.g. snowfalls, blizzards, snow load, and freezing rain); wildfires; river floods and coastal floods; thunderstorm-related phenomena (e.g. large hail, severe wind gusts, tornadoes and lightning); wind storms and heavy precipitation.

R-2.2 Description of potential ways that they have impacted or may impact critical infrastructure, and establishing 1st and 2nd thresholds. The 1st threshold means that some adverse impacts are expected, their severity depends on the resilience of the system and transportation is mainly affected. The 2nd threshold means that the weather phenomena are so severe that is likely that adverse impact will occur and CI system is seriously impacted.

R-2.3 The impacts and consequences related to exceeding a particular threshold vary across Europe (Fig.2) and depend on the resilience of the systems.

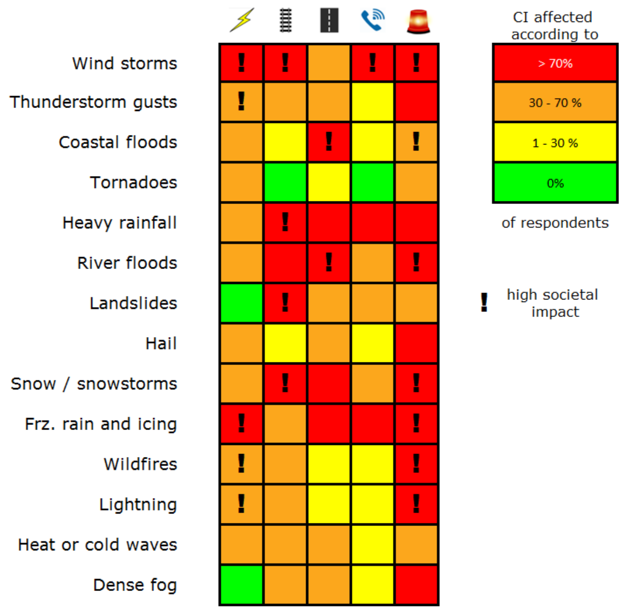

Fig.2 Vulnerability of various categories of Critical Infrastructure to various weather hazards, according to the stakeholder interviews [3]

R-2.4 Review of state-of-the-art early warning systems along with an assessment of the predictive skill of these systems.

R-2.5 Modelling probability of occurrence of the extreme events in the present and projections of changes of severe weather probability in the future.

3.2 The results of the WP3 Land Transport Vulnerability

R-3.1 The methodology for identification of critical land transport infrastructure and a review of its failures as a result of extreme weather events.

R-3.2 Two case studies describing destruction impacts of extreme weather events on critical land transport infrastructure in Slovakia and in Finland.

R-3.3 The current methods and best practices that relate to the preparedness and response to the serious impacts of extreme weather on critical land transport infrastructure and their analysis for specific problems

R-3.4 Methodology for measuring societal vulnerability due to failure of critical land transport infra-structure elements (Fig.3).

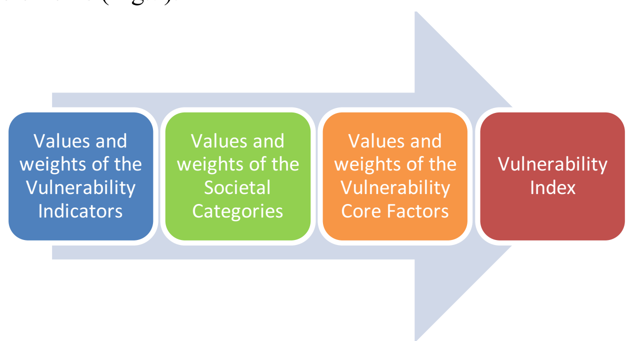

Fig.3 Application of values and weights of individual indicators for the determination of Vulnerability Index [3]

3.3 *The results of the WP4 Energy & Telecommunications System Vulnerability*

R-4.1 An overall description of Energy & Telecommunications System.

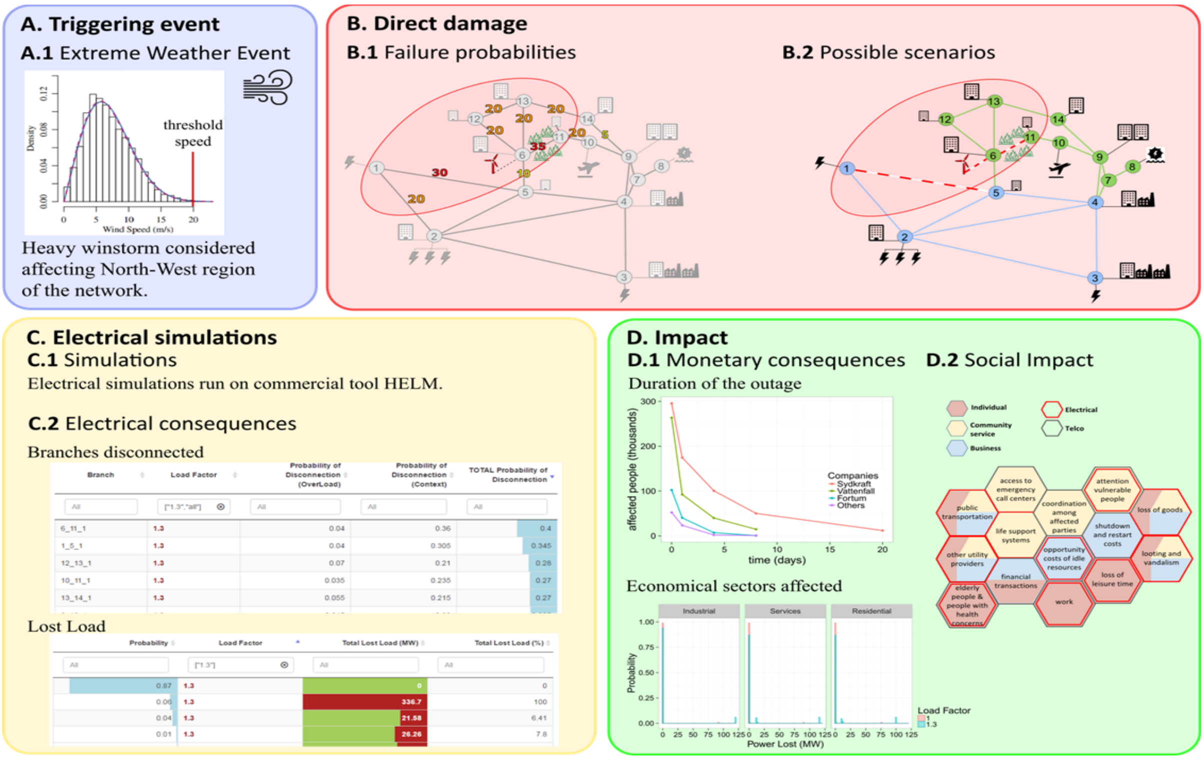

Fig.4 High Voltage Transmission Lines under the effect of heavy wind and rain [4]

R-4.2 Identification of the CI elements and their weather related threats with focus on understanding how the threats affect both the end-user and the operation

R-4.3 Interdependencies of the Electrical Power and Telecom Infrastructure with other CI.

R-4.4 Case studies of past weather-related failures in electricity and telecom networks. (Fig.4).

R-4.5 Review of the methods and procedures used in electrical power and telecommunication networks to protect critical equipment against damage from extreme weather disasters.

R-4.6 Social impact of failures in Energy & Telecommunications infrastructures.

R 4.7 Simulations for estimation of the actual distribution of power flows over the network when some elements fail.

3.4 *The results of the WP5 Risk Based Decision Making Framework*

R-5.1 Quantitative risk analysis framework for single and multiple hazards and for collateral impacts of cascading effects (Fig.5).

R-5.2 Software tool for the forecasting of the network usage given some geographically distributed consumption and generation profiles for the incident probability forecasting. The source code of this risk assessment webtool has been released as open source licence. First demonstration videos are already available on web [5].

3.5 *The results of the WP6 Quantifying Risks and Benefits*

R-6.1 Advanced risk assessment procedure for quantification of single-mode and multi-mode risks and impacts of extreme weather events on CI.

R-6.2 Assessment of the impacts of critical infrastructure failures and in the context of two case studies demonstration of the use of the RAIN Risk based Decision Making frame work and calculation of quantifiable benefits of providing resilient infrastructure (Fig.6).

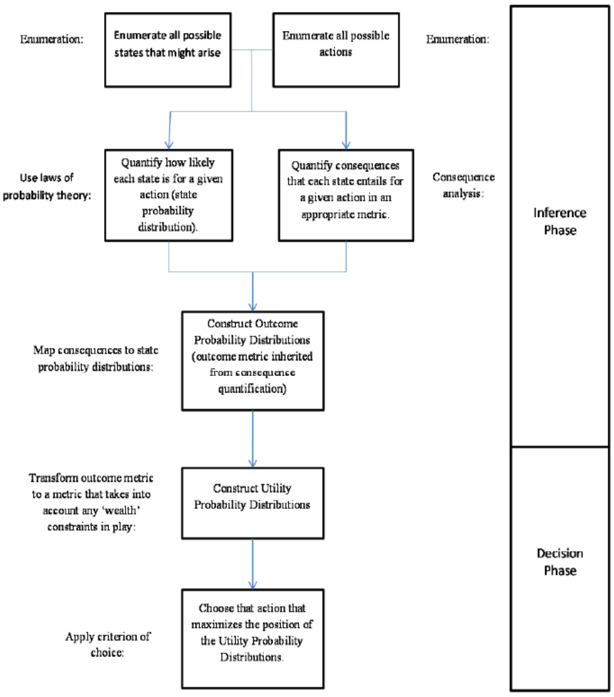

Fig.5 Quantitative Risk Based Decision Analysis [4]

3.6 The results of the WP7 Mitigation Strategies

R-7.1 Technical engineering solutions to increase the resilience of infrastructure to the effect of extreme climate events.

R-7.2 Technical Impact Matrices developed as a method for assessing the advantages and disadvantages of various maintenance strategies for reducing the impact of extreme events on infrastructure systems (Fig.7).

R-7.3 Pre-standardisation Document & Review of Crisis Coordination and Response Arrangements in the European Union which assesses the latest developments of the EU crisis coordination and decision-making arrangements and gives recommendations on how EU policies and infrastructure protection guidelines could be improved.

R-7.4 Summary of the effects of climate hazards on European infrastructure and presentation of mitigation procedures, and adaptation and coping with potential impacts to alleviate the impact on citizens.

Fig.6 Case Study Areas [6]

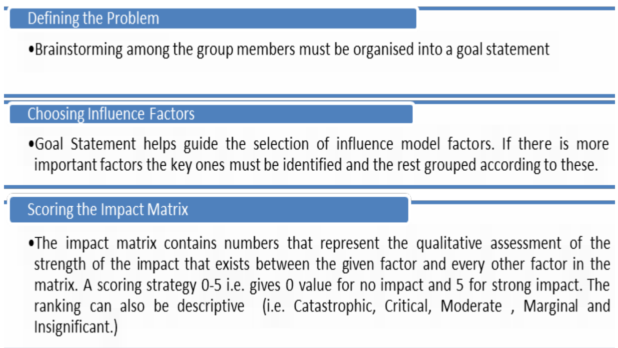

Fig.7 Methodology for Technical Impact Matrix [6]

4 Exploitation of the RAIN Project Results in Education of the Infrastructure Protection Professionals on the FSE UNIZA

Linking research projects to education has a significant impact on the quality of graduates in each study program. From the results of the project, achieved in the context of the work packages, a lot of deliverables in the form of research reports and practical case studies can be used.

In 2015 the Accreditation Commission confirmed the Faculty of Security Engineering, University of Žilina accreditation for bachelor and engineer degree programmes that focus on the field of security and protection of critical infrastructure. The study programme „Security and protection of critical infrastructure“ (thereinafter SPCI) is primarily focused on the main ECI fields – energy a transport, is multidisciplinary oriented, is focusing on various types of infrastructure networks and is based on the needs of practice. To demonstrate the contents of the study programme we only provide a selection of the most important courses for our full-time bachelor´s degree students and full-time engineer´s degree students in the study program SPCI.

Among the most important courses in the bachelor studies we rank:

• **general courses** e.g. Mathematics; Engineering geometry; Physics; Economics; Informatics; Logistics; Occupational safety and health; Technical drawing; Management; Basic of mechanics; Operational research; Managerial Statistics and others.

• **profiling courses**, e.g. Energy infrastructure; Transport infrastructure; Protection of critical infrastructure; Nuclear, chemical and biological protection; Protection of people and property; Production equipment and technologies in power engineering; Risk management; Civil protection; Crisis management; Topography, Cartography and Geographic information systems; Transport equipment and technologies; Protection of critical infrastructure objects in sectors energy and transport; Dangerous substances and articles and others.

Graduates of the bachelor degree study program Security and protection of critical infrastructure are qualified experts on the state administration and municipality, manufacturing and non-manufacturing corporate entities that operate in the field of security service. They are able to analyse basic problems and processes in security services. They can apply the appropriate system approach when identifying threats, analysing risks and designing (or proposing) practices to minimize them, when managing the removal of consequences of critical phenomena. They can use information and communication technologies, general tools of crisis and security management and analyse data obtained by monitoring the risk-bearing factors. By gaining the wide range of theoretical and practical knowledge, they find employment in lower managerial functions of critical infrastructure operators.

Among the most important courses in the engineer studies we rank:

• **general courses**, e.g. Stochastic Models of Operational research; Managerial Information Systems; Risks of industrial processes; Managerial Methods and Techniques; Psychology; Forecasting and planning and others.

• **profile subjects**, e.g. Transport in crisis situations; Protection of critical infrastructure objects; Crisis management; Building and transport structures; Protection against terrorism; Planning of critical infrastructure protection; Controlling and information systems of critical infrastructure; Risk management of critical infrastructure; Project of CI element protection and others.

Graduates of the master degree study program can identify threats and sources of risks in social, economic, natural, technical and technological processes. They are able to analyse, evaluate and design (propose) practices with the use of methods and techniques to minimize the risks. They have good knowledge of the theory of protection of critical infrastructure with the emphasis on energetics and transport. They are able to design and implement preventive actions, monitor and analyse the development of risk-bearing and crisis factors and prepare an adequate response. As a result, they can manage a continuity of operation of the critical infrastructure and renew systems effectively in the ex post phase. The complete curriculum for both levels of study programme SPCI is available on website [7].

The main advantage and a specific feature of the study programme especially is the intersection of knowledge and skills from the fields of crisis and security management [8]. The graduate´s knowledge and skills are focused on risk management, security management and ways of securing protection of important structures [9].

The RAIN project has successfully achieved the main objective in the form of developed a risk-based decision making framework for facilitating risk assessment of Critical infrastructure elements against extreme weather events and decisions on the mitigation measures for CI protection. Incorporating RAIN project results into the curriculum contributes to the better specification and innovation of the content of the more profile courses, e.g. Energy infrastructure, Transport infrastructure, Civil protection, Protection of critical infrastructure objects in the energy and transport sector, Protection of people and property, Transport in crisis situations, Crisis management, Planning of critical infrastructure protection, Controlling and information systems of critical infrastructure, Risk management of critical infrastructure, Project of CI element protection and others.

The overview of the planned use of the results of the RAIN project within the selected profiling courses of the study program is given in Tab.1.

Tab.1. RAIN project results use in courses

	Profiling course	Possible use of the results
Bachelor degree	Energy infrastructure	R2.1 – 2.5, R4.1 – 4.7,
	Transport infrastructure	R2.1 – 2.5, R3.1 – 3.4
	Protection of critical infrastruture	R5.1 – 5.2, R6.1 – 6.2,
	Protection of people and property	R6.1 – 6.2,
	Production equipment and technologies in power engineering	R4.1 – 4.7, R7.1 – 7.4
	Risk management	R2.1 – 2.5, R6.1 – 6.2,
	Protection of critical infrastruture objects in sectors energy and transport	R2.1 – 2.5; R3.1 - 3.4, R4.1– 4.7, R 6.1 - 6.2
Master degree	Transport in crisis situations	R 2.1 – 2.5, R 3.1 - 3.4; R 7.1 – 7.4,
	Protection of critical infrastruture objects:	R 6.1 – 6.2, R 7.1 – 7.4
	Planning of critical infrastructure protection	R 2.1 - 2.5, R 6.2,
	Controlling and infor-mation systems of critical infrastructure	R 7.1 – R 7.4 R 5.1 – 5.2,
	Risk management of critical infrastructure	R 5.1 – 5.2, R 6.1 – 6.2,
	Project of CI element protection	R 3.1 - 3.4, R 4.1 – 4.7, R 6.1 –6.2, R 7.1 – R 7.4

The project results contribute to the state-of-the-art on the field of Critical Infrastructure Protection and, overall, they constitute a consistent methodological approach to the management of infrastructure networks in response to the extreme weather events.

The project solution was completed on 4/2017, so only results from the first phase of the project solution have been gradually integrated into the content of the courses by now. The ambition of the authors, as members of the project consortium, is the successive implementation of more key project results into the education process. A great deal of the innovative ideas and achieved results of the RAIN project have been gradually including into the lectures for the students studying at the University of Žilina, Faculty of Security Engineering, Security and Protection of Critical Infrastructure Study program. In this way the students have opportunity to obtain access to the knowledge produced by highly experienced multidisciplinary team formed by researchers from the eight EU countries. They can become acquainted with a lot of innovative outputs promoted with examples of applications highlighting their potential of use in their future employment. From the survey conducted with CI operators and weather services they can obtain the understanding on the needs of CI operators and managers, their preparedness, vulnerability of the system and the actions taken in order to reduce the risks, from various parts of the EU.

5 Conclusions

Security of infrastructures and utilities was a part of security research activities of the FP7 Security Research. In this context the Faculty of Security Engineering of the Zilina University became a member of consortium that prepared and solved project titled Risk Analysis of Infrastructure Networks in response to extreme weather – RAIN. The topic of this project was impact of extreme weather events on critical land transport and energy & telecommunications infrastructures. The aim of this paper is to present the ways of exploitation of the RAIN project results in education of critical infrastructure protection professionals at the Faculty of Security Engineering, University of Žilina within the study programme "Security and Protection of Critical Infrastructure".

Exploitation of RAIN Project Results in education of Critical Infrastructure Protection professionals at the University of Žilina confirms the fact that linking research and education is a basic condition for the best academic institutions, where publishing innovative ideas and producing successful, well-informed students are key objectives.

Acknowledgement

This paper was supported by the European Union within the FP7 project No. 608166 "Risk Analysis of Infrastructure Networks in response to extreme weather" and by VEGA grant No. 1/0240/15 "Process model of critical infrastructure safety and protection in the transport sector".

References

[1] EASAC, Trends in extreme weather events in Europe. Halle/Germany: German National Academy of Sciences Leopoldina 2013

[2] A. O'Connor, RAIN project, Grant agreement no: 608166, 2013. Retrieved from http://rain-project.eu/

[3] A. O'Connor, W. Brazil, Mid Term Report: 1st Periodic Report, RAIN 2015.

[4] P. van Gelder et al, D5.5 RAIN Workflow Integration.TU Delft: Netherlands 2016. Retrieved from http://rain-project.eu/

[5] RAIN project. Software tool: Retrieved from (https://www.youtube.com/watch?v=gM6Ugu0F jo8&feature=youtu.be&list=PLPBl6rsXvRsCxbg-QMYoYsAdlrya92joZ)

[6] A. O'Connor, Final Report Part A: Publishable Summary, RAIN Final Report, 2017.

[7] Faculty of Security Engineering, University of Zilina. Study Plans for Study Programme "Security and Protection of CI". 2017. (in Slovak). Retrieved from http://fbi.uniza.sk/ktvi/

[8] T. Lovecek et al, Currently required competencies of crisis and security managers and new tool for their acquirement The eSEC portal. ICETA 2015 Proceedings, Starý Smokovec, Slovakia, 2015.

[9] M. Luskova, B. Leitner, "Critical Infrastructure Protection in Higher Education in Slovakia", INTED 2017-11th annual International Technology, Education and Development Conference Proceedings,Valencia, Spain 2017.