Guze Sambor

Kołowrocki Krzysztof

Maritime University, Gdynia, Poland

EU-CIRCLE: A pan-European framework for strengthening critical infrastructure resilience to climate change
Project taxonomy and methodology – Resilience terminology and methodology

Keywords

resilience, safety indicators, risk, business continuity, terminology, methodology

Abstract

The main aim of the paper is to present resilience terminology and methodology. The terms and definitions have been outlined alphabetically, with accordance to notations for resilience, risk, response, business continuity and communications, that are analysed within the scope of the EU-CIRCLE project. Moreover, the resilience indicators are defined and presented as the basic methodology in the field of strengthening critical infrastructure resilience to climate change, covered by the further EU-CIRCLE reports.

1. Introduction

As the history of terrorist attacks and natural disasters shows, the biggest challenge is to quickly restore to normal operation the places and services, where this event occurred. Especially, it is important to critical infrastructures functioning in the affected area. Nowadays, one of the most important thing is the protection concerning actual and predicted climate changes. Predictions on near future climate changes demand special actions concerning adaptation of big number of different areas of societies functioning. The reduction of the EU's vulnerability to the impact of climate change is one of the main goal of EU's politics in this field of activity. One of results of intensive works in this field processed last years, related to climate fluctuations, is launch of the research project "A pan-European framework for strengthening Critical Infrastructure resilience to climate change – EU-CIRCLE", realized under the European Union's Horizon 2020 research and innovation program.

The main EU documents launch an adaptation strategy, covering the whole of the EU. The strategy takes account of global climate change impacts, such as disruptions to supply chains or impaired access to raw materials, energy and food supplies, and their repercussions on the EU.

The report covers all recognized, and collected by EU-CIRCLE project participants, terms and definitions concerned among the Critical infrastructure and climate change also with the resilience, used in other previous and current projects, and in available literature as well. Main parts of this paper present selected contents of the third section of the report – terminology existing in resilience field.

Moreover, the paper introduces resilience methodology connected to resilience impacts, being the base for works undertaken in this field, covered by further EU-CIRCLE reports.

2. Resilience terminology

In this chapter, the general terminology for resilience is presented. Furthermore, the particular parts give the terminology for risk, response, business continuity and communications, that are analysed within the scope of the EU-CIRCLE project according to the report [D1.1. EU-CIRCLE Taxonomy, 2015].

Acceptable risk. The level of potential losses that a society or community considers acceptable given existing social, economic, political, cultural, technical and environmental conditions. In engineering terms, acceptable risk is also used to assess and define the structural and non-structural measures that are needed in order to reduce possible harm to people, property, services and systems to a chosen tolerated level, according to codes or "accepted practice" which are based on known probabilities of hazards and other factors. [Slandail terminology]

Awareness (of risk) The awareness of risk means for an individual to realise and to accept to be vulnerable to a major danger associated with a hazard. [Marchand], [SMARTeST, 2011]

Biological monitoring. The use of medical tests (for example, blood, urine, exhaled air) to determine whether a person has been or is being exposed to a substance. [IAPA]

Business continuity management system. Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. [ISO/IEC 22301, 2012]

Business continuity. Business Continuity (BC) is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. [ISO 22301:2012], [ISO/IEC 22301, 2012]

Business continuity management. Business Continuity Management (BCM) is defined as a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. [ISO 22301, 2012], [ISO/IEC 22301, 2012]

Business continuity plan. A documented set of procedures and information intended to deliver continuity of critical functions in the event of a disruption [Pitt, 2008]

Business impact analysis. Process of analysing activities and the effect that a business disruption might have upon them. [ISO/IEC 22301, 2012]

Capability. The ability of a suitably organized, trained, and equipped entity to access, penetrate, or alter government or privately owned information or communications systems and/or to disrupt, deny, or destroy all or part of a critical infrastructure. [US President's Commission on Critical Infrastructure Protection, 1997]

Capacity. The combination of all the strengths, attributes, and resources available to an individual, community, society, or organization, which can be used to achieve established goals. [IPCC, 2012a]

Category of emergency. One of three types of emergencies: Operational, Energy, and Continuity of Government Causal Analysis. A review of an activity to determine the root cause, to identify less than adequate contributing systemic factors, and to prevent further concerns. [US Department of Energy, 1999]

Cause. Element which alone or in combination has the intrinsic potential to give rise to risk. A risk source can be tangible or intangible. [DECS 07/5007, 2014]

Classification level. A designation assigned to specific elements of information based on the potential damage to national security if disclosed to unauthorized persons. The three classification levels in descending order of potential damage are Top Secret, Secret, and Confidential. [US Department of Energy, 1999]

Communication and consultation. Continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk. [ISO/IEC 27000, 2013], [ISO/IEC 31000, 2009]

Community resilience is the capability to anticipate risk, limit impact, and bounce back rapidly through survival, adaptability, evolution, and growth in the face of turbulent change. [Shaw, 2014]

Confidentiality. Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC 27000, 2013]

Contingency plan. A plan for emergency response, backup operations, and post-disaster recovery in a system, as part of a security program, to ensure availability of critical system resources and facilitate continuity of operations in a crisis. [ENISA]

Contingency planning. A management process that analyses specific potential events or emerging situations that might threaten society or the environment and establishes arrangements in advance to enable timely, effective and appropriate responses to such events and situations. [ISDR Terminology of disaster risk reduction]

Control. An existing mechanism, process, procedure or action which can be verified, which seeks to reduce the likelihood and/or consequence of a risk. Controls include any process, policy, device,

practice, or other actions which modify risk. [DECS 07/5007, 2014]

Coping capacity. The ability of people, organizations, and systems, using available skills and resources, to face and manage adverse conditions, emergencies, or disasters. [Dickson et al, 2012], [ISDR Terminology of disaster risk reduction]

Corrective disaster risk management. Management activities that address and seek to correct or reduce disaster risks which are already present. [ISDR Terminology of disaster risk reduction]

Cost-benefit analysis. Monetary measurement of all negative and positive impacts associated with a given action. Costs and benefits are compared in terms of their difference and/or ratio as an indicator of how a given investment or other policy effort pays off seen from the society's point of view. [SWD(2013) 134 final]

Crisis management. Planning, preventive, and response activities for addressing the causes of a terrorist incident; these activities include proactive measures for: prevention; crisis mitigation, operational response; and, criminal prosecution. [US Department of Energy, 1999]

Critical facilities. The primary physical structures, technical facilities, and systems that are socially, economically, or operationally essential to the functioning of a society or community, both in routine circumstances and in emergencies. [Dickson et al, 2012]

Critical infrastructure accident consequences mitigation. Efforts and actions to prevent and reduce effects of potential hazards coming from CI accident by their elimination or reduction of their consequences by changing decreasing their dangerous interactions with CI operating environment and making alerts.

Critical infrastructure accident consequences reduction. Efforts and actions to reduce negative effects of CI accident by changing and decreasing their dangerous interactions with CI operating environment.

Critical infrastructure redundancy (in climate change context). The properties of a critical infrastructure that allow for use alternate options, choices, and substitutions under stress, in order to satisfy functional requirements in threat situations of disruption, degradation, or loss of functionality coming from climate change.

Critical infrastructure redundancy (in climate change context). The speed with which disruptions coming from climate change can be overcome, in order to contain losses and avoid future disruption, and with which safety, functionality and stability of critical infrastructure can be restored.

Critical infrastructure resilience to climate change. The ability of a critical infrastructure to continue providing its essential services when it is exposed to threats associated with coming out from the climate change harmful events as well as its speed of recovery and ability to return to normal operation after those threats has receded.

Critical infrastructure resilience. The ability of a critical infrastructure to continue providing its essential services when threatened by a harmful event as well as its speed of recovery and ability to return to normal operation after the threat has receded.

Critical infrastructure resourcefulness (in climate change context). The ability of a critical infrastructure to identify problems, establish priorities, and mobilize needed resources and services when threatened by harmful events coming from the climate change.

Critical infrastructure risk management framework. A planning and decision-making framework that outlines the process for setting goals and objectives, identifying infrastructure, assessing risks, implementing risk management activities, and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience. [US Homeland Security, 2013]

Critical infrastructure robustness (in climate change context). The inherent strength or the ability of infrastructure to withstand external demands coming from climate change without degradation or loss of functionality.

Critical infrastructure vulnerability. The possibility of a critical infrastructure coming to the safety state subset worse than a critical safety state in time shorter than its fixed value, due to some external factors, causing negative effects on itself, other objects and its operating environment.

Critical parts or items. The parts of machinery, equipment, materials, structures or other areas that are more likely than other components to result in a major problem or loss when worn, damaged, abused, misused, or improperly applied. [IAPA]

Criticality analysis. Procedure for identifying processes and/or sub-processes, or systems and/or subsystems, whose disruptions or destruction would have far-reaching consequences for the operation of critical infrastructures. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Current risk rating. The estimated level of risk taking into consideration the existing controls in place. [DECS 07/5007, 2014]

Danger zone. An area or location where the probability of injury is high (for example, in the vicinity of saw blades). [IAPA]

Debilitated. A condition of defence or economic security characterized by ineffectualness. [Moteff J., 2003], [US President's Commission on Critical Infrastructure Protection, 1997]

Decision criteria. Thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result. [ISO/IEC 27000, 2013]

Defensive communication strategy. Indicates partial reporting within and outside the business organization, suppressing and even denial of crisis. This strategy is also called the policy of concealing and suppression. [Metzinger et al, 2014]

Disaster recovery. The process of restoring a system to full operation after an interruption in service, including equipment repair / replacement, file recovery / restoration. [ENISA]

Disaster risk. The likelihood over a specified time period of severe alterations in the normal functioning of a community or a society due to hazardous physical events interacting with vulnerable social conditions, leading to widespread adverse human, material, economic, or environmental effects that require immediate emergency response to satisfy critical human needs and that may require external support for recovery. [IPCC, 2012a]

Disaster risk management. The systematic process of using administrative directives, organizations, and operational skills and capacities to implement strategies, policies and improved coping capacities in order to lessen the adverse impacts of hazards and the possibility of disaster. [EU-ADAPT], [ISDR Terminology of disaster risk reduction]

Disaster risk reduction. Denotes both a policy goal or objective, and the strategic and instrumental measures employed for anticipating future disaster risk; reducing existing exposure, hazard, or vulnerability; and improving resilience. [IPCC, 2012a]

Disaster risk reduction plan. A document prepared by an authority, sector, organization, or enterprise that sets out goals and specific objectives for reducing disaster risks together with related actions to accomplish these objectives. [Dickson et al, 2012], [ISDR Terminology of disaster risk reduction]

Early warning system. The set of capacities needed to generate and disseminate timely and meaningful warning information to enable individuals, communities and organizations threatened by a hazard to prepare and to act appropriately and in sufficient time to reduce the possibility of harm or loss. [ISDR Terminology of disaster risk reduction]

Economic risk. The probability of exceedance as a function of the economic damage. [Skanata,]

Economic security (also Global economic competitiveness). The confidence that the nation's goods and services can successfully compete in global markets while maintaining or boosting real incomes of its citizens. [Moteff, 2003], [US President's Commission on Critical Infrastructure Protection, 1997]

Effectiveness. Extent to which planned activities are realized and planned results achieved. [ISO/IEC 27000, 2013]

Emergency. An emergency is the most serious event and consists of any unwanted operational, civil, natural-phenomenon, or security occurrence that could endanger or adversely affect people, property, or the environment. [US Department of Energy, 1999]

Emergency management. Assets providing mitigation, prevention, preparedness (including planning training, and exercising), response (including coordination, resource acquisition, and resource prioritization), recovery efforts, and public information before, during, and after disasters and catastrophic events [US-DHS]

Emergency plan. Detailed procedures for responding to an emergency, such as a fire or explosion, a chemical spill, or an uncontrolled release of energy. An emergency plan is necessary to keep order, and minimize the effects of the disaster. [IAPA]

Emergency services. The set of specialized agencies that have specific responsibilities and objectives in serving and protecting people and property in emergency situations.[ISDR Terminology of disaster risk reduction]

Emission scenario is a plausible representation of the future development of emissions of substances that are potentially radiotively active (e.g. greenhouse gases, aerosols), based on a coherent and internally consistent set of assumptions about driving forces (such as demographic and socioeconomic development, technological change) and their key relationships. Concentration scenarios, derived from emission scenarios, are used as input to a climate model to compute climate projections. In IPCC (1992) a set of emission scenarios was presented which were used as a basis for the climate projections in IPCC (1996). These emission scenarios are referred to as the IS92 scenarios. In the IPCC Special Report on Emission Scenarios (Nakienovi and Swart, 2000) new emission scenarios, the so-called SRES scenarios, were published, some of which were used, among others, as a basis for the climate projections presented in TAR-IPCC (2001) and 4AR-IPCC (2007). [SWD(2013) 134 final]

Evacuation. A protective action that calls for the controlled relocation of personnel from a hazardous or potentially hazardous area. [US Department of Energy, 1999]

Exposure refers to the presence (location) of people, livelihoods, environmental services and resources, infrastructure, or economic, social, or cultural assets in places that could be adversely affected by physical events and which, thereby, are subject to potential future harm, loss, or damage. [SREX Ch1]

Extensive risk. The widespread risk associated with the exposure of dispersed populations to repeated or persistent hazard conditions of low or moderate intensity, often of a highly localized nature, which can lead to debilitating cumulative disaster impacts. [ISDR Terminology of disaster risk reduction]

Extreme scenarios. Those scenarios used in vulnerability assessments and/or radiological and toxicological sabotage assessments, should provide the analyst with an upper bound on the severity of potential consequences Hazard. A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to a facility or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation). [US Department of Energy, 1999]

First aid. The immediate care given to a person who is injured or who suddenly becomes ill. It can range from disinfecting a cut and applying a bandage to helping someone who is choking or having a heart attack. [IAPA]

Incapacitation. An abnormal condition when the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact. [US President's Commission on Critical Infrastructure Protection, 1997]

Indicator. Measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs. [ISO/IEC 27000, 2013]

Information security continuity. Processes and procedures for ensuring continued information security operations. [ISO/IEC 27000, 2013]

Information security. Preservation of confidentiality, integrity and availability of information. [ISO/IEC 27000, 2013]

Infrastructure assurance. Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat inflicted damage. For instance, incident mitigation, incident response, and service restoration. [US President's Commission on Critical Infrastructure Protection, 1997]

Infrastructure protection. Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures. For instance, threat deterrence and vulnerability defence. [US President's Commission on Critical Infrastructure Protection, 1997]

Inherent risk rating. The level of risk without taking into account existing systems and procedures to control or manage the risk (raw risk). [DECS 07/5007, 2014]

Intensive risk. The risk associated with the exposure of large concentrations of people and economic activities to intense hazard events, which can lead to potentially catastrophic disaster impacts involving high mortality and asset loss. [ISDR Terminology of disaster risk reduction]

Joint probability. Joint probability analysis gives the probability of two or more conditions which affect risk occurring at the same time. For example, high river levels can impede sewer outfalls. [DEFRA, 2010]

Land-use planning. The process undertaken by public authorities to identify, evaluate and decide on different options for the use of land, including consideration of long term economic, social and environmental objectives and the implications for different communities and interest groups, and the subsequent formulation and promulgation of plans that describe the permitted or acceptable uses.

Level of risk. Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood. [ISO/IEC 27000, 2013], [ISO/IEC 31000, 2009]

Likelihood. A probabilistic estimate of the occurrence of a single event or of an outcome., for example, a climate parameter, observed trend, or projected change lying in a given range. Likelihood may be based on statistical or modelling analyses, elicitation of expert views, or other quantitative analyses. [IPCC, 2012b]

Low regrets policy. A policy that would generate net social and/or economic benefits under current climate and a range of future climate change scenarios. [IPCC, 2014]

Management of critical infrastructure. Ensuring conditions for the operation and continuous activity of critical infrastructure. [Croatian Law on critical infrastructures]

Material safety data sheet. A form that contains detailed information about the possible health and

safety hazards of a product and how to safely store, use and handle the product. [IAPA]

Maximum tolerable period of disruption. Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. [ISO/IEC 22301, 2012]

Measure. A plan or course of action intended to mitigate a risk. [Klaver et al, 2011]

Minimum business continuity objective. Minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption. [ISO/IEC 22301, 2012]

Mitigation of critical infrastructure accident consequences (with climate-weather change influence). Policies and actions to reduce the consequences of hazards caused by climate change extreme events.

Moderate risk. This risk requires action to be scheduled and monitored and responsibility is assigned to the Business Unit Manager for their attention. [DECS 07/5007, 2014]

Monitor. To check, supervise, observe critically or record the progress of an activity, action or system on a regular basis in order to identify change. [DECS 07/5007, 2014]

Monitor and review. A process for measuring the efficiency and effectiveness of the organization's Risk Management processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities including re-evaluation of the scope and compliance with decisions. [ENISA]

Natural hazard. Natural process or occurrence which may cause death, injury or illness of people, property damage, loss of goods and services, financial loss, interruption of social and economic activities or environmental damage. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Nonstructural measures. Any measure not involving physical construction that uses knowledge, practice, or agreement to reduce risks and impacts, in particular through policies and laws, public awareness raising, training, and education. [Dickson et al., 2012], [UNISDR, 2009]

Offensive communication strategy. Means complete, sincere and timely information of the public thus preventing rumours, avoiding insecurity and loss of confidence. [Metzinger et al, 2014]

Operational risk. Operational risks relate to the day-to-day delivery of activities, operational business plans and objectives. Operational risks typically have a short term focus. Operational risks may have the ability to impact strategic and other operational risks. [DECS 07/5007, 2014]

Optimization of critical infrastructure accident consequences (with climate-weather change influence). Applications of procedures and methods addressed to critical infrastructure accident losses minimization.

Partnership. A relationship between two or more entities wherein each accepts responsibility to contribute a specified, but not necessarily equal, level of effort to the achievement of a common goal. The public and private sector contributing their relative strengths to protect and assure the continued operation of critical infrastructures. [US President's Commission on Critical Infrastructure Protection, 1997]

Prediction. A statement of the expected time, place and magnitude of a future event. [Slandail terminology]

Preparedness. Preparedness is a continuous cycle of planning, organising, training, equipping, exercising, evaluation and improvement activities to ensure effective coordination and the enhancement of capabilities to prevent, protect against, respond to, recover from, and mitigate the effects of all hazards. [UNISDR], [Klaver et al, 2011]

Prevention. The systematic application of recognized principles to reduce incidents, accidents, or the accident potential of a system or organization. [IAPA], [US Homeland Security, 2013]

Prioritized activities. Activities to which priority must be given following an incident in order to mitigate impacts. [ISO/IEC 22301, 2012]

Probability. A measure of our strength of belief that an event will occur. Probability can be expressed as a fraction, % or decimal. [FLOODsite, 2009]

Probabilistic method. Method in which the variability of input values and the sensitivity of the results are taken into account to give results in the form of a range of probabilities for different outcomes. [FLOODsite, 2009]

Probability density function (distribution). Function which describes the probability of different values across the whole range of a variable (for example flood damage, extreme loads, particular storm conditions etc). [FLOODsite, 2009]

Prospective disaster risk management. Management activities that address and seek to avoid the development of new or increased disaster risks. [ISDR Terminology of disaster risk reduction]

Protection. All activities aimed at ensuring the functionality, continuity and integrity of critical *infrastructures* in order to deter, mitigate and

neutralise a threat, risk or vulnerability. [EU Council Directive, 2008]

Protocols. Ground rules or rules of conduct. [US Department of Energy, 1999]

Public awareness. The extent of common knowledge about disaster risks, the factors that lead to disasters and the actions that can be taken individually and collectively to reduce exposure and vulnerability to hazards. [ISDR Terminology of disaster risk reduction]

Public confidence. Trust bestowed by citizens based on demonstrations and expectations of: (1) Their government's ability to provide for their common defence and economic security and behave consistent with the interests of society; and (2) Their critical infrastructures' ability to provide products and services at expected levels and to behave consistent with their customers' best interests. [US President's Commission on Critical Infrastructure Protection, 1997]

Recovery. Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. [US Homeland Security, 2013]

Recovery organization. Organization responsible for coordinating all recovery activities. Responsibilities include, but are not limited to, prioritization of activities; protection of worker and general public health and safety; dissemination of information; coordination of site and offsite activities; collection of data and assessment of long-term effects associated with the release of hazardous materials; formulation and implementation of long-term protective actions for the affected areas; and providing assistance as requested to state and local agencies in formulation of long-term protective actions for affected offsite areas. [US Department of Energy, 1999]

Recovery point objective. Point to which information used by an activity must be restored to enable the activity to operate on resumption. [ISO/IEC 22301, 2012]

*Recovery procedures***.** Procedures that include dissemination of information to federal, state, tribal, and local organizations regarding the emergency and possible relaxation of public protective actions; planning for decontamination actions; establishment of a recovery organization; development of reporting requirements; and establishment of criteria for resumption of normal operations. [US Department of Energy, 1999]

Recovery time objective. Period of time following an incident within which

- product or service must be resumed, or
- activity must be resumed, or
- resources must be recovered [ISO/IEC 22301, 2012]

Reliability. The probability that a system will adequately accomplish its tasks for a specific period of time, under the expected operating conditions. [Sadowsky et al, 2003]

Requirement. Need or expectation that is stated, generally implied or obligatory. [ISO/IEC 22301, 2012]

Residual life. The residual life of a defence is the time to when the defence is no longer able to achieve minimum acceptable values of defined performance indicators in terms of its serviceability function or structural strength. [FLOODsite, 2009]

Residual risk rating. The remaining level of risk after all treatment plans have been implemented. [DECS 07/5007, 2014]

Residual risk. The risk that remains after risk management and mitigation measures have been implemented. [FLOODsite, 2009]

Resilience measures. Resilience measures are designed to reduce the impact of water that enters property and businesses, and could include measures such as raising electrical appliances [DEFRA, 2010]

Resilience. The sufficient ability of an object to continue its operational objective in the conditions including harmful impacts and the ability to mitigate and/or to neutralize those harmful impacts.

Resistance. The ability of a system to remain unchanged by external events. [FLOODsite, 2009]

Resources. All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective. [ISO/IEC 22301, 2012]

Response termination. In general, response activities are terminated when the situation has been stabilized. At this point, potential threats to workers, the public, the environment, and national security have been characterized, conditions no longer meet established emergency categorization criteria, and it appears unlikely that conditions will deteriorate. In coordination with response organizations, the emergency is then declared terminated and activities focus on recovery. [US Department of Energy, 1999]

Response. Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. [US Homeland Security, 2013]

Retrofitting. Reinforcement or upgrading of existing structures to become more resistant and resilient to the damaging effects of hazards. [Slandail terminology], [Dickson et al, 2012]

Return period. An estimate of the average time interval between occurrences of an event (e.g., flood or extreme rainfall) of (or below/above) a defined size or intensity. [IPCC, 2012a]

Return value. The highest (or, alternatively, lowest) value of a given variable, on average occurring once in a given period of time (e.g., in 10 years). [IPCC, 2013]

Risk. The probability that a particular vulnerability of a system will be exploited, either intentionally or accidentally. [Sadowsky et al, 2003]

Risk acceptability. The level of risk which the society is consciously willing to accept, with regard to social, political and economic cost-benefit analysis. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Risk acceptability criteria. Specified properties according to which risk acceptability is assessed or decided upon. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Risk acceptance. It describes the willingness to tolerate a risk, whereby the acceptable risk refers to the level of loss a society or community considers acceptable given existing social, economic, political, cultural, technical and environmental conditions. [FMMEP, 2007]

Risk analysis. The analysis of an organization's information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets and identifies controls that need improvement. [Sadowsky et al, 2003]

Risk appetite. Amount and type of risk that an organisation is willing to pursue or retain. [DECS 07/5007, 2014]

Risk assessment. A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation. [ENISA]

Risk attitude. Organization's approach to assess and eventually pursue, retain, take or turn away from risk. [ISO/IEC 31000, 2009]

Risk avoidance. Decision not to become involved in, or action to withdraw from, a risk situation. [ENISA]

Risk categories. The categories used by the organisation to group similar opportunities or risks for the purposes of reporting and assigning responsibility. [DECS 07/5007, 2014]

Risk communication. A process to exchange or share information about risk between the decision-maker and other stakeholders. The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk. [ENISA]

Risk control. Actions implementing risk management decisions. [ENISA]

*Risk criteria***.** Reference values according to which risk significance is assessed. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Risk description. Structured statement of risk usually containing four elements: sources, events, causes and consequences. [DECS 07/5007, 2014]

Risk elements. Material and immaterial property that may be damaged or destroyed, which could have consequences for the operation of infrastructure or the functioning of systems and subsystems of the infrastructure. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Risk estimation. Process used to assign values to the probability and consequences of a risk. [ENISA]

Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. [ISO 31010]

Risk financing. Provision of funds to meet the cost of implementing risk treatment and related costs. [ENISA]

Risk identification. Process to find, list and characterize elements of risk. [ENISA], [ISO/IEC 31000, 2009]

Risk management. The systematic practice of managing uncertainty to minimize potential harm and loss. [Dickson et al, 2012]

Risk management framework. Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. [ISO/IEC 31000, 2009]

Risk management measure. An action that is taken to reduce either the probability of event or the consequences of event or some combination of the two. [FLOODsite, 2009]

Risk management plan. Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. [ISO/IEC 31000, 2009]

*Risk management process***.** The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. [DECS 07/5007, 2014], [ISO/IEC 31000, 2009]

Risk map is a map that portrays levels of risk across a geographical area. [SEC(2010)1626]

Risk mapping. The process of establishing the spatial extent of risk (combining information on probability and consequences). Risk mapping requires combining maps of hazards and vulnerabilities. The results of these analyses are usually presented in the form of maps that show the magnitude and nature of the risk. [FLOODsite, 2009]

Risk matrix. Tool for ranking and displaying risks by defining ranges for consequence and likelihood. [DECS 07/5007, 2014], [Nad et al, 2014]

Risk of maritime accident. The possibility of maritime accident in the fixed maritime area and time interval.

Risk of maritime environment degradation. The possibility of environment degradation in the fixed maritime area and time interval.

Risk optimization. Process, related to a risk to minimize the negative and to maximize the positive consequences and their respective probabilities. Risk optimization depends upon risk criteria, including costs and legal requirements. [ENISA]

Risk owner. Person with the accountability and authority to manage risk. [DECS 07/5007, 2014]

Risk perception. Risk perception is the view of risk held by a person or group and reflects cultural and personal values, as well as experience. [FLOODsite, 2009]

Risk profile. The change in performance, and significance of the resulting consequences, under a range of loading conditions. In particular the sensitivity to extreme loads and degree of uncertainty about future performance. [FLOODsite, 2009]

Risk reduction. Actions taken to lessen the probability, negative consequences or both, associated with a risk. [ENISA]

Risk register. An auditable record of the project risks, their consequences and significance, and proposed mitigation and management measures. [FLOODsite, 2009]

Risk retention. Acceptance of the burden of loss, or benefit of gain, from a particular risk. [ENISA]

Risk scenario is a representation of one single-risk or multi-risk situation leading to significant impacts, selected for the purpose of assessing in more detail a particular type of risk for which it is representative, or constitutes an informative example or illustration. [SEC(2010)1626]

Risk sharing. Form of risk treatment involving the agreed distribution of risk with other parties. [DECS 07/5007, 2014]

Risk significance (in context). The separate consideration of the magnitude of consequences and the frequency of occurrence. [FLOODsite, 2009]

Risk tolerance. An organisations or stakeholders readiness to bear the risk after risk treatment in order to achieve its objectives. [DECS 07/5007, 2014]

Risk transfer. The practice of formally or informally shifting the risk of financial consequences for particular negative events from one party to another. [IPCC, 2014].

Risk treatment. Process of selection and implementation of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk. [ENISA]

Risk-informed decision making. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. [US Homeland Security, 2013]

Risk-informed decision making. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. [2013 NIPP]

Robustness. The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to the effects of a hazard in efficient manner, including through the preservation of its essential basic structures and functions. Then robustness signifies that a system will retain its system structure (function) intact (remains unchanged or nearly unchanged), when exposed to perturbations and can be measured as the probability that a system will not go into the critical state or worse in time shorter than assumed level T, due to some external factors. [Disaster resilient infrastructure].

Search and rescue stations. Facilities housing search and rescue response personnel and their equipment. This station are intended to provide immediate response capability. [US-DHS]

Sensitive critical infrastructure protection related information. Facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations. [EU. Council Directive, 2008]

Sensitive data of critical infrastructure. Data on critical infrastructure that have been labelled as classified information in accordance with special regulations. [Croatian Law on critical infrastructures]

Sensitivity. Sensitivity is the degree to which a system is affected, either adversely or beneficially, by climate variability or change. The effect may be direct (e.g., a change in crop yield in response to a change in the mean, range or variability of temperature) or indirect (e.g., damages caused by an increase in the frequency of coastal flooding due to

sea-level rise). [Climate Change 2007: Synthesis Report]

Social resilience. The capacity of a community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organising itself to increase its capacity for learning from past disasters for better future protection and to improve risk reduction measures. [FLOODsite, 2009]

Social risk. Relationship between frequency and the number of people suffering from a specified level of harm in a given population from the realization of specified hazardous. [Skanata D.,]

Social vulnerability. This can be defined as the characteristics of a person or group in terms of their capacity to anticipate, cope with, resist, and recover from the impact of a natural hazard. (cf vulnerability below) [SMARTeST, 2011]

Socio-economic scenarios. Scenarios concerning future conditions in terms of population, gross domestic product and other socio-economic factors relevant to understanding the implications of climate change. [SWD(2013) 134 final]

Stakeholder. Any individual, group or organization that can affect, be affected by, or perceive itself to be affected by, a risk. [ENISA]

Stakeholder engagement. Process through which the stakeholders have power to influence the outcome of the decision. Critically, the extent and nature of the power given to the stakeholders varies between different forms of stakeholder engagement. [FLOODsite, 2009]

Standards. Set of rules or codes mandating or defining product performance (e.g., grades, dimensions, characteristics, test methods and rules for use). [Verbruggen et al, 2011]

Strategic risk. A strategic risk has the ability to impact on the achievement /delivery of the Department's strategic objectives/directions. Strategic Risks relate to the highest level of objective, which typically have a long term focus and are linked to the Strategic Plan. [DECS 07/5007, 2014]

Strengthening critical infrastructure resilience to climate change. Increasing CI capacity through its components and subsystems parameters improving and its operating environment parameters modification to achieve its characteristics stronger what allow its functioning in its operating environment to be able to absorb and to recover from hazardous events appearing as a result of climate change.

Strengthening critical infrastructure resilience. Efforts, like policies, procedures and actions, taken to prolong the proper and effective functioning of a critical infrastructure and providing its essential services when it is exposed to threats.

Structural measures. Any physical construction to reduce or avoid the impacts of hazards, or application of engineering techniques to achieve hazard resistance and resilience in structures or systems. [UNISDR, 2009**]**, [Dickson et al, 2012]

Technical-technological threat. Threat arising from technological and industrial conditions, procedures, infrastructure failure or specific human activities, which may cause death, injury or illness, property damage, loss of goods and services, interruption of social and economic activities or environmental damage. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Technological hazard. A range of hazards emanating from the manufacture, transportation, and use of such substances as radioactive materials, chemicals, explosives, flammables, agricultural pesticides, herbicides and disease agents; oil spills on land, coastal waters or inland water systems; and debris from space. [US Department of Energy, 1999]

The process of developing a 'plan' for business continuity and specific disaster recovery involves:

- the development of business risk and impact analysis;
- documenting activities prior to an event;
- identifying and authorising detailed activities for managing the business recovery phase;
- identifying and authorising detailed activities for the disaster recovery phase;
- testing and auditing the business recovery phase;
- training staff in the business recovery process; and
- implementing a process for keeping the plan up to date [Savage, 2002]

Threat. Occurrence, human activity, substance or state that may cause death, injury or illness, property damage, environmental damage, disruption or interruption of social or economic functions. [Croatian Methodology for the operational risk analysis of critical infrastructure]

Threshold is a level of magnitude of a system process at which sudden or rapid change occurs. A point or level at which new properties emerge in an ecological, economic or other system, invalidating predictions based on mathematical relationships that apply at lower levels. [SWD(2013) 134 final]

Treatment. Additional mechanisms, processes, procedures or actions to be implemented, which seek to reduce the current likelihood and/or consequence

and reach the Residual Risk Rating. [DECS 07/5007, 2014]

Trusted information communication entity. Autonomous organization supporting information exchange within an information sharing community. [ISO/IEC 27000, 2013]

Uncertainty. A state of incomplete knowledge that can result from a lack of information or from disagreement about what is known or even knowable. [IPCC, 2014]

Uncertainty analysis. Uncertainty analysis is the process of assessing the extent of uncertainty in model results or predictions, in order to communicate their fitness as a basis for decision-making. [FLOODsite, 2009]

Vulnerability. A flaw or weakness in a system's design, implementation, or operation that can be exploited by an intruder to violate the system's security policy. [Sadowsky et al, 2003]

Vulnerability Analysis. Vulnerability of critical infrastructures, their parts or risk elements is crucial for determining the extent to which a sector, infrastructure or its part has been affected and the damage incurred (the greater vulnerability, the greater are the effects and consequences of adverse events to products and services). [Croatian Methodology for the operational risk analysis of critical infrastructure]

3. Resilience methodology

This chapter of the paper is introducing the taxonomy, specified in the report, in regard to methodology related to resilience indicators..

The safety and resilience indicators, crucial for operators and users of the critical infrastructure, defined as a complex system in its operating environment that significant features are inside-system dependencies and outside-system dependencies, can be obtained using an original and innovative probabilistic approach to modelling of operation threats and extreme weather hazards impact on its safety.

In the first step of the proposed approach, starting from a simplest pure safety model without considering outside impacts, the critical infrastructure (and its assets) following practically useful safety indicators are defined:

- the critical infrastructure safety function (SafI1),
- the critical infrastructure risk function (SafI2),
- the critical infrastructure fragility curve (SafI3),
- the mean value of the critical infrastructure unconditional lifetime up to the exceeding the critical safety state (SafI4),
- the standard deviation of the critical infrastructure unconditional lifetime up to the exceeding the critical safety state (SafI5),
- the moment the critical infrastructure risk function exceeds a permitted level (SI6),
- the intensities of the critical infrastructure degradation/ageing (SafI7),
- the losses associated with the critical infrastructure accident (SafI8).

In the second step of the proposed approach, this simplest safety model is joined with the critical infrastructure operation process model to create a safety model of critical infrastructure related to its operating environment. A slight generalization is a model of a critical infrastructure safety related to its operation process including operating environment threats. Next, a model of critical infrastructure safety related to the climate-weather change process in its operating area is proposed. More general is a model considering jointly the operation process and the climate-weather change process influence on the safety of a critical infrastructure. At the end, a most general safety model of a critical infrastructure under the influence of its operation process including operating environment threats related to climate-weather change process including extreme weather hazards is proposed. It is the integrated model of a critical infrastructure safety, linking its multistate safety model and the joint model of its operation process including operating environment threats and the climate-weather change process including extreme weather hazards at its operating area, considering variable at the different operation and climate-weather states impacted by them the critical infrastructure safety structures and its assets safety parameters. For those models, the following safety indicators are respectively defined:

- the intensities of the critical infrastructure degradation related to the operation process impact (SI9),
- the coefficients of the operation process impact on the critical infrastructure intensities of degradation (SafI10),
- the intensities of the critical infrastructure degradation related to the operation process including operating environment threats impact (SafI11),
- the coefficients of the operation process including operating environment threats impact on the critical infrastructure intensities of degradation (SafI12),
- the intensities of the critical infrastructure degradation related to the climate-weather change process impact (SafI13),

- the coefficients of the climate-weather change process impact on the critical infrastructure intensities of degradation (SafI14),
- the intensities of the critical infrastructure degradation related to the operation process and the climate-weather change process impact (SafI15),
- the coefficients of the operation process and the climate-weather change process impact on the critical infrastructure intensities of degradation (SafI16),
- the intensities of the critical infrastructure degradation related to the operation process operating environment threats and the climate-weather hazards impact (SafI17),
- the coefficients of the operation process related to the climate-weather change process impact on the critical infrastructure intensities of degradation (SafI18),
- the losses associated with the critical infrastructure accident related the climate-weather change process impact (SafI19),
- the coefficient of the climate-weather change process impact on the losses associated with the critical infrastructure accident (SafI20).

These all safety indices are defined in general for any critical infrastructures and their networks with varying in time their safety structures and their assets safety parameters influenced by changing in time operation conditions including environment threats and climate-weather conditions including climate-weather extreme weather hazards at their operating areas.

After finalising those tasks, the next step can be done to perform the tasks terminating methodological framework, where the devised risk and impact assessment framework on interconnected and interdependent critical infrastructures may be transformed into a resilience and adaptation framework. At this stage, the following critical infrastructure resilience indicators can be defined:

- the indicator of critical infrastructure resilience to operation process impact (ResI1),
- the indicator of critical infrastructure resilience to operation process including operating threats impact (ResI2),
- the indicator of critical infrastructure resilience to climate-weather process impact (ResI3),
- the indicator of critical infrastructure resilience to operation process and climate-weather impacts (ResI4),
- the indicator of critical infrastructure resilience to operation process threats and climate-weather hazards impacts (ResI5),
- the indicator of the environment resilience to the losses associated with the critical infrastructure accident related to the climate-weather change (ResI6).

Thus, the way we should go in the research further activity is investigating and solving the problems of optimization of critical infrastructure safety and finding optimal values of safety and resilience indictors, critical infrastructure accident consequences optimisation and mitigation, critical infrastructure resilience to climate-weather change analysis and strengthening critical infrastructure resilience to climate-weather change. This activity will result in business continuity models for critical infrastructure under climate pressures elaboration, cost-effectiveness analysis and modelling and finally in the framework for critical infrastructure adaptation to climate change creation.

All models, supported by suitable computer software, will be placed at Interactive Internet Website allowing the critical infrastructure stakeholders and operators direct usage.

4. Conclusions

In the paper the selected terms from the fifth section of the report [D1.1. EU-CIRCLE Taxonomy, 2015] about resilience, risk, response, business continuity and communication terminology are presented. Furthermore, the resilience methodology, covered by the resilience indicators, are defined.

The paper is the first improving of the EU-CIRCLE Project taxonomy in field of the resilience, risk, response, business continuity and communication

Acknowledgements

The paper presents the results developed in the scope of the EU-CIRCLE project titled “A pan – European framework for strengthening Critical Infrastructure resilience to climate change” that has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 653824. http://www.eu-circle.eu/

References

Bogalecka M., Kołowrocki K., Modeling, identification and prediction of environment degradation initiating events process generated by critical infrastructure accidents. Journal of Polish Safety and Reliability Association, Summer

Safety and Reliability Seminars, Vol. 6, No 1, 47-66, 2015a

Bogalecka M., Kołowrocki K., The process of sea environment threats generated by hazardous chemicals release. Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, Vol. 6, No 1, 67-76, 2015b

Brooks N., Vulnerability, Risk and Adaptation: A Conceptual Framework. Working Paper 38, Tyndall Centre for Climate Change Research, University of East Anglia, Norwich, 2003

Cerullo V., Cerullo M.J., Business continuity planning: a comprehensive approach. Information Systems Management, 21(3), 70-78, 2004

Climate Change 2007: Synthesis Report, <https://www.ipcc.ch/publications_and_data/ar4/syr/en/annexessglossary-e-i.html>

Community resilience to extreme weather – the CREW Project, Final Report, 2012, <www.extreme-weather-impacts.net>

CPNI, Business Continuity Planning, http://www.cpni.gov.uk/Security-Planning/Business-continuity-plan/

Croatian Law on critical infrastructures, Official Gazette - Narodne novine 56/13, 2013

Croatian Methodology for the operational risk analysis of critical infrastructure. Official Gazette - Narodne novine 56/13

DECS 07/5007, Framework. Fraud, Corruption, Misconduct and Maladministration Control. Government of South Australia, Department for Communities and Social Inclusion, 2012

Definitions of community resilience: An analysis, A CARRI Report, Community & Regional Resilience Institute, 2013

DEFRA, Surface Water Management Plan Technical Guidance, UK. 2010, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/69342/pb13546-swmp-guidance-100319.pdf>

DHS Lexicon, NIPP 2013, Partnering for Critical Infrastructure Security and Resilience

DHS Risk Lexicon. Risk Steering Committee. 2010 Edition. U.S. Department of Homeland Security, 2010

Dickson E., Baker J.L., Hoornweg D., Tiwari A., Urban Risk Assessments, Understanding Disaster and Climate Risk in Cities, International Bank for Reconstruction and Development/ World Bank, Washington, DC, 2012

Disaster resilient infrastructure, IDNDR Programme Forum 1999, "Partnerships for a safer world in 21st century.

D1.1, EU-CIRCLE Taxonomy, EU-CIRCLE Project Report, 2015

D1.2, Identification of existing infrastructures in the Baltic Sea and its seaside, their scopes, parameters and accidents in terms of climate change impacts, EU-CIRCLE Project Report, 2015

ENISA, European Union Agency for Network and Information Security. Glossary https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary, 2004

European Union, European Commission, Communication from the Commission on Critical Infrastructure Protection in the fight against terrorism, COM (2004)702 final, Brussels, 2004

European Union, European Commission, White Paper: Adapting to climate change: Towards a European framework for action. COM(2009)147 final, Brussels, 2009

European Union, European Commission Directorate, General Justice, Freedom and Security, Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector, 2009

European Union, European Commission, Communication from the Commission: An EU Strategy on adaptation to climate change, COM(2013)216 final, Brussels, 2013

European Union, European Commission, Commission Staff working document: Climate change adaptation, coastal and marine issues, SWD(2013)133 final, Brussels, 2013

European Union, European Commission, Commission Staff working document: Adapting infrastructure to climate change, SWD(2013)137 final, Brussels, 2013

European Union, European Council, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, 2008

EU-ADAPT, <http://climate-adapt.eea.europa.eu/glossary>

EU-ADAPT, EC Climate-ADAPT compilation of termes from the IPCC's 4th assessment reports of the different working groups (Working Group I, II and III) and the UN ISIDR, <http://climate-adapt.eea.europa.eu/glossary>

FLOODsite, Samuels P., Gouldby B., 2009, FloodSite: Language of Risk - Project definitions, <http://www.floodsite.net/html/partner_area/project_docs/T32_04_01_FLOODsite_Language_of_Risk_D32_2_v5_2_P1.pdf> floodsmart.gov, <https://www.floodsmart.gov/floodsmart/pages/glossary_A-I.jsp>

FMMEP, Pasche, E., 2007, Flood Mapping Manual Editorial Group Glossary, Hamburg University of Technology, TUHH.

IAPA, Glossary of Occupational Health and Safety Terms. Industrial Accident Prevention Association, 2007

IPCC, 2012b: Glossary of terms. In: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation [Field, C.B., V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, K.J. Mach, G.-K. Plattner, S.K. Allen, M. Tignor, and P.M. Midgley (eds.)]. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC). Cambridge University Press, Cambridge, UK, and New York, NY, USA, pp. 555-564.

IPCC, 2014a: Annex II: Glossary [Agard, J., E.L.F. Schipper, J. Birkmann, M. Campos, C. Dubeux, Y. Nojiri, L. Olsson, B. Osman-Elasha, M. Pelling, M.J. Prather, M.G. Rivera-Ferre, O.C. Ruppel, A. Sallenger, K.R. Smith, A.L. St. Clair, K.J. Mach, M.D. Mastrandrea, and T.E. Bilir (eds.)]. In: Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part B: Regional Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change [Barros, V.R., C.B. Field, D.J. Dokken, M.D. Mastrandrea, K.J. Mach, T.E. Bilir, M. Chatterjee, K.L. Ebi, Y.O. Estrada, R.C. Genova, B. Girma, E.S. Kissel, A.N. Levy, S. MacCracken, P.R. Mastrandrea, and L.L. White (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, pp. 1757-1776

IPCC, 2014b: Annex II: Glossary [Mach, K.J., S. Planton and C. von Stechow (eds.)]. In: Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change [Core Writing Team, R.K. Pachauri and L.A. Meyer (eds.)]. IPCC, Geneva, Switzerland, pp. 117-130

IPCC, 2014c: Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change [Field, C.B., V.R. Barros, D.J. Dokken, K.J. Mach, M.D. Mastrandrea, T.E. Bilir, M. Chatterjee, K.L. Ebi, Y.O. Estrada, R.C. Genova, B. Girma, E.S. Kissel, A.N. Levy, S. MacCracken, P.R. Mastrandrea, and L.L.White (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, 1132 pp

ISDR Terminology of disaster risk reduction, Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction (UNISDR), 2009

ISO 22301:2012, http://www.iso.org/iso/catalogue_detail?csnumber=50038

ISO 31 010, Risk management Risk assessment techniques [IEC/ISO 31010:2009; EN 31010:2010

ISO Guide 73:2009, Risk management – Vocabulary

ISO Guide 73:2009, Upravljanje rizicima -- Terminološki rječnik.

ISO/IEC 14001:2004, Environmental Management

ISO/IEC 22301:2012, Business Continuity Management System

ISO/IEC 26000:2010, Social Responsibility

ISO/IEC 27000:2013, Information Security Management System

ISO/IEC 31000:2009, Risk Management

Klaver M.H.A., Luiijf H.A.M., Nieuwenhuijsen A.H., RECIPE project, Good practices manual for CIP policies, For policy makers in Europe, 2011

Kołowrocki K., Safety of critical infrastructures. Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, Vol. 4, No 1, 51-72, 2013b

Kołowrocki K., Reliability of Large and Complex Systems, Amsterdam, Boston, Heidelberd, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sidney, Tokyo, Elsevier, 2014

Kołowrocki K., Soszyńska-Budny J., Reliability and Safety of Complex Technical Systems and Processes: Modeling - Identification - Prediction - Optimization, London, Dordrecht, Heildeberg, New York, Springer, 2011

Kołowrocki K., Soszyńska-Budny J., Introduction to safety analysis of critical infrastructures. Proc. International Conference on Quality, Reliability, Risk, Maintenance and Safety Engineering - QR2MSE-2012, Chendgu, China, 1-6, 2012

Kołowrocki, K. 2013. Safety of critical infrastructures, Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, 4(1): 51-72.

Kołowrocki, K. and Soszyńska-Budny, J. 2011. Reliability and Safety of Complex Technical Systems and Processes: Modeling – Identification – Prediction – Optimization. Springer, London, Dordrecht, Heildeberg, New York.

Kołowrocki, K. and Soszyńska-Budny, J. 2016a. How to Model and to Analyze Operation Threats

and Climate-Weather Hazards Influence on Critical Infrastructure Safety – An Overall Approach, EU-CIRCLE Report D.3.3-GMU0.

Kołowrocki, K. and Soszyńska-Budny, J. 2016b. Critical Infrastructure Operation Process (CIOP), CIOP Model 1, EU-CIRCLE Report D3.3-GMU0.

Kołowrocki, K. and Soszyńska-Budny, J. 2016d. Critical Infrastructure Operating Area Climate-Weather Change Process (C-WCP) Including Extreme Weather Hazards (EWH), C-WCP Model 3, EU-CIRCLE Report D3.3-GMU0.

Kołowrocki, K. and Soszyńska-Budny, J. 2016f. Critical Infrastructure Operation Process General Model (CIOPGM) Related to Operating Environment Threats (OET) and Extreme Weather Hazards (EWH), CIOP Model 5, EU-CIRCLE Report D3.3-GMU0.

Kołowrocki, K. and Soszyńska-Budny, J. 2016g. Integrated Model of Critical Infrastructure Safety (IMCIS) Related to Its Operation Process, IMCIS Model 1, EU-CIRCLE Report D3.3-GMU0.

Kołowrocki, K., Soszyńska-Budny, J. and Torbicki, M. 2016a. Integrated Model of Critical Infrastructure Safety (IMCIS) Related to Climate-Weather Change Process Including Extreme Weather Hazards (EWH), IMCIS Model 3, EU-CIRCLE Report D3.3-GMU0.

Kołowrocki, K., Soszyńska-Budny, J. and Torbicki, M. 2016b. Integrated Model of Critical Infrastructure Safety (IMCIS) Related to Its Operation Process and Climate-Weather Change Process, IMCIS Model 4, EU-CIRCLE Report D3.3-GMU0.

Kołowrocki, K and Soszyńska-Budny J., An overall approach to modelling operation threats and extreme weather hazards impact on critical infrastructure safety, Proc. European Safety and Reliability Conference – ESREL 2017, ….., 2017, to appear

Moteff J., Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Report for Congress, February 2005

Moteff J., Parfomak P., Critical Infrastructure and Key Assets: Definition and Identification. Report for Congress, October 2004

Nad I., Adelsberger Z., Skanata D., Analiza rizika poslovanja kriticnih infrastruktura (Risk analysis of the critical infrastructure operations). University of Applied Sciences, Velika Gorica, 2014

NIPP: Partnering for Critical Infrastructure Security and Resilience, U.S. Department of Homeland Security, 2013

Pescaroli G., Alexander, D., A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor. In: Planet@Risk, 2(3): 58-67, 2015 Davos: Global Risk Forum GRF Davos <https://planet-risk.org/index.php/pr/article/view/208/355>

Pitt M. The Pitt review - learning lessons from the 2007 floods, London: Cabinet Office 2008

Polish Parliament, Act of 26 April 2007 on Crisis Management, Warsaw, 2007

Sadowsky G., Dempsey J.X., Greenberg A., Mack B.J., Schwartz A., Information Technology Security Handbook, The International Bank for Reconstruction and Development/ The World Bank, Washington, DC, 2003

Savage M., Business continuity planning, Work Study, Vol 51, No 5, pp-254-261, 2002

SEC 1626 final of 21.12.2010. ; Commission staff working paper: Risk Assessment and Mapping Guidelines for Disaster Management

Shaw R., Izumi T., Civil Society Organization and Disaster Risk Reduction: The Asian Dilemma, Springer Science $ Buziness Media, p. 244, 2014

Skanata D. Risk Assessment, Management & Criteria. University of Applied Sciences, Velika Gorica

Slandail terminology, The Slandail project's disaster lexicon, 2015

SMARTeST, Nigel Lawson, 2011, SMARTeST - Glossary,
<http://www.floodresilience.eu/images/smartestglossary.pdf>

Soszyńska-Budny J., Optimizing Reliability of Critical Infrastructures with Application to Port Oil Piping Transportation System. Proc. 11th International Fatigue Congress – ICF 2014, Melbourne, Australia, 2014, Advances Materials Research Vols. 891-892, 2014

SRES ANNEX, https://www.ipcc.ch/pdf/special-reports/srex/SREX-Annex_Glossary.pdf

SREX Ch1, Lavell, A., M. Oppenheimer, C. Diop, J. Hess, R. Lempert, J. Li, R. Muir-Wood, and S. Myeong, 2012: Climate change: new dimensions in disaster risk, exposure, vulnerability, and resilience. In: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation [Field, C.B., V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, K.J. Mach, G.-K. Plattner, S.K. Allen, M. Tignor, and P.M. Midgley (eds.)]. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change

(IPCC). Cambridge University Press, Cambridge, UK, and New York, NY, USA, pp. 25-64.

SWD 134 final, An EU Strategy on adaptation to climate change, Guidelines on developing adaptation strategies, Brussels, 16.4.2013

UNISDR Terminology, United Nations International Strategy for Disaster Reduction, 2009 <http://www.unisdr.org/we/inform/terminology>

US Department of Energy, Office of Emergency Management and Oak Ridge Associated Universities, Glossary and Acronyms of Emergency Management Terms, 1999

US Department of Transportation, Maritime Administration, Glossary of Shipping Terms, 2008

US-DHS, Infrastructure Taxonomy, Infrastructure Information Collection Division, Office of Infrastructure Protection, U.S. Department of Homeland Security, 2008

US Homeland Security, Transportation System, Critical Infrastructure and Key Resources, 2007

US Homeland Security, National Infrastructure Protection Program, Partnering for Critical Infrastructure Security and Resilience, 2013

US President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, 1997