

Tchórzewska-Cieślak Barbara

Pietrucha-Urbanik Katarzyna

Dawid Szpak

Rzeszow University of Technology, Rzeszow, Poland

Review of methods for identifying threats including the critical infrastructure systems within the Baltic Sea

Keywords

failure, system safety, safety management, threats.

Abstract

In the analysis of the operation of critical infrastructure systems it is important to perform the analysis of the safety of the operation. The daily operation of such systems is inherently associated with the occurrence of various types of random undesirable events. Therefore, in the paper the methods used in the analysis of the risk of threats in critical infrastructure systems within the Baltic Sea, were presented.

1. Introduction

The critical infrastructure (CI) is a complex technological system, working continuously and requiring a high safety level. The problem for the exploiters is the distance between the particular subsystems and their elements, which makes the precise system monitoring especially difficult. Such system is unique and its particular elements have different functions, and simultaneously they interact forming an integral whole. Their correct interaction determines optimal functioning as concerns technical, economic and reliability aspects [2, 6, 16]. Critical infrastructure of cities should be constantly watched both for functional as well as security reasons. The safety and risk management in the municipal systems such as within the Baltic Sea is the base to prevent the occurrence of some serious failures that, as the daily experience shows, can lead to the economic, environmental and even human losses [3, 37, 38]. Unreliability of the critical infrastructure can be measured by the probability, frequency and duration of the undesirable events [2, 10, 11, 26].

Safety of the critical infrastructure means the ability to execute its functions despite of the fact that incidental undesirable events occur [18, 19].

In such grasp reliability means the ability to cover its function in the steady states of system operation, and

safety is determined as the possibility to survive the incidental states. The basic measure determining the level of safety of the critical infrastructure is risk connected with its operating [24].

According to the international standards the areas of scientific research on risk and safety are classified as follows:

- RAM (Risk Assessment and Management),
- ESR (Engineering, Safety and Reliability),
- EER (Environmental and Ecological Risk),
- HR (Health Risk),
- REL (Risk in Everyday Life),
- TR (Technological Risk),
- NH (Natural Hazard),
- PR (Political Risk).

Directive 96/82/EC Seveso II on the control of major-accident hazards involving dangerous substances has been valid since February 3, 1999. The name of the directive is associated with the disaster which happened in 1976 in Italy, in the town of Seveso, in chemical plant producing pesticides and herbicides. The released gas cloud contained tetrachlordibenzo-p-dioxin (TCDD).

The Directive has introduced the following concepts that have been adopted in the analysis of safety of all the technical systems:

- major accident prevention policy,
- safety management system,

- strategy for the prevention of major accidents,
- plant with increased risk,
- plant at high risk,
- internal emergency plan,
- external emergency plan,
- safety report.

In article 8 of the Directive appears a new term - "domino effect", understood as the sequence of events leading to a major accident. One of the techniques of risk analysis recommended by the directive is the so called Preliminary Hazards Analysis - PHA. Risk analysis involves determining the risk value.

Danger and hazard are the factors that determine the magnitude of the risk. Danger is considered a cause of loss. It is characterized by some kind of arranged time sequence of successive phases. In the first phase threat appears, which creates danger (e.g. an incidental water pollution in a source) [4, 5, 8, 12, 14]. In the second phase danger becomes real (e.g. polluted water appears in the distribution subsystem). In the third phase the effects of real danger are revealed (e.g. water consumers' gastric problems) [9, 33, 34]. Hazard is identified as a set of conditions and factors that have a direct impact on the second phase of danger [17, 21, 25]. The severity of any given danger is fundamentally based on the hazard. Hazard as a risk factor determines the magnitude of losses resulting from risk realization [20, 22, 23, 27].

The quality methods of the analyses of risk allow to determine the relative measure of risk that is the base to rank the risk connected with the undesirable events [1, 28-30, 35, 36].

Ensuring the continuity of the technical system requires the use of knowledge about the reliability and security that are very well characterized by the concept of risk. It includes an assessment of the dependence between threats and used protective barriers [7, 31, 32, 40].

The aim of the work is to propose the methods for the identification of risks Including the critical infrastructure systems within the Baltic Sea.

2. Types of undesirable events

Threats can be divided in the following way:

- the type of causes: internal or external,
- duration: rarely occurring, long-term (which could cause a domino effect), cyclic (recurring),
- range: local, extensive (regional, global),
- stability in the field range: spreading in the field or retardant in the field.

Factors influencing the navigational hazard are [13]:

- external factors: reservoir parameters (width, depth, shape), the positioning parameters (accuracy, availability, quantity, frequency of operation), hydro-meteorological conditions

(wind, current, visibility, sea state), parameters of ships movement (vessel size, the intensity, the speed), system parameters for traffic control and labeling (VTS and its type, pilotage, AIS, signage systems, radio communications), actions of the forces of nature,

- internal factors related of the ship: type of ship (size, steering, load, maneuvering parameters), kind of equipment (navigation systems, ECDIS, Radar, ARPA, communication, positioning, ergonomic bridge), management (emergency procedures, route planning, correction maps, surveys),
- human factors: the captain, the pilot, the watch officer (education, fatigue, experience, stress, fear, confidence, exposure time, excess or insufficient amount of information, language and communication problems with commands, errors made by system operator),
- other factors: legal and administrative, deliberate or incidental actions of the third party.

3. Hazards identification

Hazard identification is usually performed using expert methods. The most important methods of detailed risk analyzes include:

- HAZID - Hazard Identification. This is the first stage of analysis of the risks and possible consequences, which is often an introduction to the analysis of risks in technical systems. HAZID method involves identifying hazards using the knowledge of an expert or group of experts. Properly performed the identification of hazards should be characterized by the following features:
 - creativity and the ability to identify all, also had not taken into account, the types of threats,
 - identification of significant risks,
 - the use of knowledge from experience particularly in the field of accident.
- HAZOP - Hazard and Operability Analysis. This is an analysis performed by teams of experts under the guidance of the leader. This shall be done by using a keyword list and is used primarily in the safety analysis of large industrial systems,
- FMEA - Failure Modes and Effect Analysis. The method used to analyse security systems and technical installations. Based on the analysis of the reliability of the individual components of the system,
- SWIFT - Structured What-If Technique Checklist. This session is conducted by a team of experts. Basic questions asked during brainstorming is: "What if?", "How is it possible?" and "Is it possible?". The answers provided information on

the types of threats and potential accident scenarios,

- Influence Diagram, the method used to determine the statistical dependencies between failure causes and effects. Influence diagrams are used for the analysis of human reliability (system operators),
- checklist for each activity. It involves filling in a list prepared and analyzed what hazards may potentially exist in the system,
- spatial analysis. It is a process of exploration (extraction) of information hidden in the data set. The simplest case analysis of spatial data is a visual examination of the distribution on the basis of imaging in the form of traditional maps,
- Fault Tree Analysis (FTA) graphically illustrates the dependence between events that influence the occurrence of the adverse event called peak event. In preparing the tree the so-called functors (logic gates) are used, specifying, inter alia, the product of logical events and the logical events.

One of the most common ways to conduct a hazard analysis is the study of the risks of using data from:

- previous safety analyses,
- the conclusions of occurring undesirable events and their causes,
- the experience of experts from the operation of existing systems.

4. Risk connected with critical infrastructure operation within the Baltic Sea

The factors which form the probability that the negative consequences occur are, among others, the following:

- the probability that the undesirable event occurs,
- frequency and a degree of exposure,
- the possibility of avoidance or minimization of the negative consequences.

Risk assessment is a process consisting of a number of the systematic steps, in which the study of different kinds of threats connected with the CI operating is performed. The basic purpose of this kind of activities is to collect the information necessary to estimate the system safety [39]. Risk assessment should contain:

- establishment of a ranking of the undesirable events,
- determination of the level (value) of risk,
- proposal of the activities aiming at risk minimization,
- establishment of the time after which the risk can obtain its critical value as a result of different processes, eg. materials ageing.

In the process of risk assessment in the CI one should take into account the information concerning:

- system operating (exploitation) conditions,
- data regarding the operation of the particular system elements and the dependence between them,
- data concerning energy supply,
- data regarding the possible failures in the system,
- distinction of the states of operating and the states of failure in the system,
- information concerning the causes of failures,
- data regarding the possible consequences of the undesirable events.

Risk assessment includes the so called risk analysis, which is the process aiming at the determination of the consequences of the failures (undesirable events) in the CI, their extend, sources of their occurrence and the assessment of the risk levels. Reactive security management is based on the identification of potential threats on the basis of the hazards existing in CI. This strategy is not very effective in identifying trends and forecasting future sources of threats. Proactive security management strategies are oriented towards creating database of undesirable events from different sources. The analysis of the causes of the occurrence of the undesirable events in the CI can be performed by means of different methods presented in the next sections.

5. Registration of undesirable events

Information about the failure should be recorded on a specially prepared for this purpose failure cards and in form of extensive database of various operating data.

The scheme of protocol of failure removal was shown in the figure 1 [38].

The condition for the proper implementation of the process is to oblige the people managing the technical system to currently complete failure cards and periodically provide acquired data to experts in order to verify and assess the obtained information.

Emergency events do not appear without a reason but there are a chain of undesirable events. The use of developed failure card will allow to know the causes and the consequences of each undesirable event, as well as the further evaluation of the technical system safety.

Report date:

Naftoport Oil Terminal
 (Address)

PROTOCOL OF FAILURE REMOVAL OF THE NAFTOPORT OIL TERMINAL
 - Report No.

Date of failure notification: _____ time

Details of the failure
 notifier: _____
(name, address, phone number)

Notification accepted by: _____
(name of an employee of the water supply company)

Place of failure ¹⁾: _____

Name of failure object: _____

Condition of object before failure: _____

Repairs carried out before the failure ²⁾: _____

Description of failure ³⁾: _____

Cause of failure ⁴⁾: _____

Persons removing failure: _____

time from _____ to _____

Losses associated with failure: _____

The duration of the preparatory work (date): _____
 _____ time

Date of repair start: _____ time

Date of completion repair: _____ time

Completion of after-failure work (date): _____
 _____ time

Method of failure removal: _____

Used material and equipment: _____

Difficulties, threats and damages ⁵⁾: _____

Measures to prevent the repeating of similar failure in future: _____

Date: _____

Foreman signature: _____

Supervisor signature: _____

- ¹⁾ construction, route, warehouse, workshop, machine room, others.
- ²⁾ types and date of the last overhaul, the information on the conducted technical acceptance made after the renovation, others
- ³⁾ conduct of staff, operation of protection, protective and signalling devices, others
- ⁴⁾ determining who caused failure, determining which staff is to blame e.g. supervision, repair team, suppliers, natural disasters, no information available
- ⁵⁾ including the cost of man-hour, losses in fixed assets and working capital, the value of uncompleted production, others

Figure 1. The exemplary protocol of the Naftoport Oil Terminal failure, on the basis of [38]

System safety management in the initial phase means to create a database of undesirable events with particular emphasis on their frequency and negative consequences associated with them. In the fundamental phase of safety management decisions are made about the choice of protection measures against risks, introducing them to the practice of exploitation and control of the effectiveness of the used solutions.

5. Matrix methods for risk assessment

5.1. The two parametric risk matrix

Procedures for risk analysis cover the whole activity aiming to identify threats, to estimate risk and its size. The appearance of the extraordinary event produces the state of emergency to which some potential of danger is assigned. Then determination of the acceptable risk level relies on an introduction of the criteria values.

The presented matrix is one of the simplest. From the mathematical point of view risk (r) is defined as following [29, 30, 37]:

$$R = P \cdot C \quad (1)$$

where P is a measure of the system operating unreliability corresponding with category of probability - frequency, C is a measure of the consequences corresponding with category of consequences – damages, expressed in financial units.

In *Table 1* the two parametric risk matrix is presented, assuming the following risk scales and corresponding point weights:

- probability (P): little – 1, medium – 2, large – 3,
- consequences (C): little – 1, medium – 2, large – 3.

Table 1. The two parametric risk matrix.

C	1	2	3
P	r		
1	1	2	3
2	2	4	5
3	3	6	9

According to the basic matrix for risk assessment given above we can analyse different undesirable events assuming the following scale of risk:

- the tolerable risk – a number of points from 1 to 2,
- the controlled risk – a number of points from 3 to 4,
- the unacceptable risk – a number of points from 6 to 9.

5.2. The three parametric risk matrices

Taking into account that CI is a complex technical system built from subsystems and elements that are firmly interconnected it makes sense to expand the CI operating risk matrix by next parameters influencing risk size. The three parametric matrix for risk assessment is proposed. The parameters are following: the frequency of the threat occurrence (P), threat consequences (C) and the exposure to threat (E). The exposure to threat should be related to the period of time when the public water pipe has been used as a source of drinking water. The numerical risk assessment is a product of the above mentioned parameters [29, 32, 37]:

$$r = P \cdot C \cdot E \quad (2)$$

The following scales and weights of the particular parameters are assumed:

- scale of threat frequency (P):
 - almost impossible incidents (1 in 100 years); with weight 0.1,
 - occasionally possible incidents (1 in 20 years); with weight 1.0,
 - little probable incidents (1 in 10 years), with weight 2.0,
 - quite probable incidents (once a year), with weight 5.0,
 - very probable incidents (10 times a year), with weight 10.0,
- scale of threat consequences size (C):
 - little loss up to $5 \cdot 10^3$ EUR ; with weight 1.0,
 - medium loss from $5 \cdot 10^3$ to $5 \cdot 10^4$ EUR, with weight 3.0,
 - large loss $5 \cdot 10^4$ EUR – 10^5 EUR; with weight 7.0,
 - very large loss 10^5 – 10^6 EUR, with weight 15.0
 - serious disaster, losses over 10^6 EUR; with weight 50.0,
- scale of exposure to threat (E):
 - slight, once a year or less often , with weight 0.5,

- minimal, a few times a year; with weight 1.0,
- occasionally, several times a month, with weight 2.0,
- often, several times a week, with weight 5.0,
- constant, with weight 10.0.

The numerical risk assessment determined in this way takes the values within the range 0.05 to $5 \cdot 10^3$. The levels of risk in the five stage scale are shown in table 2.

Table 2. The levels of risk

Class	Description	Numerical values	Risk level
1	very little	$0,05 < r \leq 5$	tolerable
2	little	$5 < r \leq 50$	
3	medium	$50 < r \leq 200$	controlled
4	large	$200 < r \leq 400$	
5	very large	$400 < r \leq 5000$	unacceptable

The risk assessment we can calculation according to the formula [29, 31, 32]:

$$r = P \cdot C \cdot S \quad (3)$$

where P is point weight connected with the probability that the representative undesirable event occurs, from 1 to 5, C is point weight connected with the magnitude of losses, from 1 to 5, S is point weight connected with the public feelings, from 1 to 3.

Point scale to measure risk is within the range 1 to 75. The following risk levels are assumed: $r = 1 \div 12$ – the tolerable risk, $r = 15 \div 36$ – the controlled risk, $r = 40 \div 75$ – the unacceptable risk.

5.3. The four parametric matrix for risk assessment

CI should be provided with different protection and monitoring systems which increases its operating and safety reliability. That is why the fourth parameter characterising the size of this protection has been introduced to the risk matrix connected with CI operating [29, 30, 32, 37].

The four parametric matrix for risk assessment has been proposed, according to the formula [29]:

$$r = \frac{P \cdot C \cdot N}{O} \quad (4)$$

where P is point weight connected with the probability that the representative undesirable event appears, C is point weight connected with the size of losses, N is point weight connected with a number of the endangered inhabitants, O is point weight connected with CI protection against extraordinary threat.

Parameter (O) is inversely proportional to the size of risk. Analogically as in the two and three parametric methods every time the size of parameters P,C,N and O are described according to the following point scale: low – L= 1, medium – M = 2, high – H = 3. In this way the point scale to measure risk in the numerical form within the range [0,33÷27] has been obtained. In table 3 the four parametric risk matrix is shown; the particular numerical values were obtained using the formula (6).

The description of the risk components.

- category for a number of the endangered inhabitants – N:
 - low – a number of the endangered inhabitants less than 5 000 – N=1,
 - medium - a number of the endangered inhabitants from 5 001 to 50 000 – N=2,
 - high - a number of the endangered inhabitants higher than 50 001 – N=3,
- category for the probability that failure occurs – P:
 - low – unlikely – once in 10 ÷ 50 years - P=1,
 - medium – quite likely – once in 1 ÷ 10 years - P=2,
 - high – likely - 1 ÷ 10 times a year or more - P=3,
- category for consequences – C:
 - little - financial losses up to 5 . 10³ EUR - C=1,
 - medium - financial loss up to 10⁵ EUR - C=2,
 - large - financial loss over 10⁵ EUR - C=3,
- category for protection – O. If the total number of points equals :
 - 7÷10 – high protection level - O = 3,
 - 12÷34 – medium protection level - O = 2,
 - over 34 – low protection level - O = 1.

Table 3. Risk categories.

Risk category	Point scale
Tolerable	$0,33 \leq r \leq 3,0$
Controlled	$4,0 \leq r \leq 8,0$
Unacceptable	$9 \leq r \leq 27$

The exemplary application of the method is following :

- the probability that the given undesirable event occurs is $P = M = 2$,
- predicted losses are estimated as $C = M = 2$,
- the protection level defined on the base of the supplementary questionnaire $O = H = 3$,
- the number of the endangered inhabitants using the water pipe $N = L = 1$.

The numerical risk value read from table 4 is: $r = 1.33$ which, according to table 5, means the tolerable risk.

5.4. Application of FMEA in the analysis of CI

In the FMEA method the global assessment, taking into account the fact that the undesirable events occur at random, is carried out by using a number of risk priority LPr according to the formula [32, 37]:

$$LPr = LPP \cdot LPW \cdot LPK \quad (6)$$

where LPP is a number of priority for the appearance of failure – defines probability of a possibility of the appearance from the slightly little (impossible) to the very possible.

LPW is a number of priority for the detectability – defines probability of failure detection, the early warning system or the delayed warning, LPK is a number of priority for a inhabitant – defines probability of the intensity of effects for people.

To each of these three numbers of priority a weight from the scale 1 to 10 is assigned. In this way LPR can take the values from a range 1 to 1000. The assessment of LPr is carried out by using some evaluation forms that comprise the existing state and the improved state. In Table 4 the suggested values of the particular priority numbers were presented.

Table 4. The values of the priority numbers.

LPP		LPW		LPK	
Improbable <10 ⁻⁶	1	Very little probability > 10 ⁻¹	1	Little > 10 ⁻¹	1
Very little probability 10 ⁻⁵ – 10 ⁻⁶	2-3	Moderately probable 10 ⁻¹ – 10 ⁻³	2-5	Noticeable significant 10 ⁻¹ – 10 ⁻³	2-3
Little probability 10 ⁻³ – 10 ⁻⁵	4-6	Little probability 10 ⁻³ – 10 ⁻⁵	6-8	Large 10 ⁻³ – 10 ⁻⁵	4-6
Moderately probable 10 ⁻¹ – 10 ⁻³	7-8	Very little probability 10 ⁻⁵ – 10 ⁻⁶	9	Large 10 ⁻⁵ – 10 ⁻⁶	7-8
Very probable > 10 ⁻¹	9-10	Improbable < 10 ⁻⁶	10	Catastrophic < 10 ⁻⁶	9-10

The high number of LPr means the high priority in the procedures of removing and minimization of the hazard connected with the undesirable events. It is assumed that for LPr ≥ 100 it is obligatory to take some precautions, and LPr reduced to 10% is treated as a negative result of the carried out actions.

6. Description of the logical trees methods

6.1. The fault tree method

Fault Tree Analysis (FTA) presents graphic relations between the events influencing the occurrence of a specific undesirable event called “the pick event” [15, 32]. Creating the tree we use the so called functors (logical gates) which determine, among others, events logical product and events logical sum. In figure 2 the basic symbols used to create the fault tree according to PN-IEC1025:1994 are shown and in table 5 the exemplary gates with their quantitative description are presented.

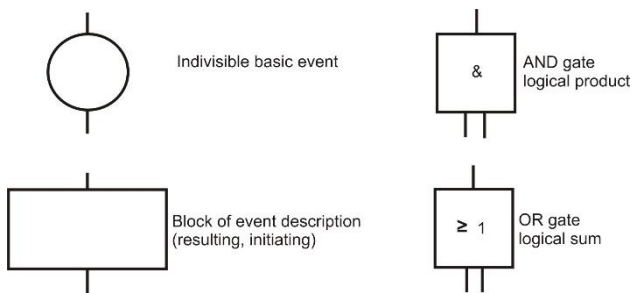


Figure 2. The basic symbols in the fault tree method.

Table 5. The basic logical gates.

Gate	Graphic symbol	Logic operation	Unreliability index
AND		$W = w_1 \wedge w_2$	$U = \prod_{i=1}^n U_i$
OR		$W = w_1 \cup w_2$	$U = 1 - \prod_{j=1}^M (1 - U_j)$

OR gate – in this gate the output event takes place when any of the input events takes place
 AND gate – in this gate the output event takes place when all the input events take place.

Fault tree quantitative analysis relies on the determination of frequency (intensity) or probability that the pick event occurs.

In Table 6 the basic formulas to calculate probability or intensity of the output events for gates connected with logical product (AND) and logical sum (OR) are given.

Table 6. Computational formulas for probability and intensity of the output events for gates AND and OR.

Gate „OR”
$P(X + Y) = P(X) + P(Y) - P(X) \cdot P(Y)$
$\lambda(X + Y) = \lambda(X) + \lambda(Y)$
$P(X+Y+Z) = P(X) + P(Y) + P(Z) - P(X) \cdot P(Y) - P(X) \cdot P(Z) - P(Y) \cdot P(Z) + P(X) \cdot P(Y) \cdot P(Z)$

Gate “AND”
$P(X \cdot Y) = P(X) \cdot P(Y)$
$\lambda(X \cdot Y) = \lambda(X) \cdot P(Y) = P(X) \cdot \lambda(Y)$

Example of the method application.

In Figure 3 the exemplary fault tree model created for the scenario: undesirable event causing interference in functioning of sea ports, is presented.

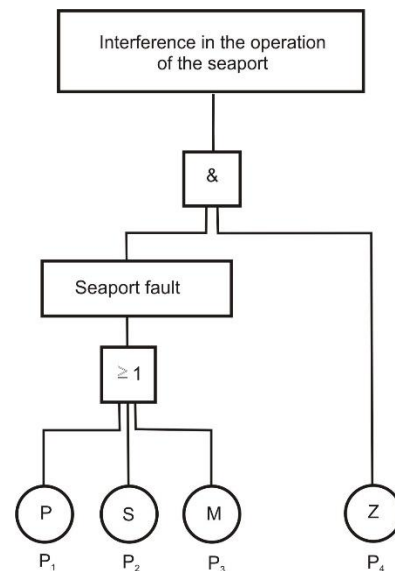


Figure 3. Illustration of the fault tree: P – event connected with the technical failure, R – event connected with the failure of the control system, M – event connected with the operator error, Z – event connected with unreliability (probability that seaport protection against existing threat will not be available).

Calculations for probability of the event:

$$P_s = P_1 + P_2 + P_3 \quad (7)$$

$$\Lambda = P_s \cdot P_4 \quad (8)$$

6.2. The Event Tree Method

To analyse risk connected with CI operating we often use Event Tree Analysis. The event tree method allows to anticipate the possible scenarios of the events sequence development after the so called undesirable initiating event or pick event occurs. In the event tree technique scenarios are built in relation to the safety barriers operation [30, 32]. On every tree level two logical states, success (yes) and failure (no), which are identified with the situation that the given barrier operates or does not operate, are considered. The qualitative as well as the quantitative event tree analysis is possible. In the quantitative analysis to a branch which describes success the probability P_i is assigned, and to a branch identified with failure $1 - P_i$.

Examples of the method application

In *Figure 4* the event tree analysis after the pick event occurrence - interference in functioning sea ports - is presented.

Particular probability values are:

- disaster $P_I = U(K) \cdot (1 - P_1)$,
- serious failure $P_{II} = U(K) \cdot P_1 \cdot (1 - P_2)$,
- failure $P_{III} = U(K) \cdot P_1 \cdot P_2 \cdot (1 - P_3)$,
- situation is controlled $P_{IV} = U(K) \cdot P_1 \cdot P_2 \cdot P_3 \cdot (1 - P_4)$.

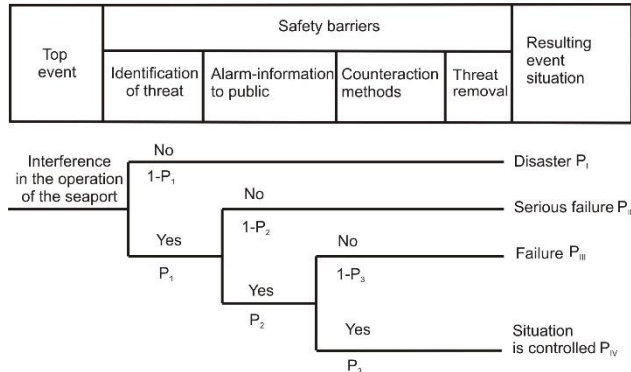


Figure 4. The event tree of interference in functioning sea ports.

6.3. The combined model for risk analysis using the logical trees method - cause and consequence analysis

This method is a combination of two methods: the fault tree method and the event tree method. Causes and consequences of the initiating event (critical event), the event starting a series of events (the domino effect), are considered. The analysis begins by identifying the critical event and then the consequences of this event are analysed by the event tree that represents situations that may occur after initiation of a critical event [29, 32]. The causes are analysed using the fault tree. This method was developed as a reliable tool to ensure safety of critical systems, which have direct impact on health, property and the environment. Different development paths of hazardous situation can be identified.

The procedure consists of five stages:

- selection of event or situations for analysis,
- identification of the safety function of the individual system elements,
- determining event paths starting from the initiating event (the event tree),
- determination of the elementary events for the initiating event (the consequence tree),
- setting criteria of activities.

Analysed event can be chosen in two ways: as an event being the consequence of previous events (as in

the consequence tree) or the initiating event (as in the event tree).

This method may be presented schematically by showing the causes and the consequences of a specific event.

In *Figure 5* the possibility to combine the fault tree method and the event tree method for the scenario of events for interference in functioning sea ports is presented.

The probabilities were defined as:

- P_0 - probability that the resulting event occurs (interference in the operation of the seaport),
- P_1 - probability that the event will not be detected,
- P_2 - probability that the counteraction methods will not be taken,
- P_I - probability that the situation is controlled,
- P_{II} - probability of the failure occurrence after implementation of counteraction methods,
- P_{III} - probability of the critical situation occurrence.

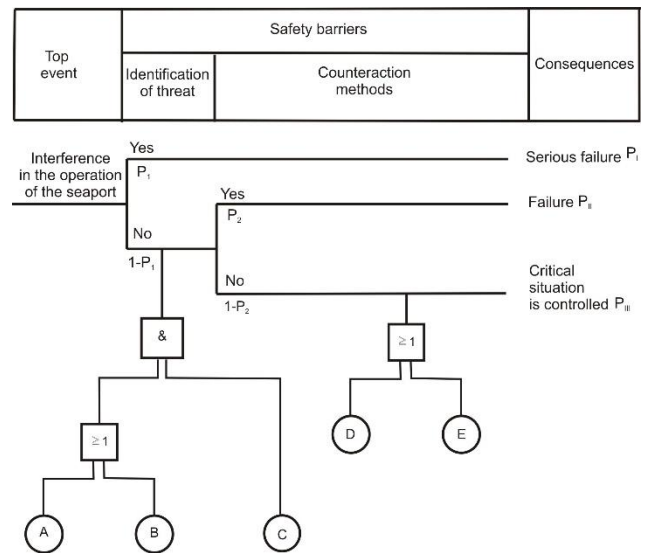


Figure 5. The combined model of logical trees.

Particular kinds of probability are following:

$$P_I = P_0 \cdot (1 - P_1) \tag{9}$$

$$P_{II} = P_0 \cdot P_1 \cdot (1 - P_2) \tag{10}$$

$$P_{III} = P_0 \cdot P_1 \cdot P_2 \tag{11}$$

For the following actors:

- A – lack of possibility to reveal interference in the operation of the seaport (P_A),
- B – error of operator (P_B),
- C – operator neglected the seriousness of the situation (P_C),
- D – lack of control or ineffective procedures to counteract critical situation (P_D).

where:

$$P_1 = P_C \cdot [P_A + P_B - P_A \cdot P_B] \tag{12}$$

$$P_2 = P_A + P_D - P_A \cdot P_D \quad (13)$$

Safety management in critical system means management by assumed for the system goals, which relies on: minimization of risk of failure (prevention), minimization of a number of failures (active action) and minimization of the consequences of failures (passive action).

8. Conclusions

- Every human activity is burdened with risk. One can distinguish a voluntary risk and an enforced risk. When a voluntary risk is accepted it is often underestimated, and when an enforced risk is evaluated it is often overestimated.
- Risk analysis and evaluation is the most important procedure in water supply system safety management.
- We can observe constant efforts to change the notion of risk acceptance. Especially important and actual are actions that concentrate on the integration of technological risk and environmental risk.
- If one assumes that undesirable events are unavoidable, it should lead to forecasting of their frequency and potential losses connected with them, and this is a domain of risk analyses and evaluation, according to the rule “to measure a risk in order to be able to manage it”.
- The most important in CI safety operating management is to assess integrated risk and to present this risk in a graphic way in the given territory. Risk estimation is a very useful tool which supports management in crisis.
- The most effective and advanced method that can be used nowadays in design analyses which aiming at ensuring the reliable functioning uses new information technologies to analyse and assess risk connected with water supply to urban population.
- It should be remembered that the results of recording failure will be visible only in the future. The proposed method of recording failures will allow to gain knowledge necessary for further reliability and safety analyses. In order to use the obtained data to determine the appropriate reliability parameters at first they must be prepared. The purpose of this preparation is to obtain statistical samples in accordance with adapted structures of dividing examined subsystems into elements and set for them reliability states.

Acknowledgements



The paper presents the results developed in the scope of the HAZARD project titled “Mitigating the Effects of Emergencies in Baltic Sea Region Ports” that has received funding from the Interreg Baltic Sea Region Programme 2014-2020 under grant agreement No #R023. <https://blogit.utu.fi/hazard/>

References

- [1] Apostolakis, G. & Kaplan, S. (1981). Pitfalls in risk calculations. *Reliability Engineering and System Safety*, 2, 135-145.
- [2] Aven, T. (1992). *Reliability and Risk Analysis*. Copyright by Elsevier.
- [3] Aven, T. (2010). Conceptual framework for risk assessment and risk management. Summer Safety & Reliability Seminars. *Journal of Polish Safety and Reliability Association*, 1, 15-27.
- [4] Billinton, R. & Allan, R.N. (1992). *Reliability Evaluation in Engineering Systems. Concepts and Techniques*. Copyright by Plenum Press. London.
- [5] Birolini, A. (1990). *Qualität und Zuverlässigkeit technischer Systems. Theorie, Praxis, Management*. Copyright by Springer, Berlin.
- [6] Bishop, C.M. (2006). *Pattern Recognition and Machine Learning*. Springer: New York.
- [7] Blischke, W., Murthy, D.N.P. (2000). *Reliability: Modeling, Prediction and Optimization*. Copyright by J. Wiley and Sons, New York.
- [8] Chen, C.W., Liu, K.FR., Tseng, CP., Hsu, WK. & Chiang, WL. (2012). *Hazard management and risk design by optimal statistical analysis*. *Natural Hazards*, 64, 2, 1707-1716.
- [9] Dhillon, S. (1986). *Human Reliability with Human Factors*. Pergamon Press: New York.
- [10] Drzazga, M., Kołowrocki, K., Soszyńska-Budny, J. & Torbicki, M. (2016). Port oil piping transportation critical infrastructure assets and interconnections. *Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars*, Vol 7, No 1, pp. 37-42.
- [11] Dziula, P. & Kołowrocki, K. (2016). Identification of climate related hazards, the Global Baltic Network of Critical Infrastructure Networks, is exposed to. *Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars*, Vol 7, No 1, pp. 43-52.

- [12] Faber, M. H. & Steward, M. G. (2003). Risk Assessment for Civil Engineering Facilities: Critical Overview and Discussion. *Reliability Engineering and System Safety*, 80, 173-184.
- [13] Gucma, L. (2009). *Wytyczne do zarządzania ryzykiem morskim*. Wydawnictwo Naukowe Akademii morskiej w Szczecinie. Szczecin 2009.
- [14] Guikema S. D., Pate-Cornell M.E. (2002). Component choice for managing risk in engineered systems with generalized risk/cost functions. *Reliability Engineering and System Safety*, 78, 227-238.
- [15] Hadipriono, F. C. & Toh, H.S. (1989). Modified fault tree analysis for structural safety. *Civil Engineering and Environmental Systems*, 6 (4), 1989, 190-199.
- [16] Haimes, Y. Y. (1998). Risk analysis of fracture and failure, *Materials Research Innovations*, 2(1)/1998, pp. 16-21.
- [17] Haimes, Y.Y, Moser D. & Stakhin, E. (2006). Risk Based Decision Making in Water Resources *Journal of Infrastructure Systems, ASCE*, 2006 12, 401-415.
- [18] Haimes, Y.Y. (1998). *Risk Modelling, Assessment and Management*. Wiley, New York.
- [19] Haimes. Y.Y. (2009). On the Complex definition of risk: a systems-based approach, *Risk Analysis*. 29 (12), 1647-1654.
- [20] Hastak H. & Baim E. (2001). Risk factors affecting management and maintenance cost of urban infrastructure. *Journal of Infrastructure Systems*, 7 (2), 67–75.
- [21] Hubbard, D.W. (2009). *The failure of risk management*, Wiley. New York.
- [22] Kaplan, S. (1997). The words of risk analysis, *Risk Analysis*, 7(4), 407-417.
- [23] Kaplan, S. & Garrick, B.J. (1981). On the quantitative definition of risk. *Risk Analysis* 1(1), 1981, s. 11-27.
- [24] Kołowrocki, K. & Soszyńska-Budny, J. (2011). *Reliability and Safety of Complex Technical Systems and Processes: Modeling – Identification – Prediction – Optimization*. Springer, London.
- [25] Kuo, W. & Zuo, M. J. (2003). *Optimal reliability modeling*. Copyright by Wiley, New Jersey.
- [26] McGill, W.L., Ayyub, B.A. & Kaminskiy, M. (2005). Risk Analysis for Critical Asset Protection. *Risk Analysis*, Wiley Blackwell, 27(5), 1265-1281.
- [27] Pham, H. (2003) *Handbook of Reliability Engineering*. Springer, London.
- [28] Pietrucha-Urbanik, K. & Tchórzewska-Cieślak, B. (2014). *Water Supply System operation regarding consumer safety using Kohonen neural network*; in: Safety, Reliability and Risk Analysis: Beyond the Horizon – Steenbergen et al. (Eds), Taylor & Francis Group, London: 1115-1120.
- [29] Rak, J. (2004). *Istota ryzyka w funkcjonowaniu systemu zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
- [30] Rak, J. (2009). *Bezpieczeństwo systemów zaopatrzenia w wodę*. PAN, Instytut Badań Systemowych. Warszawa.
- [31] Rak, J.R. (2015). *Propozycja oceny dywersyfikacji objętości wody w sieciowych zbiornikach wodociągowych*, Czasopismo Inżynierii Łądowej, Środowiska i Architektury, JCEEA, t. XXXII, z. 62 (1/15), s. 339-349. DOI:10.7862/rb.2015.23
- [32] Rak, J.R. & Tchórzewska-Cieślak, B. (2007). *Czynniki ryzyka w eksploatacji systemów zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
- [33] Rak, J., Pietrucha-Urbanik, K. (2015). *New directions for the protection and evolution of water supply systems - smart water supply*. Czasopismo Inżynierii Łądowej, Środowiska i Architektury - Journal of Civil Engineering, Environment And Architecture. JCEEA, z. 62 (3/I/2015), pp. 365-373. DOI: 10.7862/rb.2015.121
- [34] Rak, J., Tchórzewska-Cieślak B. (2005). *Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
- [35] Schneeweiss, W. G. (2001). *Reliability Modeling*. Copyright by Lilole – Verlag, Hagen, 2001.
- [36] Smith, D.J. (2001). *Reliability, Maintainability and Risk*. Copyright by Butterworth – Heinemann.
- [37] Tchórzewska-Cieślak, B. (2008). *Niezawodność i bezpieczeństwo systemów komunalnych*. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów.
- [38] Tchórzewska-Cieślak, B., Pietrucha-Urbanik, K. & Szpak, D. (2016). Developing procedures for hazard identification. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars*, Vol 7, No 1, pp. 209-215.
- [39] Zio, E. (2007). An introduction to the basics of reliability and risk analysis, Series on Quality, *Reliability and Engineering Statistics*, Singapore.
- [40] Zio, E. (2009). *Computational Methods for Reliability and Risk Analysis*. Springer.