Journal of Polish Safety and Reliability Association
Summer Safety and Reliability Seminars, Volume 7, Number 3, 2016

Guze Sambor

Kołowrocki Krzysztof
Maritime University, Gdynia, Poland

An approach to Baltic Port, Shipping, Ship Traffic and Operation Information Critical Infrastructure Network operation process

Keywords

shipping, ship traffic, port operation, information systems, operation process, parameters

Abstract

The goal of the article is to analysis of static and dynamic industry installations existing in the Baltic Sea Region performed to classify them as a network of networks. As the result of this analysis, the Baltic Port, Shipping, Ship Traffic and Port Operations Information Critical Infrastructure Network composed of three single critical infrastructure networks are distinguished. In the next step, the operation process for every installations and finally for network of networks are defined.

1. Introduction

To describe the critical infrastructure installations in Southern Baltic Sea Region, we have to use the definitions of selected basic notions concerned with critical infrastructures and climate and weather impacts on their safety included in the report [5].

All of these should be considered as 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.

In this definition of a system, the product or the process are not only important but also the influences that the surrounding environment (including human interactions) may have on the product's or process's safety performance.

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, for instance: another ship activity in the ship operating environment that can result in an accident with serious consequences for the ship and its operating environment, terrorist attack changing the system operation process in an unsafe way.

The system inside dependencies are dependencies within a system itself i.e. relationship between components and subsystems in a system causing state changes of other components and subsystems and in a consequence resulting in changes of the system state.

The system outside dependencies are dependencies coming from the system operating environment (external factors), including changes of the system state caused by outside this system conditions e.g. climate changes, changes of its functionality, location, other objects, government and human decisions (regulations, economic, public policy).

In the next step, 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.

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 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.

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 dependant relationships between themselves interacting at various levels of their complexity.

The critical infrastructure accident is an event that causes changing the critical infrastructure safety state into the safety state worse than the critical safety state that is dangerous for the critical infrastructure itself and its operating environment.

The critical infrastructure network cascading effects are called degrading effects occurring within a critical infrastructure and between critical infrastructures in their operating environment, including situations in which one critical infrastructure causes degradation of another ones, which again causes additional degradation in other critical infrastructures and in their operating environment.

The critical infrastructure threat is the occurrence of an unwanted circumstance or event, that may cause damage, functioning disruption or service interruption to critical infrastructures.

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

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

The critical infrastructure vulnerability is the critical infrastructure feature that makes it easily influenced by some external threat and hazards coming from its operating environment.

The critical infrastructure exposure is the fact or the condition of being exposed to something (of being subjected to an action or an influence), for instance being exposed to severe weather.

According to the fact that the maritime sector sustains society and the economy through the movement of people and vital goods, such as food and energy (transportation of oil and gas), the maritime sector is considered as critical infrastructure [6]. In the current approach, the ports with supported infrastructure (roads, railways, piers, breakwaters, power lines, ICT networks, etc.) are considered as the maritime critical infrastructure [23]. The aspects of maritime critical infrastructures protection take into account only the ensuring the security and defence of ports. However, this concept should be completed by other supported infrastructures like ships, a coastal radar system, a vessel traffic services (VTS) system and an automated identification system. Thus, it is possible to define [5]:

- maritime transportation network – based on the ports and supported infrastructure;
- maritime information network, i.e. the ship traffic and operation information network (*Figure* 1).

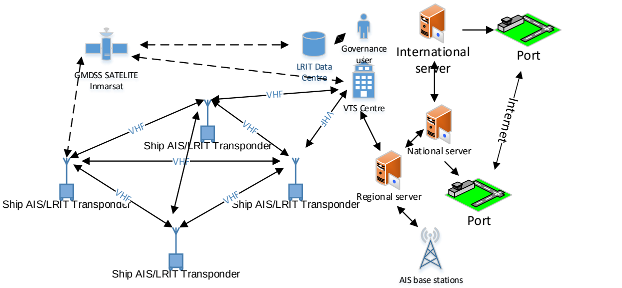

Figure 1. The schema of the ship traffic and port operation information network [5]

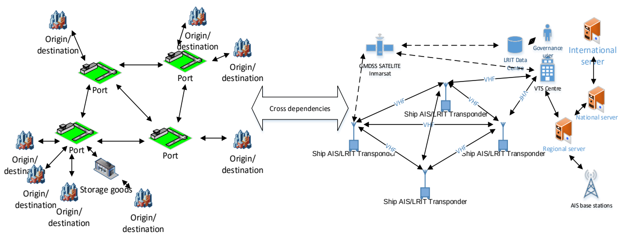

Figure 2. The schema of the maritime transportation and information network [5]

All of these elements should be also recognized as the critical infrastructure networks. It is clear that there are inner and outer dependencies between the ports, ships and ship traffic and operation information networks. This approach allows to define the maritime transportation and information critical infrastructure network (*Figure 2*).
All of these facilities are exposed to various unfavourable factors, including environmental and climatic conditions.

2. Port, Shipping, Ship Traffic and Port Operation Information System

There are the following 8 main critical infrastructure networks operating in the Baltic Sea 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 port operation information critical infrastructure network.

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.

2.1. Baltic Port Critical Infrastructure Network

In the report [5], the Baltic Port Critical Infrastructure Network (BPCIN) is defined and composed of 18 following core ports placed at the Baltic seaside:
1. The Port of Aarhus (P_1);
2. The Copenhagen – Malmö Port (P_2);
3. The Lübecker Hafen-Gesellschaft (P_3);
4. The Port of Rostock (P_4);
5. The Port of Tallinn (P_5);
6. The Freeport of Riga (P_6);
7. The Freeport of Ventspils (P_7);
8. The Klaipeda State Seaport (P_8);
9. The Port of Gdańsk (P_9);
10. The Port of Gdynia (P_{10});
11. The Szczecin-Swinoujście Port (P_{11});
12. The Port of Helsinki (P_{12});
13. The Port of Turku (P_{13});
14. The Port of Hamina-Kotka(P_{14});
15. The Port of Gothenburg (P_{15});
16. The Port of Luleå (P_{16});
17. The Port of Stockholm (P_{17});
18. The Port of Trelleborg (P_{18}).

The detailed description is presented in paper [1] and [6].

2.2. Baltic Shipping Critical Infrastructure Networks

The set of ships operating at the Baltic Sea waters at the fixed moment of time (or at the fixed time interval) is called the dynamic Baltic Shipping Critical Infrastructure Network (BSCIN). The influence of climate change on the BSCIN its safety is crucial. This is described in details in paper [2] and [6].

2.3. Baltic Ship Traffic and Port Operation Information Critical Infrastructure Network

We define the Baltic Ship Traffic and Port Operation Information Critical Infrastructure Network (BSTPOICIN) composed of 121 AIS base stations and 25 DGPS stations listed below (*Figures 3* and *4*):
1. Traffic and port operation information system 1 - AIS Szczecin ($TPOIS_1$), Poland,
2. Traffic and port operation information system 2 - AIS Police ($TPOIS_2$), Poland,
3. Traffic and port operation information system 3 - AIS Swinoujscie ($TPOIS_3$), Poland,
4. Traffic and port operation information system 4 - AIS Kikut ($TPOIS_4$), Poland,
5. Traffic and port operation information system 5 - AIS Niechorze ($TPOIS_5$), Poland,
6. Traffic and port operation information system 6 - AIS Gaski ($TPOIS_6$), Poland,
7. Traffic and port operation information system 7 - AIS Jarosławiec ($TPOIS_7$), Poland,
8. Traffic and port operation information system 8 - AIS Czolpino ($TPOIS_8$), Poland,
9. Traffic and port operation information system 9 - AIS Rozewie ($TPOIS_9$), Poland,
10. Traffic and port operation information system 10 - AIS Hel ($TPOIS_{10}$), Poland,
11. Traffic and port operation information system 11 - AIS Krynica Morska ($TPOIS_{11}$), Poland,
12. Traffic and port operation information system 12 - AIS Baltiysk ($TPOIS_{12}$), Russia,
13. Traffic and port operation information system 13 - AIS Iantarniy (Amber) ($TPOIS_{13}$), Russia,
14. Traffic and port operation information system 14 - AIS Klaipeda ($TPOIS_{14}$), Lithuania,
15. Traffic and port operation information system 15 - AIS Liepaja Port ($TPOIS_{15}$), Latvia,
16. Traffic and port operation information system 16 - AIS Riga ($TPOIS_{16}$), Latvia,
17. Traffic and port operation information system 17 - AIS Saulkrasti ($TPOIS_{17}$), Latvia,
18. – 22. Traffic and port operation information systems 18 – 22 - Five AIS base stations in Estonia: $TPOIS_{18}$ - $TPOIS_{22}$,

23. – 31. Traffic and port operation information systems 23 – 31 - Nine AIS base stations in Russia: $TPOIS_{23}$ - $TPOIS_{31}$,
32. – 59. Traffic and port operation information systems 32 - 59 - Twenty-eight AIS base stations in Finland: $TPOIS_{32}$ - $TPOIS_{59}$,
60. – 96. Traffic and port operation information systems 60 – 96 - Thirty-seven AIS base stations in Sweden: $TPOIS_{60}$ - $TPOIS_{96}$,
97. – 109. Traffic and port operation information systems 97 - 109 - Thirteen AIS base stations in Denmark: $TPOIS_{97}$ - $TPOIS_{109}$,
110. – 121. Traffic and port operation information systems 110 - 121 - Twelve AIS base stations in Germany: $TPOIS_{110}$ - $TPOIS_{121}$,
122. Traffic and port operation information system 122 - DGPS base station in Dziwnow ($TPOIS_{122}$), Poland,
123. Traffic and port operation information system 123 – DGPS base station in Rozewie ($TPOIS_{123}$), Poland,
124. Traffic and port operation information system 124 – DGPS base station in Baltiysk ($TPOIS_{124}$), Russia,
125. Traffic and port operation information system 125 – DGPS base station in Kleipada ($TPOIS_{125}$), Lithuania,
126. Traffic and port operation information system 126 – DGPS base station in Ventospills ($TPOIS_{126}$), Latvia,
127. Traffic and port operation information system 127 – DGPS base station in Ristna ($TPOIS_{127}$), Estonia,
128. Traffic and port operation information system 128 – DGPS base station in Narva ($TPOIS_{128}$), Estonia,
129. Traffic and port operation information system 129 – DGPS base station in Shepelevskiy ($TPOIS_{129}$), Russia,
130. Traffic and port operation information system 130 – DGPS base station in Klamila ($TPOIS_{130}$), Russia,
131. Traffic and port operation information system 131 – DGPS base station in Porkkala ($TPOIS_{131}$), Finland,
132. Traffic and port operation information system 132 – DGPS base station in Turku ($TPOIS_{132}$), Finland,
133. Traffic and port operation information system 133 – DGPS base station in Mantyluoto ($TPOIS_{133}$), Finland,
134. Traffic and port operation information system 134 – DGPS base station in Marjaniemi ($TPOIS_{134}$), Finland,
135. Traffic and port operation information system 135 – DGPS base station in Bjuroklubb ($TPOIS_{135}$), Sweden,
136. Traffic and port operation information system 136 – DGPS base station in Jarnas ($TPOIS_{136}$), Sweden,
137. Traffic and port operation information system 137 – DGPS base station in Skutskar ($TPOIS_{137}$), Sweden,
138. Traffic and port operation information system 138 – DGPS base station in Hjortonsudde ($TPOIS_{138}$), Sweden,
139. Traffic and port operation information system 139 – DGPS base station in Nynashamn ($TPOIS_{139}$), Sweden,
140. Traffic and port operation information system 140 – DGPS base station in Hoburg ($TPOIS_{140}$), Sweden,
141. Traffic and port operation information system 141 – DGPS base station in Holmsjo ($TPOIS_{141}$), Sweden,
142. Traffic and port operation information system 142 – DGPS base station in Kullen ($TPOIS_{142}$), Sweden,
143. Traffic and port operation information system 143 – DGPS base station in Gotheborg ($TPOIS_{143}$), Sweden,
144. Traffic and port operation information system 144 – DGPS base station in Skagen ($TPOIS_{144}$), Denmark,
145. Traffic and port operation information system 145 – DGPS base station in Blavandshuk ($TPOIS_{145}$), Denmark,
146. Traffic and port operation information system 146 – DGPS base station in Wustrow ($TPOIS_{146}$), Germany.

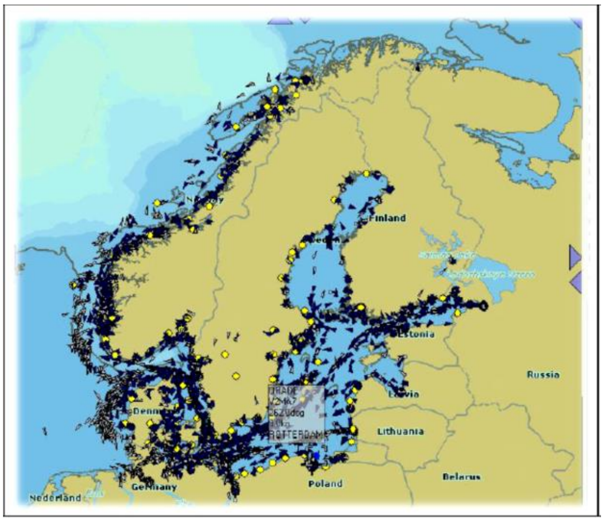

Figure 3. The map of Baltic Sea Region area – the yellow points represent the AIS base stations [3]

The distribution of AIS base station is presented in *Figure 3*. Besides, the Baltic Marine DGPS network is presented in *Figure 4*.

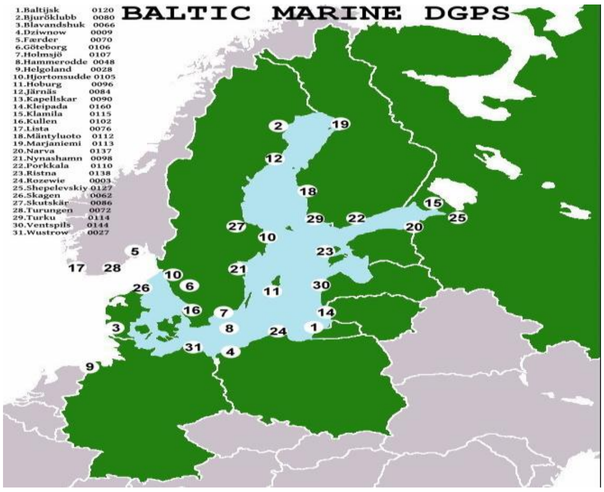

Figure 4. Baltic Marine DGPS Stations

The detailed information about this critical infrastructure network is presented in [6] and [12].

2.4. Baltic Port, Shipping, Ship Traffic and Port Operation Information Critical Infrastructure Networks

In this report we consider the network composed of the following three critical infrastructure networks which operates in Baltic Sea Region area:

- $CIN^{(1)}$ - the Baltic Port Critical Infrastructure Network (BPCIN),
- $CIN^{(2)}$ - the Baltic Shipping Critical Infrastructure Network (BSCIN),
- $CIN^{(3)}$ - the Baltic Ship Traffic and Port Operation Information Critical Infrastructure Network (BSTPOICIN).

This network of networks is characterized by strong interacting and interconnections These three critical infrastructure networks have to be consider commonly and they are called the Baltic Port, Shipping, Ship Traffic and Port Operation Information Critical Infrastructure Network (BPSSTPOICIN). Every of them has strong influence on the another. They constitute the complex network with strong inner and outer dependencies. Moreover, we suppose that the operation processes of these critical infrastructure networks have an influence on their safety and depend on their operating area within the Baltic Sea Region.

3. Port, Shipping, Ship Traffic and Port Operation Information Network operation process

We can divide the Baltic Sea area D into a grid of renctagles D_{ab}, i.e. $D=\bigcup_{a=1}^{m}\bigcup_{b=1}^{n} D_{ab}$, where $a=1,2,...,m,$ $b=1,2,...,n,$ $m,n\in N$. The grid dimension ($m\times n$) depends on the assumed accurancy of geographical coordinates (see *Figure* 5).

Figure 5. An exemplary grid of the Baltic Sea region according to the geographical coordinates

We assume that the critical infrastructure networks $CIN^{(i)}, i=1,2,3$ during its operation process are taking numbers of different operation states, described in Sections 3.1 – 3.3.

3.1. Operation Process of Port Critical Infrastructure Network

We assume that the critical infrastructure network $CIN^{(1)}$ during its operation process are taking numbers of different operation states defined as follows.

$$[Z^{(2)}]_{1\times\nu^{(2)}} = [z_1^{(2)},\ z_2^{(2)},\ \ldots,\ z_{\nu^{(2)}}^{(2)}], \qquad (1)$$

where $z_a^{(2)}$ are the numbers of ships in the port P_a, $a=1,2,...,\nu^{(2)}$, $\nu^{(2)}\in N$, is the number of ports under the consideration in the the Baltic Sea Region D
($\nu^{(2)}=18$ for whole Baltic Sea Region).

Further, we define the critical infrastructure networks $CIN^{(i)}, i = 1,2,3$, operation processes $Z^{(i)}(t)$, $t \in < 0, +\infty)$, as follows:

$$Z^{(2)}(t) = [Z^{(2)}(t)]_{1\times\nu^{(2)}} = [z_1^{(2)}(t), z_2^{(2)}(t), ..., z_{\nu^{(2)}}^{(2)}(t)]. \qquad (2)$$

with discrete operation states from the set defined by (1), where the operation subprocesses $z_a^{(2)}(t)$ assume the values equal to the numbers $z_a^{(2)}$ of ships in the ports P_a, $a = 1,2,...,\nu^{(2)}$, at the moment $t \in < 0, +\infty)$;
In detailed definitions of the states and the operation process $Z^{(2)}(t)$ of the Baltic Port Critical Infrastructure Network $CIN^{(2)}$, consisted of all ports with their facilities, where the operation states are defined by the numbers of vessels in ports P_a, $a = 1,2,...,\nu^{(2)}$, either waiting for port services or being under port services, the impacts of those numbes of ships and their port operations interactions should be include.
Taking into account the above assumption to describe the operation process of the port critical infrastructure network we consider the $n^p = 18$ main Southern Baltic Sea ports. In the port we consider the number of ships:

- entering to the port,
- outgoing into the port,
- waiting,
- handled (loaded/unloaded).

According to (1) – (2), we assume that the operation process for a single port P_a, $a = 1,2,...,18$, is given by the following vector with dimension 4:

$$[Z^{(2)}(t)]_{1\times 4} = [z_1^{(2)}(t), z_2^{(2)}(t), z_3^{(2)}(t), z_4^{(2)}(t)]$$
$$= [n_1^{(2)}(t), n_2^{(2)}(t), n_3^{(2)}(t), n_4^{(2)}(t)], \qquad (3)$$

where
$n_1^{(2)}(t)$ - number of the entering ships in the port P_a, $a = 1,2,...,18$, at the moment $t \in < 0, +\infty)$,
$n_2^{(2)}(t)$ - number of the outgoing ships in the port P_a, $a = 1,2,...,18$, at the moment $t \in < 0, +\infty)$,
$n_3^{(2)}(t)$ - number of the waiting ships in the port P_a, $a = 1,2,...,18$, at the moment $t \in < 0, +\infty)$,
$n_4^{(2)}(t)$ - number of the handled(loaded/unloaded) ships in the port P_a, $a = 1,2,...,18$, at the moment $t \in < 0, +\infty)$.

Thus, the operation states are defined as follows:

$z_0^{(2)} = [0,0,0,0]$, $z_1^{(2)} = [1,0,0,0]$, ..., $z_{n_1}^{(2)} = [n_1,0,0,0]$,
$z_{n_1+1}^{(2)} = [0,1,0,0]$, $z_{n_1+2}^{(2)} = [0,2,0,0]$,...,
$z_{n_1+n_2}^{(2)} = [0,n_2,0,0]$,..., $z_{n_1 n_2}^{(2)} = [n_1,n_2,0,0]$,
$z_{n_1 n_2+1}^{(2)} = [0,0,1,0]$, $z_{n_1 n_2+2}^{(2)} = [0,0,2,0]$,...,
$z_{n_1 n_2+n_3}^{(2)} = [0,0,n_3,0]$, ..., $z_{n_1\cdot n_2\cdot n_3}^{(2)} = [n_1,n_2,n_3,0]$,
$z_{n_1\cdot n_2\cdot n_3+1}^{(2)} = [0,0,0,1]$, $z_{n_1\cdot n_2\cdot n_3+2}^{(2)} = [0,0,0,2]$,
$z_{n_1\cdot n_2\cdot n_3+n_4}^{(2)} = [0,0,0,n_4]$, ..., $z_{n_1\cdot n_2\cdot n_3\cdot n_4}^{(2)} = [n_1,n_2,n_3,n_4]$.

It means, we consider the $n_1 \cdot n_2 \cdot n_3 \cdot n_4$ operation states for every ports P_a, $a = 1,2,...,18$.

3.2. Operation Process of Shipping Critical Infrastructure Network

The network $CIN^{(2)}$ during its operation process are taking numbers of different operation states defined as follows

$$[Z^{(1)}]_{m\times n} = \begin{bmatrix} z_{11}^{(1)} & z_{12}^{(1)} & \cdots & z_{1n}^{(1)} \\ z_{21}^{(1)} & z_{22}^{(1)} & \cdots & z_{2n}^{(1)} \\ \cdots & & & \\ z_{m1}^{(1)} & z_{m2}^{(1)} & \cdots & z_{mn}^{(1)} \end{bmatrix}, \qquad (4)$$

where $z_{ab}^{(1)}$ are the numbers of ships in the regions D_{ab}, $a = 1,2,...,m$, $b = 1,2,...,n$, $m,n \in N$.
Further, we define the critical infrastructure networks $CIN^{(i)}, i = 1,2,3$, operation processes $Z^{(i)}(t)$, $t \in < 0, +\infty)$, as follows:

$$Z^{(1)}(t) = [Z^{(1)}(t)]_{m\times n} = \begin{bmatrix} z_{11}^{(1)}(t) & z_{12}^{(1)}(t) & \cdots & z_{1n}^{(1)}(t) \\ z_{21}^{(1)}(t) & z_{22}^{(1)}(t) & \cdots & z_{2n}^{(1)}(t) \\ \cdots & & & \\ z_{m1}^{(1)}(t) & z_{m2}^{(1)}(t) & \cdots & z_{mn}^{(1)}(t) \end{bmatrix}, \qquad (5)$$

with discrete operation states from the set defined by (4) where the operation subprocesses $z_{ab}^{(1)}(t)$ is assumed as equal to the numbers $z_{ab}^{(1)}$ of ships in the rectangles D_{ab} $a = 1,2,...,m$, $b = 1,2,...,n$, $m,n \in N$, at the moment $t \in < 0, +\infty)$.
Considering interactions between ships creating the Baltic Shipping Critical Infrastructure Network $CIN^{(1)}$, we assume that there are strong inner and

outer dependecies between the ships operating in a single fixed rectangle D_{ab}, $a=1,2,...,m,$ $b=1,2,...,n,$ $m,n \in N$, and that ships in each two adjacent rectangles influence each other as well. These influences that should be included in detailed definitions of this network operation process $Z^{(1)}(t)$ and its states strongly depend on the operation states of this network defined by the numbers of ships in these rectangles and those ships technical operations. To describe the operation process of the shipping critical infrastructure network we divide the Southern Baltic Sea area on the square matrix with dimension *m=5, n=14.* (see *Figure* 6).

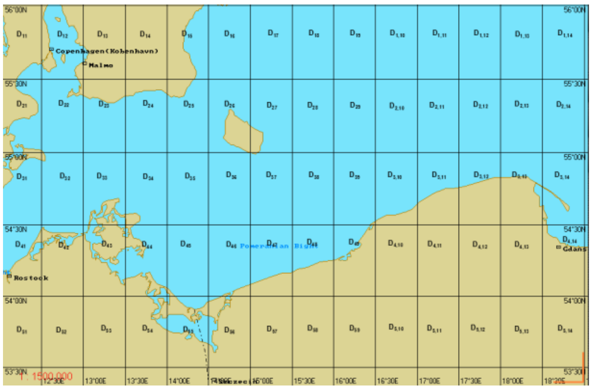

Figure 6. The division of the Southern Baltic Sea region according to the geographical coordinates

Further, we assume that the operation process is given by the rectangular matrix with accordance to (4) – (5)

$$[Z^{(1)}(t)]_{5\times 14} = \begin{bmatrix} z_{11}^{(1)}(t) & z_{12}^{(1)}(t) & \cdots & z_{1,14}^{(1)}(t) \\ z_{21}^{(1)}(t) & z_{22}^{(1)}(t) & \cdots & z_{2,14}^{(1)}(t) \\ \cdots & & & \\ z_{51}^{(1)}(t) & z_{52}^{(1)}(t) & \cdots & z_{5,14}^{(1)}(t) \end{bmatrix}, \qquad (6)$$

where the operation subprocesses $z_{ab}^{(1)}(t)$ is assumed as equal to the numbers $z_{ab}^{(1)}$ of ships in the rectangles D_{ab} $a=1,2,...,5,$ $b=1,2,...,14,$ at the moment $t \in <0,+\infty)$.

The operation states are defined as follows:

$$[z_0^{(1)}]_{5\times 14} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix},...,$$

$$[z_{n_{11}^{(1)}}^{(1)}]_{5\times 14} = \begin{bmatrix} n_{11}^{(1)} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix},...,$$

$$[z_{n_{11}^{(1)}+1}^{(1)}]_{5\times 14} = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix}, ...,$$

$$[z_{n_{11}^{(1)}+n_{12}^{(1)}}^{(1)}]_{5\times 14} = \begin{bmatrix} 0 & n_{12}^{(1)} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix},...,$$

$$[z_{n_{11}^{(1)}+n_{12}^{(1)}+...+n_{1,13}^{(1)}+1}^{(1)}]_{5\times 14} = \begin{bmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix}, ...,$$

$$[z_{n_{11}^{(1)}+n_{12}^{(1)}+n_{13}^{(1)}+...+n_{1,14}^{(1)}}^{(1)}]_{5\times 14} = \begin{bmatrix} 0 & 0 & \cdots & n_{1,14}^{(1)} \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix},...,$$

$$[z_{n_{11}^{(1)}\cdot n_{12}^{(1)}\cdot n_{13}^{(1)}\cdot...\cdot n_{1,14}^{(1)}}^{(1)}]_{5\times 14} = \begin{bmatrix} n_{11}^{(1)} & n_{12}^{(1)} & \cdots & n_{1,14}^{(1)} \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix}, ...,$$

$$[z_{n_{11}^{(1)}\cdot n_{12}^{(1)}\cdot n_{13}^{(1)}\cdot...\cdot n_{1,14}^{(1)}+1}^{(1)}]_{5\times 14} = \begin{bmatrix} n_{11}^{(1)} & n_{12}^{(1)} & \cdots & n_{1,14}^{(1)} \\ 1 & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix},...,$$

$$[z_{n_{11}^{(1)}\cdot n_{12}^{(1)}\cdot n_{13}^{(1)}\cdot...\cdot n_{1,14}^{(1)}+n_{21}^{(1)}}^{(1)}]_{5\times 14} = \begin{bmatrix} n_{11}^{(1)} & n_{12}^{(1)} & \cdots & n_{1,14}^{(1)} \\ n_{21}^{(1)} & 0 & \cdots & 0 \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix}, ...,$$

$$[z_{n_{11}^{(1)}\cdot...\cdot n_{1,14}^{(1)}\cdot n_{21}^{(1)}\cdot...\cdot n_{2,14}^{(1)}}^{(1)}]_{5\times 14} = \begin{bmatrix} n_{11}^{(1)} & n_{12}^{(1)} & \cdots & n_{1,14}^{(1)} \\ n_{21}^{(1)} & n_{22}^{(1)} & \cdots & n_{2,14}^{(1)} \\ \cdots & & & \\ 0 & 0 & \cdots & 0 \end{bmatrix},...,$$

$$[z_{n_{11}^{(1)}\cdot...\cdot n_{1,14}^{(1)}\cdot n_{21}^{(1)}\cdot...\cdot n_{2,14}^{(1)}\cdot n_{31}^{(1)}\cdot...\cdot n_{3,14}^{(1)}\cdot n_{41}^{(1)}\cdot...\cdot n_{4,14}^{(1)}\cdot n_{51}^{(1)}\cdot...\cdot n_{5,14}^{(1)}}^{(1)}]_{5\times 14} =$$

$$= \begin{bmatrix} n_{11}^{(1)} & n_{12}^{(1)} & \cdots & n_{1,14}^{(1)} \\ n_{21}^{(1)} & n_{22}^{(1)} & \cdots & n_{2,14}^{(1)} \\ \cdots & & & \\ n_{51}^{(1)} & n_{52}^{(1)} & \cdots & n_{5,14}^{(1)} \end{bmatrix}.$$

Thus, we consider the $n_{11}^{(1)} \cdot \ldots \cdot n_{1,14}^{(1)} \cdot n_{21}^{(1)} \cdot \ldots \cdot n_{2,14}^{(1)} \cdot n_{31}^{(1)} \cdot \ldots \cdot n_{3,14}^{(1)} \cdot n_{41}^{(1)} \cdot \ldots \cdot n_{4,14}^{(1)} \cdot n_{51}^{(1)} \cdot \ldots \cdot n_{5,14}^{(1)}$ operation states.

3.3. Operation Process of Ship Traffic and Port Operation Information Critical Infrastructure Network

We assume that the critical infrastructure network $CIN^{(3)}$ during its operation states process are taking numbers of different operation states defined as follows.

$$[Z^{(3)}]_{1\times\nu^{(3)}} = [z_1^{(3)},\ z_2^{(3)},\ \ldots,\ z_{\nu^{(3)}}^{(3)}], \tag{7}$$

where $z_a^{(3)}$ are the numbers of ships in the range of the information systems I_a, $a = 1,2,\ldots,\nu^{(3)}$, $\nu^{(3)} \in N$, is the number of information systems under the consideration in the the Baltic Sea Region D (for general case $\nu^{(3)} = 146$).

Further, we define the critical infrastructure networks $CIN^{(i)}, i = 1,2,3$, operation processes $Z^{(i)}(t)$, $t \in <0,+\infty)$, as follows:

$$Z^{(3)}(t) = [Z^{(3)}(t)]_{1\times\nu^{(3)}} = [z_1^{(3)}(t), z_2^{(3)}(t),\ldots, z_{\nu^{(3)}}^{(3)}(t)] \tag{8}$$

with discrete operation states from the set defined by (7), where the operation subprocesses $z_a^{(3)}(t)$ assume the values equal to the numbers $z_a^{(3)}$ of ships in the range of the information systems I_a, $a = 1,2,\ldots,\nu^{(3)}$, at the moment $t \in <0,+\infty)$.

The Shipping, Ship Traffic and Operation Information Critical Infrastructure Network $CIN^{(3)}$ is a platform to exchange the information about ships' operations and and thei cargo. Due to the fact that all informations are given mainly in electronic form, this network is very sensitive for any disruption, especially cyber attacs, but also for natural hazards. Thus, in detailed defining this network operation process and its states those features should be taken into account.

According to Section 2.3 and formulae (7) – (8), the operation process of BSTPOICIN is given by the vector

$$[Z^{(3)}(t)]_{1x146} = [z_1^{(3)}(t), z_2^{(3)}(t),\ldots,z_{146}^{(3)}(t)], \tag{9}$$

where the operation subprocesses $z_a^{(3)}(t)$ assume the values equal to the numbers $z_a^{(3)}$ of ships in the range of the information systems $TPOIS_a$, $a = 1,2,\ldots,146$, at the moment $t \in <0,+\infty)$.

The following operation states are defined:

$$z_0^{(2)} = [0,0,0,\ldots,0],\ z_1^{(2)} = [1,0,0,\ldots,0],\ \ldots,$$
$$z_{n_1}^{(2)} = [n_1,0,0,\ldots,0],\ z_{n_1+1}^{(2)} = [0,1,0,\ldots,0],$$
$$z_{n_1+2}^{(2)} = [0,2,0,\ldots,0],\ \ldots,\ z_{n_1+n_2}^{(2)} = [0,n_2,0,\ldots,0],$$
$$z_{n_1+n_2+1}^{(2)} = [0,0,1,\ldots,0],\ z_{n_1+n_2+2}^{(2)} = [0,0,2,\ldots,0],\ \ldots,$$
$$z_{n_1+n_2+n_3}^{(2)} = [0,0,n_3,\ldots,0],\ \ldots,\ z_{n_1+\ldots+n_{146}}^{(2)} = [0,0,0,\ldots,n_{146}],$$
$$z_{n_1+\ldots+n_{146}+1}^{(2)} = [1,1,\ldots,0],\ z_{n_1+\ldots+n_{146}+2}^{(2)} = [1,2,\ldots,0],\ \ldots,$$
$$z_{n_1+2n_2+\ldots+146}^{(2)} = [1,n_2,\ldots,0],\ \ldots,\ z_{n_1n_2}^{(2)} = [n_1,n_2,\ldots,0],\ \ldots,$$
$$z_{n_1\cdot n_2\cdot n_3\cdot n_4}^{(2)} = [n_1,n_2,\ldots,n_{146}].$$

It means, we consider the $n_1 \cdot n_2 \cdot \ldots \cdot n_{146}$ operation states for Baltic Ship Traffic and Port Operation Information Critical Infrastructure Network.

3.4. Operation Process of the BPSSTPOICIN

Moreover, we assume that the critical infrastructure operation processes $Z^{(i)}(t)$, $i = 1,2,3$, is a semi-Markov process [9], [18] - [21] with the conditional sojourn times $\theta_{bl}^{(i)}$ at the operation states $z_b^{(i)}$ when its next operation state is $z_l^{(i)}$, $b,l = 1,2,\ldots,\nu^{(i)}$, $i = 1,2,3,$ $b \neq l.$ Under these assumptions, the critical infrastructure network operation process may be described by:

- the vector of the initial probabilities $p_b^{(i)}(0) = P(Z^{(i)}(0) = z_b^{(i)})$, $b = 1,2,\ldots,\nu^{(i)}$, $i = 1,2,3$, of the critical infrastructure networks $CIN^{(i)}, i = 1,2,.3$ operation processes $Z^{(i)}(t)$ staying at particular operation states at the moment $t = 0$

$$[p_b^{(i)}(0)]_{1x\nu^{(i)}} = [p_1^{(i)}(0), p_2^{(i)}(0),\ldots, p_{\nu^{(i)}}^{(i)}(0)], \tag{10}$$

- the matrix of probabilities $p_{bl}^{(i)}$, $b,l = 1,2,\ldots,\nu^{(i)}$, $b \neq l$, $i = 1,2,3$, of the critical infrastructure networks $CIN^{(i)}, i = 1,2,.3$, operation processes $Z^{(i)}(t)$ transitions between the operation states $z_b^{(i)}$ and $z_l^{(i)}$

$$[p_{bl}^{(i)}(t)]_{\nu^{(i)}\times\nu^{(i)}} = \begin{bmatrix} p_{11}^{(i)}(t) & p_{12}^{(i)}(t) & \cdots & p_{1\nu^{(i)}}^{(i)}(t) \\ p_{21}^{(i)}(t) & p_{22}^{(i)}(t) & \cdots & p_{2\nu^{(i)}}^{(i)}(t) \\ \cdots & & & \\ p_{\nu^{(i)}1}^{(i)}(t) & p_{\nu^{(i)}2}^{(i)}(t) & \cdots & p_{\nu^{(i)}\nu^{(i)}}^{(i)}(t) \end{bmatrix}, \quad (11)$$

where by formal agreement

$$p_{bb}{}^{(i)} = 0 \text{ for } b = 1,2,\ldots,\nu^{(i)};$$

- the matrix of conditional distribution functions $H_{bl}^{(i)}(t) = P(\theta_{bl}^{(i)} < t)$, $b, l = 1,2,\ldots,\nu^{(i)}$, $b \neq l$, $i = 1,2,3$, of the critical infrastructure networks $CIN^{(i)}, i = 1,2,.3$, operation processes $Z^{(i)}(t)$ conditional sojourn times $\theta_{bl}{}^{(i)}$ at the operation states

$$[H_{bl}^{(i)}(t)]_{\nu^{(i)}\times\nu^{(i)}} = \begin{bmatrix} H_{11}^{(i)}(t) & H_{12}^{(i)}(t) & \cdots & H_{1\nu^{(i)}}^{(i)}(t) \\ H_{21}^{(i)}(t) & H_{22}^{(i)}(t) & \cdots & H_{2\nu^{(i)}}^{(i)}(t) \\ \cdots & & & \\ H_{\nu^{(i)}1}^{(i)}(t) & H_{\nu^{(i)}2}^{(i)}(t) & \cdots & H_{\nu^{(i)}\nu^{(i)}}^{(i)}(t) \end{bmatrix}, \quad (12)$$

where by formal agreement

$$H_{bb}{}^{(i)}(t) = 0 \text{ for } b = 1,2,\ldots,\nu^{(i)};$$

We introduce the matrix of the conditional density functions of the critical infrastructure networks $CIN^{(i)}, i = 1,2,3$, operation processes $Z^{(i)}(t)$ conditional sojourn times θ_{bl} at the operation states corresponding to the conditional distribution functions $H_{bl}{}^{(i)}(t)$

$$[h_{bl}^{(i)}(t)]_{\nu^{(i)}\times\nu^{(i)}} = \begin{bmatrix} h_{11}^{(i)}(t) & h_{12}^{(i)}(t) & \cdots & h_{1\nu^{(i)}}^{(i)}(t) \\ h_{21}^{(i)}(t) & h_{22}^{(i)}(t) & \cdots & h_{2\nu^{(i)}}^{(i)}(t) \\ \cdots & & & \\ h_{\nu^{(i)}1}^{(i)}(t) & h_{\nu^{(i)}2}^{(i)}(t) & \cdots & h_{\nu^{(i)}\nu^{(i)}}^{(i)}(t) \end{bmatrix}, \quad (13)$$

where

$$h_{bl}{}^{(i)}(t) = \frac{d}{dt}[H_{bl}{}^{(i)}(t)] \text{ for } b, l = 1,2,\ldots,\nu^{(i)},\ b \neq l,$$

and by formal agreement

$$h_{bb}{}^{(i)}(t) = 0 \text{ for } b = 1,2,\ldots,\nu^{(i)}.$$

The next steps in modelling the BNPSSTPOICIN operation process, considering taking into account just defined processes $Z^{(1)}(t)$, $Z^{(2)}(t)$ and $Z^{(3)}(t)$ interactions and interdependencess, the joint operation process of this network of critical infrastructure networks can be defined in the form of the vector

$$Z(t) = [Z^{(1)}(t),\ Z^{(2)}(t),\ Z^{(3)}(t)], \quad (14)$$

where $t \in < 0,+\infty)$.

4. Conclusions

According to the report [5], the definitions of selected basic notions concerned with critical infrastructures and climate and weather impacts on their safety have been used to describe the infrastructure installations in Baltic Sea Region.
Based on these, the following three critical infrastructure networks are distinguished: the Baltic Shipping Critical Infrastructure Network (BSCIN), the Baltic Port Critical Infrastructure Network (BPCIN) and the Baltic Ship Traffic and Operation Information Critical Infrastructure Network (BSTPOICIN). This made it possible to defined and discribed the operation processes of these networks. This has been done separately for every of them.
Next, under the general definitions of operation processes, the descriptions of the operation processes of the networks located in Baltic Sea Region have been proposed.

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] 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.

[2] 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, 2, 43-52.

[3] Dziewicki, M. (2007). *The role of AIS for small ships monitoring.* Baltic Master Report.

[4] Enisa. (2011). *Analysis of cyber security aspects in the maritime sector.*

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

[6] 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*.

[7] Ferreira, F. & Pacheco, A. (2007) Comparison of level-crossing times for Markov and semi-Markov processes. *Statistics and Probability Letters* 7, 2, 151-157.

[8] Glynn, P.W. & Haas, P.J. (2006). Laws of large numbers and functional central limit theorems for generalized semi Markov processes. *Stochastic Models* 22, 2, 201-231.

[9] Grabski, F. (2002). *Semi-Markov Models of Systems Reliability and Operations Analysis.* System Research Institute, Polish Academy of Science, (*in Polish*).

[10] Guze, S., Kołowrocki, K. & Soszyńska, J. (2008). Modeling environment and infrastructure influence on reliability and operation processes of port transportation systems. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 2, 1, 179-188.

[11] Guze, S. & Kołowrocki, K. (2016). Joint Network of Port, Shipping, Ship Traffic and Port Operation Information Critical Infrastructure Network. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 7, 2, 61-64.

[12] 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.

[13] 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.

[14] Kolowrocki, K. & Soszynska, J. (2009). Modeling environment and infrastructure influence on reliability and operation process of port oil transportation system. *Electronic Journal Reliability & Risk Analisys: Theory & Applications* 2, 3, 131-142.

[15] Kolowrocki, K. & Soszynska, J. (2009). Safety and risk evaluation of Stena Baltica ferry in variable operation conditions. *Electronic Journal Reliability & Risk Analisys: Theory & Applications* 2, 4, 168-180.

[16] Kolowrocki, K. & Soszynska, J. (2010). Reliability modeling of a port oil transportation system's operation processes. *International Journal of Performance Engineering* 6, 1, 77-87.

[17] Kolowrocki, K. & Soszynska, J. (2010) Reliability, availability and safety of complex technical systems: modelling –identification – prediction – optimization. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 4, 1, 133-158.

[18] 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.

[19] Limnios, N. & Oprisan, G. (2005). *Semi-Markov Processes and Reliability*. Birkhauser, Boston.

[20] Mercier, S. (2008). Numerical bounds for semi-Markovian quantities and application to reliability. *Methodology and Computing in Applied Probability* 10, 2, 179-198.

[21] Soszyńska, J. (2007). *Systems reliability analysis in variable operation conditions.* PhD Thesis, Gdynia Maritime University-System Research Institute Warsaw (in Polish).

[22] Soszyńska, J., Kołowrocki, K., Blokus-Roszkowska, A. et al. (2010). Prediction of complex technical systems operation processes. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars* 4, 2, 379-510.

[23] Watts, R. (2005). Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment." *Homeland Security Affairs* 1, Article 3 [available at: https://www.hsaj.org/ articles/179].