

Tchórzewska-Cieślak Barbara

Pietrucha-Urbanik Katarzyna

Szpak Dawid

Rzeszow University of Technology, Rzeszow, Poland

Methods for identifying threats of critical infrastructure systems within Baltic Sea region

Keywords

failure, system safety, safety management, risk, security, threats, FMEA, risk, safety, failure analysis, Bayes network

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 matrix and logical trees methods used in the analysis of the risk of threats in critical infrastructure systems within the Baltic Sea, were presented. The analysis and assessment of the protection of technical system was performed using the FMEA method (Failure Mode and Effect Analysis). As to analyse the cause and effect of undesirable events the method of Bayes' theorem and Java Bayes program were implemented, which allows to identify the probability of the event occurrence.

1. Introduction

The primary objective of risk management is to increase the safety of the technical system. The basis of the risk management process is the identification of threats because effective management without this knowledge is practically impossible. The most important is to recognize the technical threats [37, 47]. Besides, you should pay attention to the human and environmental factor, organizational structures and interrelationships between them [10, 38]. Only this approach guarantees avoiding the so-called unidentified risk. For the so called pure risk, associated with the operation of the technical system, standard actions have been developed. Standard solutions for the protection and safety of the technical system should be adequate to possible threats [18, 33, 44]. Generally, the concept of technical system safety is understood as the system's ability to protect its superior functional properties against internal and external threats [64].

Risk assessment is a three step procedure consisting in [22, 41, 43, 45, 46, 50]:

- hazard identification,
- probability assessment,
- consequence analysis.

The previous analyses show that priority issues related to warning system should include [26]:

- assessment of the response time to take action,
- ways of warning different groups of society (schools, hospitals, etc.),
- developing warning messages in accordance with the scale of threat which will allow implementation of protective procedures,
- scenario of population behaviour in face of warning, an indication of alternative sources for media belonging to the critical infrastructure (drinking water, electrical and thermal energy, natural gas),
- public education on the knowledge of warning and alert systems and types of threats and their consequences,
- functioning of fast response emergency service.

The analysis shows that the warning system is a special type of information system [27]. Using the basic conceptual terminology of system theory in relation to the warning system we can distinguish three main subsystems: functional, structural and utility [23, 45].

The functional subsystem consists of the following elements:

- obtaining warning signals: identifying information needs, definition of the observation area with a possible division, location of information sources, measurement of changes in the monitored parameters,
- analysis of warning signals: determination of changes measurement, the characteristics of the permissible ranges of changes, prioritization of indicators of changes, interpretation and verification of warning parameters size.
- warning signals transmission: determining subjects responsible for transmission, supervision of transmission punctuality and accuracy, reducing disruptions and distortions in the transmission.

The structural subsystem includes such elements as: sources of information (internal, external databases, historical, current, prospective) and operational teams (data collection and analysis, emergency response, emergency management centres) [1, 8].

The utility subsystem consists of the following elements:

- obtaining information: recording data from continuous monitoring, interviews and questionnaires,
- data analysis: methodology, data-processing technique, selection of indicators,
- transmission of information: information technology, data protection methods, methods of computer support in decision-making, the rules of verbal communication.

Early warning system can identify threats and launch procedures for counteracting them. Reduction of negative effects is possible because the warning system is part of response in crisis situations. Warning systems are used in the management of risk because they create possibilities for its assessment - reveal extraordinary threats and contribute to the assessment of negative consequences [9, 13, 63].

Besides, warning system determines the effectiveness of any rescue operations. Precise identification of hazard and the smooth transfer of information allow effective response by means of warnings and alarms [6, 58].

In the risk analysis historical knowledge of the system operation, analytical methods and experience of the operators should be used. In many cases, part of the risk analysis is the analysis of the human factor and reliability analysis of a man - a system dispatcher [5]. 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, 7, 21, 22]. 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, 65, 69]. Unreliability of the critical infrastructure can be measured by the probability, frequency and duration of the undesirable events [2, 11, 12, 21].

Safety of the critical infrastructure means the ability to execute its functions despite of the fact that incidental undesirable events occur [22, 24].

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 [31].

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) [5, 6, 9, 13, 18]. 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) [10, 48, 50]. Hazard is identified as a set of conditions and factors that have a direct impact on the second phase of danger [20, 27, 33].

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 [26, 29, 30, 38].

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, 39, 41, 42].

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.

The aim of the work is to propose a procedure for the identification of undesirable events, including, among others, failure time, type of failure, location of failure, extent of failure, cause of failure, consequences of failure and actions and equipment used to remove the failure. Also to propose the methods for the identification of risks including the critical infrastructure systems within the Baltic Sea. The developed method can be a support tool for operators as to increase the security level and used to expand the system of monitoring and detection of undesirable events in the considered infrastructure. In the work, the examples of application of the developed method was presented.

2. Hazard identification

Hazard identification is usually made using experts methods. The most important methods of detailed hazard analyses are [38, 46]:

- HAZID (Hazard Identification) – it is the first step in hazard analysis and possible consequences, it is often a prelude to risk analysis in technical systems,
- HAZOP (Hazard and Operability Analysis) – the analysis is carried out by teams of experts under the guidance of a leader. The HAZOP method is performed using a keyword list. It is used primarily in the safety analysis of large industrial systems,
- FMEA (Failure Modes and Effect Analysis) – it is used to analyse security of systems and technical installations. It is based on the reliability analysis of individual system components,
- SWIFT (brainstorming) (Structured What-If Checklist Technique) – it is carried out by a team of experts. Basic questions asked during the session are: "What if ?", "How is it possible ?" and "Is it possible ?". In response the types of hazards and potential accident scenarios of events are obtained,
- Influence Diagrams – they are used to determine statistical relationships between causes and effects, which help to understand the phenomena and uncertainties contained therein.

One of the most common ways to conduct a hazard analysis is the study of threats using the following data [38, 46]:

- previous analyses of safety,
- conclusions from occurred undesirable events and their causes,
- experience from the existing technical systems.

There are the following phases of management in terms of failure [38]:

- phase of prevention and risk reduction - safety management system is based on the functioning of risk management; risk analysis and assessment help determine the likelihood of a major failure and assess the losses associated with it, moreover, you can develop a scenario of progress of emergency situation in time and design barriers ensuring safety and protection, which significantly reduce the severity of the consequences of a major failure,
- stage of readiness - a logistics plan for rescue operations in case of a major failure, the final result is to develop an emergency plan. There are two aspects in response to the occurrence of a major failure :
 - organization, responding to the question "who does what?" - medical service, government and local administration, fire brigade, police,
 - hardware, allowing counteract the effects of failure - measures to counter a major failure,

- counteracting phase – it means to run operational and rescue plan; main elements of this phase are: start of emergency procedures, strategy and tactics of rescue operations, management, communication and logistical support system.
- phase of corrective action – it takes place after the end of the state of emergency and relies on feedback leading to improve the organization of system security management, it requires treatment-related actions.

Hazard identification should consider the basic factors affecting safety, which can be divided into [25]:

- external factors, resulting from the events that are not the effect of system operation, e.g. the forces of nature, deliberate action of third parties such as vandalism or terrorist attack,
- internal factors, which include, above all: hydraulic conditions of flow, material defects, ageing processes,
- human factors, that is mistakes made during the design, construction and operation, e.g. the lack of proper monitoring, lack or incorrectly conducted repairs and modernization, lack of risk management.

3. Strategies for safety management in terms of identification of operating states

Safety analysis requires the identification of operating states. From the point of view of the system operator one can distinguish the following states:

- all procedures are followed, the operator takes the correct decisions in accordance with the recommendations and indications of subsystems protecting against undesirable events, there is no failure,
- all procedures are followed, in decision making the operator takes into account the indications of protective subsystems, however, failure occurs,
- violation of procedures, in decision-making the operator does not take into account the indications of protective subsystems, failure does not occur,
- violation of procedures, in decision-making the operator does not take into account the indications of protective subsystems and failure occurs.

Complex ergonomics systems work in varying operational conditions, which implies changeability of safety indicators. Theoretical safety is associated with:

- applicable laws, technical requirements,
- protective systems,
- operating procedures.

Actual system safety is associated with:

- technical condition,

- meteorological conditions,
- efficiency of operation,
- system of staff training.

The process of ensuring the security requirements of system include:

- procedures and technical measures,
- organization and methods of operation,
- documentation and executive instructions,
- staff qualification and training programs.

Reactive security management is based on the identification of potential threats on the basis of the hazards existing in Water Supply System. 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 basic assumption is that the risk can be reduced before it occurs. The basis is a rule to take actions in the range of:

- hazard identification,
- analysis and risk assessment,
- taking adequate preventive and corrective actions in risk management.

System security management means managing by assumed objectives in terms of the system. It is implemented according to the principle "Defence In Depth", consisting of:

- minimizing the risk of failure (prevention),
- minimizing the number of failures (active action),
- minimizing the consequences of failure (passive action).

The source of the necessary data for risk analysis are:

- data gathered from the system operation with water companies,
- measurement data,
- data collected from the experts.

The source of uncertainty in the analysis of the aforementioned data is usually incomplete or uncertain knowledge of:

- quantitative and qualitative database on failures,
- assessment of the technical condition of the system,
- inaccurate and incomplete information concerning the location and identification of failure,
- assess the cause-and-effect relationship between failures,
- assessments and expert opinions.

System security management in the operational sense means risk management [18]. Ex ante approach is based on the proactive concept of avoiding or

significantly reducing the consequences of undesirable events. This is a new strategy in relation to the traditional ex post approach characterized by a reactive concept of inference based on information after failure.

There are three phases of risk management:

- risk analysis - threats identification, assessment of their frequency and based on it risk determination,
- risk evaluation - gradation of risk levels and on this basis risk values obtained earlier are assigned to one of three ranges of risk (tolerable, controlled and unacceptable),
- risk control - undertaking actions, within the framework of available economic and social conditions, in order to keep the risk at a tolerable level.

In the assessment of the system safety the following rules are applied:

- if there is the possibility of a major failure in the system one should strive to the level of safety being in force in developed countries,
- security measures for improving safety should be used in areas where they will bring the most effective results,
- no safety measure is perfect, therefore it is required to use several barriers which should provide a compact multi barrier system,
- risk should be considered as an economic category (RCBA – Risk Cost Benefits Analysis).

Safety rules formulated by D. Peterson are as follows:

- safety should be implemented systemically,
- undesirable behavior, conditions and failure are symptoms of irregularities in the security system, causes and circumstances of failures are predictable,
- safety can be managed as any other business,
- safety management procedures help identify and determine the causes of failures,
- dangerous human behavior is a normal reaction to the wrong work environment,
- an effective system of safety is created by technical equipment, employee and management procedures,
- safety system must be adapted to the culture of safety,
- the effectiveness of the security system depends on the weight attributed to safety issues.

4. 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 [16]:

- 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.

5. 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 [77]. 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.

6. Registration of undesirable events

For a complete analysis of undesirable events an extensive database of various operating data is required. Information about the failure should be recorded on a specially prepared for this purpose failure cards. The scheme of protocol of failure removal was shown in the Figure 1. Use of the failure cards will allow to obtain the necessary and accurate data on the performance of the system [69].

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. It should be remembered that the results of work 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 [69, 70].

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: _____	
<small>(name, address, phone number)</small>	
Notification accepted by: _____	
<small>(name of an employee of the water supply company)</small>	
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:	
<small>¹⁾ construction, route, warehouse, workshop, machine room, others.</small>	
<small>²⁾ types and date of the last overhaul, the information on the conducted technical acceptance made after the renovation, others</small>	
<small>³⁾ conduct of staff, operation of protection, protective and signalling devices, others</small>	
<small>⁴⁾ determining who caused failure, determining which staff is to blame e.g. supervision, repair team, suppliers, natural disasters, no information available</small>	
<small>⁵⁾ including the cost of man-hour, losses in fixed assets and working capital, the value of uncompleted production, others</small>	

Figure 1. The exemplary protocol of the Naftoport Oil Terminal failure [69, 70].

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.

7. Matrix methods for risk assessment

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 [41, 42, 65]:

$$r = P \cdot C, \quad (1)$$

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.

The three parametric risk matrix

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 [42, 49, 65]:

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

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 [42, 46, 49]:

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

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.

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 [41, 42, 49, 65].

The four parametric matrix for risk assessment has been proposed, according to the formula [42]:

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

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 $[0,33 \div 27]$ 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 $5 \cdot 10^3$ EUR – $C = 1$,
 - medium - financial loss up to 10^5 EUR – $C = 2$,
 - large - financial loss over 10^5 EUR – $C = 3$,
- category for protection – O . If the total number of points equals:
 - $7 \div 10$ – high protection level - $O = 3$,
 - $12 \div 34$ – 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 3 is: $r = 1.33$ which means the tolerable risk.

8. Description of the logical trees methods

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” [19, 49]. 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 4 the exemplary gates with their quantitative description are presented.

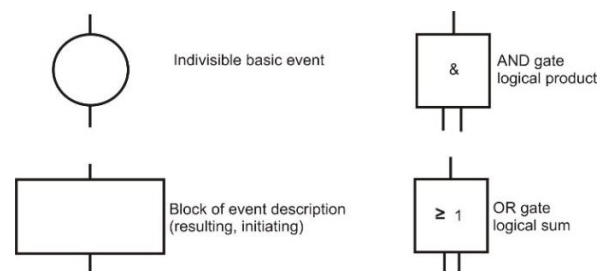
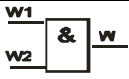
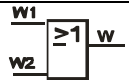


Figure 2. The basic symbols in the fault tree method.

Table 4. 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.

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 [41, 49]. 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 $1 - P_i$.

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 [42, 49, 65]. 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.

9. Development of cause-effect dependence model of undesirable events using Bayes network

Theoretical basis of Bayes network

Technical progress and the development of civilization cause that the requirements for technical objects are increasing. Man as a user of these systems aims to ensure that the objects (systems) which he uses were more durable, reliable, safe, ergonomic and simple to operate [2, 22, 42].

Daily use of technical systems is inseparably linked with the possibility of the occurrence of various types of undesirable events [1, 6, 8]. Proper assessment of the reliability of the technical system should guarantee making the right decisions concerning the choice of the best solutions in terms of technical, economic and reliability aspects, at the stage of design, construction and operation [5, 49, 65] also in hazard and interconnection analysis in port [11, 12, 69].

Indicators and measures that can be used in the process of risk analysis of technical systems, in general, are divided into:

- statistical - determined in accordance with accepted principles of mathematical statistics based on historical data from the operating system,
- probabilistic - determined on the basis of the theory of probability,
- linguistic - describing the risk parameters by means of the so-called linguistic variables, expressed in natural language using words like small, medium, large.

Random nature of the formation of failure causes that related to research is complex and is based primarily on the analysis of operational data and experts opinions. The idea of data exploration involves the use of information technology to find information in databases. There are many data exploration techniques derived directly from mathematical statistics and machine learning.

Analysis of the risks associated with the operation of technical systems requires a lot of detailed information on individual risk factors and their identification and the determination of losses that may occur as a result of the occurrence of undesirable events. Such an analysis is performed under conditions of uncertainty, caused undoubtedly by the complexity of the technical systems and individual components, the degree of dependence between them, as well as difficulties in obtaining the necessary information. The most effective form of knowledge about the uncertain environment is conditional independence which is described by the Bayes' formula.

The main aim of this work is the cause and effect analysis and assessment of undesirable events in technical systems, with particular emphasis on critical infrastructure, using Bayesian networks. Dependencies between individual events are expressed by means of conditional probabilities. The use of Bayesian networks allows determining the probability of the top event and sub-events in the network, which is a basic information for the evaluation of the system safety. The technical system should be monitored in terms of operating parameters and patrolled by teams of operating services. During repair and modernization unauthorized persons should not have access.

The Bayesian networks - BRA (Bayes Risk Analysis) are used in risk analysis due to the ability to model the dependent events. The Bayesian network is upgraded by means of experience and acquired knowledge. The network is modelled by a directed acyclic graph in which vertices represent events and edges represent causal connections between these events. In addition, the Bayesian network is not limited to two states: up state or down state (as in the event tree method and the fault tree method) and may be used for analysing the intermediate states [39, 55, 67].

The occurrence of the event X_j (cause) has some impact on the occurrence of the event X_i (effect). If the impact is not "certain" and can only be determined by the probability, then such an arrangement of events and relations between them can be modelled by a directed graph D [4, 7].

Each event is represented as a vertex of the graph. Relations between events are represented by edges. If the occurrence of the event X_j has some impact on the occurrence of the event X_i (X_i depends on X_j), then there is an edge (X_j, X_i) in the graph model, exiting the X_j and entering the X_i (direction is indicated by the arrow). The vertex X_j is called 'parent' of the vertex X_i . The set of all 'parents' of the vertex X is marked as $\pi(X)$. Figure 3 shows a general schematic diagram of Bayesian networks [62].

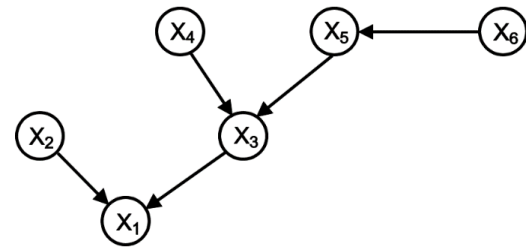


Figure 3. An example of Bayesian networks

For the graph D (figure 3) the dependencies between the events are as follows: $\pi(X_1) = \{X_2, X_3\}$, $\pi(X_2) = \{\emptyset\}$, $\pi(X_3) = \{X_4, X_5\}$, $\pi(X_4) = \{\emptyset\}$, $\pi(X_5) = \{X_6\}$, $\pi(X_6) = \{\emptyset\}$.

The basic assumption in the Bayesian networks is independence of each vertex from the vertices which are not its parents, for example, X_1 is independent of X_4, X_5, X_6 . Most often every event is identified with the corresponding random variable having the same name, on the assumption that all the random variables corresponding to the events are bivalent (1 - an event that occurs, 0 - an event opposed to the event that occurs). The relations between the vertices (events) are expressed by means of the conditional probability. For the vertex X , whose parents are in the set $\pi(X)$, these relations are represented by the conditional probability tables (CPT). In CPT, for the variable X , all the probabilities $P(X|\pi(X))$ (for all the possible combinations of variables from the set $\pi(X)$) must be specified. The table for the vertex that does not have parents includes the probabilities that the random variable X will take its particular values [15, 62].

The Bayes' theorem has the form:

$$P(A/B) = \frac{P(B/A) \cdot P(A)}{P(B)}, \quad (5)$$

where $P(A)$ is a priori probability of the occurrence of event A, $P(B)$ is a priori probability of the occurrence of event B, $P(A/B)$ is a conditional probability of the occurrence of event A under the condition of the occurrence of event B. It is also called a posterior probability because it derives or depends on the value of B. $P(B/A)$ is a conditional probability of the occurrence of event B on condition of the occurrence of event A.

If the network has n vertices, X_1, \dots, X_n , the total probability distribution of all the random variables is shown as the relation [7, 62]:

$$P(X_1, \dots, X_n) = \prod_{i=1}^n P(X_i | \pi(X_i)), \quad (6)$$

For the network in Figure 3, a combined probability distribution is as follows:

$$P(X_1, X_2, X_3, X_4, X_5, X_6) = P(X_1 | X_2, X_3) \cdot P(X_2) \cdot P(X_3 | X_4, X_5) \cdot P(X_4) \cdot P(X_5 | X_6) \cdot P(X_6) \quad (7)$$

To determine the total probability distribution without using the Bayesian network it is necessary to know all the values of $P(X_i, \dots, X_n)$ for all the possible combinations of variables X_1, \dots, X_n , which gives 2^n values of the probabilities. Using the Bayesian network it is sufficient to know the conditional probabilities for each vertex. With given values of its direct ancestors (parents) the total number of required values is given by the formula:

$$LP = \sum_{i=1}^n 2^{|\pi(X_i)|} \quad (8)$$

where n is the number of vertices of the Bayesian network and $|\pi(X_i)|$ is the number of elements of the set $\pi(X_i)$.

10. Example of application - analysis of the risk of interference in the functioning of the seaport using Bayesian networks

The Bayesian network can be used in decision-making model for risk analysis of interference of the complex technical systems. In this work the risk analysis model that can be used in making decisions by the seaport companies (concerning the modernization or renovation), is presented. The model was introduced to the program JavaBayes.

Figure 4 shows the developed Bayesian network diagram that can be used to analyse the risk of interference of the sea port.

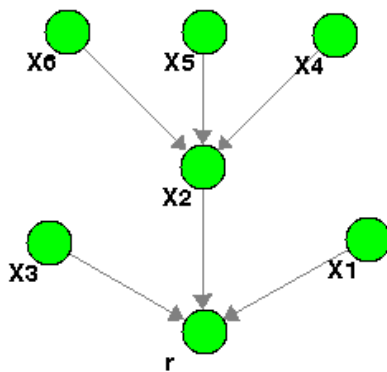


Figure 4. Bayesian networks for analysis of the risk of interference of the sea port

The following symbols were used in the analysis:

- r – the risk of interference in the operation of the seaport in the five-point scale:
 - neglected risk – $r = r_Z$,
 - tolerable risk – $r = r_T$,
 - controlled risk – $r = r_K$,
 - intolerable risk – $r = r_{NT}$,

- unacceptable risk – $r = r_{NA}$,
- X_1 – ship collision with the port construction
- X_2 – seaport fault
 - X_4 – technical failure,
 - X_5 – failure of the control system,
 - X_6 – operator error,
- X_3 – seaport protection against existing threat
 - very little – x_{31} ,
 - little – x_{32} ,
 - medium – x_{33} ,
 - large – x_{34} ,
 - very large – x_{35} .

In the study it was assumed that the event in the given node takes exactly one of the possible values:

- 1 – event occurs,
- 0 – event does not occur.

For each of the vertices belonging to the developed Bayesian network the CPT is defined: $P(r | X_1, X_2, X_3)$, $P(X_1)$, $P(X_2 | X_4, X_5, X_6)$, $P(X_3)$, $P(X_4)$, $P(X_5)$, $P(X_6)$.

Using the formula (2) the values of probability for each risk category, ie. $P(r = r_Z, r_T, r_K, r_{NT}, r_{NA})$ were calculated. Aggregation is performed according to the general formula:

$$P(r = r_Z, r_T, r_K, r_{NT}, r_{NA}) = \sum P(r = r_i | X_1 = X_j, X_2 = X_k, X_3 = X_l) \cdot P(X_1 = X_j) \cdot P(X_2 = X_k) \cdot P(X_3 = X_l) \quad (9)$$

where r_i is a risk value, $i = r_Z, r_T, r_K, r_{NT}, r_{NA}$, X_j is the occurrence or lack of occurrence of the event X_j ; $j = 1, 0$, X_k is occurrence or lack of occurrence of the event X_2 ; $j = 1, 0$, and X_l is a given value of the event X_3 ; $j = x_{31}, x_{32}, x_{33}, x_{34}, x_{35}$.

The model allows to determine the probability of the particular risk level. The result of modelling are the probability values for each risk level. The risk assessment is based on the interpretation of the result (application of risk with the highest and lowest probability of occurrence).

The developed model enables also determining the partial probabilities for the events included in the defined Bayesian network.

The model may be modified or extended depending on the specifics of the analysed technical system.

Example of application

For risk analysis of disruption in the seaport functioning the model using Bayesian networks (Bayes Risk Analysis – BRA), developed in step 3, was used.

Calculations were performed using JavaBayes program, to which the developed model was introduced. For each of the vertices of the Bayesian network shown in Figure 5 the conditional probability tables are defined. For the assumptions, the analysis of risk of disruption in the seaport functioning showed that the risk is at a negligible level. The program also allows determining the probability of intermediate events in the Bayesian network.

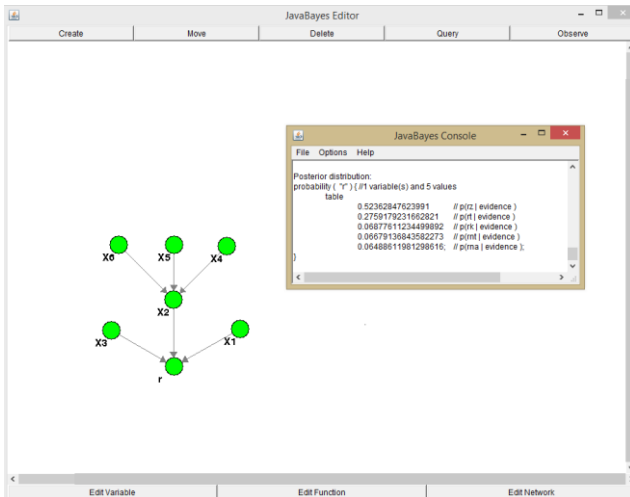


Figure 5. The graphical environment of JavaBayes program - the results of the risk analysis.

In the analysis and assessment of the risk of disturbance in the sea port functioning even the least likely events should be taken into account because they can cause disastrous consequences. For the safety of seaports the most important is the continuity of their operation.

Methods derived from Bayes' theorem are the statistical inference methods that allow to combine information from the generalized data with current information obtained from current research.

The proposed method of risk analysis using the Bayesian network is used primarily in the decision-making processes. The Bayesian network shows cause-and-effect dependencies between events.

Using the developed method one obtains the information as to what level of risk (in the adopted scale) occurs and with what probability. In this way, the proposed model can be an important element in the decision-making process for the operators of the sea port. The model can be modified for all the elements of the sea port. Its use should be part of the safety management and decision-making on exploitation and modernization.

11. The use of the FMEA method to analyze the risk of failure in technical system

The failure modes and effects analysis (FMEA) method is a technique for determining the ways in

which equipment can fail and the consequences of the failure in terms of reliability and safety. The FMEA method belongs to one of the most frequently used tools for quality planning and management analysis and risk assessment because of its versatility. The method of failure modes and effects analysis has been developed for the Apollo space program in the 1960s, as to verify the designs of spacecrafts in order to ensure maximum safety of astronauts. Since that time it is widely used in whole industry, as chemical, electronic, construction, etc. Risk analysis is a key phase of the process of water supply safety management. It consists of threats identification and qualification of their consequences and frequency. Sources of information about the operation of water supply facilities are in the determined form, through standards, regulations, orders and sometimes in the probabilistic form, as field tests, modelling and simulation [14, 31, 32, 48, 53, 68, 70]. The FMEA method can be applied in different areas, it depends on the analysed system and the planned objectives. The failure modes and effects analysis constitutes an inductive method of risk analysis, which for the assumed failure of the component seeks the successive events and determines the possible final effects. The FMEA can be applied at the level of systems, subsystems and components [27, 35, 54]. Before taking decision on the scope and application of the FMEA in a particular system or element it is necessary to consider the overall life-time of the system as well as other activities. The procedure of the FMEA includes many stages, as defining the system and its decomposition into subsystems, objects and elements. Components of the system have the possible failures assigned to them, then the frequency of occurrence and the possibility of detection and prevention are determined and the potential effects and consequences are analysed [IEC 60812]. Also the FMEA analysis include evaluation and assessment of risk associated with various types of threats. The qualitative result of the FMEA is a list of potential threats to technical system users safety. The significance of threat is determined by different parameters with associated point weights [41, 50, 60]. The quantitative result of the FMEA is risk estimation through the point weights, so the final result of the FMEA is the determination of the risk priority number RPN. In the paper the method of analysis and safety assessment of technical system was presented using the failure mode and effects analysis method (FMEA), which assumes independence of events. The developed model was presented on the example of analysis of risk of failure of the technical system.

The main objectives of the FMEA analysis, in accordance with the principle of "continuous improvement", include eliminating defects in the

product or production process by recognizing the reasons for their appearance, taking appropriate preventive actions, avoiding the emergence of recognized and hypothetical defects in new products or processes through the use of knowledge and experience with previous analyzes [24, 28].

12. Example of application - the use of the FMEA method to analyze the functioning of the seaport

Technical assessment of the safety system can be performed using the FMEA method, on the basis of Risk Priority Number - *RPN*, according to the formula [24, 40, 57, 61]:

$$RPN = S \cdot O \cdot D, \quad (10)$$

where:

S – point weight associated with the importance of undesirable event, severity,

O – point weight associated with the frequency of undesirable event, occurrence,

D – point weight associated with the ability to detect undesirable event, detection.

The individual parameters are described by an integer from 1 to 10, which is assumed on the basis of expert knowledge and experience of technical system exploiter. The result of the analysis is the *RPN*, taking values ranging from 1 to 1000. The higher *RPN* value, the lower level of safety [61]. The general assumptions of the method are as follows:

- undesirable events are random, they are inseparable from the functioning of the technical system,
- early identification of potential undesirable events and the introduction of corrective or remedies actions allow to significantly reduce the frequency of these events,
- each undesirable event has a specific cause and effect. The method allows to establish cause and effect relationships in the occurrence of individual undesirable events.

The final effect of the analysis is the value of *RPN*, which can be the basis for adopting the proper management plan, as well as for identifying the weak points of the system. Complete elimination of the causes of undesirable events is impossible, therefore measures should be taken to reduce their frequency, reduce the adverse effects of undesirable events and increase the possibilities of their detection. The safety assessment is based on comparison of the obtained value with the adopted scale. In the paper five levels of safety were proposed [50, 61]:

- neglected level of safety (NLS) – $RPN \leq 20$, in which as a result of the technical system operation there is not any threat to users lives or health,
- tolerable level of safety (TLS) – $20 < RPN \leq 40$, in which as a result of the technical system operation there is not any threat to users lives or health, however, may be felt slight inconvenience associated with its operation,
- controlled level of safety (CLS) – $40 < RPN \leq 60$, in which as a result of the technical system operation, there may be a threat to users' health, but there are sufficient safety barriers,
- intolerable level of safety (ILS) – $60 < RPN \leq 100$, in which as a result of the technical system operation, there may be a threat to users' health,
- unacceptable level of safety (ULS) – $RPN > 100$, beyond which as a result of the technical system operation users are at risk of loss of health or lives

Table 5. The assessment criteria and point weights for the importance of undesirable event – parameter *S*, on the basis of [9, 10, 19, 23]

Importance of undesirable event	Linguistic description	Point weight of <i>S</i> parameter
very low	There is no discernible effects, failure does not affect functioning of the technical system	1
low	Disruptions in the operation of individual subsystems are not felt by the technical system users	2
		3
moderate	Disruptions in the operation of individual subsystems cause a high degree of dissatisfaction by the technical system users	4
		5
		6
high	The system does not work, there may be a threat to the technical system users' health	7
		8
very high	Undesirable event is a threat to the technical system users' health and lives	9
		10

Table 6. The assessment criteria and point weights for the frequency of undesirable event – *O* parameter, on the basis of [9, 10, 19, 23]

Probability of undesirable event	Frequency occurrence	Point weight of <i>O</i> parameter
very low	> 1 for 20 000 d	1
low	(1 for 4000 d – 1 for 20 000 d>	2
	(1 for 1000 d – 1 for 4000 d>	3
moderate	(1 for 400 d – 1 for 1000 d>	4
	(1 for 80 d – 1 for 400 d>	5
	(1 for 40 d – 1 for 80 d>	6
high	(1 for 20 d – 1 for 40 d>	7
	(1 for 8 d – 1 for 20 d>	8

very high	(1 for 2 d – 1 for 8 d >	9
	< 1 for 2 d	10

Table 7. The assessment criteria and point weights for the possibility of not detecting the undesirable event – parameter D, on the basis of [9, 10, 19, 23]

Not detecting the undesirable event	Linguistic description	Point weight of D parameter
very low	Complete monitoring, on-line equipment, potential undesirable event almost certainly will be detected	1
low	Potential undesirable event is detected by automated checks, which lead to error detection and protection from its development	2
		3
moderate	Undesirable event will not be detected until the loss of productivity	4
		5
		6
high	Undesirable event will not be detected until inspection	7
		8
very high	There is no monitoring system, there is no chance to detect potential undesirable event	9

Based on the information contained in Tables 5-7, the appropriate values of parameters *S*, *O* and *D* should be assumed and the RPN value should be determined. All potential undesirable events that may occur in a seaport should be analysed. Table 8 should be complemented by the expert team taking into account the information presented in this article. Table 8 shows an example of analysis for one of the undesirable event.

FMEA method can be an important tool to improve products and processes for managing sea ports, primarily due to the fact that it is quite simple and clear tool. Nevertheless, FMEA can, however, be used to analyse very complex processes.

After determining the risk value, the next step should be to rank the undesirable events in terms of the threat posed to technical system users' and present proposals for corrective or remedies actions (after the given event has reached the NAPB level) and to test their effectiveness.

Corrective or remedies actions include, among others:

- developing a response plan in the event of a crisis situation,
- indication of persons responsible for corrective actions,
- informing the persons responsible for the operation of the technical system about the effects of potential negligence,

- proper organization of the work of renovation teams,
- regular employee training,
- regular inspections of technical condition of individual subsystems/elements,
- developing a method of providing users with information about the threat,
- successive renovation or replacement of the oldest elements of the technical system,
- proper monitoring of the technical system operation.

Table 8. Risk analysis – FMEA method, on the basis of [16, 17, 24, 40, 61].

Phase of the process	Requirement/Function/Characteristic	Potential type of failure	Potential effect of failure	Severity - S	Potential cause of failure	Prevention	Occurrence - O	Control	Detection - D	RPN	Rank
Ensuring the transport safety of the	Ship's entrance to the port	Ship collision with the construction of port	Ship damage	8	Human error	Developing a response plan in the event of a crisis, instruction/training of operators	4	Regular inspections of the technical condition of technical devices, monitoring of the operation of technical devices	3	96 NTPB	1
					Ship failure		3		72 NTPB	2	
Damage to technical devices	Developing a response plan in the event of a crisis, instruction/training of operators	Ship failure	Ship damage	8	Human error	Developing a response plan in the event of a crisis, instruction/training of operators	4	Regular inspections of the technical condition of technical devices, monitoring of the operation of technical devices	3	96 NTPB	1
					Ship failure		3		72 NTPB	2	
Regular inspections of the technical condition of technical devices, monitoring of the operation of technical devices	Developing a response plan in the event of a crisis, instruction/training of operators	Ship failure	Ship damage	8	Human error	Developing a response plan in the event of a crisis, instruction/training of operators	4	Regular inspections of the technical condition of technical devices, monitoring of the operation of technical devices	3	96 NTPB	1
					Ship failure		3		72 NTPB	2	

The main effect of the analysis should be to reduce the probability of occurrence of undesirable events and increase the possibility of their detection.

The FMEA method can be used to analyse the functioning of any technical system, including the sea port. It allows making decisions in the case of lack of complete information, based on the knowledge and experience of the technical system users and external

experts. The proposed method can help to maintain or improve the safety of technical system. In case of lack of data or unreliable data the fuzzy approach can be applied, which can include different opinions and knowledge of experts. The determination of undesirable events that threaten the safety of the operation of technical system is based on the choice that distinguishes the consequences of failures. The performed analysis through identification types and symptoms of threats and the causes of failures can help in determining the effects of failures and create a ranking of criticality, as well as ways to prevent failures and establish projects for remedies actions. Adaptation of the FMEA method is based on the expert's method, from which it is also due to the possibility of its application. The FMEA method constitutes one of the firstly systemic approaches to the analysis of undesirable events in technical system. It can be performed starting from the level of a single element of the system or from the level of the whole system.

13. Conclusions

- 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 relationship between threats and used protective barriers.
- Issues related to risk are analysed in many scientific disciplines, including widely understood environmental engineering. Although they are not the mainstream of design and operational analysis, they are presented as a component describing the basic issues of technical systems safety.
- Obtaining reliable operating data relating to failure, repair, overhaul is essential to conduct proper risk management policy.
- Emergency events (catastrophic) do not appear without a reason but there are a chain of undesirable (critical) 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.
- Identification of the system state can be fraught with errors. There is a possibility that the actual state of the system is identified as other state. In case of binary systems the first and second kind errors are possible. The first type error is to qualify system in upstate as system in down state. The second type error is to qualify system in down state as system in upstate.
- System safety depends on a number of factors, including technical, social, economic, political and environmental. Among the technical factors the reliability of system is crucial. Safety is understood as the ability of the system to protect the internal values from external threats.
- 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.
- 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/>

"Scientific work granted by **Poland's Ministry of Science and High Education** from financial resources for science in the years 2016-2019 awarded for the implementation of an international co-financed project."

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] Bernardo, J.M. & Smith, A.F.M. (1993). *Bayesian theory*. Wiley: Chichester.
- [5] Billinton R. & Allan R.N. (1992). *Reliability Evaluation in Engineering Systems. Concepts and Techniques*. Copyright by Plenum Press. London.
- [6] Birolini, A. (1990). *Qualität und Zuverlässigkeit technischer Systems. Theorie, Praxis, Management*. Copyright by Springer, Berlin.
- [7] Bishop, C.M. (2006). *Pattern Recognition and Machine Learning*. Springer: New York.
- [8] Blischke, W. & Murthy, D.N.P. (2000). *Reliability: Modeling, Prediction and Optimization*. Copyright by J. Wiley and Sons, New York.
- [9] Chen, C.W., Liu, K.F.R., Tseng, C.P., Hsu, W.K. & Chiang, W.L. (2012). Hazard management and risk design by optimal statistical analysis. *Natural Hazards*, Vol. 64, No. 2, 1707-1716.
- [10] Dhillon, S. (1986). *Human Reliability with Human Factors*. Pergamon Press: New York.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] Gilchrist, W. (1993). *Modeling failure mode and effect analysis*, International Journal of Quality & Reliability Management, 10(5), 16-23.
- [15] Grabski, F. & Jaźwiński, J. (2001). *Metody bayesowskie w niezawodności i diagnostyce*. Wydawnictwa Komunikacji i Łączności, Warszawa.
- [16] Gucma L. (2009). *Wytyczne do zarządzania ryzykiem morskim*. Wydawnictwo Naukowe Akademii morskiej w Szczecinie. Szczecin 2009.
- [17] Gucma, L. (2005). *Modelowanie czynników ryzyka zderzenia jednostek pływających z konstrukcjami portowymi i pełnomorskimi*, Wyd. 44, Studia - Akademia Morska w Szczecinie.
- [18] 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*, no. 78, 227-238.
- [19] Hadipriono, F. C. & Toh, H.S. (1989). Modified fault tree analysis for structural safety. *Civil Engineering and Environmental Systems*, 6 (4), 1989, 190-199.
- [20] Haimes. Y.Y. (2009). On the Complex definition of risk: a systems-based approach, *Risk Analysis*. 29 (12), 1647-1654.
- [21] Haimes, Y. Y. (1998). Risk analysis of fracture and failure, *Materials Research Innovations*, 2(1)/1998, pp. 16-21.
- [22] Haimes, Y.Y. (1998). *Risk Modelling, Assessment and Management*. Wiley, New York.
- [23] Haimes, Y.Y, Moser D. & Stakhin, E. (2006). Risk Based Decision Making in Water Resources, *Journal of Infrastructure Systems*, ASCE, 2006 12, 401-415.
- [24] Hamrol, A. & Mantura, W. (1999). *Zarządzanie jakością – teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa-Poznań.
- [25] Hartig, J.A. (1983). *Bayes theory*. Springer, New York.
- [26] Hastak H. & Baim E. (2001). Risk factors affecting management and maintenance cost of urban infrastructure. *Journal of Infrastructure Systems*, 7 (2), 67-75.
- [27] Hubbard, D.W. (2009). *The failure of risk management*, Wiley. New York.

- [28] IEC 60812:2006. *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*.
- [29] Kaplan, S. (1997). The words of risk analysis, *Risk Analysis*, 7(4), 407-417.
- [30] Kaplan, S. & Garrick, B.J. (1981). On the quantitative definition of risk. *Risk Analysis*. 1(1), 1981, s. 11-27.
- [31] Kołowrocki, K. & Soszyńska-Budny, J. (2011). *Reliability and Safety of Complex Technical Systems and Processes: Modeling – Identification – Prediction – Optimization*. Springer, London.
- [32] Kołowrocki, K., Kuligowska, E. & Soszyńska-Budny, J. (2017). *Critical infrastructure operation process including operating environment threats*. *Journal of Polish Safety and Reliability Association Summer Safety and Reliability Seminars*, 8(2), 7–14.
- [33] Kuo, W. & Zuo, M. J. (2003). *Optimal reliability modeling*. Copyright by Wiley, New Jersey.
- [34] Kwietniewski M., Roman M. & Kłoss-Trębaczkiwicz H. (1993). *Niezawodność wodociągów i kanalizacji*. Wydawnictwo Arkady, Warszawa.
- [35] Liu, H. C., Liu, L., Bian, Q. H., Lin, L., Dong, N. & Xu, P. C. (2011). *Failure mode and effects analysis using fuzzy evidential reasoning approach and grey theory*, *Expert Systems with Applications*, 38, 4403–4415.
- [36] Liu, H.C., Liu, L. & Liu, N. (2013). *Risk evaluation approaches in failure mode and effects analysis: A literature review*, *Expert Systems with Applications*, 40, 828–838.
- [37] McGill W.L., Ayyub B.A. & Kaminskiy M. (2005). *Risk Analysis for Critical Asset Protection*. *Risk Analysis*, Wiley Blackwell, 27(5), 1265-1281.
- [38] Pham, H. (2003) *Handbook of Reliability Engineering*. Springer, London.
- [39] 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*.
- [40] Pillay, A. & Wang, J. (2003). *Modified failure mode and effects analysis using approximate reasoning*, *Reliability Engineering & System Safety*, 79, 69–85.
- [41] Rak J. (2009). *Bezpieczeństwo systemów zaopatrzenia w wodę*. PAN, Instytut Badań Systemowych. Warszawa.
- [42] Rak J. (2004). *Istota ryzyka w funkcjonowaniu systemu zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
- [43] Rak J. (2004). *Metody matrycowe oceny ryzyka w systemach zaopatrzenia w wodę*. Ośrodek Informacji "Technika Instalacyjna w Budownictwie", *INSTAL*, z. 3, 42-45.
- [44] Rak J. (2003). *Metoda szacowania ryzyka zagrożenia systemu zaopatrzenia w wodę*. PZITS O/Dolnośląski, *Ochrona Środowiska*, z. 2, 33-36.
- [45] Rak J. (2005). *Podstawy bezpieczeństwa systemów zaopatrzenia w wodę*. Wydawnictwo – Drukarnia Liber Duo Kolor Lublin, Monografie Komitetu Inżynierii Środowiska PAN, Lublin, vol. 28, 1-215.
- [46] Rak J. (2003). *Ryzyko w funkcjonowaniu operatora SZW - analiza ergonomiczna*. Wydawnictwo Sigma Not, Gaz, Woda i Technika Sanitarna, t. LXXVII, z 6, 211-214.
- [47] Rak J. & Kwietniewski M. (2011). *Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
- [48] Rak, J. & Pietrucha-Urbanik, K. (2015). *New directions for the protection and evolution of water supply systems - smart water supply*. *Czasopismo Inżynierii Lądowej, 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
- [49] Rak J.R. & Tchórzewska-Cieślak B. (2007). *Czynniki ryzyka w eksploatacji systemów zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
- [50] Rak, J. & Tchórzewska-Cieślak B. (2005). *Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
- [51] Rak J. & Tchórzewska-Cieślak B. (2006). *Metoda zintegrowanej oceny ryzyka awarii w podsystemie dystrybucji wody*. Wydawnictwo Sigma NOT. Gaz, Woda i Technika Sanitarna. z. 1, 11-15.
- [52] Rak J., Tchórzewska-Cieślak B. (2003). *Ryzyko w eksploatacji systemów zbiorowego zaopatrzenia w wodę*. Wydawnictwo Seidel-Przywecki Sp. z o.o.
- [53] Rak, J. & Tchórzewska-Cieślak, B. (2010). *The possible use of the FMEA method to ensure health safety of municipal water*, *Journal of KONBiN* 2010, No. 2, 3 (14, 15), 143–154.
- [54] Rak, J. & Tchórzewska-Cieślak, B. & Studziński, J. (2013). *Bezpieczeństwo systemów zbiorowego zaopatrzenia w wodę*, Instytut Badań Systemowych PAN, Warszawa.

- [55] Ritter, G. & Gallegos, T. (2002). *Bayesian object identification: variants*, Journal of Multivariate Analysis 81: 301-334.
- [56] Schneeweiss W. G.: *Reliability Modeling*. Copyright by Lilole – Verlag, Hagen, 2001.
- [57] Sharma, R.K., Kumar, D. & Kumar P. (2005). *Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling*, International Journal of Quality & Reliability Management, 22(9), 986–1004.
- [58] Smith D.J. (2001). *Reliability, Maintainability and Risk*. Copyright by Butterworth – Heinemann.
- [59] Stamatis, D.H. (1995). *Failure mode and effect analysis: FMEA from theory to execution*, ASQC Press, New York.
- [60] Stewart, M. & Melchers, R. (1997). *Probabilistic risk assessment of engineering systems*, Copyright by Chapman and Hall, London.
- [61] Szpak, D. (2017). *Method of water consumers safety analysis and assessment*. E3S Web of Conferences, 17, 00092, 1–8.
- [62] Tchórzewska-Cieślak, B. (2014). *Bayesian model of urban water safety management*. Global NEST Journal, Vol 16, No 4, pp 667-675.
- [63] Tchórzewska-Cieślak, B. (2010). Failure risk analysis in the water distribution system. *Summer Safety & Reliability Seminars. Journal of Polish Safety and Reliability Association*, 1, 247–255.
- [64] Tchórzewska-Cieślak, B. (2011). *Metody analizy i oceny ryzyka awarii podsystemu dystrybucji wody*. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów.
- [65] Tchórzewska-Cieślak, B. (2008). *Niezawodność i bezpieczeństwo systemów komunalnych*. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów.
- [66] Tchórzewska-Cieślak, B. (2009). Water supply system reliability management. *Environmental Protection Engineering*, 35, 29–35.
- [67] Tchórzewska-Cieślak, B. & Pietrucha-Urbanik, K. (2015). *Risk management in water distribution system operation and maintenance using Bayesian theory*. Progress in Environmental Engineering - Tomaszek and Koszelnik (eds.). Taylor & Francis Group, London.
- [68] Tchórzewska-Cieślak, B. & Szpak, D. (2015). *Propozycja metody analizy i oceny bezpieczeństwa dostawy wody*, Ochrona Środowiska, 37(3), 43–47.
- [69] 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.
- [70] Tchórzewska-Cieślak, B., Pietrucha-Urbanik, K. & Szpak, D. (2017). *Development of cause-effect dependence model of undesirable events using Bayes network*. 2017, Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, 8(1), 149–156.
- [71] Tchórzewska-Cieślak, B., Pietrucha-Urbanik, K. & Szpak, D. (2017). *Review of methods for identifying threats including the critical infrastructure systems within the Baltic Sea*. Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, 8(1), 139–148.
- [72] Tchórzewska-Cieślak, B., Pietrucha-Urbanik, K. & Szpak, D. (2018). *The use of the FMEA method in the analysis and assessment of technical systems safety*. Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, 9(3), 95–100.
- [73] Thompson, W.E. & Springer, M.D. (1972). *Bayes analysis of availability for a system consisting of several independent subsystems*. IEEE Transactions on Reliability, 21(4), 212–218.
- [74] Wang, Y.M., Chin, K.S., Poon, G.K.K. & Yang, J.B. (2009). *Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean*, Expert Systems with Applications, 36, 1195–1207.
- [75] Zhang, T.L. & Horigome, M. 2001. *Availability and reliability of system with dependent components and time-varying failure and repair rates*. IEEE Transactions on Reliability. 50(2), 151-158. DOI: 10.1109/24.963122.
- [76] Zio, E. (2007). *An introduction to the basics of reliability and risk analysis*, Series on Quality, Reliability and Engineering Statistics, Singapore.
- [77] Zio, E. (2009). *Computational Methods for Reliability and Risk Analysis*. Springer.
- [78] Zitrou, A., Bedford, T. & Walls, L. 2010. *Bayes geometric scaling model for common cause failure rates*. Reliability Engineering & System Safety, 95(2): 70-76. DOI: 10.1016/j.ress.2009.08.002.