Blokus-Roszkowska Agnieszka

Bogalecka Magda

Kołowrocki Krzysztof
Maritime University, Gdynia, Poland

Methodology for Baltic Sea Region critical infrastructures safety and resilience to climate change analysis

Keywords

critical infrastructure, European Critical Infrastructure, Baltic Sea Region, climate change, safety, resilience

Abstract

The paper presents the terminology of critical infrastructure including definitions of general terms and definitions of more detailed notions. The European Programme for Critical Infrastructure Protection is introduced and infrastructures specified as being critical are listed. There is also presented the approach to the identification and designation of European Critical Infrastructures. Next, presented terminology and taxonomy refer to critical infrastructure networks at Baltic Sea Region. Finally, notions related to climate change and resilience and vulnerability of critical infrastructures to climate change are given. Considering strategy of critical infrastructures resilience strengthening there are distinguished and defined concepts of robustness, resourcefullness, redundancy, response and recovery.

1. Introduction

To ensure compatibility in this paper and in next papers, concerned with this topic, we start with fixing the "working terminology". The first and most important term is the notion of the Critical Infrastructure (CI). Following the definition given in [26] *critical infrastructure* means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. In this paper we adopt definition presented in the EU-CIRCLE Taxonomy, according which *critical infrastructure* is a complex system in its operating environment that significant features are inside-system dependencies and outside-system dependencies, that in the case of its degradation have significant destructive influence on the health, safety and security, economics and social conditions of large human communities and territory areas [17].

2. State of art

Before the considerations on critical infrastructure at Baltic Sea Region taxonomy, we refer to definitions of selected basic notions concerned with critical infrastructures and climate and weather impacts on their safety included in the report [17].

The European Programme for Critical Infrastructure Protection (EPCIP), which has been laid out in EU Directives by the Commission (e.g., EU COM(2006) 786 final), sets the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity. The EPCIP aims to respond not only to terrorism, but also includes, through cross-sectorial approach, criminal activities, natural disasters and other causes of accidents [25]. In the paper we use notation *hazard* in term of natural hazards classified as severe and extreme weather and climate events, while *threats* refer to events coming from human activity and other systems or infrastructures. The general objective of EPCIP is to raise critical infrastructure protection capabilities across all EU Member States against natural hazards and other threats. The underlying

rationale is that disruption to infrastructures providing key services could harm the security and economy of the EU as well as the well-being of its citizens [23], [25].

According to [12], [17], *protection of critical infrastructure* includes activities whose objective is to ensure functionality, continuous operation and delivery of critical infrastructure services/goods, as well as to prevent natural hazards and other threats to critical infrastructure.

The EPCIP has proposed a list of European critical infrastructures based upon inputs by its Member States. The European Commission's "Green Paper" on EPCIP specifies 11 infrastructures as being critical [24]:

1. Energy
2. Information and communication technology (ICT)
3. Water
4. Food
5. Health
6. Financial
7. Public and legal order and safety
8. Civil administration
9. Transportation
10. Chemical and nuclear industry
11. Space and research.

The approach to the identification and designation of European Critical Infrastructures is particularly presented in Directive 2008/114/EC [26]. We start with the definition of *European Critical Infrastructure* (*ECI*), given in this document, according which ECI means 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 [26]. Further, EU Directive establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. According to this document [26] "There are a certain number of critical infrastructures in Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such ECIs should be identified and designed by means of a common procedure."

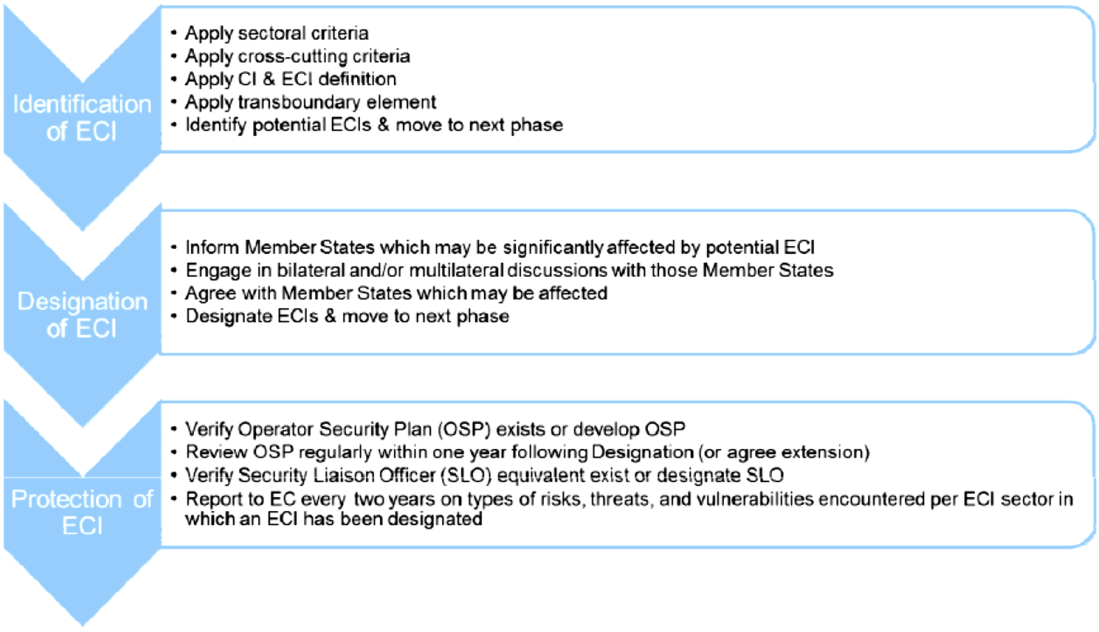

Figure 1. The ECI process [25]

The Directive also requires owners/operators of designated ECI to prepare Operator Security Plans (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for critical infrastructure protection). The Operator Security Plan (OSP) should cover the identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection and prioritisation of counter-measures and procedures. One of the important elements in preparing the Operator Security Plan is to draw attention to *sensitive critical infrastructure protection related information*, defined as 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 [26].

As Commission staff working document on the review of the European Programme for Critical Infrastructure Protection [25] indicates, the ECI process, specified in the Directive 2008/114/EC, can be divided broadly into three distinct phases: identification of potential ECI, designation of ECI, and protection of ECI. The scheme of the ECI process, adopted from [25], is presented in *Figure 1*.
The cross-cutting criteria shall comprise the casualties criterion (assessed in terms of the potential number of fatalities or injuries), economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects) and public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services). The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The sectoral criteria shall take into account the characteristics of individual ECI sectors [26].

2.1. Critical infrastructure terminology

The critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term of critical infrastructure are facilities for [10]:

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices));
- agriculture, food production and distribution;
- heating (e.g. natural gas, fuel oil, district heating);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbours, inland shipping);
- financial services (banking, clearing);
- security services (police, military).

Generally, *critical facilities* are 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. Critical facilities are elements of the infrastructure that support essential services in a society. They include such things as transport systems, air and sea ports, electricity, water and communications systems, hospitals and health clinics, and centres for fire, police and public administration services [17], [38], [48].
Critical Infrastructure community includes critical infrastructure owners and operators (those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity), both public and private; departments and agencies; regional entities; governments; and other organizations from the private and non-profit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting practices and ideas for doing so [49].
Critical infrastructures are usually interconnected and mutually dependent in various and complex ways, creating critical infrastructure network. The *critical infrastructure network* is a set of interconnected and interdependent critical infrastructures interacting directly and indirectly at various levels of their complexity and operating activity, the *interconnected critical infrastructures* that are critical infrastructures in mutually direct and indirect connections between themselves and the *interdependent critical infrastructures* that are critical infrastructures in mutually dependant relationships between themselves interacting at various levels of their complexity. *CI network cascading effects* are 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 [17].
Dependency of CI is defined as a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other [39], [45].
Authors in [45] distinguish four principal classes of interdependencies: physical, cyber, geographic and logical. Two infrastructures are *physically interdependent* if the state of each is dependent on the material output(s) of the other. An infrastructure has a *cyber interdependency* if its state depends on information transmitted through the information infrastructure. Infrastructures are *geographically interdependent* if a local environmental event affects components across these infrastructures due to physical proximity. All interdependencies between infrastructures that cannot be classified as physical, cyber or geographic; are called logic interdependencies. 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 [45].

2.2. Climate change terminology

In this paper, considering events that influence critical infrastructures that may cause loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, ecosystems and environmental resources, we focus on the natural hazards associated with weather and climate change, also called as *climate hazards* and defined as natural phenomena coming out from climate change. By WMO *natural hazards* are severe and extreme weather and climate events that occur naturally in all parts of the world, although some regions are more vulnerable to certain hazards than others. Natural hazards become natural disasters when people's lives and livelihoods are destroyed [17], [53]. On the other hand, according to [51], *natural disaster* is a physical capability with the ability to destroy or incapacitate critical infrastructures. It is a violent, sudden and destructive change in the environment without cause from human activity, due to phenomena such as floods, earthquakes, fire and hurricanes [17], [47].

The IPCC, defines *hazard* as the potential occurrence of a natural or human-induced physical event or trend or physical impact that may cause loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, ecosystems and environmental resources [35]-[36]. In this paper and report [18], the term hazard is used in the context of natural hazard and refers to climate-related physical events or trends or their physical impacts. As it was mentioned in Section 2, we assume that dangerous events coming from human activity and other systems or infrastructures operation are traced to *threats*. In contrast to this definition, according to [43], the threat is the source in a harmful state, while the hazard is the source in a harmless state with potential to change into a threat. Other words, a hazard is a potential, dormant, absent, or contained threat.

The Inter-governmental Panel on Climate Change (IPCC) defines *climate change* as [32]: "a change in the state of the climate that can be identified (e.g., by using statistical tests) by changes in the mean and/or the variability of its properties, and that persists for an extended period, typically decades or longer. Climate change may be due to natural internal processes or external forcing, or to persistent anthropogenic changes in the composition of the atmosphere or in land use". For the purposes of this article, we adopted similar definition, according which *climate change* refers to any change in climate over time, either due to natural variability or as a result of human activity [17]. This usage differs from the definition presented by the United Nations Framework Convention on Climate Change (UNFCCC), which distinguish climate change attributable to human activities and climate variability attributable to natural causes [35]-[36]. The UNFCCC defines 'climate change' as: 'a change of climate which is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability observed over comparable time periods' [32].

Here, similarly as in [33]-[36], we assume that, *climate variability* refers to variations in the mean state and other statistics (such as standard deviations, the occurrence of extremes, etc.) of the climate at all spatial and temporal scales beyond that of individual weather events. Variability may be due to natural internal processes within the climate system (internal variability), or to variations in natural or anthropogenic external forcing (external variability). In turn, *climate stationarity* refers to the stationarity of extremes of climate and weather i.e. that the frequencies and intensities of extremes observed in the past adequately represent those that will occur in the future [1].

Climate change scenario is a coherent and internally-consistent description of the change in climate by a certain time in the future, using a specific modelling technique and under specific assumptions about the growth of greenhouse gas and other emissions and about other factors that may influence climate in the future [42]. And further, *climate model* is a numerical representation of the climate system that is based on the physical, chemical, and biological properties of its components, their interactions, and feedback processes, and that accounts for all or some of its known properties [33]-[36]. And according to [17], *climate-weather change process* is the process of the climate-weather states changing considered in time for a fixed area, while *extreme weather event* refers to meteorological conditions that are dangerous and happen at a particular place and time and can generate severe hazards.

2.3. Resilience terminology

Reducing the vulnerabilities of critical infrastructures and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be limited as far as possible.

In terms of critical infrastructures *secure/security* means reducing the risk to critical infrastructure by physical means or defensive cyber measures to

intrusions, attacks, or the effects of natural or manmade disasters [49].

Safety plan from owner/manager of critical infrastructure indicates a plan that ensures confidentiality, integrity and availability of the organizational, human, material, information-communication and other solutions, as well as permanent and graded security measures necessary for the continuous functioning of critical infrastructure [12].

There are existing many concepts of risk. Some of them, for example definition presented in [39], define risk as a combination of the consequences of an event (hazard) and the associated likelihood/probability of its occurrence. Other concepts define risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization [16]. Relating to climate and climate change, risk can be also understood as the result of interaction of physically defined hazards with the properties of the exposed systems i.e., their sensitivity or vulnerability [17].

One of the Operator Security Plans elements, described in Section 2, can be *critical infrastructure risk management framework* defined as 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 [49].

Risk assessment is defined as overall process consisting of three steps: risk identification, risk analysis and risk evaluation [13], [37]. And *risk management process* is the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk [13], [37].

Further in this section, there are presented concepts related to resilience, vulnerability, adaptation and mitigation.

Resilience can be understood as the ability of a system and its component parts to anticipate, absorb, accommodate, or recover from the effects of a hazardous event in a timely and efficient manner, including through ensuring the preservation, restoration, or improvement of its essential basic structures and functions [14], [34], [39].

According to Bruneau et al. [9], resilience of systems can be conceptualized as having four infrastructural qualities:

• *Robustness*: the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.
• *Redundancy*: system properties that allow for alternate options, choices, and substitutions under stress.
• *Resourcefulness*: the capacity to mobilize needed resources and services in emergencies.
• *Rapidity*: the speed with which disruption can be overcome and safety, services, and financial stability restored [44].

The resilience framework also addresses the technical, organizational, social, and economic dimensions of infrastructure. Examples of technical, organizational, social, and economic activities that support the qualities of a resilient community are presented in *Table 1* adopted from [44].

Table 1. Matrix of resilience qualities with examples pertaining to the technical, organizational, social, and economic dimensions of infrastructure [44]

Dimension/Quality	Technical	Organizational	Social	Economic
Robustness	Building codes and construction procedures for new and retrofitted structures	Emergency operations planning	Social vulnerability and degree of community preparedness	Extent of regional economic diversification
Redundancy	Capacity for technical substitutions and "work-arounds"	Alternate sites for managing disaster operations	Availability of housing options for disaster victims	Ability to substitute and conserve needed inputs
Resourcefulness	Availability of equipment and materials for restoration and repair	Capacity to improvise, innovate, and expand operations	Capacity to address human needs	Business and industry capacity to improvise
Rapidity	System downtime, restoration time	Time between impact and early recovery	Time to restore lifeline services	Time to regain capacity, lost revenue

Source: Kathleen Tierney, director of the Natural Hazards Center, University of Colorado at Boulder, personal communication.

According to [49], vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
Referring to the definition of hazards and threats adopted in this article, we accept the definition of vulnerability given in [12], with a small correction. Then, *vulnerability* can be defined as essential properties of the system, parts of the system, assets, community and the environment which make them susceptible to adverse effects of natural hazards and other threats.
Vulnerability in terms of reliability can be measured as the probability that a system will come to the critical state or worse in time shorter than assumed level, due to some external factors, causing large negative effects that influence on other sensitive systems (consequences above a fixed level). Similar approach has been presented in [29], where the vulnerability of an infrastructure system is defined as the probability of at least one disturbance with negative societal consequence larger than some large (critical) value, during a given period time.
Vulnerability encompasses a variety of concepts and elements including sensitivity or susceptibility to harm and lack of capacity to cope and adapt [35]. Thus, the concept of vulnerability is closely related to the *adaptation*, which in terms of climate change includes initiatives and measures to reduce the vulnerability or increase the resilience of natural and human systems to actual or expected climate change impacts. There can be distinguished various types of adaptation, such as anticipatory and reactive, private and public, and autonomous and planned [30]-[31].
Detection of impacts of climate change for a system or infrastructure is defined as the identification of a change from a specified baseline. The baseline characterizes behaviour in the absence of climate change and may be stationary or non-stationary [35]-[36]. In the paper, the term impact primarily refers to the effects on critical infrastructures and systems belonging to critical infrastructures of extreme weather and climate events and of climate change. Impacts are referred to as consequences and outcomes [35]-[36]. Depending on the consideration of adaptation, one can distinguish between potential impacts and residual impacts. *Potential impacts* are defined as all impacts that may occur given a projected change in climate, without considering adaptation. *Residual impacts* are the impacts of climate change that would occur after adaptation [30].
By the IPCC the *mitigation* of disaster risk and disaster can be defined as the lessening of the potential adverse impacts of physical threats, including those that are human-induced, and natural hazards through actions that reduce hazard, exposure, and vulnerability [33]. Mitigation of the climate change effects in relation to critical infrastructures can be implemented through policies and action to reduce potential negative consequences of hazards caused by climate change extreme events.

3. Critical infrastructure networks at Baltic Sea Region taxonomy

We define the *Baltic Sea critical infrastructure* as a complex system located and operating within the Baltic Sea and ashore that significant features are inside-system dependencies and outside-system dependencies, that in the case of its degradation have significant destructive influence on the health, safety and security, economics and social conditions of large human communities and territory areas. The definition of a complex system and other basic notion concerned with critical infrastructure are presented in [4], [18].
The *Baltic Sea critical infrastructure network* defined as a set of interconnected and interdependent critical infrastructures located within the Baltic Sea and ashore, interacting directly and indirectly at various levels of their complexity and operating activity [18].
The *Baltic Sea critical infrastructures global network* ("network of networks") is defined as a set of interconnected and interdependent critical infrastructures located within the Baltic Sea and ashore around that function collaboratively using the Critical Infrastructure Operation Process General Model (CIOPGM). The Critical Infrastructure Operation Process General Model (CIOPGM) will be constructed using Modelling Critical Infrastructure Operation Process (CIOP) including Operating Environment Threats (OET), performed in [21], and Modelling Climate-Weather Change Process (C-WCP) including Extreme Weather Hazards (EWH), performed in [22].
Considering definitions of main notions from the above methodology concerned with critical infrastructures and their networks, the Global Baltic Network of Critical Infrastructure Networks (GBNCIN) is composed of the following 8 main critical infrastructure networks operating in the Baltic Sea Region [18], [20]:

- port critical infrastructure network, described in [5], [18];
- shipping critical infrastructure network [8], [18];
- oil rig critical infrastructure network [18], [40];
- wind farm critical infrastructure network [18], [41];
- electric cable critical infrastructure network [6], [18];

- gas pipeline critical infrastructure network [2], [18];
- oil pipeline critical infrastructure network [15], [18];
- ship traffic and port operation information critical infrastructure network [18], [27].

3.1. Critical infrastructure taxonomy

We classify the above distinguished shipping critical infrastructure network to the class of so called dynamic installations and the remaining distinguished 7 critical infrastructures to the class of so called static industry installations. Further, we can define *threats to Baltic Sea critical infrastructure or critical infrastructure network* as the occurrence of an unwanted circumstance or event that may cause damage, functioning disruption or service interruption to critical infrastructures located in the Baltic Sea Region. Considering critical infrastructures in the Baltic Sea Region [18], we also distinguish *dynamic threats* i.e. threats associated with dynamic installations, *static threats* that are classifies as threats associated with static installations, and natural climatic hazards i.e. hazards associated with climate and weather change. In particular, we pay attention to the natural hazards related to climate-weather change.

Critical infrastructure operation process general model related to climate-weather change is defined as the critical infrastructure operation process joint model related to operating environment hazards and climate-weather change extreme events linking the critical infrastructure operation process model and the climate-weather change process model [17].

Critical infrastructure integrated safety model related to climate-weather change includes modelling the critical infrastructure operation process according to the critical infrastructure operation process general model related to climate-weather change process and modelling the critical infrastructure inside dependencies between its components and subsystems according to the critical infrastructure safety general model [17]. The final stage of such integrated critical infrastructure safety model is construction of the model, including the above two models of critical infrastructure operation process general model and safety general model.

3.2. Climate change taxonomy

Applying presented before classification of dangerous events having impact on critical infrastructure networks operating in the Baltic Sea Region we focus on natural climatic hazards, defined in Section 2.2.

Among the climatic hazards having influence on functioning of critical infrastructure networks we can distinguish wind, temperature, humidity, cloudiness, precipitation or solar radiation as well as occurrence extreme weather events, defined in Section 2.2, such as hurricanes or storms. In the Baltic Sea Region there can be also noticed changes in weather patterns, such as the movement of wind and the cloud formations. Changes in atmospheric conditions can lead to changes in the sea surface, which in turn can alter the weather patterns. Sea-surface height is an important indicator of climate variability and long-term change as shows the results of simulations of projected changes in sea-level extremes. Climate change causes shifts in air and sea currents, which can change weather patterns. Variations of wind and precipitations patterns, which are associated with changes of synoptic pressure, can be seasonal.

Regional weather patterns are altered by global warming, the weather become more extreme and sea level rise. The study, presented in [28], that took into account available global sea-level rise scenarios and simulated regional wind speed changes, project large increases of storm surge levels at the entrance to the Baltic Sea and in the eastern Baltic. *Storm surge* is the temporary increase, at a particular locality, in the height of the sea due to extreme meteorological conditions (low atmospheric pressure and/or strong winds). The storm surge is defined as being the excess above the level expected from the tidal variation alone at that time and place [33]-[34].

Storm tracks are regions with a high frequency of storms. The storms tend to have a preference for the north-eastern part of the North Atlantic, but are affected by the NAO [11].

According to IPCC, the *climate prediction* or climate forecast is the result of an attempt to produce an estimate of the actual evolution of the climate in the future, e.g., at seasonal, inter-annual or long-term time scales, while the *climate projection* is the response of the climate system to emissions or concentration scenarios of greenhouse gases and aerosols, or radiative forcing scenarios, often based on simulations by climate models [32].

In particular, for listed before critical infrastructure networks operating in the Baltic Sea Region, forming the Global Baltic Network of Critical Infrastructure Networks, we consider following hazard parameters [19]: wind speed, wind direction, sea level, wave height, sea water temperature, air temperature, soil temperature, rainfall level, snowfall level, ice thickness, fog density, flood level, landslide speed and wildfire level. Of course, not all types of hazards and hazard parameters have influence on considered critical infrastructures located in the Baltic Sea

Region, or have some consequences for particular range of the hazard parameter.

Basic notions related to climate and weather changes, in particular to climate changes in the Baltic Sea Region having impact on critical Infrastructures located and operating in the Baltic Sea Region, are storms, sea-level rise, extreme coastal high water, significant wave height, which definitions are provided below.

WMO defines *storms* as an atmospheric disturbance involving perturbations of the prevailing pressure and wind fields, on scales ranging from tornadoes (1 km across) to extratropical cyclones (2000-3000 km across). On the Beaufort scale storm refers to wind with a speed between 48 and 55 knots and Beaufort number 10 of wind force [52].

Sea-level rise is defined as an increase in the mean level of the sea. Eustatic sea-level rise is a change in global average sea level brought about by an increase in the volume of the world ocean. Relative sea-level rise occurs where there is a local increase in the level of the sea relative to the land, which might be due to sea rise and/or land level subsidence. In areas subject to rapid land-level uplift, relative sea level can fall [30]. We can distinguish two types of sea level data, relative and absolute. *Relative sea level trends* show how sea level change and vertical land movement together are likely to affect coastal lands and infrastructure, while *absolute sea level trends* provide a more comprehensive picture of the volume of water in the world's oceans, how the volume of water is changing, and how these changes relate to other observed or predicted changes in global systems (e.g., increasing ocean heat content and melting polar ice caps) [50].

Extreme coastal high water, also referred to as extreme sea level, depends on average sea level, tides, and regional weather systems. Extreme coastal high water events are usually defined in terms of the higher percentiles (e.g., 90th to 99.9th) of a distribution of hourly values of observed sea level at a station for a given reference period [33]-[34].

Term *significant wave height* refers to the average height of the highest one-third of the wave heights (trough to peak) from sea and swell occurring in a particular time period [17].

3.3. Resilience taxonomy

Considering climate-weather change impacts on critical infrastructures in the Baltic Sea Region in the next step we will describe consequences and resilience strategy of critical infrastructure installations in this region, mentioned before. We understand *critical infrastructure resilience* to climate change as the CI capacity being able to absorb and to recover from hazardous events appearing as a result of climate change [17].

Strengthening critical infrastructure resilience to climate change means 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 [17]. Analyzing the strategy of resilience strengthening of CI located in Baltic Sea Region [19] we distinguish robustness, resourcefullness, redundancy, response and recovery. *Robustness,* in climate change context, is the inherent strength or the ability of infrastructure to withstand external demands coming from climate change without degradation or loss of functionality. Hence, robustness signifies that a system/infrastructure 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, due to some external factors [29]. Critical infrastructure *resourcefulness* is 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. *Redundancy* is 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. It can be measured as 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. *Response* means reaction (policies and action) during or immediately after a disaster in order to reduce its impacts, to ensure functioning of basic systems (infrastructures) and to prevent transitions of the system or infrastructure into crisis situation. It usually includes activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs [47]. *Recovery* can be defined as the restoration, and improvement where appropriate, of facilities, livelihoods and living conditions of disaster-affected communities, including efforts to reduce disaster risk factors [48].

With resilience there are concerned other notions, such as resistance or retrofitting. *Resistance* is the

ability of a system to remain unchanged by external events [46]. *Retrofitting* is a reinforcement or upgrading of existing structures to become more resistant and resilient to the damaging effects of hazards [14].

The concept of infrastructure resilience is also closely related to *critical infrastructure vulnerability*, that can be understood as 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 [17].

4. Conclusion

In the paper the terminology and methodology on Baltic Sea Region critical infrastructures are presented. More detailed description of the Global Baltic Network of Critical Infrastructure Networks and belonging to it installations in Baltic Sea Region, defined in this paper, is given in the report [18] and in [4]. Presented in the paper working terminology is also used in the EU-CIRCLE project titled "A pan – European framework for strengthening Critical Infrastructure resilience to climate change". Presented methodology and terminology refers to climate-weather change and its impact on critical infrastructures as well as critical infrastructure resilience and resilience strengthening to climate change. Some notions and terminology specific for particular critical infrastructure networks, located in the Baltic Sea Region, for example Gas Pipelines Critical Infrastructure Network and Baltic Electric Cable Critical Infrastructure Network, are indicated and described in papers [3], [7].

Acknowledgments

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

[1] ASCE (2015). *Adapting Infrastructure and Civil Engineering Practice to a Changing Climate*. Committee on Adaptation to a Changing Climate, 82-93.

[2] Blokus-Roszkowska, A., Bogalecka M., Dziula, P. et al. (2016). Gas Pipelines Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 1-6.

[3] Blokus-Roszkowska, A., Bogalecka, M., Dziula, P. et al. (2016). Methodology for Gas Pipelines Critical Infrastructure Network safety and resilience to climate change analysis. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 83-91.

[4] Blokus-Roszkowska, A., Bogalecka, M. & Kołowrocki, K. (2016). Critical Infrastructure networks at Baltic Sea and its seaside. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 7-14.

[5] Blokus-Roszkowska, A., Guze, S., Kołowrocki, K. et al. (2016). Port Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 15-28.

[6] Blokus-Roszkowska, A., Kołowrocki, K. & Soszyńska-Budny, J. (2016). Baltic Electric Cable Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 29-36.

[7] Blokus-Roszkowska, A., Kołowrocki, K. & Soszyńska-Budny, J. (2016). Methodology for Electric Cables Critical Infrastructure Network Safety and Resilience to Climate Change Analysis. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 151-162.

[8] Bogalecka, M., Kołowrocki, K., Soszyńska-Budny J. et al. (2016). Shipping Critical Infrastructure Network. Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars 7, 1-2, 43-52.

[9] Bruneau, M., Chang, S., Eguchi, R. et al. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* 19, 4, 733-752.

[10] Caverzan, A. & Solomos, G. (2014). *Review on resilience in literature and standards for critical built-infrastructure*. JRC science and policy report. European Commision.

[11] CGU (2015). *Climate Science Glossary*. [available at: https://docs.google.com/document/d/1FtoxQwrQXY1a5DNbk7LGOxzc8DvciZjvArLRDFMRY1o/edit, last accessed: 19th February 2016].

[12] Croatian Parliament. (2013). *Croatian Law on critical infrastructures*. Official Gazette no. 56/13.

[13] DECS (2015). *Fraud, Corruption, Misconduct and Maladministration Control*. DECS 07/5007, Framework.

[14] Dickson, E., Baker, J. L., Hoornweg, D. et al. (2012). *Urban Risk Assessments, Understanding Disaster and Climate Risk in Cities*. International Bank for Reconstruction and Development/World Bank, Washington, DC.

[15] Drzazga, M., Kołowrocki, K. & Soszyńska-Budny, J. (2016). Oil Pipeline Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 53-60.

[16] ENISA (2015). *European Union Agency for Network and Information Security ENISA – Glossary*. [available at: *https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary*, last accessed: 19th February 2016].

[17] EU-CIRCLE Report D1.1-GMU1. (2015). *EU-CIRCLE Taxonomy*.

[18] EU-CIRCLE Report D1.2-GMU1. (2016). *Identification of existing critical infrastructures at the Baltic Sea area and its seaside, their scopes, parameters and accidents in terms of climate change impacts*.

[19] EU-CIRCLE Report D1.3-GMU4. (2015). *Contributions to generating Questionnaire of End User Needs*.

[20] EU-CIRCLE Report D1.4-GMU3. (2016). *Holistic approach to analysis and identification of critical infrastructures within the Baltic Sea area and its surroundings – Formulating the concept of a global network of critical infrastructures in this region ("network of networks" approach).*

[21] EU-CIRCLE Report D2.1-GMU2. (2016). *Modelling outside dependences influence on Critical Infrastructure Safety (CIS) – Modelling Critical Infrastructure Operation Process (CIOP) including Operating Environment Threats (OET).*

[22] EU-CIRCLE Report D2.1-GMU3. (2016). *Modelling outside dependences influence on Critical Infrastructure Safety (CIS) – Modelling Climate-Weather Change Process (C-WCP) including Extreme Weather Hazards (EWH).*

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

[24] European Union, European Commission. (2005). *Green Paper on a European Program for Critical Infrastructure Protection*. COM(2005)576 final. Brussels.

[25] European Union, European Commission. (2012). *Commission staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP)*. Brussels, 22.6.2012 SWD(2012) 190.

[26] European Union, European Council. (2008). *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.

[27] Guze, S. & Ledóchowski, M. (2016). Ship Traffic and Port Operation Information Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 65-72.

[28] HELCOM (2013). Climate change in the Baltic Sea Area - HELCOM thematic assessment in 2013. *Baltic Sea Environment Proceedings No. 137*.

[29] IDNDR (1999). *Partnerships for a Safer World in the 21st Century*. The International Decade for Natural Disaster Reduction for the IDNDR Programme Forum 1999.

[30] IPCC (2007). *Climate Change 2007: Impacts, Adaptation and Vulnerability. Working Group II Contribution to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, [available at: *http://www.ipcc.ch/publications_and_data/ar4/wg2/en/contents.html*].

[31] IPCC (2007). *Climate Change 2007: Mitigation of Climate Change. Working Group III Contribution to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, [available at: *https://www.ipcc.ch/pdf/assessment-report/ar4/wg3/ar4_wg3_full_report.pdf*].

[32] IPCC (2007). *Climate Change 2007: The Physical Science Basis. Contribution of Working Group I to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, [available at: *http://www.ipcc.ch/publications_and_data/ar4/wg1/en/contents.html*].

[33] IPCC (2012). Glossary of terms. In: *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation* [Field, C. B., Barros V., Stocker T. F. et al. (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, 555-564.

[34] IPCC (2012). *Summary for Policymakers. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change.*

Cambridge University Press, Cambridge, UK, and New York, NY, USA.

[35] IPCC (2014). *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. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, [available at: *http://ipcc-wg2.gov/AR5/images/uploads/WGIIAR5-PartA_FINAL.pdf*].

[36] IPCC (2014). *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. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA, [available at: *http://ipcc-wg2.gov/AR5/images/uploads/WGIIAR5-PartB_FINAL.pdf*].

[37] ISO (2009). *Risk Management*. Information Security Management System ISO/IEC 31000:2009, [available at: *http://www.iso.org/iso/home/ standards/iso31000.htm*].

[38] ISO, Technical Committees (2009). *United Nations International Strategy for Disaster Reduction (UNISDR)*. 2009 ISO 22301:2012, [available at: *http://www.iso.org/iso/catalogue_detail?csnumber=50038*].

[39] Klaver, M. H. A., Luiijf, H. A. M. & Nieuwenhuijsen, A. H. (2011). RECIPE project. *Good practices manual for CIP policies. For policy makers in Europe.*

[40] Kołowrocki, K., Kuligowska, E. & Reszko, M. (2016). Methodology for oil rig critical infrastructure network safety and resilience to climate change analysis. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 187-195.

[41] Kołowrocki, K., Kuligowska, E. & Reszko, M. (2016). Methodology for wind farms critical infrastructure network safety and resilience to climate change analysis. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 179-186.

[42] Levina, E. & Tirpak, D. (2006). *Adaptation to climate change: key terms.* Organisation for Economic Co-operation and Development (OECD). International Energy Agency.

[43] Newsome, B. O. (2016). *What's the difference between a hazard and a threat?* Practical skills and applied knowledge in security, defense, and risk management. [available at: *http://www.brucenewsome.com/hazard-threat.html*, last accessed: 19th February 2016].

[44] O'Rourke, T. D. (2007). Critical Infrastructure, Interdependencies, and Resilience. *The BRIDGE* 37, 1, National Academy of Engineering, 22-29.

[45] Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructures interdependencies, *IEEE Control Syst* 21, 6, 11-25.

[46] Samuels, P. & Gouldby, B. (2009). *FloodSite: Language of Risk – Project definitions*. [available at: *http://www.floodsite.net/html/partner_area/project_docs/T32_04_01_FLOODsite_Language_of_Risk_D32_2_v5_2_P1.pdf*].

[47] SLANDAIL (2015). *Slandail terminology*. The *Slandail* project's disaster lexicon. [available at: *http://slandailterminology.pbworks.com/w/page/82629973/Slandail%20Terminology*].

[48] United Nations. (2009). *UNISDR Terminology on Disaster Risk Reduction*. United Nations International Strategy for Disaster Reduction (UNISDR).

[49] US Department of Homeland Security. (2013). *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. [available at: *https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience*].

[50] US Environmental Protection Agency US EPA (2015). *Glossary of Climate Change Terms.* [available at: *http://www.epa.gov/climatechange/glossary.html*, last accessed: 19th February 2016].

[51] US President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations: Protecting America's Infrastructures*.

[52] WMO (2015). *International Meteorological Vocabulary*. WMO - No. 182, [available at: *http://wmo.multicorpora.net/MultiTransWeb/Web.mvc*].

[53] WMO (2015). *Natural hazards*. [available at: *https://www.wmo.int/pages/themes/hazards/index_en.html*, last accessed: 19th February 2016].