SAFETY AND SECURITY OF BALTIC SEA AREA CRITICAL INFRASTRUCTURE NETWORKS - INTEGRATED MANAGEMENT SYSTEM

PRESENTATION AT HAZARD WORKSHOP ORGANIZED BY PSRA ON 15.02.2019 IN GDYNIA

PROJECT PARTNER:

POLISH SAFETY AND RELIABILITY ASSOCIATION (PL)

KOŁOWROCKI KRZYSZTOF

SOSZYŃSKA-BUDNY JOANNA

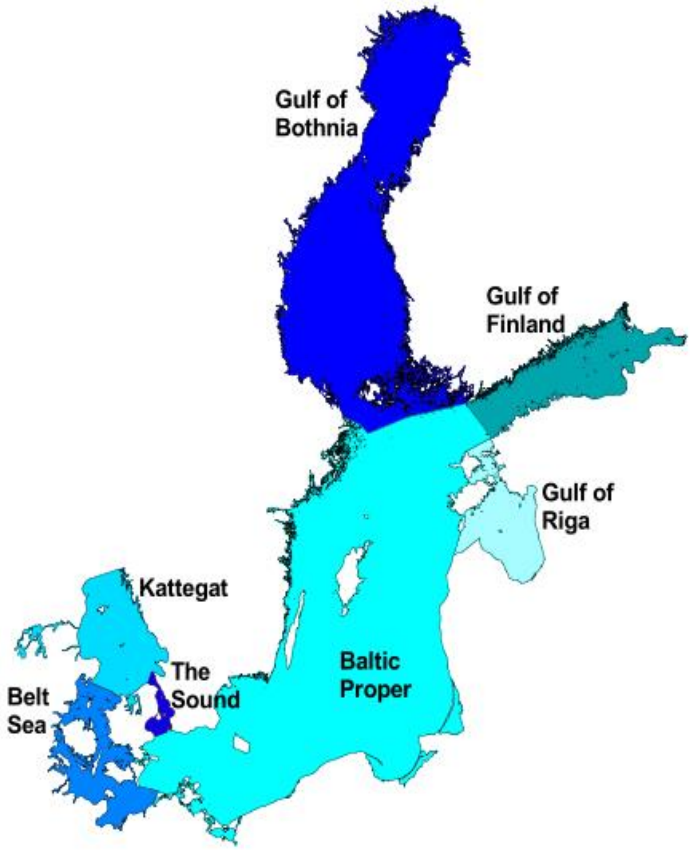
Contents

Contents

Contents

1. Baltic Sea basin
1.1.Baltic Sea geographical and climatological parameters

a)



b)

Figure 1. The Baltic Sea a) sub-basins [HELCOM, 2010], b) drainage basin (source: http://maps.grida.no/baltic/)

1.2. Baltic Sea environmental impacts of human activities

Figure 2. HELCOM member states (source: https://en.wikipedia.org/wiki/HELCOM)

1.2. Baltic Sea environmental impacts of human activities

Figure 3. Exclusive economic zones at the Baltic Sea (source: http://maps.helcom.fi/)

2. Critical infrastructure networks at Baltic Sea and its seaside
2.1. Critical infrastructures and their operation environment methodology

Before the considerations on critical infrastructure installations at Baltic Sea Region, we refer to definitions of selected basic notions concerned with critical infrastructures and climate and weather impacts on their safety.

We start with the notion of the **complex system** that is defined as a set or group of interacting, interrelated or interdependent elements or parts, that are organized and integrated to form a collective unity or an unified whole, to achieve a common objective.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.1. Critical infrastructures and their operation environment methodology

The **system operating environment** is defined as the surroundings in which a system operates, including air, water, land, natural resources, flora, fauna, humans and their interrelations.

The **system operating environment threat** is an unnatural event that may cause the system damage and/or change its operation activity in the way unsafe for the system and its operating environment

2. Critical infrastructure networks at Baltic Sea and its seaside
2.1. Critical infrastructures and their operation environment methodology

The **climate related hazard** is a natural physical event coming out from climate change that may cause loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, and environmental resources.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.1. Critical infrastructures and their operation environment methodology

Now, we can define the **critical infrastructure** as 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.

Further, we may define the **country's critical infrastructure** as a critical infrastructure complex system and assets located in the country which is essential (vital) for the national security, governance, public health and safety, economy and public confidence of this country.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.1. Critical infrastructures and their operation environment methodology

More general notion is the **regional critical infrastructure** defined as critical infrastructure the network of interconnected and interdependent critical infrastructures located in the considered region that function collaboratively in order to ensure a continuous production flow of essentials, goods and services.

And particularly, the **European critical infrastructure** is the he network of interconnected and interdependent critical infrastructures located in EU member states that function collaboratively in order to ensure a continuous production flow of essentials, goods and services.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.1. Critical infrastructures and their operation environment methodology

To explain two last definitions, we need to be familiar with the following three notions, the **critical infrastructure network** which 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 dependent relationships between themselves interacting at various levels of their complexity.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.1. Critical infrastructures and their operation environment methodology

The **strengthening critical infrastructure resilience** is defined as efforts, like policies, procedures and actions, taken to prolong the proper and effective functioning of a critical infrastructure and providing its essential services when it is exposed to unnatural threats and natural hazards.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.2. Critical infrastructure installations at Baltic Sea region

Considering definitions of main notions from the above methodology concerned with critical infrastructures and their networks and the nature and features of the industrial installations at the Baltic Sea Region, we are convinced to distinguish the following 8 **main critical infrastructure networks** operating in this region :

- port critical infrastructure network;
- shipping critical infrastructure network;
- oil rig critical infrastructure network;
- wind farm critical infrastructure network;
- electric cable critical infrastructure network;
- gas pipeline critical infrastructure network;
- oil pipeline critical infrastructure network;
- ship traffic and operation information critical infrastructure network.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.2. Critical infrastructure installations at Baltic Sea region

Moreover, we suggest to call the network of all those distinguished 8 networks operating at Baltic Sea Region the Global Baltic Network of Critical Infrastructure Networks.

INTERDEPENDENT LAYERS – three-layered grid of the Baltic Sea

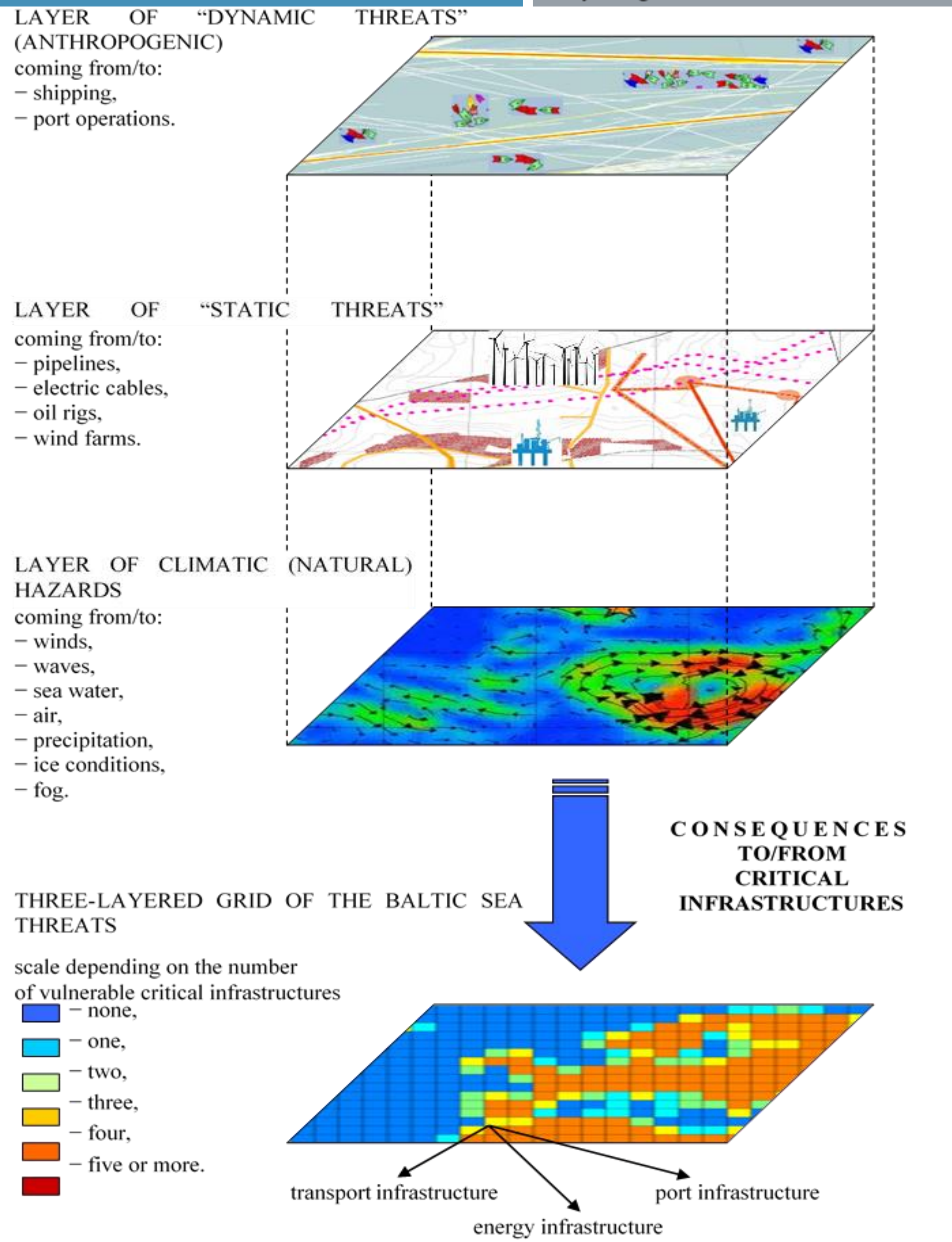


Figure 4. The model of area-picture of potential threats from/to critical infrastructures in the Baltic Sea Region.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.2. Critical infrastructure installations at Baltic Sea region

The Baltic Sea is facing an expansion in all sectors (*Figure 5*). This growth increase demand for the space and resources of the sea, and can consequently lead to conflicts within maritime sectors and between sectors. The Baltic Sea is already one of the most densely trafficked sea regions in the world. In addition to the pressures from place-based maritime activities, the already stressed Baltic Sea ecosystem is exposed to further pressures from diffuse sources like agricultural and industrial pollution and climate change.

2. Critical infrastructure networks at Baltic Sea and its seaside
2.2. Critical infrastructure installations at Baltic Sea region

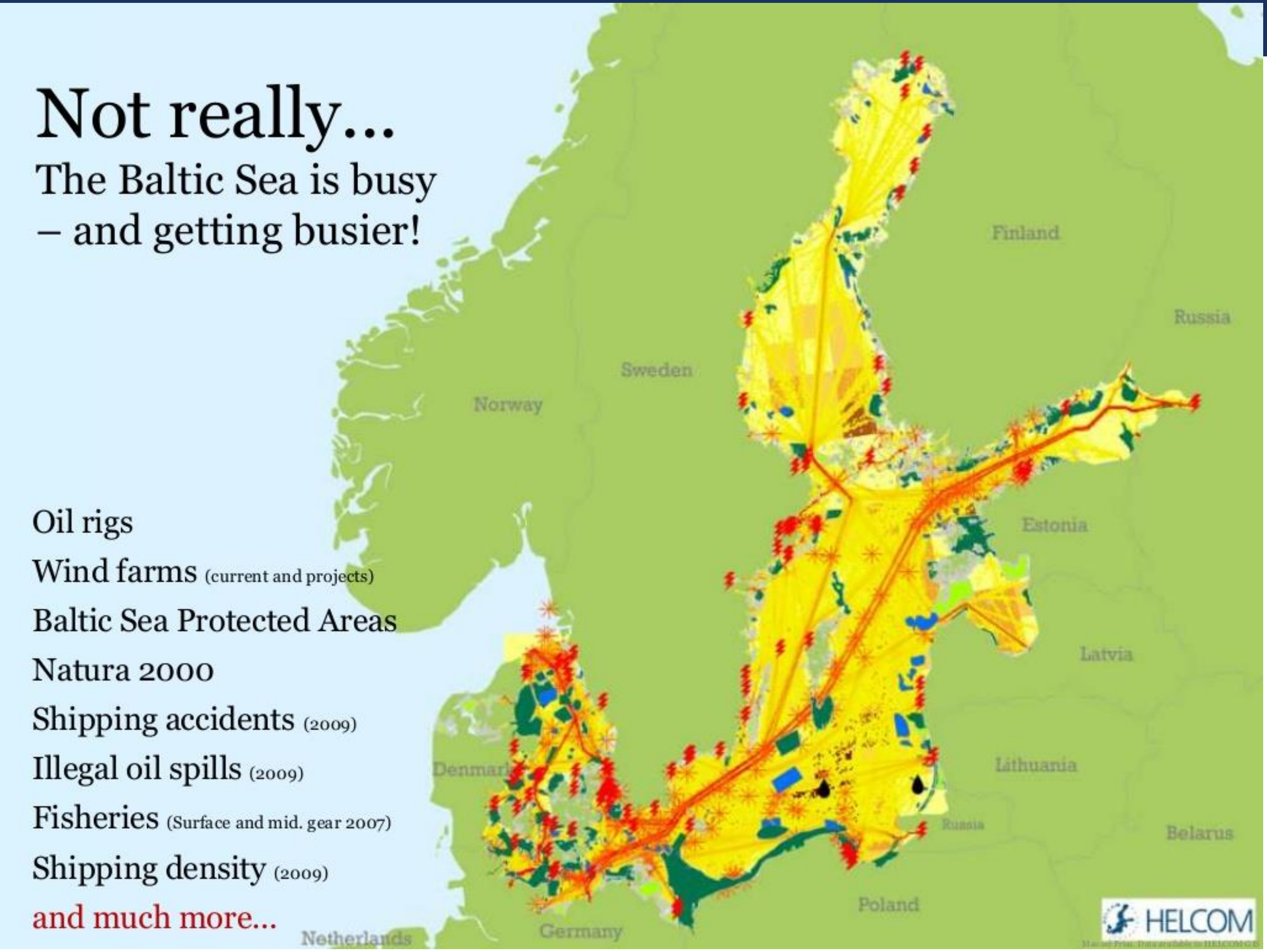


Figure 5. Components of spatial planning at BSR: critical infrastructures, obstructions, dangerous areas, protected areas, shipping accidents, traffic density, fisheries, oil spills and Natura 2000.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.1. Main project aims

The proposed project is aimed at proposing new methods and developing advanced tools capable to support effective modelling and decision making in the process of evaluating and controlling relevant risks in time including the safety and security aspects.

The methods for analysis and assessment of relevant risks for different time horizons will be developed including long term conditions and consequences due to potential accidents and resulting pollution and environment degradation.

Its main focus is on the creation and implementation of new techniques, procedures and strategies to improve and to reduce and control dynamic risks of real ports and maritime complex infrastructure systems, installations and processes related to the inside impacts (organisation structure, subsystems and components' interactions) and the outside impacts (coming from their operating environment threats and natural hazards).

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.1. Main project aims

The project will propose new methods ensuring and improving safety and security of critical infrastructure networks in various sectors with a special stress on their adoption to port and water of Baltic Sea area.

With the created and adopted methods and tools, the project will improve and link conventional approaches within current methods and procedures of safety and security of critical infrastructure networks in various sectors, by providing an integrated package of solutions consisting of various packages of theoretical and practical tools.

These methods and tools will allow to create an original and coherent theory of safety and security of critical infrastructure networks that will be ready for direct use by safety theoreticians and practitioners dealing with safety and security of port and maritime critical infrastructures and processes.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.1. Main project aims

The main deliverable and impact of the project on the development of science will be the development and ordering safety and security knowledge and creating new coherent theory of critical infrastructure networks' safety and security and improving significantly the safety and security of human overall activity in port and maritime sectors by creating the

Integrated Critical Infrastructure Safety and Security Management System (ICISSMS)

to be implemented at the created

Internet Critical Infrastructure Safety and Security Management Centre (ICISSMC).

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system

3.1. Main project aims

The center **ICISSMC** will carry permanent education, dissemination and consultancy services to various port and maritime industry and administration sectors including seminars, conferences, training courses and fully operational interactive internet service as the main gate to all critical infrastructures safety and security related resources and knowledge.

The results of the project will have an significant impact on the development of safety and security science and reducing negative influence of the risk of operating environment threats coming from human industrial activity and natural hazards coming from climate-weather change.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.2. Project proposal description

The analytical methods proposed will be complemented with the statistical methods for operation, safety and security data processing that will include an innovative and original approach to the methods of safety and security evaluation and optimization on the basis of the existing rough and incomplete empirical data.

Moreover, in the case of impossibility of analytical methods application, the Monte Carlo simulation method will be proposed.

The Monte Carlo simulation method will also be proposed as a tool to control safety and security of critical infrastructure networks and their accidents consequence in real time to have information on their security and safety state and to predict the consequences of their accidents in the nearest future.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.2. Project proposal description

Thus, these all approaches will fulfill a comprehensive solution of problems the project is concerned with.

The activities also performed in the project will be research and technology development, innovation and demonstration, scientific experiments expanding knowledge, newly developed tools practical testing, education and training.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.2. Project proposal description

Joint considering of the inside and outside of the port and maritime critical infrastructures dependencies and including other outside dangerous events and hazards coming from the environment and from other dangerous processes is an original approach to analysis of safety and security of complex port and maritime critical infrastructure networks.

This joining is a main novel aspect of the project proposal allowing to develop significant and new results concerned with the modeling, identification, evaluation, prediction and optimization of the safety and security of the complex port and maritime critical infrastructures related to their operation processes and their inside and outside interactions and impacts.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.2. Project proposal description

The analytical methods in systems' safety and security modeling, identification, evaluation, improvement and optimization proposed in the project will significantly extend the state of the art in this field by introducing new possibilities of investigation of the complex critical infrastructure networks s related to their inside dependences and outside dependencies and hazards, and in final effect, by the creation of an original and comprehensive theory of safety and security of port and maritime critical infrastructure networks.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.3. Project research team conception

To implement the project successfully and to achieve the results useful for the Baltic Sea region, it is supposed that the project consortium will be composed of the partners, the researchers and practitioners, from all 9 countries of the HELCOM member states (*Figure 2*, Section 1):

Partner 1. The Denmark’s Team;

Partner 2. The Estonia’s Team;

Partner 3. The Finland’s Team;

Partner 4. The Germany’s Team;

Partner 5. The Latvia’s Team;

Partner 6. The Lithuania’s Team;

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.3. Project research team conception

Partner 7. The Poland's Team involved in the project will include the following partners:

- Gdynia Maritime University (GMU),
- Gdynia Naval Academy (GNA),
- Gdańsk University of Technology (GUT),
- Polish Safety and Reliability Association (PSRA), the coordinator of the Poland's Team,
- Maritime Search and Rescue Service (MSRS),
- Rzezów University of Technology (RUT),
- System Research Institute (SRI);

Partner 8. The Russia's Team;

Partner 9. The Sweden's Team.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.4. Partner cooperation added value

The project partners are convinced that the formation of the above is joint Project Research Team will lead to the development of high advanced research with serious impact on the development of the world science and knowledge in the field of safety and security with the wide possibilities of practical applications in the port and maritime sector.

The participants will widely discuss the sensibility and possibility of the creating the competitive international consortium in the field of safety and reliability of port and maritime installations and processes and applying successively for EU grant for this serious and viable project for the Baltic Sea region.

The project will be completed with the results dissemination and exploitation, including workshops, training courses, publications and practical demonstration of results.

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.4. Partner cooperation added value

The main deliverable and impact of the project on the development of science will be the development and ordering safety and security knowledge and creating new coherent theory of critical infrastructure networks' safety and security published in 2 monographs-guidebooks (theoretical added value):

- Theory of safety and security of port and maritime critical infrastructure networks;
- Risk analysis of port and maritime critical infrastructure network accident consequences and improving significantly the safety and security of human overall activity in port and maritime sectors by creating (practical added value):
- The Integrated Critical Infrastructure Safety and Security Management System (ICISSMS);

to be implemented at created:

- The Internet Critical Infrastructure Safety and Security Management Centre (ICISSMC).

3. Safety and security of Baltic Sea area critical infrastructure networks - integrated management system
3.4. Partner cooperation added value

The project ambitious objectives and research activity are strategically very important to collaborating partners from social, economy, environmental and technological dimensions and will have a significant impact on reinforcing their competitiveness and excellence in overall safety and security research activity in general, and particularly in safety and security of port and maritime critical infrastructure networks scientific and technological advances and knowledge.

4. Main steps in project implementation

4.1. The first primary step of project activity

4.2. The second step of project activity

4.3. The third step of project activity

4.4. The fourth step of project activity

4.5. The fifth step of project activity

4.6. The sixth step of project activity

4.7. The seventh final step of project activity

4. Main steps in project implementation
4.1. The first step of project activity

At the primary step of project activity, the analysis of industry installations and other systems placed within the Baltic Sea area, including their current status and prognosis of their future developments will be performed. Moreover, the specification of criteria determining particular installations and systems as critical infrastructures will be done.

After that, 8 Baltic Critical Infrastructure Networks (BCINs) for various existing in the Baltic Sea port and water areas industrial installations will be defined and analyzed. Moreover, an effort will be made in order to create a global network of all considered in this region critical infrastructures in the form of Baltic critical infrastructure network of networks called the Global Baltic Network of Critical Infrastructure Networks (GBNCIN).

4. Main steps in project implementation
4.2. The second step of project activity

The second step in the project research will be focused on the essential developing of tools concerned with modelling, identification and prediction of [34], [48], [70]-[75],[78]-[79]:

- the critical infrastructure operation process (CIOP);

- the weather change process (WCP) at the critical infrastructure operating area;

- the joint critical infrastructure operation and weather change process (CIOWP);

and their adaptations to 8 single Baltic Critical Infrastructure Networks (BSCINs) and to the Global Baltic Network of Critical Infrastructure Networks (GBNCIN).

4. Main steps in project implementation
4.2. The second step of project activity

At this research step, after modelling Critical Infrastructure Operation Process (CIOP) including Operating Environment Threats (OET) and modelling Weather Change Process (WCP) including Extreme Weather Hazards (EWH), the results will be join to construct the Critical Infrastructure Operation Process General Model (CIOPGM) related to Operating Environment Threats (OET) and Extreme Weather Hazards (EWH).

Similarly, after identification methods and procedures of Critical Infrastructure Operation Process (CIOP) including Operating Environment Threats (OET) and identification methods and procedures of Weather Change Process (WCP) including Extreme Weather Hazards (EWH), the results will be considered together in order to create the identification methods and procedures of unknown parameters of Critical Infrastructure Operation Process General Model (CIOPGM) related to Operating Environment Threats (OET) and Extreme Weather Hazards (EWH).

4. Main steps in project implementation
4.2. The second step of project activity

Further, practical applications of the results of the above project activity will be done to modelling the particular BSCINs and the GBNCIN operation processes at the Baltic Sea area using the CIOPGM related to Operating Environment Threats (OET) and Extreme Weather Hazards (EWH) in this region and to evaluation of their unknown parameters.

Moreover, fixing the assets of single BSCINs and GBNCIN and identifying climate related hazards in their operating environment will be done.

4. Main steps in project implementation
4.3. The third step of project activity

This stage of the project activity will be focused on the essential developing of tools concerned with [71]:

- the critical infrastructures safety modelling;
- the critical infrastructures safety prediction;
- the critical infrastructures safety optimization;

and their applications to the single BSCINs and the GBNCIN.

4. Main steps in project implementation
4.3. The third step of project activity

At this stage of research activity, after modelling safety of multistate ageing systems with independent components and modelling safety of multistate ageing systems with dependent components and subsystems, the Integrated Model of Critical Infrastructure Safety (IMCIS) related to its operation process including operating environment threats (with other critical infrastructures influence, without climate-weather change influence) will be designed and the methods and procedures of identification of its unknown parameters will be proposed. Further, the adaptation of Integrated Model of Critical Infrastructure Safety (IMCIS) to critical infrastructure safety prediction will be done and the adaptation of Integrated Model of Critical Infrastructure Safety (IMCIS) to critical infrastructures network safety and “cascading effects” prediction (without climate-weather change influence) will be performed as well.

4. Main steps in project implementation
4.3. The third step of project activity

Practical applications of the results of the above activity will be performed to the particular 8 BSCINs and the GBNCIN (case studies 1-9) safety modelling, identification and prediction (without considering climate-weather change influence).

4. Main steps in project implementation
4.4. The fourth step of project activity

This step in project research will be focused on the essential developing of tools concerned with:

- the critical infrastructure operating environment threats and weather extreme hazards impacts assessment general model;

- the modelling critical infrastructure accident consequences;

and their adaptation to the chemical spill and other dangerous for the environment consequences generated by the accident of the single BSCINs and GBNCIN.

4. Main steps in project implementation
4.4. The fourth step of project activity

At this stage, the impact assessment model will be created starting with the integration of the Integrated Model of Critical Infrastructure Safety (IMCIS) and the Critical Infrastructure Operation Process General Model (CIOPGM) into the General Integrated Model of Critical Infrastructure Safety (GIMCIS) related to operating environment threads (OET) and climate-weather extreme hazards (EWH).

Next, GIMCIS will be adapted to critical infrastructures network safety and "cascading effects" prediction related to climate-weather change influence and applied to the single BSCINs and GBNCIN safety modelling, identification and prediction (case studies 1-9).

4. Main steps in project implementation
4.4. The fourth step of project activity

The modelling critical infrastructure accident consequences will be done through designing the General Model of Critical Infrastructure Accident Consequences (GMCIAC) and the identification of its unknown parameters will be performed. Further, the GMCIAC adaptation to the prediction of critical infrastructure accident consequences will be done and its practical applications will be performed to the chemical spill and other events dangerous events for the environment consequences generated by the accident of one single BSCINs and GBNCIN operating at the Baltic Sea waters (case studies 1-9).

Additionally, at this stage, the inventory report of all impact models will be done:

4. Main steps in project implementation
4.5. The fifth step of project activity

The fifth step in project research will be focused on the essential developing of tools concerned with:

- the critical infrastructure resilience;

- the critical infrastructure business continuity under climate pressures;

- the critical infrastructure cost-effectiveness analysis;

and their adaptation to the single critical BSCINs and the GBNCIN.

4. Main steps in project implementation
4.5. The fifth step of project activity

The procedures of operation and safety optimization of critical infrastructure without and with considering WCP influence will be proposed to its resilience improving respectively by maximizing its lifetime in the set of safety states not worse than a critical safety state. Next, those procedures will be applied to optimization of operation and safety of the BSCINs and the GBNCIN without and with considering WCP influence (case studies 1-9).

Moreover, the method of critical infrastructure accident losses minimizing will be proposed and applied to the optimization BSCINs and the GBNCIN accident consequences.

Additionally, at this stage, the inventory report collecting and analyzing resilience indicators will be done.

4. Main steps in project implementation
4.6. The sixth step of project activity

At this stage of project activity, the research will be focused on practical adaptation and application of the tools developed in the project to the investigation of the hard meteorological conditions in Baltic Sea port influence on the BSCINs and the GBNCIN.

The results of earlier performed approaches to case studies 1-9 will be developed and applied to their final conduction and presentation to the invited stakeholders and critical infrastructure networks' administrative bodies during one-week seminar-meeting. The results of the following tools application to the BSCINs and the GBNCIN will be presented to the seminar audience for examination and evaluation:

4. Main steps in project implementation
4.6. The sixth step of project activity

-the Critical Infrastructure Operation Process General Model (CIOPGM) related to Operating Environment Threats (OET) and Extreme Weather Hazards (EWH) in this region;

- the methods of evaluation of unknown parameters of a port oil piping transportation system operation process related to Operating Environment Threats (OET) and Extreme Weather Hazards (EWH);

- the methods of identification of climate related hazards at the Baltic Sea area and their critical/extreme event parameters' exposure for port oil piping transportation critical infrastructure;
- the General Integrated Model of Critical Infrastructure Safety (GIMCIS);

- the methods of optimization of operation and safety without and with considering WCP influence through maximizing the lifetime in the set of safety states not worse than a critical safety state;

4. Main steps in project implementation
4.6. The sixth step of project activity

- the methods of optimization of operation and safety without and with considering WCP influence through minimizing the operation cost;

- the methods of optimization of operation and safety without and with considering WCP influence through maximizing lifetime in the set of safety states not worse than a critical safety state and minimizing operation cost;

- the inventory and comparison of the results concerned with safety;
- the new strategy assuring high safety and resilience;

- the General Model of Critical Infrastructure Accident Consequences (GMCIAC) to the chemical spill consequences generated by the accident;

- the methods of optimization of accident consequences through losses minimizing;
- the inventory and comparison of the results concerned with accident consequences;

4. Main steps in project implementation
4.6. The sixth step of project activity

- the new strategy assuring low consequences of accident concerned with chemical spills and other dangerous events;

- the new general strategy assuring high safety and resilience of critical infrastructure - operation process and safety parameters of critical infrastructure components/assets modification related to maximizing its safety characteristics and minimizing its operation cost;

- the new strategy assuring low consequences of critical infrastructure accident – initiating events, environment threats and environment degradation processes modification related to minimizing critical infrastructure accident consequences.

4. Main steps in project implementation
4.7. The seventh final step of project activity

The final step of the project research activity will be completed with the reports on the project dissemination, communication and exploitation including workshops, training courses and publications.

4. Main steps in project implementation
4.7. The seventh final step of project activity

The main deliverable and impact of the project on the development of science will be the development and ordering safety and security knowledge and creating new coherent theory of critical infrastructure networks' safety and security published in 2 monographs-guidebooks (theoretical added value):

- Theory of safety and security of port and maritime critical infrastructure networks;
- Risk analysis of port and maritime critical infrastructure network accident consequences:

and improving significantly the safety and security of human overall activity in port and maritime sectors by creating (practical added value):

- The Integrated Critical Infrastructure Safety and Security Management System (ICISSMS);

placed at new created:

- The Internet Critical Infrastructure Safety and Security Management Centre (ICISSMC).

REFERENCES

Details are given in Journal of Polish Safety and Reliability Association – JPSRA, Special Issue on HAZARD Project, Volume 10, No 1, April 2019