Requirement Engineering for Emergency Simulations

Alena Oulehlová, Jiří Barta, Hana Malachová, Jiří F. Urbánek

Requirement Engineering for Emergency Simulations

Alena Oulehlová, Jiří Barta, Hana Malachová, Jiří F. Urbánek

University of Defence, Department of Emergency Management,
Kounicova 65, 662 10 Brno, Czech Republic
jiri.barta@unob.cz, alena.oulehlova@unob.cz,
hana.malachova@unob.cz, jiri.urbanek@unob.cz

Abstract. Paper deals with requirement engineering that is used in the first phase of project SIMEX *(Research and development* of *simulation tools for training cooperation of actors in emergency management* by *subjects of critical infrastructure.* Project SIMEX focuses on the development of simulation tools and instruments for common interoperability training of crisis staff managers, security advice bodies and liaison safety employees in the energy sector with the integrated rescue system in dealing with emergencies and their consequences. This paper also deals with the analysis of different national systems providing publicly available information and evaluates the usability and benefits of implementation of information generated into simulation tool.

Keywords: critical energy infrastructure · emergency management · information systems · security · simulation tool

1 Introduction

Timeliness, completeness, objectivity, reliability, and accuracy are essential units to measure the effectiveness and efficiency of decision-making process in emergency or crisis situations. Monitoring and information tools play key role - in obtaining such information. Natural and anthropogenic hazard information represents statistics and other quantitative or qualitative data that are used by authorities. These authoritative bodies include, but not limited to, the emergency management authorities, individuals, households, non-governmental organizations, companies and scientific or research institutions. The same figure may render different information for different entities at the same time.

The basic information scheme about sources of danger and their transmission is similar to other information systems. This information scheme typically contains description of the transmission protocol through which the information is being transported, and the format of the information itself. One typical information format is a composition of three components: the sender, the recipient, and the information payload.

Prediction, origin and course of specific natural hazards are recorded with monitoring tools of individual environmental components managed by public authorities. Information systems in the Czech Republic that focus primarily on natural disasters

adfa, p. 1, 2011.

caused by atmospheric changes with strongest effects are the longest and most thoroughly monitored.

One of the tasks carried out by the state under normal conditions and particularly in crisis situations is ensuring the functioning and protection of key system components and services. This task has been implemented by the state since its formation. However, with the growth of intensity and occurrence of anthropogenic and natural threats and impacts on society, pressure increases for the state to improve the quality of its protection and resilience, and to reduce vulnerability. Individual systems and services, due to their importance to the society, have begun to be referred to as critical infrastructure.

One of the earliest establishment of national critical infrastructure protection occurred in the United States of America. Stemming from the country's comprehensive legal definition of the subjects of critical infrastructure, USA has now been one of the leading countries in critical infrastructure protection. Germany and the Great Britain later followed suit as they begun to deal with similar issues. The discussion on the critical infrastructure protection at European level was launched at the beginning of the 21st century after incidents of several crisis situations (floods, terrorist attacks, etc.). Current documents of European critical infrastructure protection (1) were created on principles of proportionality, subsidiarity, complementarity, confidentiality and cooperation among stakeholders. Based on application of principle of subsidiarity, the critical infrastructure in the European Union is divided into National Critical Infrastructure and European Critical Infrastructure.

2 Critical Energy Infrastructure in the Czech Republic

Czech Republic adopted required European standards (1) into the Act No. 240/2000 Coll., on Crisis Management (2) and related Act (3). Ministry of Interior of the Czech Republic - General Directorate of Fire Rescue Service was appointed as the responsible body, which then delegates tasks and responsibilities to various ministries and other central administrative authorities. In order to define various elements of critical infrastructure, there are cross functional and cross sectorial criteria in the nine areas of critical infrastructure (energy, water, food and agriculture, health, transport, communication and information systems, financial market and currency, emergency services and public administration). Cross functional and sectorial criteria identifying critical infrastructure elements are defined in the Government legislation document (3). Subjects of critical infrastructure have responsibility for protecting critical infrastructure elements by law (2). Each subject has to process crisis preparedness plans, where potential functional threats towards critical infrastructure element are identified and measures for its protection are set.

National critical energy infrastructure is divided into the following sectors and subsectors:

A. Electricity
   A.1 Production of Electricity
   A.2 Transmission System

A.3 Distribution System
B. Natural Gas
B.1 Transmission System
B.2 Distribution System
B.3 Gas Storage
C. Oil and Petroleum Products
C.1 Transmission System
C.2 Distribution System
C.3 Storage of Oil and Fuel
C.4 Production of Fuel
D. District Heating
D.1 Heat generation
D.2 Heat Distribution

There are 228 subjects of critical energy infrastructure in the electricity sector at the national level: 58 subjects in the production of electricity subsector, 133 subjects in the transmission system subsector, and 37 subjects in the distribution system subsector.

3 Simulation Tools for Training Cooperation by Subjects of Critical Infrastructure

Although ensuring proper function of energy infrastructure is crucial for the European Union, there are other sectors that play significant role in the system of critical infrastructure protection (3). This project, entitled “Research and development of simulation tools for training cooperation of actors in emergency management by subjects of critical infrastructure (SIMEX)”, focuses on the roles and responsibilities of the subjects in the critical energy infrastructure.

SIMEX project was selected from a competition held by the Technology Agency of the Czech Republic to support applied research and experimental development called "ALFA". It is classified in the sub-program of energy resources and environmental protection and preservation. The project started in September 2014. To meet the project objectives, it is necessary to identify the needs of individual stakeholders on mutual communication, quality and level of information exchange, potential threats and the state of hardware and software among stakeholders.

Without an in-depth initial requirements analysis of individual stakeholders it is not possible to create simulation software for common training of the Integrated Rescue System subjects of critical infrastructure that can improve coordination, cooperation, operability and interoperability of intervening units. The secondary objective of the project is to investigate the impacts of failure of critical energy infrastructure on environment, mitigation and prevention strategies for negative consequences from natural disasters, and the impact of protection and preservation of the environment.

3.1 Primary and Secondary Stakeholders

Requirement engineering is employed in order to achieve the project objectives (5, 6). At the currently ongoing first stage of requirement engineering, the project has identified primary and secondary stakeholders for energy critical infrastructure. Table 1 shows an overview of stakeholders who influence mitigation, solution and elimination of consequences of extraordinary event and crisis situation caused by failure of critical energy infrastructure. Identification of stakeholders was conducted in accordance to the recommendations of ISO CSR the Stakeholder Engagement Manual (7), and The Stakeholder Engagement Manual Volume II (8), focusing on emergency management in subjects of critical energy infrastructure.

Table 1. Summary of identified stakeholders in emergency management in subjects of critical energy infrastructure.

Primary stakeholders	Secondary stakeholders
Security Liaison employee	Ministry of Defence – Army of the Czech Republic (ensuring of selected objects)
Staff	State institution (e.g. the Government, National Security Council, The Czech Environmental Inspectorate, Energy Regulatory Office, Administration of State Material Reserves, District Security Council, Czech hydrometeorological Institute)
Parties (suppliers of spare parts, components, technologies, contracted subjects providing help in a crisis situation).	Media
Emergency services of Integrated Rescue System	Civil associations (NGO - Non-Governmental Organization)
Other emergency services of Integrated Rescue System	Banks
Ministry of Interior, Ministry of Interior – the General Directorate of Fire Rescue Service of the Czech Republic	
Ministry of Interior of the Czech Republic – Policy of the Czech Republic (ensuring of selected objects)	
Ministry of Industry and Trade	
Influenced Customers	
Influenced Suppliers	
Owners and Subject Investors	
External processor of crisis preparedness plan	

Identifying contracting party at the primary stakeholders is meant to be generic because specific names of legal entities and individuals are stated in the emergency preparedness plan of each given subject. The subject is contracted with them for specific range of services and assistance that will be performed in case of extraordinary events and crisis situations.

3.2 Requirements Engineering: A Communication With Stakeholders

Based on the definition of stakeholders, we began to communicate with them. In the first step there we addressed the state authorities (Ministry of the Interior of the Czech Republic, Ministry of the Interior - General Directorate of Fire Rescue Service of the Czech Republic, and the Ministry of Industry and Trade). Fundamental requirements for protection of subject of critical infrastructure, realization and practices of liaison exercises related to failure of some element of critical infrastructure, were found by interviewing responsible people. Public administration authorities pointed out several requirements that the simulation software for the joint training of the Integrated Rescue System and subjects of critical infrastructure should provide.

Requirements for the simulation software in terms of further research could be divided into the following groups:

- Requirements for core functions of the system;
- Interface requirements - interface with other systems, user interface, software, hardware and communication interfaces;
- Non-functional requirements - product requirements, external resources, etc.;
- Other requirements - including legislative requirements, software multilingualism, etc.

In the second phase there is established communication with the liaison safety staff in particular subjects. There are structured and controlled interviews with the liaison security staff. Questions for structured and controlled interviews are divided a number of particular areas: emergency management and crisis preparedness plans, preparation and realization of training simulating failure of element of critical energy infrastructure, and impacts of the critical energy infrastructure on environment. In case of unsuccessful communication with the liaison security staff, we have prepared a checklist that represents basis qualitative method of risk management.

3.3 Simulation Software for Training

For a successful creation of the simulation software for liaison training to work in real time with real geo-data and models of effects of extraordinary event effects or crisis situation, it is necessary to create good quality scenarios of extraordinary event and crisis situations process. Creating of such scenarios will require wide spectrum of requirements from different interfaces, non-functional and other requirements. The first step for creating the scenario is hazard (threats) identification concerning element of critical energy infrastructure. Qualitative, semi-quantitative or quantitative methods of risk analysis will be used to verify the correctness of created registry of danger for element of critical infrastructure in the emergency preparedness plan.

To determine technological threats and their impact, we will use risk analysis methods What-if, Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Mode and Effects Analysis (FMEA), a Hazard and Operability Study (HAZOP), Human Reliability Analysis (HRA), Chemical Exposure Index. For the sector of critical energy infrastructure, a special method RAMCAP Plus was developed. All Hazards

Risk and Resilience Prioritizing Critical Infrastructures use RAMCAP Plus approach (9).

This method is based on the general procedure of risk management (10). RAMCAP Plus, in addition, evaluates the environmental threats and mutual dependencies of regional threats. Evaluation of impact of environmental threats is based on semi-quantitative evaluation using historical data on frequency of natural threats. In relation to technological risk analysis and modelling of leakage, scatter, discharge, evaporation, explosion, and fire, many software tools were developed to facilitate the application of the above mentioned methods. These applicable methods include e.g. HAZOP Manager Version 7.0, Fault Tree +, EPRI HRA Calculator®, Security Risk Scorecard, Property Security Risk Survey, SFÉRA- ENERGY and other.

4 Proposed Solution of Simulator

To ensure the main function of proposed simulator for solution of extraordinary events of critical infrastructure subject (11), it will be necessary to take up real information about the occurrence of extraordinary event and its spread via interfaces that are available and used not only by the Integrated Rescue System. This information has at its disposal the sector of critical infrastructure and Emergency Services. Table 2 summarizes main information systems providing information about the dangers of natural extraordinary events, environmental impacts, and secondary sources of danger in case of spreading of extraordinary event or crisis situations on the environment.

From executed analysis of information and data provided by various information and monitoring systems in the area of environmental security imply that on the interface level the simulator will use data from CZRAD, EUMETSAT, Air Quality Information System (AQIS) and the Water Information System.

Radar Network CZRAD is used for detection of precipitation clouds (storms up to 250 km). It can be used to estimate the instantaneous precipitation intensity to about 150 km away from the radar (13). Real-time view of radar images of rainfall, in combination with images of lightning discharges and ward measurements, information on weather in a place where an element of critical energy infrastructure will be made available.

Table 2. Summary of significant information systems in the area of environmental safety and their operators[1]

Operator	Name of information system
Czech Hydrometeorological Institute	AMIS
Czech Hydrometeorological Institute	AWOS AVIMET
Czech Hydrometeorological Institute	CZRAD
Czech Hydrometeorological Institute	EUMETSAT
Czech Hydrometeorological Institute	Information system of the air quality (ISKO)
Ministry of the Environment of the Czech Republic	Integrated Pollution Register
Ministry of the Environment of the Czech Republic	Unified Information System for the Environment (JISŽP)
Ministry of the Environment of the Czech Republic	Information system SEA
Ministry of the Environment of the Czech Republic	Information system EIA
Ministry of the Environment of the Czech Republic	Integrated system of reporting compliance
Ministry of Agriculture of the Czech Republic	Information system Voda

EUMETSAT (European Organisation for the Exploitation of Meteorological Satellites) provides data on weather, climate, and environment. It has a system of meteorological satellites that observe the atmosphere, ocean and land surface (14). It also provides the latest data to the Czech Hydrometeorological Institute that uses it for rigorous prediction of weather forecast and issuing warnings.

Air Quality Information System (AQIS) monitors, evaluate, publish and archive data on air quality for territory of the Czech Republic through automatic air pollution monitoring stations. Local fluctuation of air pollution caused by accidents, extraordinary event and crisis situations (especially smog situations) are due to stations immediately recorded.

Water Information System "Voda" provides information about condition and flows on rivers, water levels in reservoirs, rainfall and water quality, water planning, register state of surface- and groundwater. Information in Voda Portal is provided by a wide range of authorities of Ministry of Agriculture and Ministry of Environment.

Apart from the above mentioned information systems, we recommend to incorporate interface with the Integrated Warning Service System of the Czech Hydro mete-

[1] Adapted in accordance with Act No. 174/2014 Coll., on significant information systems and their underlying criteria (12).

orological system. The Integrated Warning Service System issues alert for 32 dangerous phenomena, divided into 8 groups (temperature, wind, snow, frost, storm, rain, floods and fires). Alerts on storms, rains and floods are issued in cooperation with Prediction and Warning Service. Alerts on risk of flooding are already linked to the aforementioned Water Information System.

Publicly available information services provide detailed data on climate, soil, and hydrological drought that belong among the key data for the energy sector. Another optional system from the interface is Informational System POVIS (Flood Information System) that is developed for flood protection and flood authorities. The

System contains digital flood plans and books. The flood issue is added by Hydroecological Information System VÚV THM (HEIS VÚV).

National information systems are connected to external systems abroad, especially with neighbouring states for risk of flooding, or systems of European Union (MeteoAlarm, Floods Portal EFAs,) and system of international organizations, where Czech Republic is a member.

Some elements of European Critical Infrastructures are connected to the system of Critical Infrastructure Warning Information Network (CIWIN) (14). Warning Network was established by the European Commission in order to secure the exchange of best practices and provides a platform for the exchange of rapid alerts about threats and vulnerabilities.

5 Conclusion

SIMEX project is currently at the initial stage at the first phase of requirement engineering. The aim is to find out all necessary functions that the simulation tool should obtain for cooperative training of emergency management actors at subjects of critical infrastructure. We initially have identified primary and secondary stakeholders. Communication was later started with the primary stakeholders through a guided interview and checklist. At present, the results are being evaluated. For the exact definition of requirements and elimination of uncertainties in the area of user feedback, a workshop will be organized. This will be where this project puts the most pressure on the next phase.

In definition of simulation interface, there were defined broad spectrum of information and monitoring systems for technological and natural risks that could be used for creation and processing of real simulation scenarios that will subsequently be validated by training of subjects. This fact will significantly contribute to the increase reliability, portability and interoperability in real life scenario with a view to reducing environmental impacts, loss of human lives and damage to property.

References

1. European Commission. Act on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Council Directive 2008/114/EC.

2. Czech Republic. Act No. 240/2000 Coll., on Crisis Management and on amendments of certain acts (Crisis Act).
3. Czech Republic. Act No. 432/2010 Coll., on Criteria for determining the elements of critical infrastructure.
4. European Commission. *Critical Infrastructure Protection - Energy Infrastructure*. Available on-line at WWW <http://ec.europa.eu/energy/infrastructure/critical_en.htm>.
5. Software Engineering Institute. *A Framework for Software Product Line Practice, Version 5.0*. Available on-line at WWW <http://www.sei.cmu.edu/productlines/frame_report/req_eng.htm>. Carnegie Mellon University.
6. SUTCLIFFE, Alistair G. *Requirements Engineering*. In: Soegaard, Mads and Dam, Rikke Friis (eds.). The Encyclopedia of Human-Computer Interaction, 2nd Ed." Aarhus, Denmark: The Interaction Design Foundation. Available online at WWW <http://www.interaction-design.org/encyclopedia/ requirements_engineering.html>. Interaction Design Foundation.
7. The Stakeholder Engagement Manual Volume I: The guide to practitioners´ perspectives on stakeholder engagement. Available on-line at WWW <http://www.accountability.org/images/content/2/0/207.pdf>. Stakeholder Research Associates Canada Inc. p. 88. 2005. ISBN 0-9738383-0-2.
8. The Stakeholder Engagement Manual Volume II: The practitioner´s handbook on stakeholder engagement. Available on-line at WWW <http: //www.accountability.org/images /content/2/0/208.pdf>. Printed by Beacon Press. p. 168. 2005. ISBN 1901693220.
9. ASME Innovative technologies institute, LLC. *All-hazard risk and resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach*. 1. New York : ASME, 2009. 155 s. ISBN 978-0-7918-0287-8.
10. BOZEK, F., JEŠONKOVÁ, L., DVORAK, J. BOZEK, A. *General Procedure of Risk Management*. Economics and Management, No. 3, 2012. p. 15 to 24 ISSN 1802-3975
11. REHAK D, SENOVSKY P. Pr*eference Risk Assessment of Electric Power Critical Infrastructure.* Chemical Engineering Transactions, 2014, Vol. 36, pp. 469-474. ISSN 1974-9791. DOI: 10.3303/CET1436079
12. Czech Republic. Act No. 174/2014 Coll., on significant information systems and their underlying criteria.
13. Czech Hydrometeorological Institute. *Radar net CZRAD*. Available on-line at WWW <http://www.chmi.cz/ files/portal/docs/meteo/ rad/info_czrad/>.
14. EUMETSAT. *Monitoring weather and climate from space.* Available on-line at WWW: <http://www.eumetsat.int/website/home/ AboutUs/WhatWeDo/index.html>.
15. Ministry of Economy and Energy. *Critical Infrastructure Warning Information Network – CIWIN*. Available on-line at WWW: <http://www.mi.government.bg/en/themes/critical-infrastructure-warning-informatio -network-ciwin-333-300.html>.