PROBLEMY MECHATRONIKI
UZBROJENIE, LOTNICTWO, INŻYNIERIA BEZPIECZEŃSTWA

ISSN 2081-5891
E-ISSN 2720-5266

14, 1 (51), 2023, 123-134

PROBLEMS OF MECHATRONICS
ARMAMENT, AVIATION, SAFETY ENGINEERING

Evaluation of an Interactive Simulation of Continuity Related to the Operations and Recovery of Critical Infrastructure Facilities

Andrzej GRABOWSKI, Zuzanna URBAŃSKA,
Dariusz KALWASIŃSKI*

Central Institute for Labour Protection − National Research Institute,
16 Czerniakowska Str., 00-701 Warsaw, Poland
Corresponding author's e-mail address and ORCID:
dakal@ciop.pl; https://orcid.org/0000-0002-1176-6998

Received: August 15, 2022 / Revised: September 10, 2022 / Accepted: December 6, 2022 / Published: March 31, 2023.

DOI 10.5604/01.3001.0016.2963

Abstract. Maintaining the continuous operation of Critical Infrastructure (CI) facilities and restoring them after a disaster is an important task for the functioning of individual communities and even the country as a whole. For this reason, tools are being developed to assist staff responsible for the operation of CI facilities. One interesting example of this type of tool is interactive training simulations implemented in virtual reality. This type of simulation allows procedures to be practised in situations where the continuity of the CI facility is threatened, and the procedures to be followed after a CI facility failure. This paper presents the possibilities of interacting with the virtual environment during a training simulation. Preliminary results are also discussed. Concerning research into the usability of such a training tool, the acceptance of the technology used etc.
Keywords: Critical Infrastructure, reliability, virtual reality, training application design

1. INTRODUCTION

Critical infrastructure facilities are designed to operate for a long time (several decades). This is made possible through the maintenance, updating and integration of new technologies. It is also often necessary to increase capacity to meet changing and growing demands. This leads to the need to incorporate flexibility and adaptability to future (unknown at the design stage) requirements into the design in order to respond effectively to the ever-changing technology, societies, economic environment, legislation and policies that determine the service demand profiles and corresponding expected performance of critical infrastructure facilities.

These issues are difficult to analyse because, due to the complexity and diversity of the critical infrastructure facilities, emerging near-misses can arise at a whole-system level as a response to theoretically safe elementary events. This makes it difficult to take into account all the risks in a system of interdependent critical infrastructures. This means there are significant uncertainties in characterising potential failure scenarios for critical infrastructure facilities [1].

From a practical point of view, it is a fact that the functioning of critical infrastructure facilities is disrupted by an increasing number of system-level failures, which are the result of small perturbations and cascading faults growing to a large scale. Not surprisingly, the protection and resilience of critical infrastructure has become a national and international priority. A thorough vulnerability analysis and resilience assessment is needed to ensure the protection and continuity of critical infrastructure facilities [2].

Classical methods of system vulnerability and risk analysis cannot always capture the (structural and dynamic) complexity of CI; a full analysis of these systems cannot be carried out by classical methods. A framework is needed to integrate methods capable of looking at the problem from different perspectives (topological and functional, static and dynamic), suitable for dealing with high system complexity and associated uncertainties [3]. New methods for analysing IK resilience have therefore been proposed in the literature [4, 5].

As described earlier, CI is exposed to many types of threats, such as natural hazards, ageing and component failure, surge in load demand, climate change, and deliberate attacks. This means that critical infrastructure protection is becoming increasingly important. Particular emphasis is placed on traditional physical protection and the strengthening of available resources [6-9]. Protecting the functioning of CI, requires modelling the vulnerability of CI components against various threats, followed by a system-wide risk and vulnerability analysis.

In recent years, lessons learnt from some catastrophic accidents have extended the focus on increasing CI resilience, as well as adaptation and rapid recovery from the effects of a disruptive event [9-12].

CI systems should not only be reliable, but also capable of overcoming disruptions [13]. Government policy has also evolved to encourage efforts that would allow CI to continue to operate at a certain level or be quickly restored to full capacity after a disruption [14]. As a consequence, resilience is now considered an essential attribute of CI, which should be guaranteed by the proper design, operation and management of CI functioning.

CI sites are not isolated, but highly interconnected and interdependent [15-18]. For example, water and telecommunications systems need a constant supply of electricity to maintain normal operations, while electricity systems require the provision of water and various telecommunications services to generate and deliver power. Interdependencies can improve operational efficiency, but at the same time can increase the vulnerability of the overall system. Failures at a single CI site can cause cascading failures, causing faults on a regional or national scale. In addition, as the population and demand for resources grows, most CI facilities are becoming increasingly stretched. Increasing demands have not been met by adequate capacity and efficiency growth, and major power outages (affecting 1 million or more people) occur on average every four months in the US [19]. The sensitivity of a single CI facility can easily be increased due to interdependencies.

2. VIRTUAL ENVIRONMENT OF CRITICAL INFRASTRUCTURE SITES

The reference facilities selected to evaluate the usability of interactive training simulations on business continuity and recovery of critical infrastructure facilities were a power station, a combined heat and power plant, a gas compressor station and a water treatment plant. The content of example virtual training simulation environments is shown in Figure 1.

Fig. 1. A fragment of one of the interior rooms of the virtual environment of a CHP plant (left) and a fragment of the virtual environment of a gas compressor station (right)

3. POSSIBLE INTERACTIONS IN VIRTUAL REALITY

Emergency development scenarios of a critical infrastructure facility using the example of: power plant, CHP plant, gas compressor station and water treatment plant.

In all scenarios, the simulation is about playing the role of an employee of a Critical Infrastructure (CI) facility, similar to the non-computer-assisted RPG simulation games used to practice emergency management. However, the type of tasks performed by the simulation participant varies. Depending on the simulation scenario, the trainee supervises the operation of the CI facility or takes part in activities to restore the CI facility and neutralise the consequences of the failure.

The three scenarios for the virtual environments of the CHP plant, natural gas compressor station and water treatment plant are primarily concerned with keeping the CI facility running. The participant in the simulation is in the control centre of the IK facility, where a variety of the information about the functioning of the individual components reaches them (Fig. 2). Sources of information can include video monitoring, sensor readings, measurement results (e.g. flow meter readings), and CI facility staff. The scenario focuses on the correct course of action when a situation occurs that indicates possible damage or a cyberattack. The simulation participant's task is to react quickly to sensor indications or information from staff so that the operation of the CI facility does not come to a halt. This is an important part of the training, as many failures or malfunctions of CI components are due to management errors, negligence or inadequate maintenance. A further advantage of the simulation is that the training section shows the possible causes and also the consequences of a situation occurring, as well as the process of responding to malfunctioning telemetry, e.g. by verifying indications through the use of hand-held measuring equipment or an on-site inspection at various points of the CI facility. The participant in the simulation also has the option to give commands to various employees at the CI facility (Fig. 3).

A different type of approach is used for the five power plant scenario options. The simulation is then more dynamic in nature and concerns the conduct of operations by one of the employees who was on the CI site when the accident occurred. The task of the simulation participant, who is free to move around the CI facility, is to carry out activities to assess the consequences of the accident, secure the various components of the CI facility, neutralise the hazards and assist the injured (Fig. 3). These are typical actions necessary to be carried out when the CI facility needs to be restored. In simplistic terms, this scenario can be said to have a 'tactical' action character, in contrast to previous scenarios for which the 'strategic' action character was predominant.

Fig. 2. Control stations in the water treatment plant (left) and gas compressor station (right)

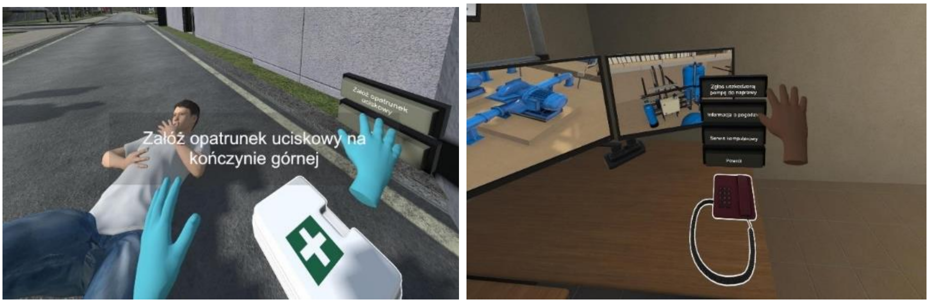

Fig. 3. Examples of interactions with the virtual environment: giving pre-medical first aid (left) and making phone calls (right)

4. PRELIMINARY TEST RESULTS

At the end of the participatory study, tests were additionally conducted on the impact of the virtual environment on the trainee and the subjectively assessed usability *System Usability Scale* (SUS) [20] and the acceptance of technology (TAM)

Results related to the level of symptoms of so-called simulator sickness are shown in Fig. 4. These symptoms were measured using Kennedy's SSQ *(Simulator Sickness Questionnaire*) on a scale of 1 to 4 before and after the training simulation. Contact with the virtual environment causes a slight, negligibly small increase in the occurrence of these symptoms.

The realism of the virtual environment was measured using the SPQ *(Spatial Presence Questionnaire*) on a scale of 1 to 7 (Fig. 4). The highest scores were obtained for the attention commitment component (97% of the maximum value) and possible actions (89% of the maximum value).

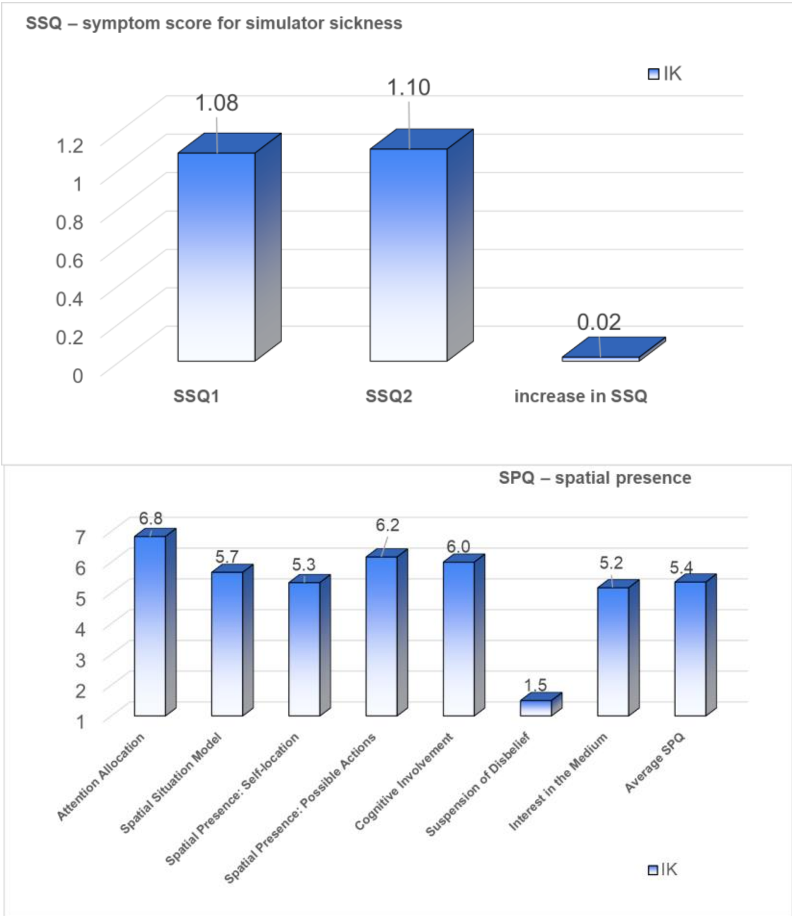

Fig. 4. Change in the level of symptoms of so-called simulator sickness (left) and assessment of the realism of the virtual environment (right)

This means that the training simulation is highly engaging, which should have a positive effect on remembering information. The high value of the possible actions component is a result of the extensive interactions with the virtual environment and the complexity of the prepared simulation of the operation of the CI facility. The lowest value is for the component sustaining disbelief (21%), which means that the experts were aware all the time that they were participating in a training simulation.

Usability was measured using the SUS questionnaire. The mean value obtained (85) indicates that both systems are considered useful as, according to data from 206 studies presented in [22], the median SUS value is 70.91 (the usefulness of the developed training simulation is higher than for most other systems). According to the review study, the fourth quarter is in the range of 78.51 to 93.93. The result obtained is within this range.

According to the data presented in [22], a higher result was obtained in only 7% of the studies. This indicates that the expert-assessed usability of the developed VR system is very high.

The results of the technology acceptance and overall training quality assessment are shown in Figure 5.

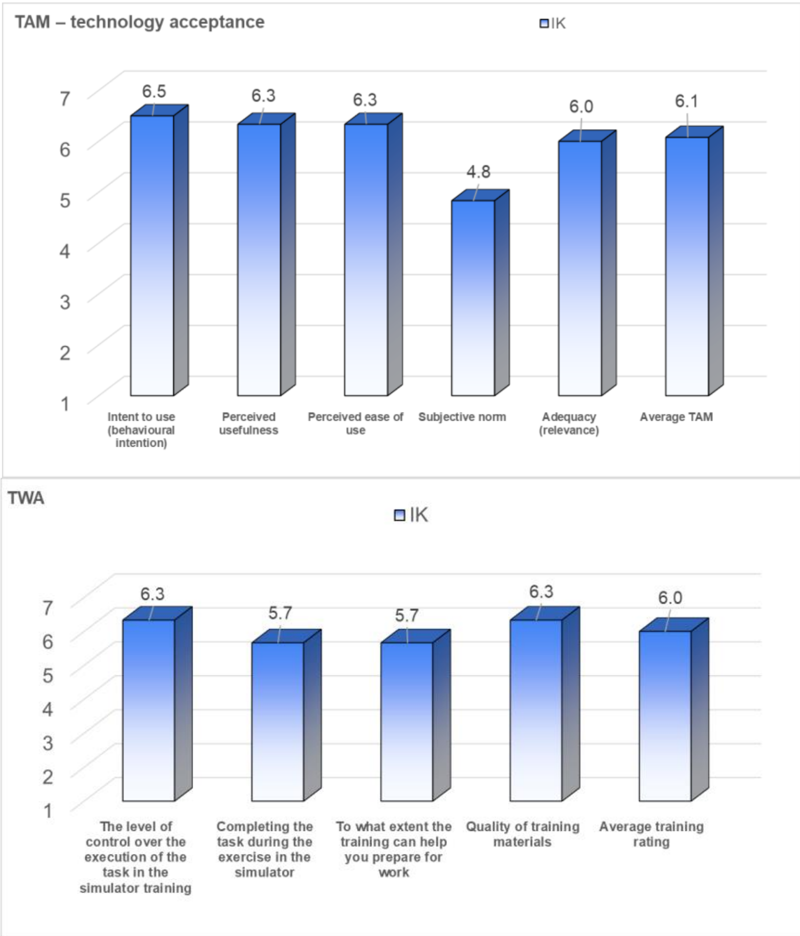

Fig. 5. Level of technology acceptance (left) and overall assessment of training quality (right)

The overall level of acceptance of the technology is very high (87% of the maximum value). From a practical implementation point of view, two components of this questionnaire are the most important: intention to use and subjectively perceived usefulness. Very high values were obtained for both of these components, 93% and 90% of the maximum value respectively.

The overall level of the training (86% of the maximum value) and the quality of the training materials (90% of the maximum value) were also rated very well.

The results collected using the NASA Task Load Index questionnaire on a scale of 1 to 20 and the Dundee Stress State Questionnaire (DSSQ) on a scale of 1 to 7 are shown in Fig. 6.

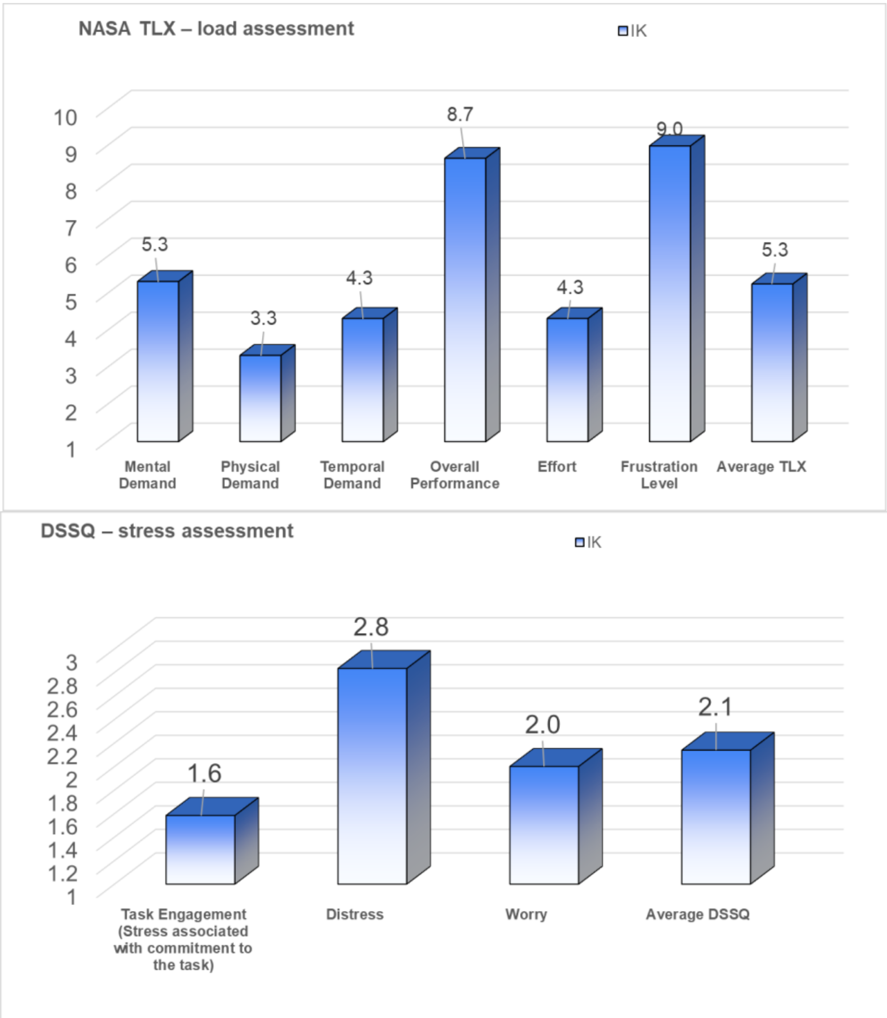

Fig. 6. Assessment of the burden of participating in a VR simulation (left) and stress levels (right)

The results clearly indicate that participation in a VR training simulation is associated with relatively low stress (e.g. using the developed interface is not difficult or frustrating) and is not a source of additional stress. This result also indicates that the VR simulation was prepared correctly.

5. CONCLUSIONS

Four different virtual environments (power plant, CHP plant, gas compressor station and water treatment plant) were developed with the implementation of variant training scenarios. Prior to the research with the experts, all changes were tested on an ongoing basis, which provided information on the necessary corrections and modifications to be made. Virtual environments were changed, including a complete redesign and significant expansion of the control room stations at the three CI facilities. The results of the internal tests also provided valuable information, which was used to modify the control interface and the course of interaction with the virtual environment. A wide range of possibilities have been added for the interaction between the VR environment and the simulation participant.

On the one hand, the trainee has access to the visualisation of a wide variety of data sources (e.g. sensor indications, telemetry, alarm signals, telephone or face-to-face conversations with employees, surveillance video or a direct on-site visit to the premises where damage to or malfunctioning components in the CI facility have occurred), while on the other hand, he or she has a wide range of possibilities for influencing the state of the virtual environment (e.g. switching machines on/off, giving orders to colleagues directly or by telephone, reporting information about a cyberattack, providing assistance to those affected, personally verifying the condition of machines and even maintaining/repairing them or cooperating with fire brigade officials to neutralise the effects of a failure). The work has resulted in extensive and extensively tested training simulations on both 'strategic' (maintaining the continuity of the CI facility) and 'tactical' (post-disaster operations linked to the neutralisation of threats and the restoration of the CI facility to proper functioning) levels.

The fully developed and intensively tested training simulations were verified with CI experts, including CI staff. The results obtained confirm the very high usability of the training simulations developed and the very high level of acceptance of the technology. The realism of the simulation related, among other things, to possible interactions with elements of the virtual environment was also rated very well. Similarly, the overall quality of the training and course materials. On the other hand, training simulation does not cause a significant increase in the level of simulator sickness symptoms, nor is it associated with high levels of stress or strain.

It follows that being in the developed virtual environment does not adversely affect the comfort of the trainee. From a practical point of view, indicators of intention to use and perceived usefulness are important, so it is worth noting that the expert ratings are also very high in this area.

FUNDING

This publication has been drawn up on the basis of the results of Stage V of the multi-annual programme: “Improvement of work safety and conditions”, financed in the period 2020-2022 with regard to scientific research and development works from the resources of the Ministry of Education and Science /National Centre for Research and Development. Programme coordinator: Central Institute for Labour Protection — National Research Institute, Warsaw, Poland.

REFERENCES

[1] Zio, E., and T. Aven. 2011. “Uncertainties in smart grids behavior and modeling: what are the risks and vulnerabilities? How to analyze them?”. *Energy Policy* 39 (10) : 6308-6320.

[2] Rigaud, Eric, and Franck Guarnieri. 2006. Proposition of a conceptual and a methodological modeling framework for resilience engineering. In *Proceedings of the 2nd Symposium on Resilience Engineering*. 8 pages. France: Juan-les-Pins.

[3] Kröger, Wolfgang, and Enrico Zio. 2011. *Vulnerable systems*. Springer.

[4] Wang, Shuliang, Liu Hong, Xueguang Chen, Jianhua Zhang, and Yongze Yan. 2011. Review of interdependent infrastructure systems vulnerability analysis. In *Proceedings of the 2nd International Conference on Intelligent Control and Information Processing (ICICIP).* pp. 446-451, China: Harbin, 25-28 July 2011.

[5] Ouyang, Min. 2014. “Review on modeling and simulation of interdependent critical infrastructure systems”. *Reliability Engineering and System Safety* 121 (C) : 43-60.

[6] Bush, W. George. 2002. *Homeland Security Pres Dir-3* (HSPD-3). USA: Washington, DC.

[7] Bush, W. George. 2003. *Homeland Security Pres Dir-7* (HSPD-7) USA: Washington, DC.

[8] Clinton, Bill. 1998. *Presidential decision directive PDD-63, protecting America’s critical infrastructures*. USA: Washington, DC.

[9] Lewis, G. Ted. 2006. *Critical infrastructure protection in homeland security: defending a networked nation*. Wiley-Interscience.

[10] Obama, Barack. 2013. *Presidential policy directive 21: critical infrastructure security and resilience*. USA: Washington, DC.
[11] Pursiainen, Christer. 2009. "The challenges for European critical infrastructure protection". *Journal of European Integration* 31 (6): 721-739.
[12] Cimellaro, Paolo Gian, Andrei M. Reinhorn, and Michel Bruneau. 2010. "Framework for analytical quantification of disaster resilience". *Engineering Structures* 32 (11) : 3639-3649.
[13] Zio, Enrico. 2009. "Reliability engineering: old problems and new challenges". *Reliability Engineering Systems Safety* 94 (2) : 125-141.
[14] Moteff, D. John. 2012. Critical infrastructure resilience: the evolution of policy and programs and issues for congress. In *Congressional Research Service Report*. R42683, www.crs.gov.
[15] Rinalidi, M. Steven, James P. Peerenboom, and Terrence Kelly. 2001. Identifying, understanding and analyzing critical infrastructure interdependencies. In *IEEE Control System Magazine* pp. 11-25.
[16] Peerenboom, P. James, R.E. Fisher, Steven M. Rinaldi, and Terrence Kelly. 2002. "Studying the chain reaction". *Electric Perspectives* 27 (1) : 22-35
[17] Benoit, Robert, M.H. Senay, M.E.P. Plamondon, and J.P. Sabourin. 2003. *Characterization and ranking of links connecting life support networks*. Canada, Ontario: Office of Critical Infrastructure Protection and Emergency Preparedness.
[18] Ouyang, Min. 2014. "Review on modeling and simulation of interdependent critical infrastructure systems". *Reliability Engineering & System Safety* 121 : 43-60.
[19] Lave, B. Lester, Jay Apt, Alex Farrell, and M. Granger Morgan. 2005. Increasing the security and reliability of the USA electricity system. In *The economic impacts of terrorist attack*s (H.W. Richardson, P. Gordon, J.E. MooreII - Eds.), Edward Elgar Publishing, Inc., Cheltenham, pp. 57-70.
[20] Brooke, John. 2013. "SUS: a retrospective". *Journal of Usability Studies* 8 (2) : 29-40.
[21] Venkatesh, Viswanath, and Fred D. Davis. 2000. "A theoretical extension of the technology acceptance model: Four longitudinal field studies". *Management Science* 46 (2): 186–204.
[22] Bangor, Aaron, Philip T. Kortum, and James T. Miller. 2008. "An Empirical Evaluation of the System Usability Scale". *International Journal Of Human-Computer Interaction*, 24(6), 574-594.

Ocena interaktywnej symulacji zachowania ciągłości funkcjonowania i przywracania sprawności obiektów infrastruktury krytycznej

Andrzej GRABOWSKI, Zuzanna URBAŃSKA,
Dariusz KALWASIŃSKI

*Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy,
ul. Czerniakowska 16, 00-701 Warszawa.*

Streszczenie. Zachowanie ciągłości funkcjonowania obiektów Infrastruktury Krytycznej (IK) oraz przywracania ich sprawności po awarii jest istotnym zadaniem z punktu widzenia funkcjonowania poszczególnych społeczności, a nawet całego kraju. Z tego względu rozwijane są narzędzia wspomagające kadry odpowiedzialną za funkcjonowanie obiektów IK. Jest z interesujących przykładów tego typu narzędzi są interaktywne symulacje szkoleniowe realizowane w wirtualnej rzeczywistości. Tego typu symulacja pozwala na przećwiczenie procedur postepowania w sytuacjach, gdy zagrożona jest ciągłość funkcjonowania obiektu IK, oraz procedur postępowania po awarii obiektu IK. W artykule przedstawione są możliwości interakcji z środowiskiem wirtualnym w czasie symulacji szkoleniowej. Omówione są również wstępne wyniki badań dotyczących m.in. użyteczności takiego narzędzia szkoleniowego oraz akceptacji zastosowanej technologii.

Słowa kluczowe: infrastruktura krytyczna, niezawodność, rzeczywistość wirtualna, projektowanie aplikacji szkoleniowych