Crisis Situation Operational Investigation and Modelling in the Organizations of Critical Infrastructure

JIŘÍ F. URBÁNEK, JITKA JOHANIDISOVÁ & JIŘÍ J. URBÁNEK
Department of Crisis Management
College of Regional Development
Žalanského 68/54, 16300 Prague
CZECH REPUBLIC
jiri.urbanek@unob.cz http://www.vsrr.cz

Abstract: - Crisis situation operational investigation and modelling in the organizations of critical infrastructure is main theme of this paper. The cases of crisis situations have an origin in accidental, incidental, disruptive and emergency events operational occurrence in the organizations of critical infrastructure especially. Their crisis managements need operational coping of crisis situations according pre-prepared crisis scenarios. The forms, characteristics, behaviour and utilization of these crisis scenarios have various qualities, depending on real critical infrastructure organization. Paper´s first objective is to find and investigate the critical zones and functions in critical situations models of the DYVELOP method. They are able to identify problematic critical zones and functions, displaying critical interfaces among actors of crisis situations. Second objective proposes the discovering and modelling of the cycling cases and their phases, which the crisis management is obliged for successful coping of crisis situations. Several times cycling of these cases is necessary condition for the encompassment of the both the emergency event and the mitigation of organization´s damages. Uninterrupted and continuous cycling process brings crisis management fruitfulness and it is good indicator and controlling actor of organizational continuity and its sustainable development advanced possibilities in any crisis. The locations of critical interfaces are the flags of crisis situation in real organization of critical infrastructure. The research reliable rules and algorithmic procedures are derived for the detections of these interfaces.

Key-Words: - crisis situation, models, algorithms, coping, management, Organizations of critical infrastructure

1 Introduction

European critical infrastructure (ECI) is defined in [1] as the assets, systems and their sections, situated in EU member state that are important for a preservation of the most important social functions, for the health, security, economic and social conditions ensuring of the population, whose the disturbance or destruction would have weighty impact for member state in a consequence of these function´s malfunction. In the same sense, the Czech critical infrastructure (CzCI) [2] is defined. Simultaneous and future security situations need better method for emergency planning and preparedness for crisis situations investigation and modelling in above critical infrastructure organizations (further only Organizations). Every crisis situation has an origin in the accident or incident occurrence, arising from relevant threats and perils in certain systems, processes, factors, environments and circumstances of real Organizations. The accident or incident will be titled further as an disruptive event (DE) in critical infrastructure context. Its crisis management needs operational coping of crisis scenarios in advance prepared by organization´s security unit. The forms, characteristics, behaviour and utilization of these crisis scenarios have various qualities, depending on real organization. But they must be parameterized by real time at real environments in scenario´s model, using investigative, analytic, evaluative, modelling and simulative tools of the DYVELOP method (Dynamic Vector Logistics of Processes) [3]. It shows that crisis situation must be generally modelled, operated and coped in cyclic threats/ peril life cycles. Uninterrupted cycling process is good indicator and controlling actor of organization continuity abilities and its sustainable development advanced possibilities in the crisis [4]. The cycles have several steps, formally classified as the cases. Several times cycling of these cases is a condition for the encompassment of emergency event by organizational crisis management finally. The solutions of these cases presuppose organization´s critical functions identification. Their flags are critical or crisis interfaces appearances among the

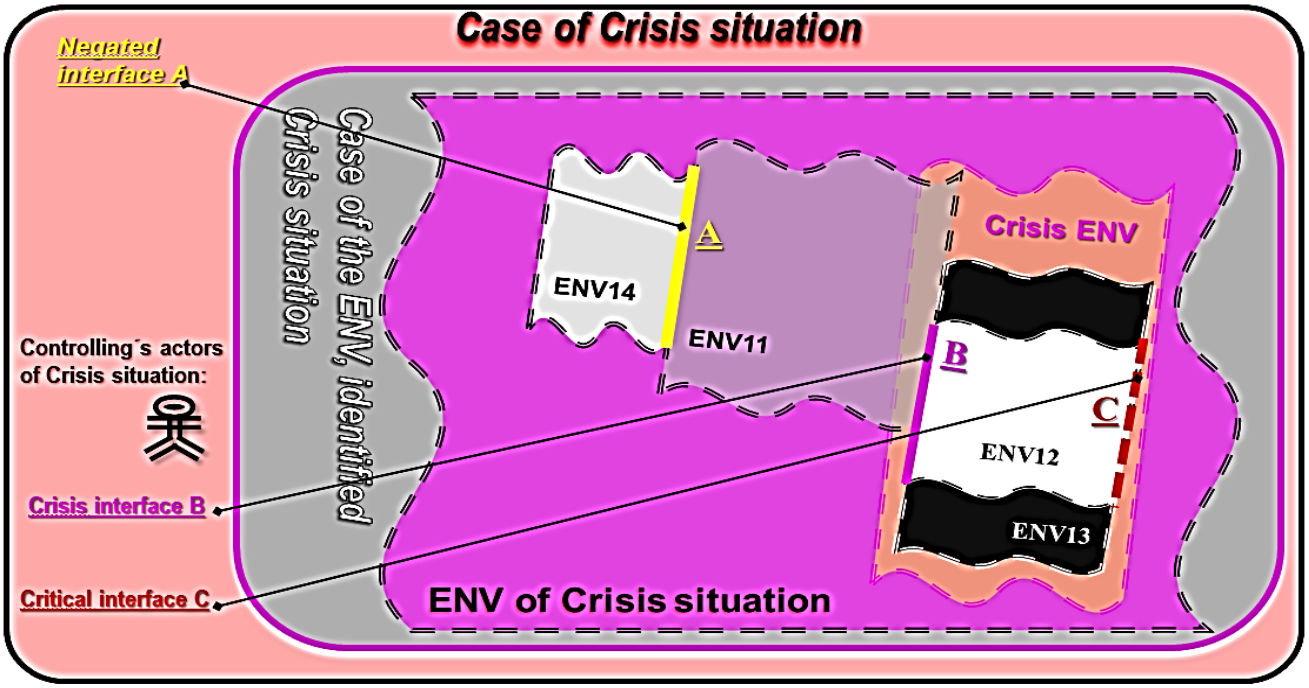

Fig. 1 Negated, critical and crisis interfaces at the ⟨⟨*Case of Crisis situation*⟩⟩.

entities of DYVELOP model of existing crisis situation in real Organization.

Within our research, reliable rules and algorithmic procedures are derived for the detections of these interfaces in CzCI. It brings new possibility for a displaying and exact evaluation of CzCI´s organizational security awareness. Special accent is put on computerised assistance for the both the crisis situation modelling and the situational estimation in real time. It allows modelling and simulation processes for better decision making of crisis/ disaster management in the CzCI. The objectives our current research work reflect first and second objectives, defined in the abstract: First objective is to find and investigate critical zones and functions in critical situations models, which are displayed as the critical and/ or crisis interfaces of entities (here the environments – ENV) at the Fig. 1. Second objective proposes the discovering and modelling of the cycling cases and their phases, which the crisis management is obliged for successful coping of crisis situations, see Figs. 2, 3 and 4.

2 Problem Formulation

The interface represents outer contour (boundary) of entity´s symbol, expressing blazonry the relative role or relationship on process scene model, symbolizing information change or transformation. See Fig. 1, where the entity´s negated interface (A), having NOT function, relation or Boole´s operator, it has always character of the collision, conflict, problem, crisis and/or battle. Critical interface (C) needs at least two antagonistic entities occurrence. The C is shown on just a single line, shared by the both or more these entities in the models. A typical characteristic for the C is that through themselves the critical functions are running or passing on relevant crisis situation or event. Crisis interface B is a joint of two negated entities ⟨⟨ ENV 11 and 12⟩⟩ and two antagonistic (black X white) entities ⟨⟨ENV 12 and 13⟩⟩. Critical function´s scene of this case has nested task-case *⟨⟨Case of the ENV, identified Crisis situation⟩⟩* at the Fig.1. The environment ⟨⟨Crisis ENV⟩⟩ has partially embedded three negated entities (environment´s symbols are used) ⟨⟨ ENV11; 12; 13⟩⟩ and it include the both the critical and the crisis interfaces. An icon of "little man" is controlling actor of ´Crisis situation´ processes. Partial result of our current work and first objective answer is that the models of DYVELOP method are able for the modelling of the critical and even crisis interfaces. It is a presumption for successful displaying of emergency event´s /situation´s models of critical infrastructure organizations.

3 Problem Solution

Any crisis situation (CS) scenario is characterized by more than one critical or crisis interfaces. Our next task is to model such the CS and then to bring

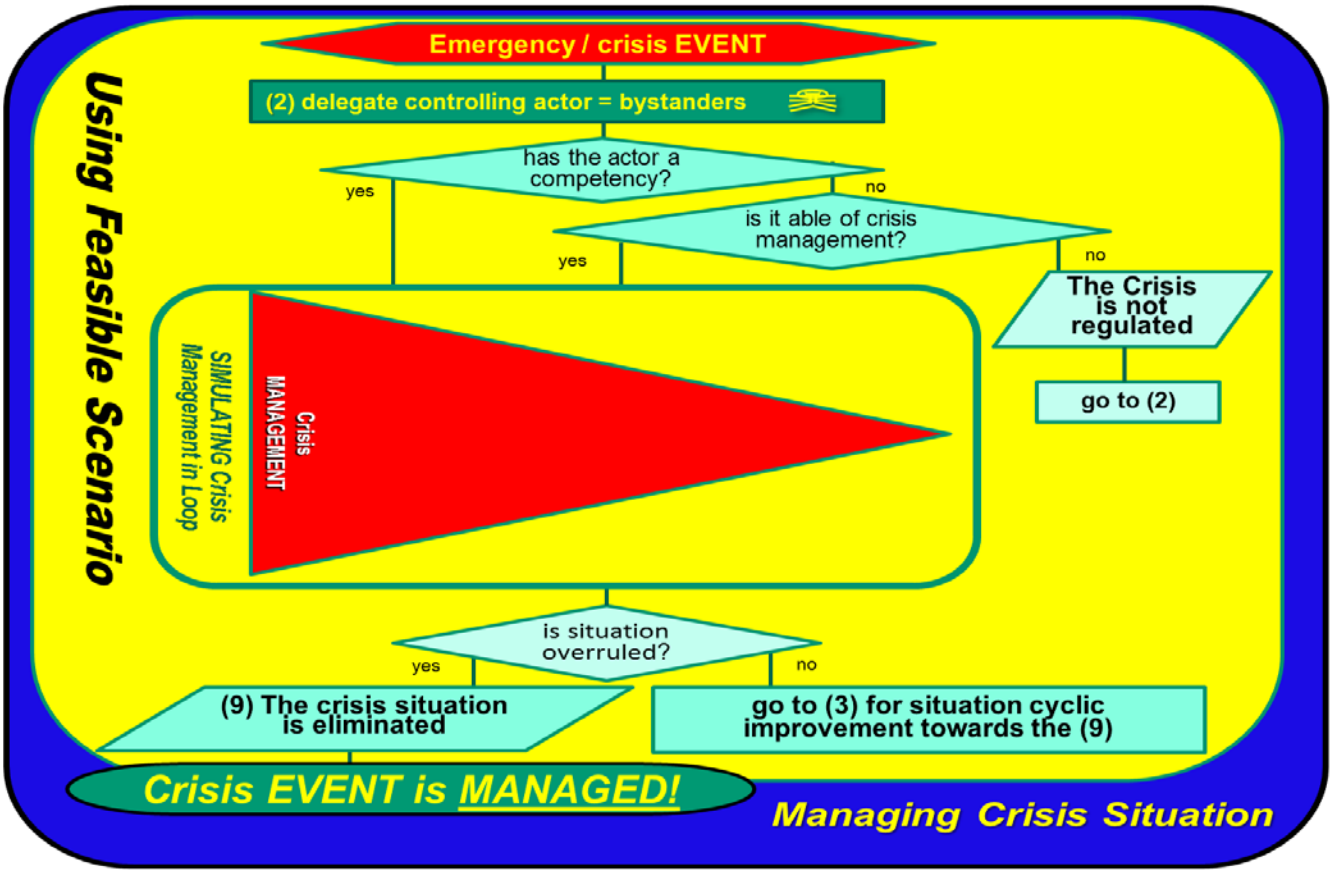

Fig. 2 Feasible algorithmic scenario of crisis management operation - 1st layer

feasible simulation of its scenario solution. Formal graphic DYVELOP´s model of this CS is from two-layer blazon. 1st layer is displayed at Fig. 2.

Here the algorithmic scenario serves for virtual crisis management operation with many critical interfaces in the CS, simulating state metamorphosis from incoming process system (starting block) ⟨⟨Emergency / crisis EVENT⟩⟩ to terminal activity case (final block) *⟨⟨ Crisis EVENT is managed!⟩⟩*. The feasibility of this algorithmic scenario is facilitated ("fortune having"), by "a bystanders", which is presented here as a controlling actor, capable of competent crisis management. Then it has control over a Case Simulator *⟨⟨ SIMULATING Crisis Management in Loop⟩⟩* in the frame of predefined scenario. It inherently takes a role of crisis management, within process system (triangle symbol) ⟨⟨Crisis MANAGEMENT⟩⟩. At Figure 3, the Case Simulator´s core is the cycling loop with next six using cases = consequent steps in 2nd layer: *⟨⟨(3) Displaying of crisis situation (Blazon, model) ⇒ (4) Sharing more critical interfaces ⇒ (5) Simulating of situational regulation ⇒ (6) Designing of Process Systems ⇒ (7) operating of crisis situation ⇒ (8) testing & improving of crisis situation⟩⟩*.

Complete algorithmic scenario has several decision making blocks. For this reason is possible expect the decreasing of scenario complexity [5]. But in a true, here rich scenarios embranchment is supporting for the crisis scenarios feasibility in a training of the CzCI.

The playing entities are not only in cooperative relations in real critical infrastructure scene. But always there have been numerous participating ´enemies´, which are in apparent or hidden opponent roles with prosperous organization system. They can overgrow till in antagonistic dramatically irreconcilable relations, resulting to crisis scene or even to battle theatre. But for a purpose of this paper, the main behaviour of modelled entities of CzCI will be trended to continuity obtaining in organizational processes.

Continual cycle is native controlling actor for any course almost of all natural or healthy man-made processes. Any uninterrupted cycling of the processes is good indicator of sustainable development. General research question asserts to the foreground of organization system´s vulnerability and security during not only economic, but even any process of ´life cycles´: *How are resilient and resistant organizational "life cycle processes" against relevant threats, perils and hazards?* [6]. The

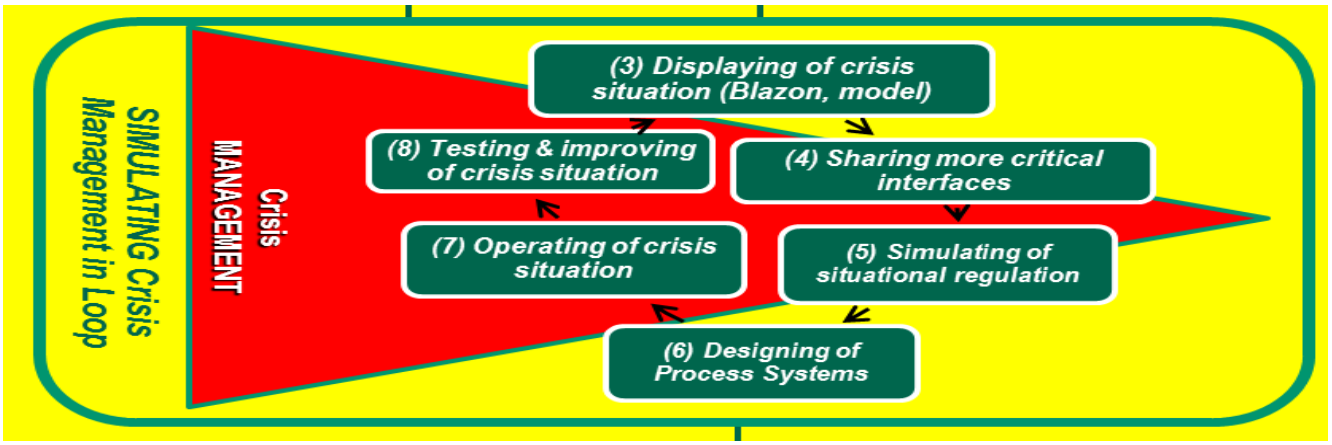

Fig. 3 Feasible loop scenario of crisis management operation, nested detail of Case Simulator of 2nd layer

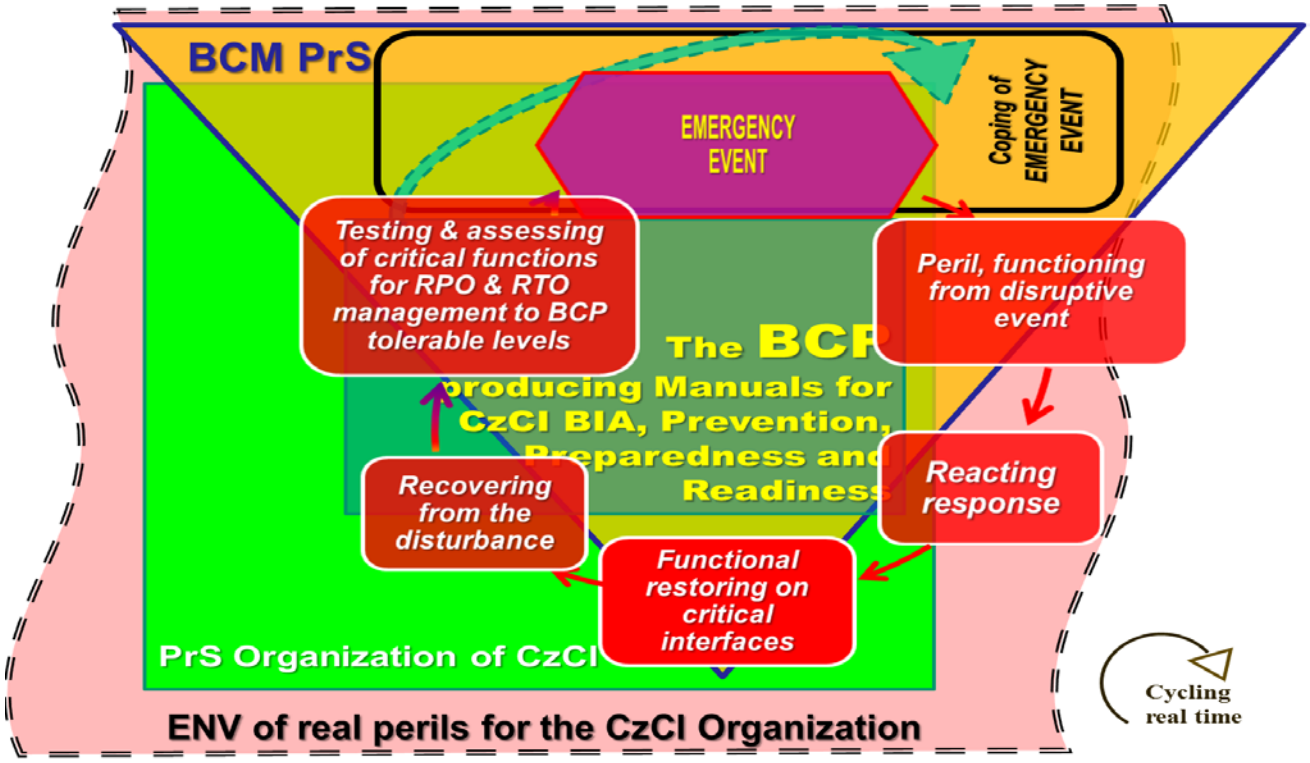

Fig. 4 Business continuity management system´s operation in Czech critical infrastructure

answer is given by our research in CzCI, reflecting first and second objectives, (defined in abstract):

- By means minimizing of the quantity and functions of critical zones and critical interfaces especially;
- And by means ´steadiness and permanency improvement´ of cycling processes and their robustness & resilience against continuity erosion.

In the Fig. 4, two-layer blazon is displayed. Here, the CzCI´s crisis management PrS (Process System) [7] named ⟨⟨BCM PrS⟩⟩ (triangular symbol) defines relationships with organizational total management system of the ⟨⟨PrS Organization of CzCI⟩⟩ (big tetragonal symbol) and with The Business Continuity Planning PrS ⟨⟨The BCP, producing Manuals for CzCI BIA, Prevention, Preparedness and Readiness⟩⟩ (nested small tetragonal symbol). It sets and innovates the continuity cyclic process approach of total integrated management system activities and processes in whole CzCI organization, using Business Impact Analysis (BIA) and others evaluative tools. Helpful can be the analytic, planning, testing and auditing procedures, according of international and global standards [8], [9] and [10] in blazoning scenario at Fig. 4. They all use for the processes improvement by means of systematically and permanent prevention, preparedness & readiness. They all are operated and integrated into organizational threat´s environment ⟨⟨ENV of real

perils for the CzCI Organization⟩⟩. They provide threats prediction, prevention, preparedness and readiness, as well as the risk analysis and scenario design for continuity solution and testing of organizational acceptance and maintenance services for the ⟨⟨PrS Organization of CzCI⟩⟩. These services are implemented only, if an ⟨⟨EMERGENCY EVENT⟩⟩ (hexagon symbol) occurs in necessary crisis/ emergency operation, then leadership take the ⟨⟨BCM PrS⟩⟩. It is clear that this ⟨⟨BCM PrS⟩⟩ response procedure is initiating only after ad hoc ⟨⟨EMERGENCY EVENT⟩⟩ occurrence, which activates ´critical functions at critical interfaces´. Then it immediately acts and operates scenario procedures (use cases) in the cycle at Figure 4: *⟨⟨Peril, functioning from disruptive event ⇒Reacting response ⇒Functional restoring on critical interfaces ⇒Recovering from the disturbance ⇒Testing & assessing of critical functions for RPO & RTO management to BCP tolerable levels⟩⟩.* In real time cycling, these use cases cycles are multiple repeating for the RPO & RTO successful obtaining. It brings ⟨⟨EMERGENCY EVENT⟩⟩ elimination and consequently it is issuing to terminal asked the *⟨⟨Coping of EMERGENCY event⟩⟩.* It guarantees satisfy CzCI Organization continuity and survival, subsequently improving the processes of the PrS ⟨⟨The BCP, producing Manuals for CzCI BIA, Prevention, Preparedness and Readiness⟩⟩. The RPO is Recovery Point Objective, identifying maximum tolerable functions loss for each activity, which cannot be exceeded. The RTO is Recovery Time Objective, identifying acceptable amount of time to restore the functions, till the MTPD - Maximum Tolerable Period of Disruption.

4 Conclusions and acknowledgements

In this article, the both objectives of our current research work are discussed and successful solved, reflecting first and second objectives, defined in the abstract. Future societal security and continuity of Czech critical infrastructure Organizations are investigated via crisis continuity scenarios and methodological cycling approach understanding. It can bring emergency event coping, if the testing of CzCI organizational acceptance phase is rolled up into terminal crisis coping, but just if the next test cycle is not requested. A criterion, if the functions are critical, is explicitly defined at first blazon in the Fig. 1. Feasible scenario of emergency event impact is mathematically derived in crisis cycle at algorithmic blazon with controlling actor displaying.

Organizational business continuity scenarios, necessary for crisis/ emergency preparedness, planning, management & coping, are modelled by means of DYVELOP method, displaying at the blazons [5]. The blazons are the most comprehensible, using live Power Point presentation. Therefore, they are presented layer after layer in real time, as it will be carried out at the Conference in Prague.

Results, presented in this article, were partially obtained as main author´s contribution to the solution of the projects: 1) Technology Agency of the Czech Republic with the topic ´Research and Development of Simulation Instruments for Interoperability Training of Crisis Management Participants and Subjects of Critical Infrastructure´ No. TA04021582; 2) Institutional research of the College of Regional Development Prague.

References:

[1] Green Book about European Programme for Critical Infrastructure Protection. 2005. online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576

[2] Act. 2000. No. 240/2000 Coll., on crisis management and amending certain Laws (Crisis Law) from 28 June 2000. In: Collection of law No. 118/2011, no. 44, pp. 1114 – 1135. ISSN 1211-1244.

[3] URBANEK, J. F. et al. New Instrument of Integrated Waste Management – DYVELOP. 15th International Conference on Solid Waste Technology and Management, *The Journal of Solid Technology and Management.* Philadelphia, U.S.A., 1999. ISSN 1091-8043.

[4] AIKMAN, D. et al. *Funding liquidity risk in quantitative model of systematic stability*. Bank of England: 2009.No. 372.

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

[6] URBANEK, J. F. et al. Accident and Incident Investigation and Modelling in Critical Infrastructure. In *ESREL Zurich*, 2015. London: Taylor & Francis Group, 2015, pp 43-47, ISBN 978-1-138-02879-1.

[7] ARLOW, J., NEUSTADT, I.. *Enterprise patterns and MDA: building better software with archetype patterns and UML*. Boston: 2004, Addison-Wesley, xxvii. Addison-Wesley object technology series. ISBN 03-211-1230-X.

[8] BS 25999-2, about societal security.

[9] ISO 22300, draft about Business Continuity Management System – BCMS.

[10] ISO 26000, about Corporate Social Responsibility – CRS.