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

Soszyńska-Budny Joanna
ORCID ID: 0000-0003-1525-9392

Maritime University, Gdynia, Poland

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

Keywords

critical infrastructure, climate-weather change, resilience

Abstract

Introductory general approach to EU-CIRCLE project taxonomy and methodology is presented. National and international critical infrastructure protection overview is performed. The critical infrastructure protection legal frames in Poland, the institutions responsible for them and their duties are presented in details. A general approach to and a scheme of operation and climate-weather change influence on critical infrastructure safety and critical infrastructure accident consequences modelling is proposed as well.

1. Introduction

Prepared in the scope of EU-CIRCLE project activity deliverable [9] includes a very wide glossary (Database and the state of art) and a preliminary EU-CIRCLE taxonomy of most common phrases used in the project with selected practical illustrations. Deliverable D1.1 provides the common preliminary EU-CIRCLE language for members of the EU-CIRCLE Project Consortium to have the same understanding of terms and concepts, to serve as a reference material in all project deliverables and a taxonomy of the main concepts, elements and definitions that are used in the project. To ensure compatibility in the usage and communication of key terms across the work packages of EU-CIRCLE project the common preliminary working terminology is fixed in D1.1.

As it is known, many of the terms needed for the EU-CIRCLE project are used in different and sometimes conflicting ways across disciplines and approaches. Thus, a standard set of definitions is fixed to support a shared understanding of the foci of the project and be applied by all members involved in it. Therefore, the definitions are formulated to reflect the work of EU-CIRCLE programme, however they should also be regarded as "living" definitions, which evolve with the project research progress and new findings emerging.

Deliverable D1.1 approaches to Critical Infrastructures analysis and protection are strictly convergent with the approach of the EU-CIRCLE project to the European Critical Infrastructures resilience to climate change and are taken into account in preparing the terminology state of the art in the form of the Glossary (Database) in Chapters 3-5. The Glossary was composed of all recognized and collected by EU-CIRCLE project participants terms and definitions concerned with the methodology including the notions and the contexts of the Critical Infrastructure and its Safety, the Climate Change and the Resilience used in other previous and current projects and in available literature as well.

The spectrum of the terms concerned with those three main notions of the EU-CIRCLE project in the form of the state of the art is sufficiently wide and exhaustive in depth. Lot of terms included in the Glossary are defined in different and sometimes conflicting ways across disciplines and approaches. Some of them are simply incorrect. The main fault in

defining some of the terms included in the Glossary was mixing the meaning of the defined notion with the values of its parameters it is characterized by.
Having in mind this terminology state of the art and considering its imperfection and faults, the EU-CIRCLE Taxonomy was proposed in D1.1 Chapter 6.
The main principles in preparation of this taxonomy, at the first steps of the EU-CIRCLE project activity, were:

- To differ between the notion and the values of the parameters it is defined by;
- To illustrate shortly the notion and its parameters with their future use in the project in order to provide a better understanding the proposed terms by all project participants;
- To use the defined notions' order consistent with the subsequent steps of the project activity instead of alphabetical order, and leaving the latter arrangement to the last steps of project activity.

The detailed definitions of notions presented in D1.1 Chapter 6 are often given together with short illustrations/interpretations of their meanings and their expected practical usage in the project activity in order to provide a better understanding and to indicate the expected approaches in the project research. Thus, the preliminary EU-CIRCLE Taxonomy presented in Chapter 6 is a bit more than a pure taxonomy, what was practically important and justified at the very early stage of the project.
However, more progressively developed and improved final version of EU-CIRCLE Taxonomy have to be provided at the end of the project activity. This progress will be done in the following, corresponding to the project successive developments, 3 stages:
- 1st improved and developed version, M24;
- 2nd improved and developed version, M30;
- EU-CIRCLE Taxonomy final version, M36.

Moreover, at Summer Safety and Reliability Seminars - SSARS 2017, the Thematic Workshop on EU-CIRCLE Taxonomy and Methodology will be conducted and the papers presented there will be published in JPSRA 2017, http://jpsra.am.gdynia.pl .
This paper is an introductory part of the EU-CIRCLE Taxonomy and Methodology 1st improved and developed version based on deliverable D1.1 and limited to the terminology exactly used in the project activity only. This improved EU-CIRCLE Taxonomy and Methodology is structured as follows:

- Chapter 1: Introduction
- Chapter 2: Critical Infrastructure Terminology and Methodology
- Chapter 3: Climate-Weather Change Terminology and Methodology
- Chapter 4: Resilience Terminology and Methodology
- Chapter 5: Critical Infrastructure Accident consequences Terminology and Mathodology
- Chapter 6 : Conclusions
- Bibliography

The EU-CIRCLE Taxonomy presented in the report it is not completed yet. It will be developed during the project activity to achieve its next developed form in project activity month 30 and its final form at the last steps of the project activity in month 36.

2. National and international approaches to critical infrastructure protection – an overview

To ensure compatibility in the usage and communication of key terms across the work packages of EU-CIRCLE project the common "working terminology" fixed at the first steps of the project activity in D1.1 should be improved and developed considering national and international approaches to this terminology.
The first and most important term for the EU-CIRCLE project is the notion of the Critical Infrastructure. To follow the European Commission approach, the Critical Infrastructure (CI) is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens.
Reducing the vulnerabilities of critical infrastructure 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.

The European Programme for Critical Infrastructure Protection (EPCIP) 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 threats to which the programme aims to respond are not only confined to terrorism, but also include criminal activities, natural disasters and other causes

of accidents. In short, it seeks to provide an all-hazards cross-sectorial approach. The EPCIP is supported by regular exchanges of information between EU States in the frame of the CIP Contact Points meetings.

A key pillar of this programme is the 2008 Directive on European Critical Infrastructures. It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. The Directive has a sectorial scope, applying only to the energy and transport sectors. 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 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:

- 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).

Regional critical infrastructure protection (CIP) programmes in EU, in the EU-CIRCLE partners' countries and in USA are as follows:

- European Union

The European Programme for Critical Infrastructure Protection (EPCIP) has been laid out in EU Directives by the Commission (e.g., EU COM(2006) 786 final). It 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:

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

Each designated ECI will have to have an Operator Security Plan (OSP) covering 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.

- Croatia

CIP is based on a regulation "National Law on Critical Infrastructure", NN56/2013 http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html Sectors of economy were determined from which the central government bodies identify individual national critical infrastructure, in order to ensure comprehensive action to protect and reduce the negative effects in case of compromising critical infrastructures, due to their importance to the overall functioning of the country and the protection of critical infrastructure at national level (e.g. energy, communication and information technology, transport etc.)
https://vlada.gov.hr/UserDocsImages//Sjednice/Arhiva//111.%20-%207.pdf

- Cyprus

In Cyprus protection of critical infrastructure lies with the Minister of Interior and is governed according to Ministerial Decree KDP 15/2012 'On the Identification and Designation of European Critical Infrastructure and Assessment of the Need to improve its Protection Regulations of 2012'. The Ministry of Interior is assisted in the protection of Critical Infrastructure by the Civil Protection Authority. The Civil Protection Authority is responsible, in cooperation with any other relevant Government Departments and Agencies, for the identification and designation of critical infrastructure. The Civil Protection Authority is also responsible for ensuring that operator security plans are in place, and that these plans are adequate.

- France

In France, the secretary-general of national defense (SGDN) http://www.sgdn.gouv.fr/, a secretary attached to the Prime Minister's Office, bears complete responsibility for organizing CIP.

Furthermore, within the Ministry of Defense, the key organizations responsible for CIP / CIIP are the Central Directorate for Information Systems Security (DCSSI)

http://www.gsit.fr/glossaire/en/Central_Directorate_for_Information_Systems_Security_French_Security_of_Information_Systems_Directorate_DCSSI.htm, the Inter-Ministerial Commission for the Security of Information Systems (CISSI), and the Advisory Office, whereas the Central Office for the Fight Against Hi-Tech Crime plays a leading role within the Ministry of the Interior. [Wenger et al, 2008/2009]

- Germany

The German critical-infrastructure protection programme is coordinated by the Federal Ministry of the Interior. Some of its special agencies like the German Federal Office for Information Security or the Federal Office of Civil Protection and Disaster Assistance BBK deliver the respective content, e.g., about IT systems.

The German critical-infrastructure protection programme is coordinated by the Federal Ministry of the Interior. Some of its special agencies like the German Federal Office for Information Security or the Federal Office of Civil Protection and Disaster Assistance BBK deliver the respective content, e.g., about IT systems.

Overall responsibility for, and coordination of, major CIP- and CIIP-related activities rests with the Federal Ministry of the Interior (BMI), together with several of its subordinated agencies, such as the Federal Office for Information Security (BSI) https://www.bsi.bund.de/EN/Home/home_node.html, the Federal Office of Civil Protection and Disaster Assistance (BBK) http://www.bbk.bund.de/EN/Home/home_node.html , the Federal Criminal Police Agency (BKA) http://www.bka.de , and the Federal Police (BPOL) http://www.bundespolizei.de/cln_049/DE/Home/home__node.html?__nnn=true. For coordination within the ministry and the subordinated agencies, a task force for critical infrastructure protection (AG KRITIS) was established at the BMI in 2002. Strategy development and implementation are also coordinated with other federal ministries, especially the Federal Ministry of Economics and Technology http://www.bmwi.de/EN/root.html, the Federal Chancellery http://www.bundeskanzlerin.de/Webs/BKin/DE/Startseite/startseite_node.html, the Federal Ministry of Justice, the Federal Ministry of Foreign Affairs, the Federal Ministry of Defense, and other relevant agencies, such as the Federal Network Agency http://www.bundesnetzagentur.de/cln_1412/EN/General/Bundesnetzagentur/Bundesnetzagentur-node.html. Furthermore, strategic partners from the private sector are consulted. [Wenger et al, 2008/2009]

- Greece

The Greece critical-infrastructure protection programme is coordinated by the KEMEA http://www.kemea.gr/index.php/en/about-kemea. KEMEA is supervised by the Minister of Public Order and Citizen Protection and it is a scientific, consulting and research agency, whose purpose is to conduct theoretical and applied research and to perform studies, particularly at the strategic level, on security policies. In 2011, KEMEA was appointed by Presidential Decree No39 (06.05.2011), as the "National Contact Point" for the protection of European Critical infrastructures (ECIs) - "ECIP contact point" – following the implementation of the 2008/114/EC Directive of the European Council of December 8th 2008 "regarding the definition and designation of the European Critical infrastructures and the assessment of the need to improve the protection of such infrastructures".

- Italy

The main Italian government bodies dealing with CIIP are the Ministry of the Interior (Postal and Communications Police) and the Ministry of Innovation and Technologies. The Ministry of Communication is also involved in various activities to improve the security of information and communication networks.

In order to improve CIIP at all levels, the public agencies also collaborate closely with the private sector. The most important Public-Private Partnership in the field of CIP is the Association of Italian Experts for Critical Infrastructures (Associazione Italiana Esperti in Infrastrutture Critiche, AIIC) http://www.infrastrutturecritiche.it/aiic/index.php?option=com_content&view=article&id=219&Itemid=125, an expert group of practitioners from both the public and the private sectors. [Wenger et al, 2008/2009]

- Norway

In Norway, the ministry or authority that has responsibility for an area during peacetime or non-crisis times also has responsibility during times of crisis and war. This system also applies to CIIP. The coordinating authority on the civilian side is the Ministry of Justice and Police. The overall authority for ICT security is the Ministry of Government Administration and Reform, which took over this task from the Ministry of Trade and Industry, while the Ministry of Defense is responsible on the military side. The Ministry of Transport and Communications has responsibility for the communication sector in

Norway, including all related security issues. The directorates and authorities that are responsible for handling the various aspects of CIIP on behalf of the ministries are answerable to the respective ministries. [Wenger et al, 2008/2009]

- Poland

The Poland critical infrastructure protection programme is coordinated by the Poland's Government Centre for Security http://rcb.gov.pl./eng/ and is presented in "Critical Infrastructure Protection in the Polish Crisis Management Framework", Summer Safety and Reliability Seminars – SSARS 2015, Gdańsk/Sopot, June 21-27th 2015. http://ssars.am.gdynia.pl, see (EU-CIRCLE, Dissemination, SSARS 2015) at*:* https://eucircle.ipta.demokritos.gr/owncloud/

The Government Centre for Security established the following 11 critical infrastructures (systems):

1. Energy, fuel and energy resources supply system
2. Communication system
3. Tele-information network system
4. Financial system
5. Food supply system
6. Water supply system
7. Health protection system
8. Transportation System
9. Rescue system
10. System ensuring the continuity of public administration activities
11. System of production, storing and use of chemical and radioactive substances, including pipelines for dangerous substances.

Within the Polish government, two ministries have responsibilities that impinge upon the country's information infrastructures and their protection – the Ministry of Science and Higher Education http://www.nauka.gov.pl/en/ and the Ministry of the Interior https://www.msw.gov.pl/en. As a public-private partnership, the Polish Competence Center for eGov and eEdu strives to provide a platform to bring together the public sector and the IT companies.

- United Kingdom

In the UK, the Centre for the Protection of National Infrastructure provides information, personnel and physical security advice to the businesses and organisations which make up the UK's national infrastructure, helping to reduce its vulnerability to terrorism and other threats. See: Category: Disaster preparedness in the United Kingdom. It can call on resources from other government departments and agencies, including MI5, the Communications-Electronics Security Group and other Government departments responsible for national infrastructure sectors.

- United States

The USA has had a wide-reaching Critical Infrastructure Protection Program in place since 1996. Its Patriot Act of 2001 defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

These have identified a number of critical infrastructures and responsible agencies:

1. Agriculture and food – Departments of Agriculture and Health and Human Services
2. Water – Environmental Protection Agency
3. Public Health – Department of Health and Human Services
4. Emergency Services – Department of Homeland Security
5. Government – Department of Homeland Security
6. Defence Industrial Base – Department of Defence
7. Information and Telecommunications – Department of Commerce
8. Energy – Department of Energy
9. Transportation and Shipping – Department of Transportation
10. Banking and Finance – Department of the Treasury
11. Chemical Industry and Hazardous Materials – Department of Homeland Security
12. Post – Department of Homeland Security
13. National Monuments and icons - Department of the Interior
14. Critical Manufacturing - Department of Homeland Security (14th sector announced 03-Mar-2008; recorded 30-Apr-2008).

The National Infrastructure Protection Plan (NIPP) defines critical infrastructure sector in the US. Presidential Policy Directive 21 (PPD-21), issued in February, 2013 entitled Critical Infrastructure Security and Resilience mandated an update to the NIPP. This revision of the plan established the following 16 critical infrastructure sectors:

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defence Industrial Base
7. Emergency Services
8. Energy
9. Financial Services

10. Food and Agriculture
11. Government Facilities
13. Healthcare and Public Health
14. Information Technology
15. Nuclear Reactors, Materials, and Waste
16. Transportation Systems
17. Water and Wastewater Systems.

National Monuments and Icons along with the Postal and Shipping sector were removed in 2013 update to the NIPP. The 2013 version of the NIPP has faced criticism for lacking viable risk measures. The plan assigns the following agencies sector-specific coordination responsibilities:

1. Chemical -Department of Homeland Security
2. Commercial Facilities -Department of Homeland Security
3. Communications - Department of Homeland Security
4. Critical Manufacturing -Department of Homeland Security
5. Dams -Department of Homeland Security
6. Defence Industrial Base -Department of Defence
7. Emergency Services - Department of Homeland Security
8. Energy - Department of Energy
9. Financial Services - Department of the Treasury
10. Food and Agriculture -Department of Agriculture
11. Government Facilities - Department of Homeland Security and General Services Administration
12. Healthcare and Public Health - Department of Health and Human Services
13. Information Technology - Department of Homeland Security
14. Nuclear Reactors, Materials, and Waste - Department of Homeland Security
15. Transportation Systems - Department of Homeland Security and Department of Transportation
16. Water and Wastewater Systems - Environmental Protection Agency.

The European Programme for Critical Infrastructure Protection (EPCIP) 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 threats to which the programme aims to respond are not only confined to terrorism, but also include criminal activities, natural disasters and other causes of accidents. In short, it seeks to provide an all-hazards cross-sectorial approach. The EPCIP is supported by regular exchanges of information between EU States in the frame of the CIP Contact Points meetings.

A key pillar of this programme is the 2008 Directive on European Critical Infrastructures. It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. The Directive has a sectorial scope, applying only to the energy and transport sectors. 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 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:

- 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).

Regional critical infrastructure protection (CIP) programmes in EU, in the EU-CIRCLE partners' countries and in USA are convergent to the above approach.

The Poland critical infrastructure protection programme is coordinated by the Poland's Government Centre for Security http://rcb.gov.pl./eng/ and is presented in "Critical Infrastructure Protection in the Polish Crisis Management Framework", Summer Safety and Reliability Seminars – SSARS 2015, Gdańsk/Sopot, June 21-27th 2015. http://ssars.am.gdynia.pl, see (EU-CIRCLE, Dissemination, SSARS 2015) at*:* https://eucircle.ipta.demokritos.gr/owncloud/

Within the Polish government, two ministries have responsibilities that impinge upon the country's information infrastructures and their protection – the Ministry of Science and Higher Education http://www.nauka.gov.pl/en/ and the Ministry of the Interior https://www.msw.gov.pl/en. As a public-private partnership, the Polish Competence Center for eGov and eEdu strives to provide a platform to bring together the public sector and the IT companies.

3. Critical 1nfrastructure protection in Poland

3.1. Critical infrastructure protection frames

Main legal basis for Critical Infrastructure protection in Poland is an Act on Crisis Management passed on 27th of April 2007 (Dz.U. z 2007 r. nr 89, poz. 590, http://rcb.gov.pl/wp-content/uploads/ustawa-o-zarz%C4%85dzaniu-kryzysowym.pdf). That Act constitutes National Crisis Management Plan (NCMP) (and local crisis managements plans) which contains:

- characterizations of threats and risk assessments of their occurrence, including those relating to the critical infrastructure, risk maps and maps of threats,
- the procedures for implementation of tasks of crisis management, including those relating to the protection of critical infrastructure,
- priorities in the scope of protection and restoration of critical infrastructure,
- (confidential) list of critical infrastructure.

NCMP is updated every two years or often if needed. According to the Act above, protection of critical infrastructure is an operator's / owner's duty, in particular by:

- preparing and implementation of critical infrastructure protection plans,
- maintaining back-up systems to ensure the safety and supporting the functioning of this infrastructure until its complete restoration,
- designating of a contact person responsible for maintaining relations with the relevant public administration.

Appropriate regulation on creating plans (by the owners/operators) for protection of critical infrastructure has been introduced on 30th of April 2010 (Dz.U. nr 83, poz.542). The Act on Crisis Management (together with Regulation from 11.04.2011, Dz.U. nr 86, poz. 471) establish Government Centre for Security (GCS) which is responsible for coordination of all activities related to crisis management and critical infrastructure. GCS prepares National Critical Infrastructure Protection Programme (NCIPP) (Regulation from 30.04.2010, Dz.U. nr 83, poz. 541). Aim of that program is to create conditions for improving the critical infrastructure security by specifying priorities, objectives, requirements and standards to ensure a smooth functioning of critical infrastructure as well as by specifying government entities responsible for the system. NCIPP contains confidential Annex 3 with criteria which allow defining of what is a critical infrastructure for the state.

3.2. Critical infrastructure protection institutions and their duties

As it was already mentioned, Government Centre of Security (GCS) http://rcb.gov.pl./eng/ is the institution responsible for critical infrastructure protection. GCS works continuously, 24 hours a day, providing immediate actions, support and management in case of any threats to critical infrastructures.

The Government Centre of Security distinguished, according to the Act on Crisis Management, following 11 critical infrastructures types (systems) listed in Section 2.

Subdivision of GCS named Critical Infrastructure Protection Unit creates common concepts, standards and promotes solutions for the protection of critical infrastructure which will later be reflected in the government documents and their implementation. It organizes cooperation between public administration bodies to ensure constant exchange of information, which accelerates and increases the effectiveness of the protection and has influence on the process of safety management of critical infrastructure.

The cooperation includes, in particular:

- creating a database of experts on issues related to critical infrastructure within the CI sectors. Database experts will speed up the process of consultation and at the same time will provide substantive support in the event of disruption of the CI and within the framework of public-private forum,
- designation of CIP contact points within the public administration and government services (including ministries, central offices, voivodeship offices, Police Headquarters, Internal Security Agency, Intelligence Agency and the Headquarters of the Border Guards and State Fire Service),
- participation in the development, revision and implementation of the National Critical Infrastructure Protection Programme.

CIP Unit also organizes cooperation between public and private sector and, in particular, between

representatives of different systems within private sector. Such cooperation is one of the key element to ensure comprehensive and efficient CIP, since, according to the law, protection is a duty of the owner/operator. Developing clear rules and procedures between the authorities, state services and both sole and dependant owners and holders of the objects, installations or facilities of critical infrastructure is an important element of cooperation. It results from the fact that the foremost part of the infrastructure, being of the key importance for the security of the state, lies in the hands of the private sector.

In case of damage to CI on the state level, the government is responsible for crisis management, in particular by conduct and coordination of all actions aim to restore proper functioning of CI. One of the main resource that is used by the government is State Fire Service (SFS), which is the main part of national fire-fighting and rescue system. That system was established as early as 1995 and later developed significantly by giving it more legal basis in updated Act on Fire Protection (Dz.U. z 2009 r. nr 178, poz. 1380, http://isap.sejm.gov.pl/Download?id=WDU20091781380&type=3) and in Regulation of Minister of Internal Affairs and Administration (Dz.U. z 2011 r. Nr 46, poz 239) . The Chief Commandant of SFS is the central authority responsible for organization of protection of infrastructure that is endangered by different factors (e.g. natural disasters).

On the level of voivodeship, the voivode is responsible for preparing local crisis management plan and, in case of threats to critical infrastructure, realization of that plan. The voivode also organizes and supervises conducting of all task related to CIP in the voivodeship area. His Department of Security and Crisis Management gathers and processes information on critical infrastructure located in the province.

The Department is also responsible for formulate and implementation of procedures in case of threats to CI as well as for cooperation, in the field of protection, between public authorities and privet owners of CI. Within this Department operates Provincial Crisis Management Centre (CMC), which is on call 24 hours a day to ensure the flow of information for crisis management. The tasks of the provincial crisis management centres include:

- cooperation with other CMCs on different levels of public administration (state, provincial, county),
- supervision over the population early warning system,
- cooperation with providers of environmental and weather monitoring,
- cooperation with entities carrying search and rescue operations.

County CMCs is a lower level group that is responsible for, among other duties, organization and implementation of duties related to critical infrastructure protection. It is led by the starost (head of county).

If, in the crisis situation, use of other resources is not possible or may not be sufficient, the Minister of National Defence, at the request of the voivode may delegate to his disposal subdivisions or branches of the Polish Armed Forces, to perform tasks in the field of crisis management. Those army troops, according to the Act on Crisis Management, may be used for:

- works related with security, of threatened objects, buildings (including CI objects),
- performing tasks related to repair and reconstruction of critical infrastructure,
- participation in ensuring operability of routes,
- carry out works requiring the use of specialized technical equipment,
- removal of hazardous materials.

All above mentioned actions undertaken by army troops are coordinated by local Crisis Management Centres, which are responsible for smooth integration of armed forces into civil system of CIP to carry out appropriate tasks.

4. EU-CIRCLE methodology

4.1 General approach

The proposed EU-CIRCLE methodology is based on the following key tasks of the project research activity:

- To understand the behaviour of critical infrastructure dependencies over time, what involves the modification of infrastructure inside and outside dependences as its operation is changing [26] including changing its structure and its components and subsystems safety parameters [14], [16];
- To use the information collected in the survey to group critical infrastructures into clusters/networks according to their dependence and/or influence in order to identify their common characteristics [26];
- To involve developing a dynamic system model [26], including critical infrastructure ageing/degradation in time [14], [16] for

expressing and simulating [22]-[24] critical infrastructure dependence and influence;

- To enable operators to examine a variety of hypothetical scenarios, focusing on the temporal aspects of critical infrastructure and the consequent effects and provide deep insides into the behaviour of the complex system/network of critical infrastructures, contributing to the design and implementation of robust critical infrastructure protection, strengthening and recovery strategies.

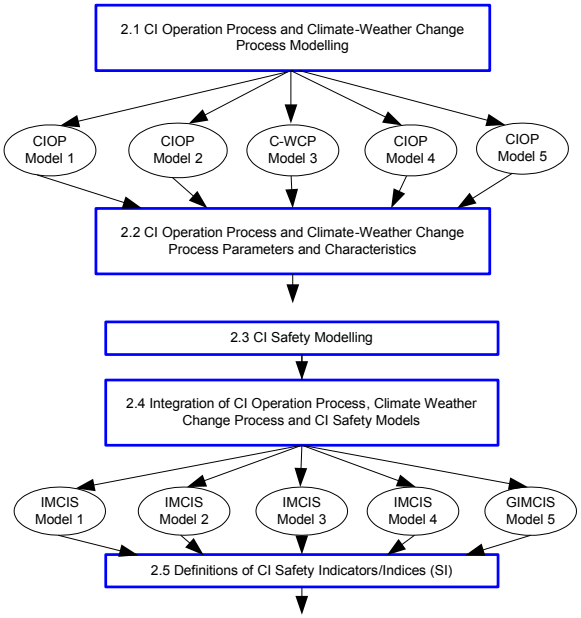
Most real complex technical critical infrastructure are strongly influenced by changing in time their operation conditions and the climate-weather conditions at their operating areas. The time dependent interactions between the operation process related to climate-weather change process states varying at the system operating area and the critical infrastructure safety structure and its components/assets safety states changing are evident features of most real technical systems including critical infrastructures [Kołowrocki 2013], [Kołowrocki & Soszyńska-Budny 2011]. The common critical infrastructure safety and resilience, its operation process and the climate-weather change process at its operating area analysis is of great value in the industrial practice because of often negative impacts of operating environment threats (OET) and extreme weather hazards (EWH) on the critical infrastructure safety and resilience. In the critical infrastructure safety analysis, the determination of its safety function and its risk function which graph corresponds to the fragility curve and other proposed in the paper safety and resilience and other features' characteristics are crucial indices for its operators and users.

Recently published paper [Kołowrocki & Soszyńska-Budny, 2017] is devoted to a comprehensive modelling of the influence of the operation process and the climate-weather change process on the safety of a critical infrastructure. Particular models of critical infrastructure safety influenced by its inside among its components and subsystems dependences and by its outside operating environment threats and climate-weather hazards are created and a reasonable perspective for their further developments and applications is marked out. A set of safety indicators for a critical infrastructure is proposed and the simplified procedures of their determination in the case of the created models of critical infrastructure safety are proposed and illustrated.

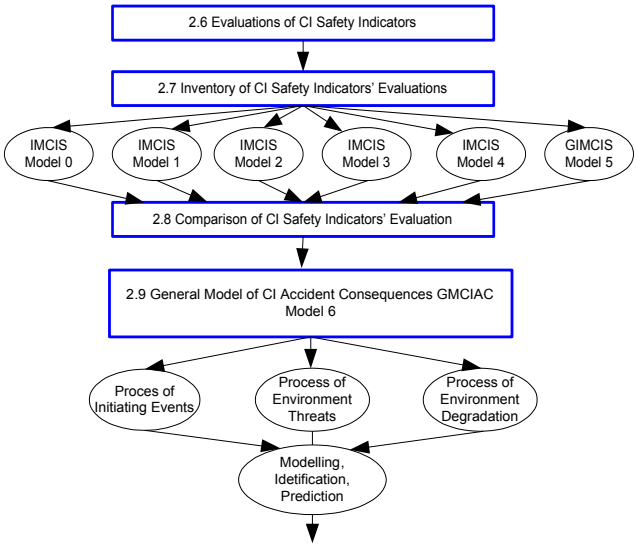
To make the effort of the formulated problem solution well organized, the scheme of a general approach to safety and resilience analysis of critical infrastructure giving subsequent steps in the research activity is presented in the next section.

4.2 Scheme of operation and climate-weather influence on critical infrastructure safety and resilience modelling

An original and innovative general approach to operation process and climate-weather change process influence on critical infrastructure safety and resilience modelling and analysis has been created in



the report [18] and in the paper [25]. The scheme of this approach is presented below in *Figure 1.*



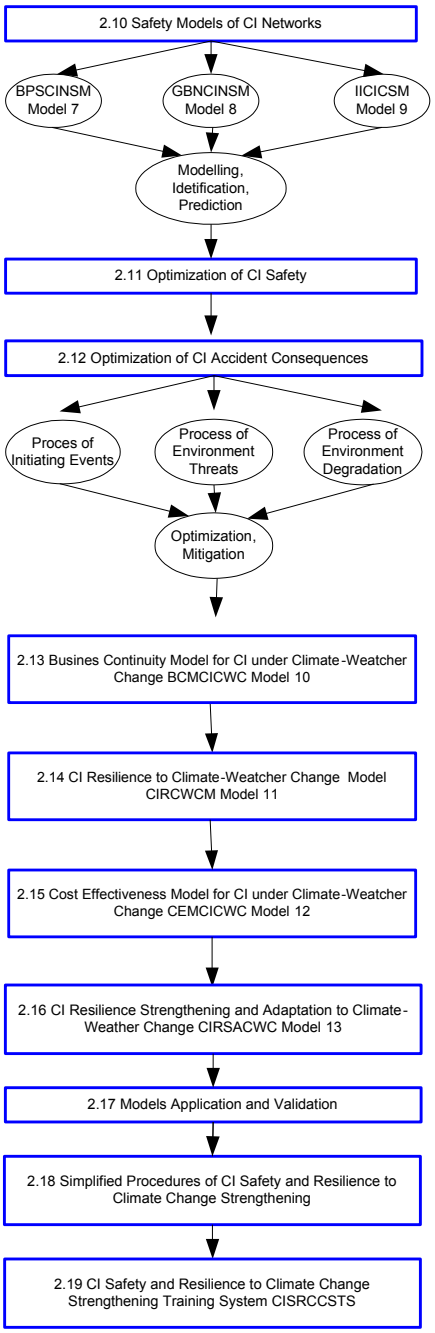


Figure 1. The scheme of general approach to operation and climate-weather change influence on critical infrastructure safety and resilience modelling

In this scheme:
- the content of scheme items 2.1-2.10 is concerned with the critical infrastructure operation process and climate-weather change process at its operating area modelling, critical infrastructure safety modelling, with the integration of the designed models into a general joint models of critical infrastructure safety related to operation and climate-weather change processes and with the modelling safety of critical infrastructure networks and their accidents consequences;
- the content of scheme items 2.11-2.16 is concerned with the critical infrastructure safety and its accident consequences optimization, business continuity, resilience and cost effectiveness modelling;
- the content of scheme item 2.17 is concerned with the case studies and the proposed models application and validation;
- the content of scheme item 2.18 is concerned with the development of simplified procedures of critical infrastructure safety and resilience to operation and climate-weather change strengthening;
- the content of scheme item 2.19 is directly concerned with the critical infrastructure safety and resilience to operation and climate-weather change strengthening training system.

Starting from a simplest pure safety Model 0 [5] without considering outside impacts on critical infrastructure defined as a multistate ageing system, the critical infrastructure and its components/assets safety functions and other safety indices like mean values and variances of lifetimes in the safety state subsets and in the particular safety states, a critical infrastructure risk function, its fragility curve, the moment of exceeding the critical safety state and intensities of ageing/degrading are defined. System components' independences are ignored and practically important modifications assuming inside critical infrastructure assets' dependences are introduced and developed.

Further, Model 0 is joined with the critical infrastructure operation process model to create Model 1 [19] devoted to safety modelling and prediction of critical infrastructure defined as a complex system in its operating environment that significant features are inside-system dependencies and outside-system dependencies. This is a general safety analytical model of a critical infrastructure related to its operation process, linking its multistate safety model and its operation process model and considering variable at different operation states its safety structure and its components' safety parameters. In this model, additional safety indices typical for the critical infrastructure related to its varying in time safety structures and its components' safety parameters caused by its operation process are introduced extending the Model 0 set of safety indicators by the components and critical infrastructure conditional intensities of ageing at particular operation states and conditional and unconditional coefficients of the operation process impact on intensities of ageing. A slight

generalization of Model 1 [19] is Model 2 [23] devoted to safety of a critical infrastructure related to its operation process including operating environment threats. It is the integrated general model of critical infrastructure linking its multistate safety model and the model of its operation process including operating environment threats and considering variable at the different operation states safety structures and their components safety parameters. Other practically significant discussed in this report critical infrastructure safety indicators are the critical infrastructure and its components intensities of degradation and the coefficients of operation process including operating environment threats influence on the critical infrastructure and its components intensities of degradation. Next, a general safety analytical Model 3 [24] of critical infrastructure safety related to the climate-weather change process in its operating area [20] is proposed. It is the integrated model of critical infrastructure safety, linking its multistate safety model and the model of the climate-weather change process at its operating area, considering variable at the different climate-weather states and impacted by them system components safety parameters. The conditional safety functions at the climate-weather particular states, the unconditional safety function and the risk function of the critical infrastructure at changing in time climate-weather conditions are defined. Other, practically significant, critical infrastructure safety indices introduced in the model are its mean lifetime up to the exceeding a critical safety state, the moment when its risk function value exceeds the acceptable safety level, the intensities of ageing of the critical infrastructure related to the climate-weather change process at its operating area and its components and the coefficients of the climate-weather change process impact on the critical infrastructure and its components intensities of ageing. More general Model 4 [24] considering together the operation process and the climate-weather change process influence on the safety of a critical infrastructure [22], i.e. the safety analytical model of a critical infrastructure under the influence of the operation process related to climate-weather change process is proposed. It is the integrated model of a critical infrastructure safety, linking its multistate safety model and the model of its operation process related to climate-weather change process at its operating area, considering variable at the different operation and climate-weather states impacted by them the system safety structures and its components safety parameters. The conditional safety functions at the operation process related to climate-weather change process particular states, the unconditional safety function and the risk function of a critical infrastructure at changing in time operation and climate-weather conditions are defined. Other, practically significant, critical infrastructure safety indices introduced in the model are its mean lifetime up to the exceeding a critical safety state, the moment when its risk function value exceeds the acceptable safety level, the intensities of ageing of the critical infrastructure and its components impacted by the operation process related to the climate-weather change process at its operating area and the coefficients of the operation process related to the climate-weather change process impact on the critical infrastructure and its components intensities of ageing. Most general Model 5 [21] covers the operating environment threats and climate-weather hazards influence on the safety of a critical infrastructure [21]. A general safety analytical model of a critical infrastructure under the influence of its operation process including operating environment threats (OET) related to climate-weather change process including extreme weather hazards (EWH) is proposed. It is the integrated model of a critical infrastructure safety, linking its multistate safety model and the joint model of its operation process including OET and the climate-weather change process including EWH at its operating area, considering variable at the different operation and climate-weather states impacted by them the critical infrastructure safety structures and its components safety parameters. The conditional safety functions at the operation process including operating environment threats and climate-weather hazards particular states, the unconditional safety function and the risk function of the critical infrastructure at changing in time its operation conditions including OET and climate-weather conditions including EWH are defined. Other, practically significant, critical infrastructure safety indices introduced in the paper are its mean lifetime up to the exceeding a critical safety state, the moment when its risk function value exceeds the acceptable safety level, the intensities of ageing of the critical infrastructure and its components impacted by the operation process including operating environment threats related to the climate-weather change process including extreme weather hazards and the coefficients of the operation process including operating environment threats related to the climate-weather change process including extreme weather hazards impact on the critical infrastructure and its components intensities of ageing. These all safety indices, proposed in Models 0-5, are defined in general for any critical

infrastructures varying in time their safety structures and components safety parameters influenced by changing in time operation conditions including environment threats and climate-weather conditions including climate-weather extreme weather hazards at their operating areas. The way of modification all considered critical infrastructure safety models into more general models for safety analysis and prediction of critical infrastructure networks and networks of critical infrastructure networks and for networks of critical infrastructure networks cascading effect analysing is proposed as well. In addition, a general approach to modelling, identification and prediction of critical infrastructure accident consequences is proposed [6]. After finalising tasks of scheme items 2.1-2.10, the next step can be done to perform the tasks formulated in scheme items 2.11-2.16, terminating methodological framework, where the devised risk and impact assessment framework on interconnected and interdependent critical infrastructures may be transformed into a resilience and adaptation framework. Thus, the way we should go in the research further activity is investigating and solving the problems of Optimization of Critical Infrastructure Safety (finding optimal values of Safety Indictors), Critical Infrastructure Accident Consequences Optimisation and Mitigation, Critical Infrastructure Resilience to Climate-Weather Change Analysis and Strengthening Critical Infrastructure Resilience to Climate-Weather Change, pointed out in the scheme of the general approach to safety and resilience analysis presented in the report [18]. This activity will results in Business Continuity Models for Critical Infrastructure under climate pressures elaboration, Critical Infrastructure Resilience Indicators defining, Cost-effectiveness analysis and modelling and finally in Framework for Critical Infrastructure adaptation to climate change creation. Similarly as in the case of critical infrastructures safety analysis, the simplified procedures for critical infrastructures resilience analysis modelling, identification, prediction and optimization are expected to be developed. All the above Models 0-13 and the results of their practical applications can be the basis for preparation of significantly simplified models and procedures that are very easy to use by the practitioners and operators of the critical infrastructures in their safety analysis. The use of these simplified procedures based on Models 0-13 is illustrated in Section 3.3 [25] for real critical infrastructure operating at the Baltic Sea Region. These simplified procedures are also expected to be modified and developed for other than safety features of critical infrastructure analysis, modelling and prediction. They also can be the basis for preparing computer software allowing to apply by practitioners these procedures automatically.

5. Conclusions

This paper is an introductory to 1st improved version of deliverable D1.1 and to 4 other papers presented at SSARS 2017 Workshop on EU-CIRCLE Taxonomy and Methodology and devoted respectively Critical Infrastructure, Climate-Weather Change and Resilience taxonomy and methodology.

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

[1] Act on Crisis Management passed on 27th of April 2007 (Dz.U. 2007 r. nr 89, poz. 590, http://rcb.gov.pl/wp-content/uploads/ustawa-o-zarz%C4%85dzaniu-kryzysowym.pdf)

[2] Act on Fire Protection (Dz.U. z 2009 r. nr 178, poz. 1380, http://isap.sejm.gov.pl/Download?id=WDU20091781380&type=3)

[3] Ben, P., Gouldby, B.P., Schultz, M.T., Simm, J.D. & Wibowo J.L (2010). Beyond the Factor of Safety: Developing Fragility Curves to Characterize System Reliability, Report in Water Resources Infrastructure Program ERDC SR-10-1, Prepared for Headquarters, U.S. Army Corps of Engineers, Washington.

[4] Blokus-Roszkowska, A. & Dziula, P. (2015). An Approach to Identification of Critical Infrastructure Systems. Proc. The International Conference of Numerical Analysis and Applied Mathematics - ICNAAM 2015 Symposium, Rhodes, Greece, ….

[5] Blokus-Roszkowska, A., Kołowrocki, K., Kuligowska, E. & Soszyńska-Budny, J. (2016). Critical Infrastructure Safety Model (CISM), Multistate Ageing Approach Independent and Dependent Components and Subsystems, CISM Model 0, EU-CIRCLE Report D3.3-GMU0.

[6] Bogalecka, M. & Kołowrocki, K. (2016). General Model of Critical Infrastructure Accident Consequences, GMCIAC Model 6, EU-CIRCLE Report D.3.3-GMU0.

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

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

[9] D1.1, EU-CIRCLE Taxonomy, EU-CIRCLE Project Report, 2015.

[10] European Commission, 2015, Critical Infrastructure, <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm>

[11] Government Centre of Security (GCS), http://rcb.gov.pl./eng/

[12] Kolobrzeg County, Crisis Management and Defence Bureau, http://www.spkolobrzeg.finn.pl/bipkod/001/004

[13] Kołowrocki, K. (2013). Safety of critical infrastructures. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars,* Vol. 4, No 1, 51-72.

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

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

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

[17] Kołowrocki, K. (2013). Safety of critical infrastructures, *Journal of Polish Safety and Reliability Associ*ation, Summer Safety and Reliability Seminars, 4(1): 51-72.

[18] Kołowrocki, K. & Soszyńska-Budny, J. (2016). 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.

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

[20] Kołowrocki, K. & Soszyńska-Budny, J. (2016). 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.

[21] Kołowrocki, K. & Soszyńska-Budny, J. (2016). 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.

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

[23] Kołowrocki, K., Soszyńska-Budny, J. & Torbicki, M. (2016). 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.

[24] Kołowrocki, K., Soszyńska-Budny, J. & Torbicki, M. (2016). 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.

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

[26] Lauge, A., Hernantes, J. & Sarriegi, J.M. (2015). Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection*, Vol. 8, 6-23.

[27] Pomeranian Voivodeship Security and Crisis Management Department, http://www.gdansk.uw.gov.pl/en/departaments/178-security-and-crisis-management-department,

[28] Pomeranian Provincial Crisis Management Centre, http://uwgdansk.ssdip.bip.gov.pl/oddzialy-wbizk/wojewodzkie-centrum-zarzadzania-kryzysowego.html

[29] PGCS, Polish Government Centre for Security, Act on crisis management, 2007

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

[31] Regulation on critical infrastructure protection plans (Dz.U. 2010 r. nr 83, poz. 542, http://rcb.gov.pl/wp-content/uploads/rozporz%C4%85dzenie-RM-ws-planach-oik.pdf)
[32] Regulation on the detailed rules for the organization on the national fire-fighting and rescue system (Dz.U. z 2011 r. Nr 46, poz 239, http://isap.sejm.gov.pl/Download?id=WDU20110460239&type=2)
[33] Regulation on the organization and operating mode of the Government Centre for Security (Dz.U. 2011 r. nr 86, poz. 471, http://rcb.gov.pl/wp-content/uploads/Regulation-on-the-organisation-and-operating-mode-of-the-Government-Centre-for-Security-pdf.pdf,in English)
[34] Regulation on National Critical Infrastructure Protection Programme (Dz.U. 2010 r. nr 83, poz. 541, http://rcb.gov.pl/eng/wp-content/uploads/2011/03/REGULATION-on-NATIONAL-CRITICAL-INFRASTRUCTURE-PROTECTION-PROGRAMME-AB.pdf,in English)