**Dziula Przemysław**
ORCID ID: 0000-0002-3930-1316

**Kołowrocki Krzysztof**
ORCID ID: 0000-0002-4836-4976

*Maritime University, Gdynia, Poland*

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

**Keywords**

critical infrastructure, operation process modeling and prediction, safety modeling and prediction

**Abstract**
The paper presents essential critical infrastructure terminology. The terms and definitions have been outlined, in respect to critical infrastructure systems, that are analysed within the scope of the EU-CIRCLE project. Moreover, taxonomy regarding terminology and methodology related to critical infrastructure safety, is presented.

## 1. Introduction

Over recent years, issues related to critical infrastructure protection, has been gaining increasing prominence in the activities of many public institutions and entrepreneurs. This is a function of a growing threat of terrorist attacks and the increasing frequency of natural hazards of various different kinds. The most significant examples are terrorist attacks (New York 2001, Madrid 2004, London 2005, Paris 2015), earthquakes and tsunamis, causing huge destruction of large areas, including sensitive objects within them (Japan 2011), and floods caused by tropical cyclones and hurricanes (Katrina – New Orleans 2005, Sandy – New York 2012). These incidents seemingly showed that security systems were not adequately prepared for proper prevention and response to crisis situations [Dziula, Siergiejczyk, 2016].

Subsequent very important matters concerning actions regarding critical infrastructure protection, are ones 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. Critical infrastructure systems seem to be ones specially sensitive for climate changes, that is why special actions on their resilience are processed. One of results of intensive works 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 works do correspond to the European Union activities concerning adaptation of infrastructure to climate changes. The base document regarding respective EU strategy is the White Paper Adapting to climate change: Towards a European framework for action [European Commission, 2009]. In general, it sets out a framework to reduce the EU's vulnerability to the impact of climate change. Activities performed according to the framework mentioned were the ground for preparing a comprehensive EU adaptation strategy, by publishing the Communication Commission on EU Strategy on adaptation to climate change [European Commission, 2013a]. The document launches 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.

In addition to above, several Staff Working Documents [European Commission, 2013b], were published, including following ones concerning critical infrastructures: SWD(2013)133 - Climate change adaptation, coastal and marine issues, and SWD(2013)137 - Adapting infrastructure to climate change.

One of the first actions started within the scope of EU-CIRCLE project, was to analyse a very wide glossary associated with critical infrastructure protection. Many of terms, that can be found across related works, are used in different and sometimes conflicting ways across disciplines and approaches. Intended result of the activities, was to provide common "EU-CIRCLE language" for participants of the project, letting to have the same understanding of terms and concepts, to serve as a reference material in all project deliverables. The outcomes of works are presented in the report [D1.1. EU-CIRCLE Taxonomy, 2015].

The report covers all recognized, and collected by EU-CIRCLE project participants, terms and definitions concerned with critical infrastructure, its safety, climate change, and the resilience, used in other previous and current projects, and in available literature as well. The terms and definitions are divided into three sections: Critical Infrastructure, Climate Change, and Resilience Terminology. Further parts of this paper present contents of the first section of the report – terminology existing in critical infrastructure field.

Moreover, the paper introduces methodology connected to critical infrastructure safety modelling, also proposed in the report [D1.1. EU-CIRCLE Taxonomy, 2015], being the base for works undertaken in this field, covered by further EU-CIRCLE reports.

## 2. Critical infrastructure terminology

The first section of the report [D1.1. EU-CIRCLE Taxonomy, 2015] - Critical Infrastructure Terminology, has been outlined in respect to different principles. The main one was to take into account international and national regulations, advising particular systems as being parts of critical infrastructure. The second one related to particular activities planned to be realised within the scope of EU-CIRCLE project. And the other one came out of the report [D1.2. EU-CIRCLE, 2015], regarding identification of existing critical infrastructures within the Baltic Sea area.

Outcomes of above indications, resulted with listing the terminology concerned with following systems belonging to critical infrastructure:

- Energy;
- Transport;
- Water;
- Information and Telecommunication Infrastructure;
- Chemical Industry;
- Buildings and Structures;
- Safety of Critical Infrastructures.

Below part of the paper presents, in alphabetical order, terms and definitions, concerning mentioned above systems belonging to critical infrastructure.

*Access.* The ability to enter a secured area and, in the case of accessing a computer, to read, write, modify, or use any of the computer's system resources. [Sadowsky et al, 2003].

*Accountability*. Ensuring that activities on supported systems can be traced to an individual who is held responsible for the integrity of the data. [Sadowsky et al, 2003]

*Asset.* An asset is any person, facility, material, information, or activity that has a positive value to a System Sector. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets may be categorized in many ways, including people, information, equipment, facilities, and activities or operations. [US Homeland Security, 2007]

*Attack.* An assault on system security from an intelligent threat; a deliberate attempt to evade security services and violate the security policy of a system. [Sadowsky et al, 2003]

*Authorization.* Granting officially approved access rights to a user, process, or program in accordance with a company's security policy. Usually authorization is completed after the user is authenticated. The user may then be authorized for various levels of access or activity. [Sadowsky et al, 2003]

*Backup.* The process of copying computer files to some other location either on the computer, or on storage devices that may be separated from the computer. Backups allow to recover data in the event that the originals are no longer available, for reasons ranging from accidental deletion to physical damage, theft, or other loss. [Sadowsky et al, 2003]

*Casualty event.* Unwanted events in which there was some kind of energy release with impact on people and/or ship including its equipment and its cargo or environment. [EMSA, 2014]

*Confidentiality.* Ensuring that sensitive data is limited to specific individuals (external and internal) or groups within an organization. The confidentiality of the information is based on the degree to which an organization must protect its information – for example, registered, proprietary, or non-proprietary. [Sadowsky et al, 2003]

*Contingency plan.* A security plan to ensure that mission-critical computer resources are available to a company in the event of a disaster (such as an earthquake or flood). It includes emergency response actions, backup operations, and post-disaster recovery. [Sadowsky et al, 2003]

*Control systems.* Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). [US Homeland Security, 2013]

*Crisis.* Situation that impacts negatively on the safety of people, property in large sizes or the environment and produces significant restrictions on the operation of competent public administration authorities due to the inadequacy of possessed capabilities and resources. [Polish Parliament, 2007]

*Crisis management.* Crisis management is the process by which an organisation deals with a major event that threatens to harm the organisation, its stakeholders, or the general public. [Klaver et al, 2011]

*Critical facilities*. The primary physical structures, technical facilities and systems which are socially, economically or operationally essential to the functioning of a society or community, both in routine circumstances and in the extreme circumstances of an emergency. [ISDR Terminology of disaster risk reduction, 2009].

*Critical Infrastructure.* Critical infrastructure is an entity (physical and information technology facilities, networks, services and assets) which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in European Union (EU) countries. [European Commission, 2004]

*Critical Infrastructure Information.* Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates law; harms the interstate commerce of the states; or threatens public health or safety;
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk management planning, or risk audit;
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation. [US Homeland Security, 2013]

*Critical Infrastructure owners and operators*. Those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity. [US Homeland Security, 2013]

*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. [NIPP, 2013]

*Criticality.* Impact level to citizens or to the government from the loss or disruption of the infrastructure. [Palmer, Shenoi, 2009], [Theoharidou et al, 2009]

*Criticality analysis.* Process of assessing the criticality level of an infrastructure. It is a special-purpose, society-centric risk analysis process that attempts to protect infrastructures that are vital to society. Criticality analysis mainly considers the societal impacts instead of the organizational impacts. The scope of the analysis is extended to cover interdependent infrastructures and, thus, possible threats and vulnerabilities. Criticality analysis is performed on large-scale CIs that provide services to large numbers of users/citizens and, thus, it usually involves higher impact scales. [Palmer C, Shenoi, 2009], [Theoharidou et al, 2009]

*Cross-sectoral criteria*. They denote the set of general criteria used to assess risk for individual systems and networks of critical infrastructures in all

sectors. [Croatian Law on critical infrastructures, 2013]

*Cyber terrorism.* Causing denial of service, illegal access, introducing a virus in any of the critical information infrastructure of the country with the intent to threaten the unity, integrity, security or sovereignty of state or strike terror in the people or any section of the people; or gaining illegal access to data or database that is restricted for reasons of the security of state or friendly relations with foreign states. [Muktesh, 2014]

*Data availability.* The fact that data is accessible and services are operational. [ENISA, 2004]

*Data confidentiality*. The protection of communications or stored data against interception and reading by unauthorized persons. [ENISA, 2004]

*Data integrity.* The confirmation that processed data are complete and unchanged. [ENISA, 2004]

*Dependency*. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on an input, interaction, or other requirement from other sources in order to function properly. [US Homeland Security, 2013]

*Distribution grids.* Radial networks that carry the electric power from the higher voltage levels to the final users. The number of levels in a distribution grid depends upon the density and magnitude of demand and the terrain. [Holmgren, 2007]

*Electricity distribution.* Passage through Grid Transformers and Substations into and from Distribution Systems. [European Commission, 2009]

*Emergency services.* A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level (county or metropolitan area). [US President's Commission on Critical Infrastructure Protection, 1997]

*Energy.* The amount of work or heat delivered. Energy is classified in a variety of types and becomes useful to human ends when it flows from one place to another or is converted from one type into another. [Gossling, 2010]

*Energy balance.* Averaged over the globe and over longer time periods, the energy budget of the climate system must be in balance. Because the climate system derives all its energy from the Sun, this balance implies that, globally, the amount of incoming solar radiation must on average be equal to the sum of the outgoing reflected solar radiation and the outgoing infrared radiation emitted by the climate system. A perturbation of this global radiation balance, be it human-induced or natural, is called radiative forcing. [Climate Change: Synthesis Report, 2001]

*Energy infrastructure.* The total system of generation, transport, distribution, trade, supply and consumption of energy. This means not only the physical network (e.g. power plants, gas pipes, heat delivery stations), but also the social (economic and institutional) network that manages and controls the physical system. Together, these networks form a socio-technical infrastructure system. It is a complex system; the technological, economic, and institutional domains are strongly interdependent. [Houwing et al, 2007]

*Energy service*. The application of useful energy to tasks desired by the consumer such as transportation, a warm room, or light. [Climate Change: Synthesis Report, 2001]

*European Critical Infrastructure*. Critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. [European Council, 2008]

*External threat.* Arise from outside of the organization by individuals, hackers, organizations, terrorists, foreign Government agents, non-state actors and pose risk like Crippling CII, Espionage, Cyber/Electronic warfare, Cyber Terrorism etc. [Muktesh, 2014]

*Gas and oil transportation*. A critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms. [US President's Commission on Critical Infrastructure Protection, 1997]

*Gas distribution.* Dedicated pipelines to power plants and major industrial users general industrial and commercial customers domestic users. [European Commission, 2009]

*Geographic dependencies.* Infrastructures are geographically dependent if a local environmental event affects components across multiple infrastructures due to physical proximity. [Rinaldi et al, 2001]

*Geographic interdependencies.* Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them. A geographic interdependency occurs when

elements of multiple infrastructures are in close spatial proximity. Given this proximity, events such as an explosion or fire could create correlated disturbances or changes in these geographically interdependent infrastructures. Such correlated changes are not due to physical or cyber connections between infrastructures; rather, they arise from the influence the event exerts on all the infrastructures simultaneously. [Rinaldi et al, 2001]

*Geological hazard.* Geological condition or occurrence that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage. [Dickson, 2012]

*Grounding.* A moving navigating ship, either under command, under power, or not under command, drifting, striking the sea bottom, shore or underwater wrecks. [EMSA, 2014]

*Independent critical infrastructures*. An independent infrastructure is one that in principle is isolated from the risks associated with other infrastructures. [Hammerli, Renda, 2010]

*Information and communications*. An infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support:

- the processing, storage, and transmission of data and information;
- the processes and people that convert data into information and information into knowledge;
- the data and information themselves. [US President's Commission on Critical Infrastructure Protection, 1997]

*Infrastructure.* Network of systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services. [US President's Commission on Critical Infrastructure Protection, 1997]

*Inland waters.* Natural waterways (e.g. rivers, lakes, bayous, estuaries) capable of carrying marine traffic. [US-DHS, 2008]

*Inside dependencies.* Dependencies within an infrastructure (system) itself i.e. relationship between components and subsystems in a system causing degradation of other components and subsystems and in a consequence causing degradation of a system. [Utne et al, 2011]

*Interdependency.* Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions. [US Homeland Security, 2013]

*Internal threat.* One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm. [Muktesh, 2014]

*Logic interdependencies.* All interdependencies between infrastructures that cannot be classified as physical, cyber or geographic; are called logic interdependencies. These links are dependent on a specific context. Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection. [Rinaldi et al, 2001]

*Marine accident.* A negative event, or a sequence of events, that result with large scale of injuries, material damages, or damage to the environment, brought about by the damage of a ship or ships. [EMSA, 2014]

*Marine incident.* An event, or sequence of events, other than a marine accident, which has occurred directly in connection with the operations of a ship that endangered, or, if not corrected, would endanger the safety of the ship, its occupants or any other person or the environment. [EMSA, 2014]

*Maritime transport.* Maritime transport is the shipment of goods (cargo) and people by sea and other waterways. Port operations are a necessary tool to enable maritime trade between trading partners. To ensure smooth port operations and to avoid congestion in the harbour it is inevitable to permanently upgrade the ports physical infrastructure, invest in human capital, fostering connectivity of the port and upgrade the port operations to prevailing standards. Hence, port operations can be defined as all policies, reforms and regulations that influence the infrastructure and operations of port facilities including shipping services. [Global Facilitation Partnership for Transportation and Trade, 2003]

*Network.* A group of components that share information or interact with each other to perform a function. [US Homeland Security, 2013]

*Outside dependencies.* Dependencies coming from the infrastructure environment (external factors) and relationship between infrastructures. Including degradation of infrastructure's state caused by outside this infrastructure changes e.g. climate changes, changes of infrastructure's functionality, location, government and human decisions (regulations, economic, public policy), also degradation of one infrastructure's state affected or correlated according to the state degradation of other infrastructures (including "loops"). [Rinaldi et al, 2001], [Utne, 2011]

*Physical dependencies.* A physical reliance on material flow from one infrastructure to another. [Rinaldi et al, 2001]

*Physical interdependencies.* Two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other. a physical interdependency arises from a physical linkage between the inputs and outputs of two agents: a commodity produced or modified by one infrastructure (an output) is required by another infrastructure for it to operate (an input). For example, a rail network and a coal-fired electrical generation plant are physically interdependent, given that each supplies commodities that the other requires to function properly. The railroad provides coal for fuel and delivers large repair and replacement parts to the electrical generator, while electricity generated by the plant powers the signals, switches, and control centres of the railroad—and in the case of electrified rail, directly powers the locomotives. [Rinaldi, 2001]

*Port.* Harbour with piers or docks. Left side of a ship when facing forward. Opening in a ship's side for handling freight. [US Department of Transportation, 2008]

*Port handling hazardous chemicals.* Port facilities of mooring, docking, loading, and unloading marine vessels with hazardous chemicals. [US-DHS, 2008]

*Prevention.* An outright avoidance of adverse impacts of hazards and related disasters. Prevention expresses the concept and intention to completely avoid potential adverse impacts through action taken in advance. Examples include dams or embankments that eliminate flood risks, land-use regulations that do not permit any settlement in high risk zones, and seismic engineering designs that ensure the survival and function of a critical building in any likely earthquake. [European Commission, 2013]

*Protected critical infrastructure information.* All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive. [US Homeland Security, 2013]

*Protection of critical infrastructure.* Indicates activities whose objective is to ensure functionality, continuous operation and delivery of critical infrastructure services/goods, as well as to prevent threats to critical infrastructure. [Croatian Law on critical infrastructures, 2013]

*Reliability.* The probability of a system failure-free performance, over certain time period, under specified environmental and duty-cycle conditions. Often expressed as mean time between failures (MTBF). [Jazwinski & Wazynska, 1993]

*Risk.* The probability of system damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, resulting with exceeding the system reliability critical safety state.

*Risk analysis.* Identification of possible negative external and internal conditions, events, or situations, determination of cause-and-effect (causal) relationships between probable happenings, their magnitude, and likely outcomes, evaluation of various outcomes under different assumptions, and under different probabilities that each outcome will take place, and application of qualitative and quantitative techniques to reduce uncertainty of the outcomes and associated costs, liabilities, or losses.

*Safety.* The ability of a system such, that during fulfilling its operational objective it does not affect destructively on itself and other objects in its operating environment and does not degrade its natural operating environment.

*Search and rescue services.* Facilities equipped to respond to maritime emergencies. [US-DHS, 2008]

*Sector.* A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. [US Homeland Security, 2013]

*Sectoral criteria.* They denote a set of specific criteria based on which the risk for systems and networks of critical infrastructures in a particular sector is assessed. [Croatian Law on critical infrastructures, 2013]

*Severe pollution.* A case of pollution which, as evaluated by the coastal State(s) affected or the flag Administration, as appropriate, produces a major deleterious effect upon the environment, or which would have produced such an effect without preventive action. [IMO, 2008]

*System of systems.* The term system-of-systems refers to an emergent class of systems that are built from components which are large-scale systems in their own right. A system is considered a 'system of systems' when its components fulfil valid purposes in their own right and continue to operate to fulfil those purposes if disassembled from the overall system, and the component systems are managed (at least in part) for their own purposes rather than the purposes of the whole. [Maier, 1998]

*Telecommunications*. Any transmission, emission, or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic systems. [US Department of Energy, 1999]

*Terrorism.* Premeditated threat or act of violence against non-combatant persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the

civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. [US Homeland Security, 2013]
*Terrorist act.* Act or threat intended to advance a political, ideological or religious cause by coercing or intimidating an government or the public, by causing serious harm to people or property, endangering life, creating a serious risk to the health and safety of the public, or seriously disrupting trade, critical infrastructure or electronic systems. [Australian National Counter-Terrorism Committee, 2011]
*Threat.* Any item that has the potential to compromise the integrity, confidentiality, and availability of data. [Sadowsky et al, 2003]
*Transmission.* Passage through sub-stations. Additional within country and between country interconnectors. [European Commission, 2009]
*Transportation infrastructure.* Physical distribution systems critical to supporting the national security and economic well-being of this nation, including the national airspace systems, airlines, and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services. [Moteff et al, 2003], [US President's Commission on Critical Infrastructure Protection, 1997]
*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]

## 3. Methodology related to critical infrastructure safety

Besides the three sections: Critical Infrastructure, Climate Change, and Resilience, the existing terminology has been divided into, as mentioned in the introduction, the report [D1.1. EU-CIRCLE Taxonomy, 2015], in further parts, is introducing methodology for critical infrastructure safety modelling; climate-weather change process description; then critical infrastructure safety related to climate-weather change modelling, identification, prediction and optimization; and finally gives an ideas on: critical infrastructure resilience to climate-weather change, plus strengthening of critical infrastructure resilience to climate-weather change. The methodology section of the report is suggesting certain terminology to be used in further parts of the EU-CIRCLE project for that purposes.

This chapter of the paper is introducing the taxonomy, specified in the report, in regard to methodology related to critical infrastructure safety.
*Complex system.* A set or group of interacting, interrelated or interdependent elements or parts, that are organized and integrated to form a collective unity or an unified whole, to achieve a common objective.
This definition lays emphasis on the interactions between the parts of a system and the external environment to perform a specific task or function in the context of an operational environment. This focus on interactions is to take a view on the expected or unexpected demands (inputs) that will be placed on the system and see whether necessary and sufficient resources are available to process the demands. These might take form of stresses. These stresses can be either expected, as part of normal operations, or unexpected, as part of unforeseen acts or conditions that produce beyond-normal (i.e., abnormal) conditions and behaviours. This definition of a system, therefore, includes not only the product or the process but also the influences that the surrounding environment (including human interactions) may have on the product's or process's safety performance.
*System operating environment.* Surroundings in which a system operates, including air, water, land, natural resources, flora, fauna, humans and their interrelations.
*System operating environment hazard.* An event that may cause the system damage and/or change its operation activity in the way unsafe for the system and its operating environment. For instance: another ship activity in the ship operating environment that can result in an accident with serious consequences for the ship and its operating environment, terrorist attack changing the system operation process in an unsafe way.
*System inside dependencies.* Dependencies within a system itself i.e. relationship between components and subsystems in a system causing state changes of other components and subsystems and in a consequence resulting in changes of the system state.
*System outside dependencies.* Dependencies coming from the system operating environment (external factors), including changes of the system state caused by outside this system conditions e.g. climate changes, changes of its functionality, location, other objects, government and human decisions (regulations, economic, public policy).
*Safety engineering.* The process following a system safety program plan. Preliminary hazard analyses, functional hazard assessments and system safety assessments are to produce evidence based on documentation that will drive safety systems which

are certifiable and will hold up in litigation. The primary focus of any system safety plan, hazard analysis and safety assessment is to implement a comprehensive process to systematically predict or identify the operational behaviour of any safety-critical failure condition or fault condition or human error that could lead to a hazard and potential mishap. This is used to influence requirements to drive control strategies and safety attributes in the form of safety design features or safety devices to prevent, eliminate and control (mitigation) safety risk. Modern system safety is comprehensive and is risk based, requirements based, functional based and criteria based with goal structured objectives to yield engineering evidence to verify safety functionality is deterministic and acceptable risk in the intended operating environment. Systems of systems, such as a modern military aircraft or fighting ship with multiple parts and systems with multiple integration, sensor fusion, networking and interoperable systems will require much partnering and coordination with multiple suppliers and vendors responsible for ensuring safety is a vital attribute planned in the overall system.

*System safety.* The ability of the system such that during fulfilling its operational objective it does not affect destructively on itself and other objects in its operating environment and does not degrade its natural operating environment.

*Complex system.* A multistate ageing system composed of interacting components and subsystems related to its operation process having significant influence on its safety through changing its structure and its components' safety parameters in the different operation states.

*Multistate ageing system.* To define the multistate system with degrading components, we assume that:

- $n$ is the number of the system components;
- $E_i$, $i = 1,2,...,n$, are components of a system;
- all components and a system under consideration have the safety state set $\{0,1,...,z\}$;
- the reliability states are ordered, the safety state 0 is the worst and the safety state z is the best;
- $T_i(u)$, $i = 1,2,...,n$, are independent random variables representing the lifetimes of components Ei in the safety state subset $\{u,u+1,...,z\}$, while they were in the safety state z at the moment $t = 0$;
- $T(u)$ is a random variable representing the lifetime of a system in the safety state subset $\{u,u+1,...,z\}$ while it was in the safety state z at the moment $t = 0$;
- the system states degrades with time t;
- $s_i(t)$ is a component $Ei$ safety state at the moment $t$, given that it was in the safety state $z$ at the moment $t = 0$;
- $s(t)$ is a system S safety state at the moment $t$, given that it was in the safety state z at the moment $t = 0$.

The above assumptions mean that the safety states of the system with degrading components may be changed in time only from better to worse.

*Multistate system critical safety state.* The system safety state to exceed which is dangerous for the system and its operating environment.

*Multistate system safety.* The ability of the system to achieve its operational objective in the safety state subset not worse than the system critical safety state.

*Multistate system safety function.* A vector

$S(t,\cdot) = [S(t,0),S(t,1),...,S(t,z)]$, $t \in <0,\infty)$,

where

$S(t,u) = P(s(t) \geq u \mid s(0) = z) = P(T(u) > t)$,

$t \in <0,\infty)$, $u = 0,1,...,z$,

is the probability that the multistate system is in the safety state subset $\{u,u+1,...,z\}$, at the moment $t$, $t \in <0,\infty)$, while it was in the safety state $z$ at the moment $t = 0$, is called the safety function of this system.

*Multistate system safety function coordinate.* The safety functions $S(t,u)$, $t \in <0,\infty)$, $u = 0,1,...,z$, are called the coordinates of the multistate system safety function $S(t,\cdot)$.

Consequently, the relationship between the distribution function $F(t,u)$ of the multistate system lifetime $T(u)$ in the safety state subset $\{u,u+1,...,z\}$ and the coordinate $S(t,u)$ of its safety function is given by

$F(t,u) = P(T(u) \leq t) = 1 - P(T(u) > t) = 1 - S(t,u)$,

$t \in <0,\infty)$, $u = 0,1,...,z$.

Under above Definition, we have

$S(t,0) = 1$ and $S(t,0) \geq S(t,1) \geq . . . \geq S(t,z)$,

$t \in <0,\infty)$,

*Multistate system risk function.* A probability

$r(t) = P(s(t) < r \mid s(0) = z) = P(T(r) \leq t)$, $t \in <0,\infty)$,

that the system is in the subset of safety states worse than the critical safety state $r$, $r \in \{1,...,z\}$ while it was in the safety state $z$ at the moment $t = 0$ is called a risk function of the multi-state system.

Under this definition, we have

$r(t) = 1 - P(s(t) \geq r \mid s(0) = z) = 1 - S(t,r)$,

$t \in <0,\infty)$,

and if $\tau$ is the moment when the system risk exceeds a permitted level $\delta$, then
$\tau = r^{-1}(\delta)$,
where $r^{-1}(t)$, if it exists, is the inverse function of the system risk function $r(t)$.

*Multistate component safety function.* A vector
$S_i(t,\cdot) = [S_i(t,0), S_i(t,1),...,S_i(t,z)]$, $t \in <0,\infty)$, $i = 1,2,...,n$,
where
$S_i(t,u) = P(s_i(t) \geq u \mid s_i(0) = z) = P(T_i(u) > t)$, $t \in <0,\infty)$, $u = 0,1,...,z$,
is the probability that the multistate component $E_i$ is in the safety state subset $\{u,u+1,...,z\}$ at the moment $t$, $t \in <0,\infty)$, while it was in the safety state $z$ at the moment $t = 0$, is called the safety function of this component.

The safety functions $S_i(t,u)$, $t \in <0,\infty)$, $u = 0,1,...,z$, are called the coordinates of the multistate component $E_i$, $i = 1,2,...,n$, safety function $S_i(t,\cdot)$.

Thus, the relationship between the distribution function $F_i(t,u)$ of the multistate component $E_i$, $i = 1,2,...,n$, lifetime $T_i(u)$ in the safety state subset $\{u,u+1,...,z\}$, and the coordinate $S_i(t,u)$ of its safety function is given by
$F_i(t,u) = P(T_i(u) \leq t) = 1 - P(T_i(u) > t) = 1 - S_i(t,u)$, $t \in <0,\infty)$, $u = 0,1,...,z$.

*Multistate system safety structure.* The multistate system safety structure is a function determining the relationship between that system lifetime T($u$) in the safety state subset $\{u,u+1,...,z\}$ and its components' lifetimes $T_i(u)$ in the safety state subset $\{u,u+1,...,z\}$.

*Multistate series system.* A multistate system is called series if its lifetime $T(u)$ in the safety state subset $\{u,u+1,...,z\}$ is given by
$T(u) = \min\limits_{1 \leq i \leq n} \{T_i(u)\}$, $u = 1,2,...,z$.
The number $n$ is called the system structure shape parameter.

The above definition means that a multi-state series system is in the safety state subset $\{u,u+1,...,z\}$ if and only if all its $n$ components are in this subset of safety states. That meaning is very close to the definition of a two-state series system considered in a classical reliability analysis that is not failed if all its components are not failed.

*Multistate parallel system.* A multistate system is called parallel if its lifetime $T(u)$ in the safety state subset $\{u,u+1,...,z\}$ is given by
$T(u) = \max\limits_{1 \leq i \leq n} \{T_i(u)\}$, $u = 1,2,...,z$.
The number $n$ is called the system structure shape parameter.

The above definition means that a multistate parallel system is in the safety state subset $\{u,u+1,...,z\}$ if and only if at least one of its $n$ components is in this subset of safety states. That meaning is very close to the definition of a two-state parallel system considered in a classical reliability analysis that is not failed if at least one of its components is not failed.

*Multistate "m out of n" system.* A multistate system is called an "$m$ out of $n$" system if its lifetime $T(u)$ in the safety state subset $\{u,u+1,...,z\}$ is given by
$T(u) = T_{(n-m+1)}(u)$, $m = 1,2,...,n$, $u = 1,2,...,z$,
where $T_{(n-m+1)}(u)$ is the $n$-$m$+1th order statistic in the sequence of the system component lifetimes $T_1(u), T_2(u), ..., T_n(u)$, $u = 1,2,...,z$.

The numbers $m$ and $n$ are called the system structure shape parameters.

The above definition means that the multistate „$m$ out of $n$" system is in the safety state subset $\{u,u+1,...,z\}$ if and only if at least $m$ out of its $n$ components are in this safety state subset and it is a multistate parallel system if $m = 1$ and it is a multistate series system if $m = n$.

*System operation process.* System activity organized by its operator that can interact with its operating environment.

*System operation state.* A system activity state determined by its particular organizational activity and its operating environment conditions.

*System operation process model.* To model the system operation process, we assume that the system during its operation process is taking $v, v \in N$, different operation states $z_1, z_2, ..., z_v$. Further, we define the system operation process $Z(t)$ on the time interval $t \in <0,\infty)$, with discrete operation states from the set $\{z_1, z_2, ..., z_v\}$.

*System operation process parameters.* The system operation process may be described by:

- the *number of operation states* $v, v \in N$,
- the *initial probabilities* $p_b(0) = P(Z(0) = z_b)$, $b = 1,2,...,v$, of the system operation process $Z(t)$ staying at the operation states $z_b$ at the moment $t = 0$;
- the *probabilities of transitions* $p_{bl}$, $b, l = 1,2,...,v$, $b \neq l$, of the system operation process $Z(t)$ between the operation states $z_b$ and $z_l$;
- the *conditional distribution functions* $H_{bl}(t) = P(\theta_{bl} < t)$, $b, l = 1,2,...,v$, $b \neq l$, of the system operation process $Z(t)$

conditional sojourn times $\theta_{bl}$, at the operation states $z_b$ when its next operation state is $z_l$, $b, l = 1,2,...,\nu$, $b \neq l$.

*System operation process model unknown parameters identification*. Application of the methods of identification of the system operation process. They are the methods and procedures for estimating the unknown basic parameters of the system operation process models and identifying the distributions of the conditional system operation processes sojourn times at the operation states. The formulae estimating the probabilities of the system operation process staying at the operation states at the initial moment, the probabilities of the system operation process transitions between the operation states and the parameters of the distributions suitable and typical for the description of the system operation process conditional sojourn times at the operation states can be applied as well. The selected distributions of the system operation process conditional sojourn times at the operation states can be tested for their choice validity. The procedure of statistical data sets uniformity analysis can be proposed to be applied to the empirical conditional sojourn times at the operation states coming from different realizations of the same system operation process. [Kołowrocki, Soszyńska-Budny, 2011]

*System operation process prediction*. Finding the characteristics of the system operation process like ones listed below and other.

*System operation process characteristics*. The system operation process may be characterized by:

- the *unconditional distribution functions* $H_b(t) = P(\theta_b < t)$ of the sojourn times $\theta_b$, $b = 1,2,...,\nu$, of the system operation process $Z(t)$ at the operation states $z_b$, $b = 1,2,...,\nu$;
- the *limit transient probabilities* $p_b$, of the probabilities $p_b(t) = P(Z(t) = z_b)$, $t \in <0,\infty)$, of the system operation process $Z(t)$ staying at the particular operation states $z_b$, $b = 1,2,...,\nu$.

*Complex system safety*. The ability of the system to achieve its operational objective in the safety state subset not worse than the system critical safety state at each of its operation states.

*Complex system safety function*. To define the complex system safety, we assume that the changes of the system operation process $Z(t)$ states have an influence on the system multistate components safety and the system safety structure. This fact has an influence on the shape of the system safety function as well. Therefore, we introduce the following defined below notions.

*System conditional safety function* of the multistate system while the system is at the operation state $z_b$, $b = 1,2,...,\nu$, is defined by the vector

$$[S(t,\cdot)]^{(b)} = [1,[S(t,1)]^{(b)},...[S(t,z)]^{(b)}],$$

where

$$[S(t,u)]^{(b)} = P(T^{(b)}(u) > t \setminus Z(t) = z_b)$$

for $t \in <0,\infty)$, $u = 0,1,...,z$, $b = 1,2,...,\nu$.

The coordinate $[S(t,u)]^{(b)}$ of the system conditional safety function is the conditional probability that the system lifetime $T^{(b)}(u)$ in the safety state subset $\{u,u+1,...,z\}$ is greater than $t$, while the process $Z(t)$ is at the operation state $z_b$. Thus, the system conditional safety function depends on the system structure at the particular operation states.

*System component conditional safety function* of the multistate system while the system is at the operation state $z_b$, $b = 1,2,...,\nu$, is defined by the vector

$$[S_i(t,\cdot)]^{(b)} = [1, [S_i(t,1)]^{(b)}, ..., [S_i(t,z)]^{(b)}], \ t \in <0,\infty), \ i = 1,2,...,n,$$

where

$$[S_i(t,u)]^{(b)} = P(T_i(u) \geq t \mid Z(t) = z_b) > t), \ t \in <0,\infty), \ u = 0,1,...,z, \ b = 1,2,...,\nu.$$

The coordinate $[S_i(t,u)]^{(b)}$ of the component conditional safety function is the conditional probability that the component lifetime $T^{(b)}(u)$ in the safety state subset $\{u,u+1,...,z\}$ is greater than $t$, while the process $Z(t)$ is at the operation state $z_b$. Thus, the component conditional safety function form depends on the system particular operation states.

Consequently, we mark by $T(u)$ the system unconditional lifetime in the safety states subset $\{u,u+1,...,z\}$, $u = 0,1,...,z$, and we define the *System unconditional safety function* by the vector

$$S(t,\cdot) = [1,S(t,1),...,S(t,z)],$$

where

$$S(t,u) = P(T(u) > t),\ t \in <0,\infty),\ \text{for } u = 0,1,...,z.$$

The coordinate $S(t,u)$ of the system unconditional safety function is the probability that the system lifetime $T(u)$ in the safety state subset $\{u, u+1,..., z\}$ is greater than $t$. In the case when the system operation time $\theta$, is large enough, the system unconditional safety function coordinates are given by

$$S(t,u) \cong \sum_{b=1}^{v} p_b [S(t,u)]^{(b)} \quad \text{for } t \geq 0,\ u = 0,1,...,z.$$

where $[S(t,u)]^{(b)}$, $u = 0,1,...,z$, $b = 1,2,...,v$, are the coordinates of the system conditional safety functions and $p_b$, $b = 1,2,...,v$, are the system operation process limit transient probabilities.

*Complex system risk function*. If $s(t)$ is the system safety state at the moment $t$, $t \in <0,\infty)$ and $r$, $r \in \{1,2,...,z\}$, is the system critical safety state, then the system risk function

$$r(t) = P(s(t) < r \mid s(0) = z) = P(T(r) \leq t),\ t \in <0,\infty),$$

defined as the probability that the system is in the subset of safety states worse than the critical state $r$, $r \in \{1,...,z\}$ while it was in the state $z$ at the moment $t = 0$ is given by

$$r(t) = 1\text{-}S(t,r),\ t \in <0,\infty),$$

where $S(t,r)$ is the coordinate of the system unconditional safety function for $u = r$ and if $\tau$ is the moment when the system risk function exceeds a permitted level $\delta$, then

$$\tau = r^{-1}(\delta).$$

*Complex system inside dependencies.* Internal dependencies and interactions within a system itself i.e. relationship between components and subsystems in a complex system causing safety state changes of its other components and subsystems and in a consequence resulting in changes of the system safety state.

*Complex system outside dependencies.* External dependencies and interactions coming from the complex system operating environment, including changes of the complex system structure and its components' safety parameters in different operation states and resulting in the complex system safety state changing caused by outside this system operational conditions related to changes of its functionality, location and other objects activity.

*Critical infrastructure integrated safety model.* Modelling complex system operation process including its outside dependencies and operating environment hazards. Modelling complex system safety including inside dependencies between its components and subsystems. Constructing integrated critical infrastructure safety model composed of a complex system operation process model and its safety model including its inside and outside dependences and operating environment hazards.

*Critical infrastructure integrated safety model unknown parameters identification.* Methods of identification of unknown parameters of the critical infrastructure safety general model.

The methods of identification of the operation processes of a critical infrastructure can be applied. They are the methods and procedures for estimating the unknown basic parameters of the critical infrastructure operation process models and identifying the distributions of the conditional critical infrastructure operation processes sojourn times at the operation states. The formulae estimating the probabilities of the critical infrastructure operation process staying at the operation states at the initial moment, the probabilities of the critical infrastructure operation process transitions between the operation states and the parameters of the distributions suitable and typical for the description of the critical infrastructure operation process conditional sojourn times at the operation states can be applied as well. The selected distributions of the critical infrastructure operation process conditional sojourn times at the operation states can be tested for their choice validity. The procedure of statistical data sets uniformity analysis can be proposed to be applied to the empirical conditional sojourn times at the operation states coming from different realizations of the same critical infrastructure operation process. The procedures and formulae estimating the unknown parameters of the critical infrastructure components' safety models on the basis of statistical data coming from the components safety states changing processes can be applied. The method of estimating the unknown intensities of departures from the safety state subsets of the multistate critical infrastructure components having different exponential safety functions at various critical infrastructure operation states can be proposed to be applied as well. This method can be applied to the statistical data collected at different kinds of the empirical experiments, including the cases of small number of realizations and non-completed investigations. Statistical testing can be applied to verifying the hypotheses concerned with the exponential forms of the multistate safety functions of the particular components of the critical infrastructures at the variable operations conditions. In the case of lack of data coming from the

components safety states changing processes, the simplified method of estimating the unknown intensities of departures from the safety state subsets based on the expert opinions can be applied. [Kołowrocki, Soszyńska-Budny, 2011]

*Critical infrastructure safety prediction.* Creating the main achievement of this task, the basis for the formulation and development of the new solutions concerned with the prediction of the safety of complex critical infrastructure related to its operation processes and its inside and outside interactions and hazards. Using analytical and Monte Carlo simulation methods in critical infrastructure safety prediction and introducing new methods of investigation of the complex critical infrastructure related to its inside dependences and outside dependencies and hazards.

*Short-term critical infrastructure safety prediction.* Critical infrastructure safety prognosis for its nearest future time activity in the fixed its operating environment.

*Short-term critical infrastructure safety prediction method.* Critical infrastructure safety prognosis using Monte Carlo simulation technique based on the *initial probabilities* of the system operation process $Z(t)$ staying at the operation states, the *probabilities of transitions* of the system operation process $Z(t)$ between the operation states and the *conditional distribution functions* of the system operation process $Z(t)$ conditional sojourn times at the operation states and on the *system components' conditional safety functions.*

*Long-term critical infrastructure safety prediction.* Critical infrastructure safety prognosis for its far time activity in the fixed its operating environment.

*Long-term critical infrastructure safety prediction method.* Critical infrastructure safety prognosis using analytical methods based on the *probabilities of transitions* of the system operation process $Z(t)$ between the operation states, the *conditional distribution functions* of the system operation process $Z(t)$ conditional sojourn times at the operation states, the *unconditional distribution functions* of the system operation process $Z(t)$ unconditional sojourn times and the *limit transient probabilities* of the system operation process $Z(t)$ at the particular operation states and on the *system conditional safety functions.*

*Critical infrastructure safety optimization*. The method of the optimization of the critical infrastructure operation process and safety determining the optimal values of limit transient probabilities at the system operation states that maximize the critical infrastructure lifetime in the safety state subset not worse than the safety critical state and/or minimize the critical infrastructure operation process cost.

*Critical infrastructure network.* A set of interconnected and interdependent critical infrastructures interacting directly and indirectly at various levels of their complexity and operating activity.

*Cascading effect in critical infrastructure network.* Degrading effects occurring within an infrastructure and between infrastructures in their operating environment, including situations in which one infrastructure causes degradation of another ones, which again causes additional degradation in other infrastructures and in their operating environment.

## 5. Conclusions

The content of the paper, introducing the first section of the report [D1.1. EU-CIRCLE Taxonomy, 2015] - critical infrastructure terminology, and taxonomy regarding methodology related to critical infrastructure safety, is the first of 3 papers presented at SSARS 2017 Workshop on EU-CIRCLE Taxonomy and Methodology, and is followed by Climate-Weather Change, and Resilience taxonomy and methodology.

All papers mentioned above will constitute the first improved version of deliverable D1.1.

## 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

Australian National Counter-Terrorism Committee, National Guidelines for protecting Critical Infrastructure from Terrorism, 2011

Climate Change: Synthesis Report, http://www.ipcc.ch/ ipccreports/tar/vol4/index.php?idp=204, 2001

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

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

Dziula P., Siergiejczyk M., *Selected* aspects of acts of law concerning crisis management and critical infrastructure protection. *Journal of Konbin*, 2 (26), 79-88, 2013

Dziula P., Kołowrocki K., Rosiński A., Issues concerning identification of Critical Infrastructure systems within the Baltic Sea area. Proc. *European Safety and Reliability Conference - ESREL 2015*, Zurich, Switzerland, 119-126, 2015

Dziula P., Siergiejczyk M., Problems Concerning Threats to Transport Systems Related to Crisis Management, Critical Infrastructure Protection, and Increasing Telematics Applications Usage. In Jerry D. VanVactor (ed.), *Crisis Management, A Leadership Perspective*. New York: Nova Science Publishers, Inc., 107-126, 2016

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

EMSA, European Maritime Safety Agency, EU Mar Taxonomy, Annual Overview of Marine Casualties and Incidents, 2014

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

Global Facilitation Partnership for Transportation and Trade, Maritime Transport and Port Operations, 2003

Gossling S., Carbon Management in Tourism: Mitigating the Impacts on Climate Change, Routledge, 2010

Hammerli B., Renda A., Protecting critical infrastructure in the EU, Centre for European Policy Studies, Brussels, 2010

Holmgren A.J., A Framework for Vulnerability Assessment of Electric Power Systems. In: A.T. Murray, T.H. Grubesic (Eds.), Critical Infrastructure Reliability and Vulnerability, Springer-Verlag, Berlin, Heidelberg, 2007

Houwing M., Heijnen P., Bouwmans I., Socio-technical complexity in energy infrastructures — conceptual framework to study the impact of domestic level energy generation storage and exchange, Proc. of the IEEE International Conference on Systems, Man and Cybernetics, Taipei, Taiwan, 906–911, 2007

IMO, International Maritime Organization, Casualty-related matters reports on marine casualties and incidents, MSC-MEPC.3/Circ.3, London, 2008

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

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

Maier M., Architecting Principles for System-of-Systems, Systems Engineering, vol. 1, 267-284, 1998

Moteff J., Copeland C., Fischer J., Critical Infrastructures: What Makes an Infrastructure Critical?, Report for Congress, 2003

Muktesh C., National Critical Information Infrastructure Protection Centre (NCIIPC), Role, Charter & Responsibilities Government of India, 2014

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

Palmer C., Shenoi S., Critical Infrastructure Protection III: Third IFIP WG 11.10 International Conference, Hanover, New Hampshire, USA, March 23-25, 2009

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

Rinaldi S.M., Peerenboom J.P., Kelly T.K., Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems Magazine, 11-25, 2001

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

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

Theoharidou M., Kotzanikolaou P., Gritzalis D., Risk-based Criticality Analysis. Critical Infrastructure Protection, Revised Selected Papers. International Conference, Hanover, New Hampshire, USA, March 23-25, 2009

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

Utne I.B., Hokstad P., Vatn J., A method for risk modeling of interdependencies in critical

infrastructures, Reliability Engineering and System Safety 96, 671-678, 2011