UDC 658.382:614.8:519.2
DOI: 10.15587/2706-5448.2026.353068

Zakhar Matsuk,
Anatolii Bielikov,
Ihor Maladyka,
Oleksandr Tyshchenko,
Vadim Kharchenko

SYMMETRIC APPROACH TO INDUSTRIAL SAFETY RISK ASSESSMENT BASED ON MUTUAL PROBABILITY CORRESPONDENCE

The object of research is the process of assessing the level of safety of complex technical systems of critical infrastructure under conditions of uncertainty. The problem of the limitations and asymmetry of risk assessment methods was investigated. Risk assessment processes were studied based on IAEA data, using a combination of theoretical and computational modeling methods. The theoretical basis was based on factor risk analysis. Dynamic and temporal dependencies were taken into account using a synthesized modular scalable dynamic Bayesian network (MSDBN), which integrated local components and their interaction into hierarchical models. Probabilistic assessments were performed using Monte Carlo simulation, as well as structural and hybrid learning algorithms for Bayesian networks. The limitations, asymmetry, and dependence on expert opinion of traditional risk assessment methods were shown. It was shown that the synthesis of Bayesian networks and the Monte Carlo method as basic approaches meets the criteria for symmetry in risk event modeling. It was established that the maximum adequacy of risk event prediction is achieved when using a modular Bayesian architecture with a multi-criteria approach through assessing the compliance of production system elements with regulatory requirements, historical analogies and/or modeling results. MSDBN improves the quality and validity of management decisions, is integrated into automated control systems, serves as a tool for digital twins, can be used in the educational process, is symmetric and suitable for assessing the effectiveness of security measures. The proposed approach is useful for state, defense and industrial systems, including under conditions of uncertainty.

Keywords: *probabilistic risk assessment, industrial safety, industrial safety, dynamic Bayesian modeling, Monte Carlo modeling, symmetric probabilistic modeling.*

Received: 23.12.2025
Received in revised form: 14.02.2026
Accepted: 25.02.2026
Published: 28.02.2026

How to cite
Matsuk, Z., Bielikov, A., Maladyka, I., Tyshchenko, O., Kharchenko, V. (2026). Symmetric approach to industrial safety risk assessment based on mutual probability correspondence. Technology Audit and Production Reserves, 1 (2 (87)), 99–112. https://doi.org/10.15587/2706-5448.2026.353068

1. Introduction

Historically, safety requirements were formed reactively – based on the analysis of the consequences of accidents, wars, man-made disasters and other extraordinary events. Regulatory regulation was gradually institutionalized, and supervision and control became mandatory components of safety. The first state acts on the prevention of hazards date back to the Zhou dynasty (China, approximately 1100 BC) [1]. Thus, safety standards served as a formalization of the accumulated experience historically.

Subsequently, there was a transition from a reactive to a proactive paradigm of safety (risk) management. In accordance with the requirements of ISO 31000:2018 [2], risk is now defined as the impact of uncertainty on the achievement of goals. Safety in this context is considered as a state of acceptable risk, achieved through systematic identification, analysis, assessment and treatment of risk [2, 3].

Modern approaches to safety riskology allow to take into account the complexity of technical and socio-technical systems. The most common is the combination of methods – expert assessments, structural analysis (FTA), simulation modeling (Monte Carlo), Bayesian networks and "bow-tie" models [3]. The need for their integration indicates the multidimensionality of the risk assessment task and the limitations of existing risk management methods.

Research on safety riskology covers the following areas:
- nuclear safety, where the concept of "safety culture" has been formed;
- modeling of the degradation of complex technical systems;
- multi-state stochastic models;
- integration of Bayesian networks with fuzzy logic;
- analysis of the human factor as a source of systemic vulnerability, etc.

Key areas of modern research include:
- study of the risks of failures of complex technical systems (energy networks, transport systems, nuclear facilities);
- study of the impact of resource scarcity and climate change in connection with social conflicts on technogenic safety;
- development of risk assessment methods using machine learning, big data analysis and scenario planning to predict complex threats.

The approaches presented in the priority areas are empirically confirmed: in nuclear energy, the need for integrated safety management is emphasized, combining technical, organizational and human aspects and focusing on probabilistic risk assessment to reduce the frequency of accidents [4]. In the field of traffic safety, multi-state hybrid models of train braking systems have been proposed for risk assessment, which take into account spatial variability of parameters and simulate the evolution of failures, supporting forecasting [5]. In industrial safety, a combination of Bayesian networks and fuzzy logic is used to model risks in complex systems with uncertainty [6], as well as optimization of occupational and ergonomic risk management based on bow-tie models [7]. The impact of the human factor is assessed in studies [8], and a systematic review [9, 10] confirms the relevance of the complex factor approach, continuous risk assessment and dynamic modeling of risk evolution.

The relevance of research in security riskology is justified by the trends towards the complexity of the technosphere, the growth of the spectrum of uncertainties associated with a decrease in the level of security at the system level [11].

Analysis of the modern methodology of security riskology indicates that it lacks a probabilistic assessment of the effectiveness of security measures, an assessment of the probability ratios of counter-dominant events (threats and measures) to establish the level of system security [12, 13]. For example, in [4] scientists emphasize the probabilistic assessment of risks, but without attention to measures; in [5–8] similarly, the probabilistic assessment of measures is out of the attention of scientists. The regulatory framework of riskology [1, 2] also does not take into account the symmetry of counter-dominant events as an element of risk processing and assessment.

Critical analysis of modern approaches allows to establish the following features of the modern methodology of security riskology:

1. Predominant focus on threat modeling.

The probability of dangerous events is assessed in sufficient detail, while the probability of the effectiveness of security measures is often taken ex post facto, as a fixed or expertly determined value.

2. Epistemological uncertainty of the second order.

Methods with expert participation depend on cognitive limitations and individual characteristics of experts, which reduces the reproducibility of results.

3. Insufficient integration of regulatory requirements and historical retrospective into stochastic models of assessing the level of security. Regulatory documents and historical precedents are mostly considered as external regulatory frameworks and are not parameterized as variables of security models.

4. Lack of a formalized symmetric approach. Existing studies have not developed a mechanism for establishing the level of safety through the ratio of the probabilities of counter-dominant events – threats and safety measures.

On the examples of major man-made disasters, in particular: the Chernobyl disaster, the Fukushima nuclear power plant accident, it is observed that the key role in the realization of risk events was played not only by threats, but also by the effectiveness or ineffectiveness of the implementation of safety measures in specific conditions of the system's functioning. This confirms the need for quantitative modeling of their mutual compliance.

Therefore, existing approaches to safety riskology remain asymmetric in terms of taking into account the mutual influence of counter-dominant events.

The scientific problem lies in the lack of a formalized symmetric probabilistic approach that would allow determining the level of safety of a complex system as a function of the ratio of the probability of threat realization and the probability of the effectiveness of safety measures, taking into account regulatory requirements, historical data and modeling results as parameterized variables. The issue of quantitatively determining the state of mutual compliance of counter-dominant events in a dynamic environment remains unresolved.

The aim of research is to develop a symmetric probabilistic approach to assessing the level of safety of complex critical infrastructure systems based on modeling the mutual correspondence of the probabilities of the implementation of counter-dominant events.

To achieve the aim, the following objectives were set:

- to perform a theoretical and methodological analysis of modern approaches to risk assessment in order to identify asymmetric limitations and formulate criteria for a symmetric stochastic model;
- to develop a formalized mathematical and algorithmic model of a symmetric description of threats and security measures with the introduction of the safety level function as an integral indicator of the mutual correspondence of probabilities;
- to carry out empirical testing of the model on the example of man-made disasters, to conduct a quantitative assessment of the adequacy of the results obtained and to analyze the influence of organizational and technical factors within the framework of a symmetric formulation.

The hypothesis of research is the assumption that the introduction of a symmetric probabilistic formalization of the mutual correspondence of threats and security measures allows to quantitatively describe the level of security as an integral function of their ratio and reduces the methodological asymmetry of existing risk-oriented models.

2. Materials and Methods

The object of research is the process of assessing the level of safety of complex technical systems of critical infrastructure under conditions of uncertainty.

The subject of research is symmetric probabilistic modeling of the mutual correspondence of counter-dominant events (threats and security measures) in the process of establishing the level of system security.

The data for research were obtained from official open sources of the IAEA (1957–2025). Aggregated data on the frequency of failures, vulnerabilities, attacks and the effectiveness of safety barriers of nuclear power facilities were used. The data were selected according to the criteria of reliability and availability for parameterization.

The methodological basis of the work is the well-known risk-oriented approach [2, 3], where risk is interpreted as the impact of uncertainty on the achievement of goals.

The work used:

- probability theory;
- principles and methods of stochastic modeling;
- elements of Bayesian updating;
- machine learning methods;
- retrospective analysis (qualitative and quantitative) of man-made events;
- structural-logical analysis of existing risk assessment methods.

The choice of methods was determined by the aim of research.

The research methods were selected according to the following criteria:

- the possibility of formalizing both threats and security measures in a single stochastic space, including in the symmetric opposition mode;
- the ability to take into account and assess uncertainty;
- the possibility of integrating regulatory requirements and historical data as parameterized constraints;
- the reproducibility of results;
- the suitability for the analysis of rare events.

The studies were based on the analysis of alternative approaches (risk matrices, FTA/ETA, expert methods, "big data" analysis models) which showed that they are mainly focused on threat modeling and do not provide a symmetric description of the probability of the effectiveness of security measures.

In view of the above, during the research, stochastic modeling was used with the formalization of the ratio (relative analysis) of the probability of threat realization (P_t) and the probability of positive-compensatory impact (effectiveness) of security measures (P_c).

During the research, the following formal formulation of the symmetric approach was used

$$S_s = B_s,$$

where S_s – the state (level) of relative safety and system performance; B_s – an indicator of the state of relative safety and system performance (safety level). B_s is the product of the ratios (balance) between the values of the probability of occurrence of events caused by the action of external and internal factors and/or conditions (hereinafter referred to as threats) that can negatively affect the state (level) of safety, and the performance of system elements at all stages of the system's existence, taking into account all system needs and the values of the probability of a positive-compensatory effect of the corresponding preventive measures to counter the specified threats, within the framework of modern professional concepts, knowledge, ideas and factors and/or other conditions that characterize the actual state of system protection from the action of the specified threats [12, 13].

During the research, the safety level function was introduced

$$S_s = f\left(\frac{P_t}{P_c}\right) \in \left[0;1\right],$$

where S_s – the state (level) of relative safety and system performance; P_t – the probability of threat realization; P_c – the probability of positive compensatory impact (effectiveness) of safety measures.

As an empirical basis for research, in order to test the developed approach, an analysis of the causes of man-made disasters at the Chernobyl NPP (1986) and the Fukushima NPP (2011) was used.

The study models are limited by the following limitations:

- event probability estimates depend on data availability;
- Bayesian updating assumes the correctness of prior distributions;
- the models do not take into account nonlinear synergistic effects of high order.

During the research, the key was not so much the use of known approaches, but the formation of a symmetry criterion and a new approach to assessing the level of system safety. The work emphasizes this, as well as the fact that existing approaches do not provide symmetric assessment properties.

The work is based on the theoretical principles of factor analysis, which were used to identify and assess key risk factors. Dynamics and time dependencies were assessed using MSDBN, which combined hierarchical models with local components and their systemic interaction.

The research was conducted taking into account the following assumptions:

- the mathematical apparatus for modeling the probability of counter-dominant events can be symmetric;
- when determining the probability of a risk event, the probability of a positive impact of organizational and technical measures (causes) can be expressed numerically, respectively, they can be combined, because the final value is dimensionless.

For probabilistic assessment, Monte Carlo simulation methods were used, as well as PC and MMHC learning algorithms for building Bayesian networks.

Computational experiments were conducted on computer systems with Intel Core i7-12700H processors (32 GB RAM) running Windows 11 (Microsoft, USA). Python 3.12 software (Python Software Foundation, USA) was used to process the simulation data. PySpark software (Apache Software Foundation, USA) was used for distributed computing. Network structures were created using the decision tree algorithm (CRT). Monitoring and visualization were provided by the Grafana (Grafana Labs, USA) and Plotly (Plotly, Inc., USA) platforms. SymPy libraries (Python Software Foundation, USA) and statistical testing were used for factor analysis. Dynamic scenarios were experimentally simulated, based on historical data of accidents at the Chernobyl and Fukushima nuclear power plants, with a time horizon of 1 to 100 hours and sampling intervals of 1 to 60 minutes. The model load varied from 1000 to 10000 Monte Carlo simulation iterations. The confidence index was chosen at the level of 95%.

The calculations were performed in an isolated virtual environment with the uncertainty for key factors fixed at 10%; the experiments were repeated three times to validate stability. Using the mathematical apparatus of the developed approach, the Grok 4.1 neural network was trained to automate the solution of problems of determining the safety level of Ukrainian NPPs (Example 2).

3. Results and Discussion

3.1. Theoretical and methodological analysis and criteria of a symmetric model.

In order to ensure the objectivity and effectiveness of such a choice, a number of criteria were formulated to assess the suitability of methods for modeling the probability of counter-dominant events.

The main criteria included the following:

- universality/symmetry of the modeling method (the ability to apply the method to model positive and negative events simultaneously);
- ability to work with critical events with any frequency (periodicity) of occurrence;
- absence or minimal dependence of the method on expert opinion at the modeling and interpretation stage;
- certainty (unambiguity, quality) of the initial data;
- justification for the choice of probability distribution;
- resistance to errors;
- ability to assess the uncertainty of the results;
- the model must be transparent for verification and validation – it must be tested on real or model data;
- compatibility with other analysis methods;
- ability of the method to be modified with new data;
- ability to add new factors and criteria;
- ability to update based on new data;
- adaptation of the model without its complete reconstruction;
- operational support for changes in the system structure;
- automation of the update process;
- sufficient mathematical accuracy;
- interpretability;
- convenience and ease of scaling;
- relative ease of automation.

In the course of the research, it was found that the following approaches partially or fully meet the above criteria:

- *Bayesian trust networks* (*BN*)*:* allow modeling complex cause-and-effect relationships between threats and corresponding security measures, providing the ability to assess the probabilities of various scenarios, taking into account both internal and external influences – these are important probabilistic directed acyclic graphical models that can effectively characterize and analyze uncertainty, which is a common problem in real systems, as well as solve the problems of explosive growth of the state space [6];
- *Monte Carlo simulation* (*MCS*)*:* provides modeling of a wide range of scenarios, including rare and critical events, allowing to obtain sufficiently accurate quantitative assessments of risks under conditions of uncertainty.

Moreover, BN is the only one of these methods that:

- supports dynamic updating based on new data without the need for a complete reconstruction of the model;
- is easily scalable and adapts to changing conditions;
- takes into account interdependencies between factors and compensatory measures.

3.2. Mathematical formalization

The conducted studies have shown that, along with the need to optimize the process of assessing the probability of threat realization, there is a growing need to create methods that allow simultaneously determining both the probability of threat occurrence and the effectiveness of the compensating (positive) impact of security measures. In this case, factors and conditions that characterize the real level of system security should be taken into account.

For illustration, an example of a developed symmetric risk-oriented probabilistic approach to ensuring industrial safety, built using a modified method, was presented.

The approach was developed for an objective quantitative assessment of technogenic risks by building Bayesian networks based on:

– *NormScore* (*NS*) – assessment of compliance of system elements with current regulatory requirements;

– *HistScore* (*HS*) – assessment of compliance of negative factors with known historical events (analogies);

– *ModelScore* (*MS*) – assessment of the results of physical or computer modeling (in the presence of uncertainty or the absence of direct regulatory/historical analogies);

– *UncertaintyScore* (*US*) – aggregated assessment of confidence in the calculation, taking into account the presence or absence of three types of confirmation (three sources).

The following structure of the BN model is proposed:

BN is built in the form of a directed acyclic graph, where:

– *Vertices* (*nodes*) – individual events, factors or technical characteristics;

– *Edges* – cause-and-effect relationships between events.

Each node has a conditional probability table (Conditional Probability Table, CPT), which is filled using a special algorithm based on three types of estimates.

Procedure for filling in the CPT.

For each event node *A*, a trio of weighted indicators is formed:

1. *NS*(*A*) ∈ [0, 1] – assessment of the compliance of the event or state with the established standards (1 – full compliance, 0 – significant violation). Usually this indicator reflects the weight of the event or state in the overall scenario.

2. *HS*(*A*) ∈ [0, 1] – degree of similarity/similarity of the event or state with already known cases in previous incidents (1 – complete coincidence, 0 – absolute uniqueness).

3. *MS*(*A*) ∈ [0, 1] – result of modeling, which determines the probability or criticality of the event.

4. *US*(*A*) ∈ [0, 1] – indicator of confidence or level of uncertainty, calculated as the arithmetic mean of the parameters *NS*, *HS* and *MS*.

The reliability of event *A* in CPT can be determined by aggregating it

$$P_i = \frac{NS(A)+HS(A)+MS(A)}{w_n+w_h+w_m}, \qquad (1)$$

where w_n, w_h, w_m, ∈ {0,1} – indicators of the presence of the corresponding source (1 – present, 0 – absent).

If, for example, historical data are not available, the formula automatically redistributes the weight between *NS* and *MS*. This allows the model to adapt to real conditions without the need for subjective intervention, which corresponds to the principles of the proposed approach, according to which estimates should reflect the real state of the system. Generalizing (informally, in the case of a chain connection of factors through BN), let's obtain the following expression

$$(Accident = True) = 1 - \prod_{i=1}^{n}(1-P_i), \qquad (2)$$

where P_i – an indicator reflecting the influence of factor *i* in a certain state (true – the factor is present, false – the factor is absent).

Accordingly, the level of confidence (*US*) in such an assessment in this case can be determined as

$$US = \frac{N+H+M}{3}, \qquad (3)$$

where *N*, *H*, *M* = 1, if *NS*, *HS*, *MS* > 0, otherwise 0.

Regarding the definition of categories and interpretation of results.

For ease of interpretation, the results of determining the probability of *P* are better evaluated by categories, where:

$P < 0.001$ – absolutely low probability;

$0.001 \le P < 0.01$ – the probability of the event exists, but is low;

$0.01 \le P < 0.1$ – the probability of the event is moderate;

$0.1 \le P < 0.5$ – the probability of the event is significant;

$0.5 \le P < 0.9$ – the probability of the event is high;

$P \ge 0.9$ – the event is almost inevitable.

3.3. Testing on examples of man-made disasters

Example 1. Applying the proposed approach (1)–(3), a general assessment of the probability of disasters at the Chernobyl NPP (1986) and the Fukushima NPP (2011) was carried out using the "backward" method, as of the date of the events.

A general list of the causes of the above-mentioned disasters, compiled based on the analysis of materials from the investigation commissions and reports of the IAEA Directorate [14, 15], Tables 1, 2.

Table 1

Table of the description of the causes of the Chernobyl disaster (USSR, 1986)

Description of events at node *A*	*NS*/*MS*	*HS*	P_i
Technical causes and design flaws			
A1. Positive steam reactivity coefficient	0.15	0.8	0.37
A2. Design flaws in control and protection rods	0.12	0.6	0.28
A3. Operation at dangerously low power	0.06	0.3	0.14
A4. Insufficient speed and reliability of emergency protection	0.08	0.5	0.22
A5. Lack of control of operational reactivity reserve	0.05	0.2	0.1
A6. Prolonged shutdown of important safety systems	0.07	0.4	0.18
A7. Uneven distribution of reactor power over the height of the core	0.05	0.4	0.17
Organizational reasons			
A8. Low level of safety culture at all levels	0.12	0.9	0.38
A9. Violation (unauthorized change) of regulations during reactor operation	0.1	0.7	0.3
A10. Ignoring incidents (Leningrad-1 in 1975, Ignalina in 1983)	0.1	0.95	0.38
A11. Ignoring known design flaws of the NPP	0.09	0.85	0.34
A12. Weak supervision/control by the regulator	0.09	0.85	0.34
A13. Insufficient training of personnel for beyond-design-basis accidents	0.08	0.8	0.32
A14. Shortcomings of instructions, contradictory requirements of the technical documentation of the plant	0.07	0.75	0.3
A15. Decision to disable the most important safety systems	0.07	0.4	0.18
A16. Insufficient analysis of the safety of the NPP when changing the test plan	0.06	0.5	0.21

Table 2

Table describing the causes of the Fukushima nuclear power plant disaster (Japan, 2011)

Description of events at node *A*	*NS/MS*	*HS*	P_i
Technical causes and design flaws			
A1. Insufficient protection against beyond-design-basis events (tsunami + earthquake)	0.079	0.3	0.153
A2. Complete loss of power supply	0.042	0.7	0.261
A3. Location of power supply sources in the area of probable flooding	0.021	0.8	0.281
A4. Limited capacity of emergency batteries	0.021	0.5	0.181
A5. Lack of autonomous heat removal systems	0.013	0.6	0.209
A6. Disconnection of the isolation capacitor (IC) at unit 1 of the NPP	0.011	0.2	0.074
A7. Lack of reliable ventilation for hydrogen removal	0.008	0	0.005
A8. Shared ventilation ducts between NPP units	0.008	0.1	0.039
Organizational reasons			
A9. Low level of safety culture ("overconfidence in safety")	0.05	0.7	0.267
A10. Ignoring the incident at the NPP (1991, lack of protection of generators from flooding)	0.159	1.0	0.439
A11. Ignoring the practice of assessing the risk of accidents at several reactors in the event of maintenance complications due to infrastructure destruction	0.124	0.2	0.149
A12. Underestimation of risk (lack of tsunami probability assessment in the NPP project), failure to implement IAEA recommendations on its assessment	0.159	0.7	0.339
A13. Inadequate training of personnel for beyond-design-basis accidents	0.081	0.8	0.321
A14. Accident management manuals did not cover beyond-design-basis circumstances and events	0.095	0.8	0.33
A15. Lack of regulations for manual control of the capacitor (IC) EB No. 1	0.074	0.3	0.149
A16. Weak supervision/control by the regulator. Lack of accounting for beyond-design-basis accidents	0.053	0.7	0.269

In our case, the analysis is facilitated because:

- risks are assessed post-facto;
- causes are established based on the results of investigations and global analysis of events;
- investigation commissions decided that the reactor accidents were caused by the coincidence of all causes and circumstances together.

In both cases, a retrospective analysis of the HS value was conducted, based on open data sources [14–17].

In both cases, the fact of the occurrence of disasters at the specified nuclear power plants was accepted as a result of physical modeling of risk events.

Thus, the values (*NS*) and (*MS*) in the events that occurred, in both cases, can be considered both "weighted" and identical at the same time.

Using the proposed method, it is possible to construct a cause-and-effect diagram of the influence of technical and organizational causes of the Chernobyl disaster, with their logical connections, on the realization of the disaster risk (Fig. 1).

A description of the causes of the Chernobyl disaster (USSR, 1986) is given in Table 1.

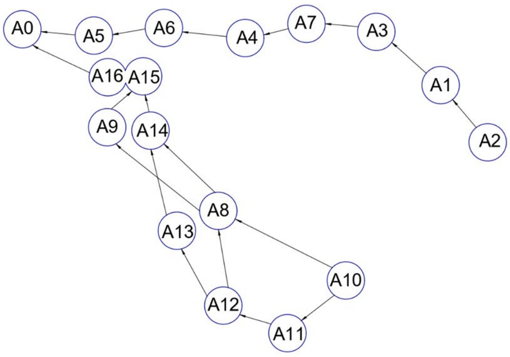

Fig. 1. Diagram of the influence of technical (*A1–A7*) and organizational (*A8–A16*) causes of the Chernobyl disaster on the realization of the risk of a disaster, where *A0* is a disaster

Using the proposed approach, a cause-and-effect diagram of the influence of organizational causes of the Chernobyl disaster on the emergence of technical causes (technical result of organizational violations) was constructed, with a demonstration of the logical connections of the causes of the accident on the diagram (Fig. 2).

The risk of a disaster at the Chernobyl nuclear power plant was calculated, and the risk of a disaster at the Fukushima nuclear power plant was calculated similarly as of the date of the catastrophic events.

Using the proposed approach, a cause-and-effect diagram of the influence of organizational causes of the Chernobyl disaster on each other (between themselves) and on the occurrence of the disaster was constructed (Fig. 3).

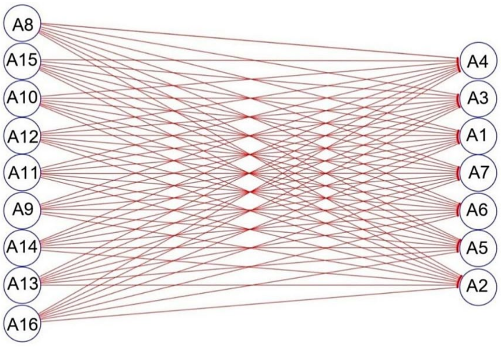

Fig. 2. Diagram of the influence of organizational causes (*A8–A16*) on the emergence of technical causes (*A1–A7*, Table 1) at the Chernobyl nuclear power plant

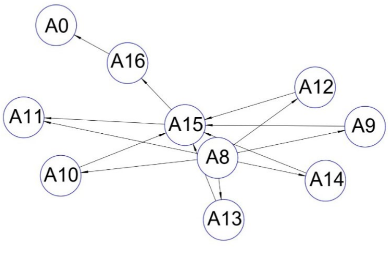

Fig. 3. Diagram of the influence of organizational causes of the Chernobyl disaster on each other (between themselves) and on the occurrence of the disaster (where *A8–A16* are the causes of the disaster, and *A0* is the disaster)

ISSN-L 2664-9969; E-ISSN 2706-5448

Analysis of the graphs (Fig. 1–3) showed that all technical causes (*A1–A7*) were influenced by all organizational causes (*A8–A16*), which means that each of the technical factors (*A1–A7*) was systematically caused by management errors.

Similarly, at the Fukushima NPP (Japan, 2011). Below is a graph (Fig. 4) with nodes and edges that reflect the structure of the disaster and its cause-and-effect relationships.

A description of the causes of the disaster at the Fukushima NPP (Japan, 2011) is given in Table 2.

The diagram (Fig. 4) reflects the cascade of events that led to the disaster, starting from organizational shortcomings (*A9*, *A12*, *A16*...) to technical failures (*A1*, *A2*, *A7*...) and the final disaster. Technical reasons (*A1–A3*, *A7*) have the highest direct impact, while organizational reasons (*A8–A16*), as at the Chernobyl NPP, create conditions for technical shortcomings.

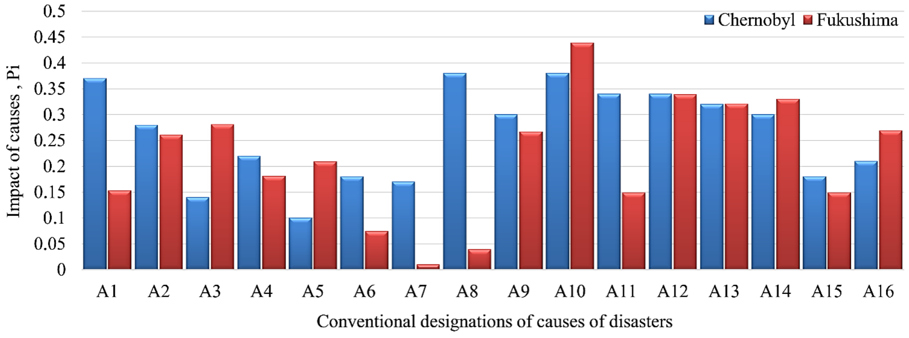

Fig. 5. Histogram comparing the criticality of the causes of the Chernobyl and Fukushima disasters

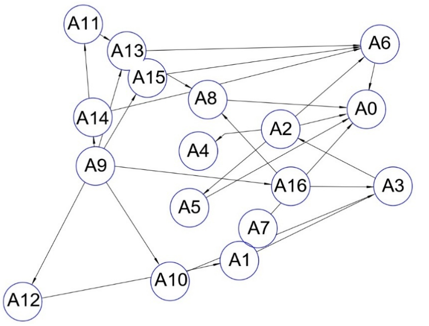

Fig. 4. Diagram of the relationship between causes *A1–A16* and consequences *A0* (disaster), Fukushima NPP

The structure of the graph corresponds to the real sequence of events at the Fukushima NPP (Japan, 2011), taking into account the features of the operation of BWR reactors (dependence on power supply, hydrogen generation, taking into account the Mark I containment type).

Cause-effect diagrams (Fig. 1–4) are constructed as directed acyclic graphs using the PC and MMHC algorithms, which use χ^2-tests to identify relationships based on IAEA reports [14–16].

The sequence of nodes reflects the chronology and criticality of the causes (Tables 1, 2), confirmed by empirical data.

Thus, according to (1)–(3), the probability of a disaster at the Chernobyl NPP (1986)/Fukushima NPP (Japan, 2011), given the coincidence of the causes identified by the commission (Tables 1, 2), at the time of the disaster was ≈99.87%/98.33%, respectively, i. e. within the proposed model, the probability of the event occurring was close to 1, which confirmed the conclusions of the investigation commissions taking into account regulatory requirements, historical retrospective and physical modeling (from the reverse). At the same time, according to (3), the level of confidence in such an assessment in the modern understanding of the events that occurred was ≈100%/97.92%, the level of uncertainty on the date of the catastrophic events was ≈0%/2.08%, the accuracy of the calculation is ≈99%.

Fig. 5 shows a histogram comparing the criticality of the causes of the disasters at the Chernobyl NPP and the Fukushima NPP.

Analysis of the data obtained (Fig. 5) showed that:

– *A10* (Fukushima NPP) – has the highest level of criticality (ignoring the previous incident);

– *A1*, *A8*, *A10* (Chernobyl NPP) – also have high values, which indicates their strong influence (previous incidents are also ignored);

– *A7* (Fukushima NPP) – has almost zero influence (lack of ventilation for hydrogen). This is explained by the fact that hydrogen arose as a result of water radiolysis and entered the premises after the reactors were damaged.

Thus, the Chernobyl disaster has more uniformly critical factors, while the Fukushima disaster has several very critical and several almost insignificant factors stretched over time.

Fig. 6 shows a comparative diagram showing the average probabilities (P_i) for the technical and organizational causes of the accidents at the Chernobyl NPP (CT, CO) and the Fukushima NPP (FT, FO), respectively.

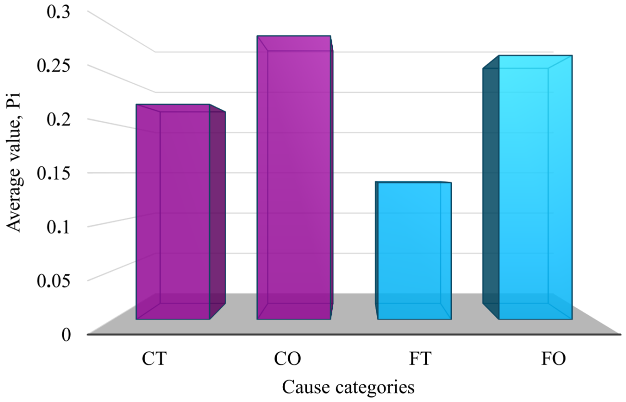

Fig. 6. Diagram comparing the criticality weight of organizational and technical causes of the disasters at the Chernobyl NPP and the Fukushima NPP

It is shown that in both disasters organizational causes have a higher average criticality than technical ones.

The modified method, built on the basis of BN, is integrated with the Industry 4.0 paradigm [18–20].

The requirements for such a method are a high degree of automation of data collection and processing processes, construction of risk models, and making informed decisions in real or close to real time.

The mathematical and algorithmic model of the symmetric description of counter-dominant events looks as follows.

The concept of the MSDBN approach as a way to solve the problem:

1. *Purpose of the method:*

– objective identification and assessment of risks and their levels;

– forecasting the probability of counter-dominant events;

– integration of models with real systems for monitoring and managing risk in real time;

– simplification of the decision-making process.

2. *Areas of application of the method:*

– national security;

– health care;

– environmental monitoring;

- civil security;
- industrial safety;
- cybersecurity;
- financial sector;
- economy and economic monitoring;
- supply logistics under uncertainty, etc.

The terminological apparatus of the method is given in Table 3.

Table 3

Terminological apparatus of the modified approach

Designations	Description
MSDBN	Modular scalable dynamic Bayesian network
Module (M_i)	Independent subgraph of a network describing a subsystem
DAG	Directed acyclic graph
Graph	Mathematical framework used to model relationships between objects
MMHC	A hybrid BM structure learning algorithm that combines constraint-based and estimation methods
PC	A BN structure learning algorithm that belongs to the category of constraint-based methods that use conditional independence tests to determine the structure of a graph
IN_{ij}	An interface node that connects modules to convey probabilistic dependencies
$N_i(t)$	A variable (discrete or continuous) at time t
$E_{ij}(t)$	The dependency between nodes $N_i(t)$ and $N_j(t + \Delta)$
CNR_i	Compliance with regulatory requirements
CHR_i	Compliance with historical analogies
PCM_i	Inferences about the probability of events from physical/computer simulations
$P_{default}$	Background probability
DQI (DQI_i)	Data quality index
Junction Tree	A method of inference in BN that used to calculate marginal and conditional probabilities. It transforms a directed acyclic graph (*DAG*) into a special structure – a tree, which allows for fast query execution
MCMC	A set of inference methods for approximating probabilities in BN
CN	A parameter that reflects how complete the data is, i.e. does it contain all the values needed for analysis
AY	A parameter that reflects how well the data correspond to real values or the actual state of the system
CY	A parameter that reflects how well the data is consistent across sources or within a single data set
TS	A parameter that reflects how relevant and timely the data is
US (US_i)	Uncertainty index
2*TBN*	Two-layer network for dynamic model
CLG	Model (Conditional Linear Gaussian, CLG) for hybrid networks
θ	Set uncertainty threshold (0.7)
$T_{horizon}$	Forecasting time horizon
X_d, X_c	Discrete and continuous variables

3. *Step-by-step algorithms of the method.*

The system is divided into modules M_i, each of which models a separate subsystem (for example, equipment, processes, area, person, etc.).

The modules are connected through standardized interface nodes IN_{ij}, which minimizes their dependencies as much as possible.

Each module can be updated independently, implementing the principles of incremental learning.

Algorithm of the method.

Initiation of a pilot project:
- system selection;
- determination of key risk factors and their parameters;
- data collection and automated pre-processing;
- integration with IoT sensors (*ERP*, *MES*), etc.;
- automatic data quality assessment (DQI_i).

Building a modular structure:
- automatic identification of modules and nodes;
- construction of DAG with IN_{ij} for modules;
- definition of interface nodes.

Parameterization of nodes and edges:
- calculation of prior and conditional probabilities;
- support for hybrid networks for continuous nodes;
- consideration of PCM and conflicts between sources.

Inference:
- distributed inference by modules (Junction Tree, MCMC);
- dynamic inference taking into account time evolution;
- use of PySpark/Dask for large systems.

Validation, interpretation, sensitivity:
- use of metrics and "what-if" scenarios;
- automatic generation of reports with visualization;
- sensitivity analysis for key risks.

Integration and automation:
- integration with monitoring and control systems;
- automation of model updates with new data;
- automation via Airflow, Kafka.

Scaling:
- gradual addition of new modules;
- optimization of calculations via cloud platforms.

4. *Data collection and pre-processing.*

Data sources:
- regulatory and legal acts, standards, databases, etc.;
- OREDA, FMEA, HAZOP (incident archives, investigation materials, e. g., Chernobyl, Fukushima);
- IoT sensors, digital twins, time series, etc.;
- modeling: CFD, FEM, MKS, etc.

Pre-automated data processing:
- cleaning: removing anomalies, filling gaps;
- normalization: standardization of continuous variables;
- data evaluation through the quality index (DQI_i)

$$DQI_i = \frac{1}{4}\left(CN + AY + CY + TS\right), \tag{4}$$

where integration: streaming processing via Kafka, Spark; data storage: Hadoop HDFS, PostgreSQL, etc.

5. *Standardization of interface nodes* IN_{ij}.

Rules for constructing IN_{ij} nodes.

Identification of connections: IN_{ij} connects modules M_i (for example, technical factors) and other modules, for example, organizational ones and can model, for example, the impact of safety culture on the technical condition of the object.

Unification of formats.

It is possible to use unified formats:

JSON – schema, data structure: ID, Type, Parents, CPT/CLG. The proposed schema is not a storage format, but is used as a formalized interface for exchanging parameters between BN modules with variable ordering [21];

Protocol: REST/gRPC API for transmitting $P(IN_{ij})$, taking into account the problems [22].

Table 4 shows the parameterization rules that determine how the probabilities and data quality for the interface nodes IN_{ij} are calculated.

Table 4

Parameterization rules

Aspect	Description	Formula
Conditional Probabilities (X_d)	Probability table for (X_d)	$P(IN_{ij} \mid P_a\ (IN_{ij}))$
Conditional Probabilities (X_c)	Probability table for (X_c)	$P(IN_{ij} \mid P_a\ (IN_{ij})) = N(\beta_0 + \sum \beta i \cdot Pa_i, \sigma^2)$
Data quality $DQIi_{IN_{ij}}$	Weighted average *DQI* of "parent nodes"	$DQIi_{IN_{ij}} = \sum w_k \cdot DQI_k$
Data sources	Standards, historical data, *PCM*	For example, *PCM* with MKS for IN_{12}

Unification.

In the context of the MSDBN approach, unification is the process of standardizing interface nodes IN_{ij} through a single format, centralized storage, API for updating (REST/gPRC) and standard parameterization rules (Table 4).

This ensures modularity, scalability and adaptability of the system, allowing for effective modeling of complex security systems with minimal subjectivity and high data reliability.

6. *Building the MSDBN structure.*

Node identification.

Automatic:

– text analysis of standards (NER, spaCy);

– clustering of time series (K-Means, DBSCAN);

– F'MEA/HAZOP analysis for risk factors.

Node classification:

– discrete (X_d): States (0 = normal, 1 = failure);

– discrete (X_s): temperature; pressure; radiation, etc.

Building a modular structure for each module:

– building a DAG using PC or MMHC;

– validation using BIC, AIC.

The independence of nodes can be determined automatically by the PC and MMHC algorithms, through χ^2-tests of conditional independence, based on NS, HS, MS data. The uncertainty of connections can be estimated (6), taking into account the data quality (*DQI*). The PC and MMHC algorithms have replaced the need for a Bayes coefficient, thanks to the automatic determination of the structure based on verified data.

Interface nodes provide for:

– reducing the number of connections between individual modules;

– applying key parameters, such as using the results of one module (M_1) as initial data for another (M_2).

The dynamic network structure (2TBN), as indicated in (5) and (6), includes:

– intra-module connections (intra-slice) within each module;

– interlayer connections (inter-slice), which ensure time evolution

$$P\left(X\left(t+1\right) \mid X\left(0:t\right)\right), \tag{5}$$

where $P(X(t+1) \mid X(0:t))$ is a conditional probability that reflects the state of all variables of the system X at the next time point $t + 1$, taking into account the entire history of its states from the initial moment ($t = 0$) to the current time (t).

The meaning of this conditional probability is to determine the probability of a specific state of the system in the future ($t + 1$), based on known data on its previous evolution.

Regarding the formalization of the mechanism of transition in time, it can be expressed as follows

$$P\left(X\left(t+1\right) \mid X\left(t\right)\right), \tag{6}$$

where $P(X(t+1) \mid X(t))$ – reflects the conditional probability of all variables of the system X at the next time point $t + 1$, taking into account only their state at the current time point t. $X(t)$ represents the state of all variables of the system at the time point t.

The essence of the expression is that to predict the future state $X(t + 1)$ it is enough to know the current state $X(t)$. This simplifies the analysis and description of the system, based only on its current state.

The equality between expressions (5), (6) reflects the assumption of a first-order Markov process. Under the conditions of coincidence, this means that the system has the property of "memoryless" with respect to all previous states, except the current one. In other words, $X(t + 1)$ is conditionally independent of $X(0:t - 1)$ provided that $X(t)$ is known.

Network scalability:

– use of decomposition by dividing the network into modules according to the Taryan algorithm;

– construction of a hierarchy of levels: System → Subsystem → → Component;

– implementation of parallelization for the inference process thanks to the Map-Reduce model.

7. *Adaptive DAG update.*

In the context of MSDBN, the following procedure is appropriate.

Change detection:

– monitor DQI_i and US_i using IoT data;

– determine the appearance of new elements $N_i(t)$ (for example, a new sensor);

– make changes to the structure (add or remove modules).

Updating the structure:

– use the appropriate Online PC and Dynamic MMHC algorithms;

– perform the reconstruction of edges $E_{ij(t)}$ and variables IN_{ij} using incremental learning.

Updating parameters:

– recalculation of $P(N_i(t))$, $P(IN_{ij}(t))$ based on new data.

Integration.

Integration consists in ensuring interaction between system modules through:

– REST/gRPC API for updating templates.

Automation.

Automation is advisable to carry out through Airflow, together with integration, these mechanisms support the adaptability and modularity of MMDBN, which is absolutely necessary when modeling complex systems.

8. *Parameterization.*

The uncertainty estimate (US_i) for a specific node can be carried out by the formula

$$US_i = 1 - \sqrt{\frac{1}{5} DOI_i^2 + \left(\frac{m_{valid}}{m_{total}}\right)^2 + \left(\frac{n_{match}}{n_{total}}\right)^2 + PCM_{val}^2 + CS_i^2}, \tag{7}$$

where US_i (Uncertainty Index for Node i) – an indicator of the level of data uncertainty for a specific variable, in the range [0, 1]. The lower the indicator, the lower the uncertainty of the event (process); DQI_i – data quality index, calculated according to the previous formula (4), in the range of values [0, 1]; m_{valid} – the number of valid (correct, verified) data records for node *i*. For example, the number of temperature measurements that have passed the verification; m_{total} – the total number of expected data records for node *i*. For example, the number of all temperature measurements that should have been obtained; m_{valid}/m_{total} – the proportion of valid records, in the range [0, 1]; Reflects the reliability of the data in terms of their validity; n_{match} – the number of records that match historical analogies (for example, archived data or FMEA/HAZOP results); n_{total} – the total number of historical records with which the comparison was made; n_{match}/n_{total} – proportion of matches with historical data, in the range [0, 1]. Reflects the correspondence of current data to historical analogies; PCM_{val} – assessment of the reliability of probabilities obtained from physical or computer modeling (*PCM* – Physical/Computer Modeling), in the range [0, 1]; 1/5 – indicates that the weight of each component contributes equally to the calculation, the total weight is 1 (100%); CS_i – measures the degree of inconsistency between two data sources for the *i*-th node

$$CS_i=\frac{\left|CRN_i-CRH_i\right|}{CRN_i+CRH_i+\in},\in=0.01, \tag{8}$$

where CRN_i – the probability or estimate obtained from the regulatory documentation; CHR_i – the probability or estimate obtained from historical data; ∊ – a small constant. It is added to the denominator to avoid division by zero in the case when $CRN_i + CHR_i = 0$.

Expression (6) is a root for normalizing the sum in the range of values [0, 1].

Squares (DOI_i^2, PCM_{val}^2 etc.) in formula (6) have a mathematical and conceptual meaning related to normalization, weighting and further interpretation of uncertainty.

Prior probabilities of MMDBN.

The formula for prior probabilities for discrete nodes of MMDBN can be as follows

$$P_{prior}\left(X_d\right)=\begin{cases}\left(w_{CRN}\cdot CRN_i\right)+\left(w_{CHA}\cdot CHA_i\right), if\ US_i<\theta,\\ P_{PCM}\left(X_d\right),\ if\ US_i\geq\theta\ and\ PCMavailable,\\ P_{default}\left(X_d\right),\ if\ otherwise,\end{cases} \tag{9}$$

where $P_{prior}(X_d)$ – the prior probability of the discrete variable X_d; w_{CRN}, w_{CHA} – the weights of the normative and historical data; CRN_i – the probability from the assessment of normative sources; CHA_i – the probability from the assessment of historical analogies; US_i – the uncertainty index for node *i*; θ – the uncertainty threshold (default 0.7); $P_{PCM}(X_d)$ – the probability from physical/computer modeling; $P_{PCM}(X_d)$ – the reserve (conservative) probability.

This formula allows to calculate the probability of the state of a discrete node (for example, the probability that a node that represents a "positive steam coefficient" to the rector has a "risk" state = 1).

The probability here depends on the level of uncertainty (US_i) and combines data from three sources: norms CRN_i, historical data CHA_i and data from physical/computer modeling PCM. Therefore, if the uncertainty is high, then only modeling is used.

In MSDBN, the fallback conservative probability $P_{default}(X_d)$ is a predefined probability that is used for discrete nodes in a BN when the main data sources (normative, historical or simulation) are unreliable or unavailable. It is a fallback approach that is used in cases where the model cannot rely on other sources of probability due to their poor quality or missing part of the data. In this case, the risks should not be underestimated. For example, for the variable "Failure", the conservative probability can be artificially inflated compared to the real data to take into account the worst possible scenario.

Weights:

In MSDBN, weights determine the level of confidence the model has in the normative and historical data when calculating the prior probabilities. The values of the weights for normative and historical data can be calculated using the following formulas:

$$w_{CRN}=\frac{\dfrac{m_{valid}}{m_{total}}}{\dfrac{m_{valid}}{m_{total}}+\dfrac{n_{match}}{n_{total}}\cdot\exp\left(-\dfrac{t_{current}-t_{last}}{\tau}\right)}, \tag{10}$$

$$w_{CHN}=1-w_{CRN}, \tag{11}$$

where w_{CRN}, w_{CHA} – weights of normative and historical data, respectively; m_{valid}, m_{total}, n_{match}, n_{total} used as in formula (7); $t_{current}$ – current time (for example, current year); t_{last} – time of last update of historical data; τ – amount of time (scale) that determines the rate of depreciation of historical data (by default τ = 5); $\exp\left(-\frac{t_{current}-t_{last}}{\tau}\right)$ – exponential factor that reduces the influence of historical data if it is outdated.

Formulas (10), (11) determine how the influence is distributed between normative (CNR_i) and historical (CHA_i) data. If historical data is outdated (the value of $t_{current} - t_{last}$ increases rapidly), the coefficient w_{CHA} decreases, and the coefficient w_{CNR} increases.

Conditional probabilities for discrete nodes.

Conditional probabilities are calculated similarly to priors, but taking into account the values of the variables of the "parent" level.

For example, for a turbine of conditional equipment *P*("Failure") = = 1 | "Vibration" = high) the same logic is used as with CNR_i, CHA_i, P_{PCM} or P_{prior}.

The formula for calculating conditional probability for discrete nodes can be as follows

$$P\left(X_d\,|\,P_a\left(X_d\right)\right)=P_{prior}\left(Similarly\right), \tag{12}$$

where $P(X_d\,|\,P_d(X_d))$ – the prior probability of a discrete variable, taking into account the values of its "parent" changes – $P_a(X_d)$; X_d – a discrete change ("Failure" = {0, 1}); $P_a(X_d)$ – a set of parent variables for X_d (e. g., {Vibration, Pressure, Temperature}); P_{prior} – the prior probability calculated by formula (9), which is used similarly for conditional probabilities.

For correctness, probability calculations should be based exclusively on open data (in our case, *IAEA* [11, 12], *OREDA*, *HAZOP* [13, 14], simulation), which are always sufficient due to the high *DQI* (0.8–0.95). The use of open data is a necessary condition for the reproducibility of the results.

Probabilities for continuous nodes – without "parents".

"Parentless" means that a particular node (variable) in a BN graph has no "parent nodes", i. e. it does not depend on other variables within the same time slice or module.

For continuous nodes without "parents" (e. g. temperature, which does not depend on other variables), the distribution is assumed to be normal based on historical data or modeling.

Such a probability distribution can be expressed as follows:

$$P\left(X_c\right)=N\left(\mu_{CHA},\delta^2_{CHA}\right). \tag{13}$$

If $US_i = \theta$, then

$$P\left(X_c\right)=PCM, \tag{14}$$

where $P(X_c)$ – the probability distribution for the variable X_c; X_c – a continuous variable (e. g., pressure); $N(\mu_{CHA}, \delta^2{}_{CHA})$ – a normal (Gaussian) distribution with parameters derived from historical analogies; μ_{CHA} – the mean value derived from historical data (e. g., average temperature from archive data); $\delta^2{}_{CHA}$ – the variance derived from historical data (e. g., temperature variation); θ – the uncertainty threshold (data reliability); PCM is the probability derived from physical or computer modeling if historical data are unreliable.

Conditional probabilities for continuous nodes with "parents" (CLG) are mathematically formalized as follows

$$P\left(X_c\,|\,P_a\left(X_c\right)\right)=N\left(\beta_0+\sum\beta_i\cdot P_{ai},\delta^2\right), \tag{15}$$

where $P(X_c|P_a(X_c))$ – the conditional distribution for the continuous variable X_c, taking into account the parent changes; X_c – a continuous variable (e. g., pressure); $P_a(X_c)$ – a set of "parent" variables (discrete or continuous), e. g., temperature, vibration; $N(\beta_i, \delta^2)$ – a normal distribution with mean and variance; β_0 – a free regression term (constant) that determines the baseline level of X_c; β_i – the regression coefficient for the i-th "parent" variable that reflects its influence on X_c; P_{ai} – the value (magnitude) of the i-th "parent" variable; $\sum\beta_i \cdot P_{ai}$ – a linear combination of the "parent" variables that determines the mean value of the distribution; δ^2 – the variance of the conditional distribution, which depends on the combination of discrete "parent" variables (if any).

The formula demonstrates the conditional distribution in a model in which the mean value of the continuous variable X_c and the variance depend linearly on the combination of "parent" variables.

In the case of unreliable data, physical modeling is used, which guarantees compliance with the proposed approach, taking into account real physical laws.

Time evolution for discrete nodes.

In second-order dynamic Bayesian networks (2TBN), it is necessary to have a formula that describes the changes in the states of discrete variables over time. For this, for example, it is possible to use a transition matrix, which is created based on collected data or modeling.

Below is an example of a mathematical expression – a description of the time evolution of discrete nodes

$$P\left(X_d\left(t+1\right)|\,X_d\left(t\right)\right)=Transition\ matrix, \tag{16}$$

where $P(X_d(t + 1) \mid X(t))$ – the conditional probability of the state of the discrete variable X_d at time $(t + 1)$, given its state at time t; $X_d(t)$ – the state of the discrete variable at time t (for example, "Failure" = 0 at time t); $X_d(t + 1)$ – the state of the discrete variable at time $t + 1$.

Transition matrix is a table of transition probabilities between states X_d (for example, "Failure = 0 | "Failure = 1), for example (for a conditional turbine), Table 5.

Table 5

Conditional probability table describing transitions between states X_d

$P(X_d(t + 1) \mid X(t) = 0$, high vibration	$X_d(t + 1) = 0;1$	
	... = 0	... = 1
$X_d(t) = 0$	0.7	0.3
$X_d(t) = 1$	0.2	0.8

Context in MSDBN: The transition matrix is formed based on:

- normative data CRN_i, if they contain information about the dynamics of the system;
- historical analogies CHA_i, reflecting the frequency of transitions between states;
- conclusions about the probability of events from physical/computer modeling PCM_i.

This model corresponds to the proposed approach, since it takes into account real dynamic characteristics of the system, such as the frequency of failures or the stability of equipment.

Time evolution for continuous nodes.

Of course, for dynamic second-order BNs (2TBNs), it is necessary to have a formula that would describe the dynamics of continuous variables in time (for example, temperature change, etc.), using a linear model with uncertainty.

Below is an example of a mathematical formalization – a description of the time evolution of continuous nodes

$$X_c\left(t+1\right)=A\cdot X_c\left(t\right)+B\cdot U\left(t\right)+\varepsilon\left(t\right),\varepsilon\left(t\right)\sim N\left(0,\Sigma\right), \tag{17}$$

where $X_c(t + 1)$ – the value of the continuous variable at the next time point $(t + 1)$; $X_c(t)$ – the value of a continuous variable at the current time t; A – the transition matrix that determines how the current state $X_c(t)$ affects the future state $X_c(t + 1)$; $U(t)$ – the external influence ("inputs") or control signals that are applied at the current time t (for example, system settings); B – the matrix that determines how $U(t)$ affects $X_c(t + 1)$; $\varepsilon(t)$ – the random factors – the "noise" that models uncertainty; $\varepsilon(t) \sim N(0, \Sigma)$ – the noise given by a normal distribution with a mean of zero and a covariance matrix Σ; Σ – the covariance matrix that characterizes the variation of the "noise" (variance) and the dependencies between its components.

Noise in this context can be considered as a random variable that models uncertainty or random deviations in the behavior of the system, which cannot be accurately predicted or explained by factors, which impact on the system is unambiguous and predictable.

The noise value $\varepsilon(t)$ determines random influences not taken into account in the model, in particular external fluctuations, measurement errors or changes in conditions. In mathematical assumptions, it is assumed that these influences have a normal (Gaussian) distribution with a mean value equal to zero, which excludes the presence of a systematic shift. Such a model allows to predict the change in continuous parameters, such as pressure or temperature, in real time, taking into account both the dynamics of internal processes in the system and the influence of external factors.

Compliance with the provisions of the proposed approach is ensured by using physical models to determine the parameters A, B and Σ, as well as automatic updating of these parameters when receiving streaming data.

Inference.

The inference process within the MSDBN model allows calculating the probabilities of system states, predicting risks and assessing the consequences of counter-dominant events, consistent with the proposed approach. Inference minimizes subjectivity, relying on NS, MS and US, ensures modularity, scalability of the model and the ability to work with IoT data in real time.

Considering the above, the implementation of the following combined approach is proposed:

a) IoT data collection, estimation of DQI_i and US_i;

b) Static inference: Method selection: Junction Tree ($US_i < \Theta$), MCMC (high degree of uncertainty), LBP (if speed is required);

c) Dynamic inference, methods: future system states – Forward Algorithm, distribution and filtering of current system states – Particle Filtering;

d) Distributed computing for scaling inference: Map-Reduce, AWS, Azure or Google Cloud, AWS Lambda, S3, PC approximation, other platforms;

e) Validation for norms and physical (other) laws: via NS, MS, using metrics of discrete and continuous nodes (ROC-AUC, F1-score, RMSE, R2, Log-likelihood, Perplexity);

f) Sensitivity analysis: local analysis – Tornado plots; global analysis – Sobol indices;

g) Automation through tools for data collection, processing and transmission: Kafka; MQTT, etc., including integration with SCADA.

The approach meets the aim of research, minimizes subjectivity, supports modularity, automation, including in real time, using objective data.

Interpretation.

For ease of interpretation, the results are best evaluated by categories, as given above.

In order to optimize the work of operators and safety managers, MSDBN results should be automatically interpreted and visualized, therefore:

- automatic reports are generated, describing cause-and-effect relationships;
- risks are visualized both as a whole and for individual modules, graphs are built, etc.

To display real-time streaming data and risk forecasts in MSDBN, simple tools such as Plotly, Grafana, and other modern tools can be used.

For example, a dashboard can show current indicators of the operational state of a nuclear reactor, the limit indicators of its operational state parameters, and the probability of their deviation beyond the norm. At the same time, the dashboard can demonstrate the overall safety level of the reactor (station).

9. MSDBN integration.

The proposed method is characterized by relative ease of integration with security systems due to the following features:

Systems: Compatibility with SAP, Oracle, Splunk platforms for data processing, ERP, MES management systems and event logs is provided. For example, SAP can provide maintenance information, which will be used in real time to update the HS indicator.

Protocols: The REST API method is used to exchange data with information systems, the MQTT protocol is used for streaming IoT data, and the OPC UA standard is used for integration with industrial controllers.

Streaming processing: Apache Kafka or RabbitMQ platforms are used to process large amounts of IoT data in real time. For example, the data stream from sensors is processed using Kafka and transmitted further to update the parameters of the A, B, Σ matrices.

10. MSDBN automation.

The automation of MSDBN processes covers the following main steps:

Data collection: IoT sensors automatically transmit data (e. g. pressure, temperature, reactivity reserve level) via MQTT or API protocols.

Model update: Thanks to incremental training, parameters (e. g. Σ) are updated without the need to completely rebuild the model. For example, if the dispersion of pressure noise increases, the parameter Σ is adjusted using a Kalman filter.

Monitoring: The system automatically generates notifications when the set risk thresholds are exceeded (for example, P ("Failure" > 0.5). These notifications are sent both personally to specialists at all levels and integrated into SCADA-systems for rapid response.

Below is a scenario analysis of risk assessment. Scenario analysis of risks for Ukrainian NPPs (2025–2030) demonstrates the application of the MSDBN method on the computing resources of the machine-learned neural network "Grok 4.1" (xAI) [23].

To solve the problem, the computational power of artificial intelligence was used.

Calculations were carried out according to formulas (1)–(17) developed by the authors, using the initial data of the problem.

Task: to determine the probability of an accident with the release of decay products of at least one reactor at the Ukrainian NPP in the period 2025–2030.

Primary initial data for calculation:

1. The total number of WWER type nuclear reactors in Ukraine is 15 units. The reactors are located at four nuclear power plants: Zaporizhzhia NPP, Khmelnytskyi NPP, Rivne NPP and South Ukraine NPP.

2. Age of reactors at Ukrainian NPPs: 12 out of 15 reactors have reached their design life (30 years), but their service life has been extended.

3. The average age of reactors operated at Ukrainian NPPs is 36.6 years.

4. Data on previous NPP accidents in the world:

4.1. Global statistics for the period from 1952 to 2025 recorded 103 accidents at civil nuclear facilities in the world with a total duration of their operation of 22,000 reactor-years.

4.2. Over the past 60 years, at civil nuclear facilities (NPPs Three Mile Island, Chernobyl and Fukushima nuclear power plants) have had 3 accidents of INES level 4+.

4.3. Presence of incidents over the past 20 years in Ukraine: – present, level 1 on the INES scale.

5. Current risks:

5.1. Military actions. Power outage, loss of cooling, nuclear power plant due to the impact of weapons of destruction on the equipment (facilities) of the nuclear power plant.

5.2. Lack of spare parts and replacement stock of units and equipment.

5.3. Dependence:

- on foreign-made fuel – 100%;
- on foreign-made spare parts – 70%.

6. World statistical estimates:

6.1. Frequency of accidents with a cost of losses exceeding 20 million USD: 0.002–0.003 per reactor-year (after Chernobyl).

6.2. Probability of an accident Three Mile Island level (INES 5): 50% in 10 years (0.05 per year) based on global estimates.

6.3. Probability of Chernobyl level accident (INES 7): 50% by 2050 based on global estimates (0.02 per year for a 25-year period).

6.4. Frequency of core meltdown accidents: 1 in 3,704 reactor-years (based on post-Fukushima analysis).

6.5. Frequency of accidents at WWER reactors: 1 major accident per 20,000 reactor-years, on average.

7. Risk factors:

7.1. Military actions:

- Zaporizhzhia NPP is located in a zone of military conflict, which increases the risk of a disaster by 10 times compared to peacetime (IAEA expert assessment);
- Mirror attacks on critical infrastructure facilities of Ukraine and the Russian Federation;
- In March 2022, Russian troops shelled the territory of the Zaporizhzhia NPP, which led to a fire in the training center. The station was captured by Russian troops;
- During 2022–2025, the Zaporizhzhia NPP was shelled 24 times, which led to damage to the infrastructure;
- On September 19, 2022, a Russian missile exploded 300 meters from the reactors of the South Ukrainian NPP, damaging the buildings. The reactors and their support systems were not damaged;
- February 24–March 31, 2022, Russian troops seized the territory of the Chernobyl NPP. Cases of increased radiation levels due to the movement of heavy equipment and soil movement were recorded;
- In March 2025, a drone attacked the "Shelter" facility above the destroyed reactor No. 4, causing a fire. The radiation background remained within normal limits;
- Disconnection of external power supply at the Zaporizhzhia NPP due to shelling – eight cases in 2024 – 2025 (increases the risk of loss of cooling);
- Shutdown of 6 reactors at the Zaporizhzhia NPP (September 2025), loss of external power supply, transition to backup power supply sources. According to the IAEA, 6 out of 7 basic principles (pillars) of nuclear safety were violated at the Zaporizhzhia NPP – control, protection, emergency response systems, redundancy, cooling, etc;
- The water level in the cooling water reservoir of the Zaporizhzhia NPP approaches a critically low level;
- In February 2026, the Russian Federation launched mandrel and missile strikes on substations and overhead power lines with a voltage of 750 kV and 330 kV. As a result of the damage, Ukrainian NPPs were forced to reduce their generation capacity.

7.2. Equipment aging. Extending the service life of 15 reactors increases the risk of equipment failure by 20%, compared to new reactors.

7.3. Safety culture. Personnel stress due to the war reduces the effectiveness of the safety culture by ≈15%.

7.4. Natural risks: the probability of earthquakes in Ukraine is low (less than 0.01 per year).

7.5. Impact of climate change: the probability of failure of the NPP cooling system due to extreme weather is $5 \cdot 10^{-3}$ per year.

7.6. Technical characteristics:

– all reactors have passive safety systems, but are not designed for direct hit by weapons;

– each reactor, on average, has 3 backup diesel generators, but their reliability, due to their long service life, is not determined.

Based on the results of calculations performed by the machine-trained xAI "Grok 4.1" [23], taking into account the initial conditions, let's obtain the following answer:

1. Over the next 5 years, the cumulative probability of an accident with the release of decay products at least at one of the 15 reactors of the Ukrainian NPP gradually increases to 94.1%.

2. Over the next 5 years, the scenario cumulative probability of an accident at least at one of the 6 reactors of the ZNPP gradually increases to 81.44%.

3. Over the next 5 years, the scenario cumulative probability of an accident at least at one of the 9 reactors of other Ukrainian NPPs, except for the ZNPP, gradually increases to 68.55%.

Below, in the graph (Fig. 7), three scenarios are shown (all NPPs, ZNPP, other NPPs without ZNPP). The graph (Fig. 7) specifies the object of analysis (15 reactors at Ukrainian NPPs) and indicates the forecast time period of 2025–2030.

"Cumulative probability": Reflects the increase in probability over time, which is a key characteristic of each corresponding line (NPP, NPP group).

"Accident of at least one reactor": Indicates an event estimated from the initial data of the problem (probability of an accident ≤ 1 reactor).

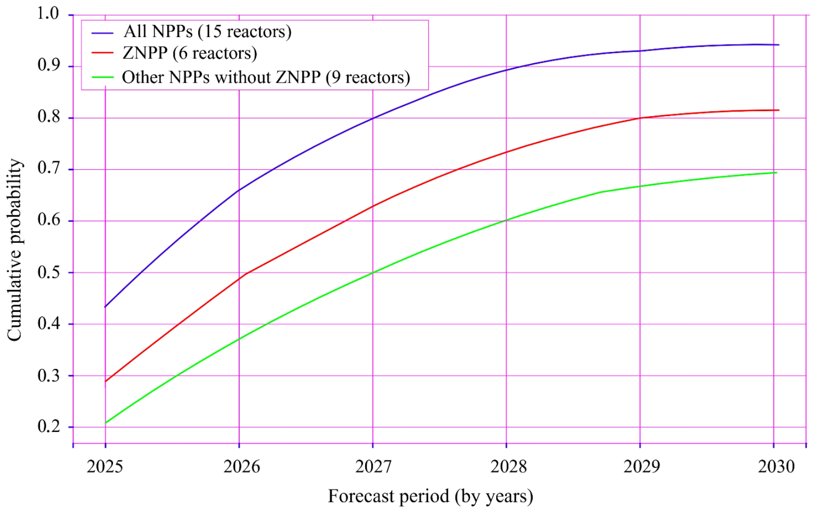

Fig. 7. Graph of scenario analysis of the cumulative probability of an accident with the release of decay products at least at one reactor of the Ukrainian NPP, in the period 2025–2030. Imagined with AI

3.4. Discussion

The results obtained show that the safety level of a complex technical system can be formalized as a function of the relative correspondence of P_t and P_c within the causal structure of the model. Retrospective testing on the examples of the Chernobyl and Fukushima disasters demonstrated that under the conditions of simultaneous implementation of the causes identified by the commissions, the calculated probability of a system disaster approaches 1 (99.87% and 98.33%, respectively). This indicates not the determinism of the risk event, but a critical imbalance between P_t and P_c.

It was established that in both cases it was organizational factors that formed the conditions for technical failures, which is reflected in high values of HS (0.7–1.0). Therefore, the dominance of organizational causes over technical ones has stochastic confirmation within the proposed model, and not only as a qualitative interpretation of IAEA reports.

Scenario analysis for Ukrainian NPPs allowed estimating the cumulative accident probability at up to 94.1% under fixed model parameters, accepted hypothesis and given scenario factors. This result is not a consequence of an absolute increase in P_t, but a systemic decrease in P_c in conditions of constant violation of safety barriers.

Classical PRA models focus on modeling the frequency of initiating events and the sequence of barrier failures, and the effectiveness of safety measures is usually taken as a parameter, not as a symmetric variable. Risk management standards [2, 3] are framework-based and do not provide a formalized mathematical procedure for estimating the quantitative relationship between P_t and P_c.

Fuzzy Bayesian Networks improve the work with epistemic uncertainty, but do not introduce a symmetric formulation of counter-dominant events.

Deep learning provides forecasting in the presence of large data sets, but has limited interpretability.

The proposed MSDBN differs in that:

– introduces a symmetric formulation into the risk assessment process;

– formalizes the uncertainty index;

– allows for incremental updating of the model structure;

– reduces the subjectivity of assessments by aggregating CRN, CHA, PCM.

The peculiarity here is the transition from an asymmetric formulation of the problem to a symmetric stochastic formalization of counter-dominant events, within which safety is described as a state of dynamic equilibrium between P_t and P_c.

Therefore, the proposed model can be considered as a stochastic interpretation of the principle of adequacy of probabilities in safety tasks.

The limitations of research are the dependence of the model on the quality and completeness of input data (especially HS), the lack of consideration of nonlinear synergistic effects of high order and the retrospective nature of the validation, increased uncertainty due to the dynamics of military risks and the limited availability of open data on the current state of the ZNPP.

The practical significance of the developed method lies in the possibility of integrating the MSDBN model into Industry 4.0 systems, digital twins, and SCADA/ERP. MSDBN allows for automatic monitoring of P_t, P_c imbalances and scenario prediction of beyond-design-basis accidents. The approach can be used as a decision-making support tool in the processes of proactive safety management of critical infrastructure, defense systems, and industrial facilities under conditions of uncertainty.

Prospects for further research include studying the capabilities of MSDBN on a wider range of critical infrastructure facilities in Ukraine. Integration of nonlinear effects and machine learning methods for automatic CPT update. The proposed MSDBN can become the basis for creating intelligent safety management systems that will have the ability to learn using mechanisms for adaptive parameter update and integration of machine learning algorithms.

The results obtained can be taken into account when justifying the possibility of using beyond-design-basis accident prediction procedures within the framework of expert assessment of projects.

4. Conclusions

1. Theoretical and methodological analysis of modern approaches to risk assessment revealed their structural asymmetry, which consists in the predominant modeling of the probabilities of threat realization in the absence of formalized quantitative consideration of the probabilities of the effectiveness of security measures. A system of criteria was formulated that allows building a symmetric stochastic model that combines regulatory compliance (CRN), historical analogues (CHA), modeling results (PCM) and uncertainty assessment (US) in a single probability space. The proposed approach eliminates the methodological gap between risk assessment and analysis of the reliability of protective barriers (security measures), providing a quantitative determination of the level of security as a function of the mutual correspondence of the probabilities of counter-dominant events. The results obtained create the prerequisites for increasing the validity of proactive security management of complex technical systems of critical infrastructure.

2. A formalized symmetric probabilistic approach was developed based on a modular scalable dynamic Bayesian network (MSDBN), within which the system security level is defined as an integral function of the ratio of threat realization probabilities (P_t) and security measures effectiveness (P_c). The features of the obtained approach are the introduction of a symmetric description of counter-dominant events, aggregation of regulatory compliance assessments, historical analogies and modeling results in a single stochastic space, as well as ensuring modularity, incremental updating and the possibility of automated scaling of calculations. Such a structure allowed to quantitatively formalize the mutual correspondence of threat probabilities and protective barriers, eliminating the asymmetry of traditional risk assessment methods. The obtained result creates the prerequisites for integrating the developed approach into systems of proactive monitoring and security management of critical infrastructure facilities, in particular into digital twins and automated control systems.

3. Empirical testing of the symmetric probabilistic approach based on MSDBN was carried out on the examples of man-made disasters at the Chernobyl NPP (1986) and the Fukushima NPP (2011). The calculated probability of a disaster occurring under the conditions of coincidence of the causes determined by the commission was 99.87% and 98.33%, respectively, with a confidence level of 97–100% and an uncertainty of no more than 2.08%. The obtained values confirmed the operability and consistency of the model with the identified causal mechanisms of risk events. Scenario analysis for Ukrainian NPPs in the period 2025–2030 showed a cumulative probability of an accident with the release of radioactive products at least at one reactor at the level of 94.1%, which demonstrated the ability of the approach to take into account contextual risks and dynamically update estimates. The testing results indicate the suitability of the developed approach for proactive quantitative safety assessment in conditions of high uncertainty and limited open data.

Acknowledgments

The authors express their gratitude to the defenders of Ukraine for the opportunity to work and engage in scientific and teaching activities during martial law.

Conflict of interest

The authors declare that they have no conflict of interest regarding this research, including financial, personal, authorship or other, which could affect the research and its results presented in this article.

Financing

The research was conducted without financial support.

Data availability

The manuscript has no related data.

Use of artificial intelligence

Disclosure of the fact of delegation of tasks to generative AI.

Generative AI tool used: xAI Grok 4.1.

The AI tool is used in section 3 of the article.

AI was used as automated computing power. The AI performed calculations using algorithms (items 3–8) and formulas (1)–(17) developed by the authors independently, using the initial data for solving the task 2 of the article and for constructing the graphs in Fig. 7.

To verify the results of the AI calculations, iterative validation using several tools was used.

In some cases, the process of obtaining the result "manually" was reproduced in Python (Python Software Foundation, USA) and errors in the AI code xAI Grok 4.1 were corrected.

The result provided by the AI tool did not affect the conclusions of research, but was useful in demonstrating the capabilities of the developed approach.

The authors bear full responsibility for the final manuscript.

Authors' contributions

Zakhar Matsuk: Conceptualization, Formal analysis, Methodology, Software, Resources, Visualization, Writing – original draft, Writing – review and editing, Project administration; ***Anatolii Bielikov***: Methodology, Formal analysis, Resources, Writing – reviewing and editing; ***Ihor Maladyka***: Software, Validation, Resources; ***Oleksandr Tyshchenko***: Formal analysis, Methodology, Validation; ***Vadim Kharchenko***: Supervision, Resources.

References

1. Borys, O. P. (2017). History of development of state fire protection and its role in formation of the system of civil protection of Ukraine. *Derzhavne upravlinnia: udoskonalennia ta rozvytok, 1,* 28–36. Available at: http://www.dy.nayka.com.ua/?op=1&z=1330 Last accessed: 25.12.2025
2. *ISO 31000:2018. Risk management – Guidelines* (2018). Geneva: International Organization for Standardization, 16.
3. *ISO 31010:2019. Risk management – Risk assessment techniques* (2019). Geneva: International Organization for Standardization, 92.
4. Blanco, C. C., Caro, F., Corbett, C. J. (2019). Managing Safety-Related Disruptions: Evidence from the U.S. Nuclear Power Industry. *Risk Analysis, 39* (*10*), 2197–2213. Portico. https://doi.org/10.1111/risa.13307
5. Zhang, J., Yin, X., Xing, J., An, X. (2023). Dynamic risk assessment for train brake system considering time-dependent components and human factors. *Computers & Industrial Engineering, 185,* 109687. https://doi.org/10.1016/j.cie.2023.109687
6. Zarei, E., Khakzad, N., Cozzani, V., Reniers, G. (2019). Safety analysis of process systems using Fuzzy Bayesian Network (FBN). *Journal of Loss Prevention in the Process Industries, 57,* 7–16. https://doi.org/10.1016/j.jlp.2018.10.011
7. Bazaluk, O., Tsopa, V., Cheberiachko, S., Deryugin, O., Radchuk, D., Borovytskyi, O., Lozynskyi, V. (2023). Ergonomic risk management process for safety and health at work. *Frontiers in Public Health, 11.* https://doi.org/10.3389/fpubh.2023.1253141
8. Mandal, M. K., Mandal, A. (2023). Human Reliability: Cognitive Bias in People–System Interface. *Human Reliability Programs in Industries of National Importance for Safety and Security.* Springer, 127–138. https://doi.org/10.1007/978-981-99-5005-8_13
9. Hollcroft, B., Lyon, B. K., Popov, G. (2022). *Risk assessment: A practical guide to assessing operational risks.* Wiley, 380. Available at: https://www.wiley.com/en-us/Risk+Assessment%3A+A+Practical+Guide+to+Assessing+Operational+Risks%2C+2nd+Edition-p-9781119755920
10. Purkait, P., Mondal, S., Changmai, S., Volli, V., Shu, C. (2024). *Hazards and safety in process industries: Case studies.* Routledge. Available at: https://www.routledge.com/Hazards-and-Safety-in-Process-Industries-Case-Studies/Purkait-Mondal-Changmai-Volli-Shu/p/book/9780367516512

11. Environment of peace: Security in a new era of risks (2022). *Stockholm International Peace Research Institute* (*SIPRI*). Available at: https://www.sipri.org/publications/2022/policy-reports/environment-peace-security-new-era-risk

12. Matsuk, Z. M. (2021). Concept of security and energy efficiency of the oil and gas industry of Ukraine. *Ukrainian Journal of Civil Engineering and Architecture, 4,* 46–57. https://doi.org/10.30838/j.bpsacea.2312.310821.46.789

13. Matsuk, Z., Belykov, A., Cheberiachko, Y., Nesterova, O. (2026). Methodology of Safety Risk: Assessment of Adequacy of Measures. *International Conference: Challenges of Ensuring Ukraine's Mineral Resources in the Context of Post-War Reconstruction* (*CEUMR*), *172,* 327–334. https://doi.org/10.4028/p-qviuu5

14. Chernobyl accident: Updating of INSAG-1 (INSAG-7) (1992). *International Atomic Energy Agency.* Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub913e_web.pdf

15. Amano, Y. (Ed.) (2015). The Fukushima Daiichi accident: Report by the Director General. *International Atomic Energy Agency.* Available at: https://www.iaea.org/publications/10962/the-fukushima-daiichi-accident

16. The Fukushima Daiichi Nuclear Accident Independent Investigation Commission: The official report (2012). *International Atomic Energy Agency.* Available at: https://warp.ndl.go.jp/en/web/20121025090656/naiic.go.jp/en/report/

17. Kelman, M., Ortynsky, V. (2021). Chernobyl disaster – a tragic lesson for all humanities: 35th anniversary of the Chernobyl accident. *Visnyk Natsionalnoho Universytetu "Lvivska Politehnika". Seria: Yurydychni Nauky, 8* (*2* (*30*)), 1–7. Available at: https://science.lpnu.ua/law/all-volumes-and-issues/volume-8-number-230-2021/chernobyl-disaster-tragic-lesson-all-humanities

18. Grabowska, S., Saniuk, S. (2022). Business Models in the Industry 4.0 Environment – Results of Web of Science Bibliometric Analysis. *Journal of Open Innovation: Technology, Market, and Complexity, 8* (*1*), 19. https://doi.org/10.3390/joitmc8010019

19. Gajdzik, B., Grabowska, S., Saniuk, S., Wieczorek, T. (2020). Sustainable Development and Industry 4.0: A Bibliometric Analysis Identifying Key Scientific Problems of the Sustainable Industry 4.0. *Energies, 13* (*16*), 4254. https://doi.org/10.3390/en13164254

20. Liao, Y., Deschamps, F., Loures, E. de F. R., Ramos, L. F. P. (2017). Past, present and future of Industry 4.0 – a systematic literature review and research agenda proposal. *International Journal of Production Research, 55* (*12*), 3609–3629. https://doi.org/10.1080/00207543.2017.1308576

21. Friedman, N., Koller, D. (2003). Being Bayesian About Network Structure. A Bayesian Approach to Structure Discovery in Bayesian Networks. *Machine Learning, 50* (*1-2*), 95–125. https://doi.org/10.1023/a:1020249912095

22. Hari Krishna, S. M., Sharma, R. (2024). Comparative Study of Orchestration using gRPC API and REST API in Server Creation Time: An Openstack Case. *International Journal of Computer Networks & Communications, 16* (*1*), 87–104. https://doi.org/10.5121/ijcnc.2024.16106

23. xAI. (2025). *Grok* (*Version 4.1*) *[Computer software]*. Available at: https://x.ai/grok

✉***Zakhar Matsuk,*** *PhD, Associate Professor, Department of Labor Protection, Civil and Technogenic Safety, Ukrainian State University of Science and Technology, SEI "Prydniprovska State Academy of Civil Engineering and Architecture", Dnipro, Ukraine, e-mail: matsuk.zachar@pdaba.edu.ua, ORCID: https://orcid.org/0000-0001-6114-9536*

Anatolii Bielikov, *Doctor of Technical Sciences, Professor, Department of Labor Protection, Civil and Technogenic Safety, Ukrainian State University of Science and Technology, SEI "Prydniprovska State Academy of Civil Engineering and Architecture", Dnipro, Ukraine, ORCID: https://orcid.org/0000-0001-5822-9682*

Ihor Maladyka, *PhD, Associate Professor, Head of Department of Geodesy, Land Management, Building Structures and Life Safety, Cherkasy State Technological University, Cherkasy, Ukraine, ORCID: https://orcid.org/0000-0001-8784-2814*

Oleksandr Tyshchenko, *Doctor of Technical Sciences, Professor, Department of Geodesy, Land Management, Building Structures and Life Safety, Cherkasy State Technological University, Cherkasy, Ukraine, ORCID: https://orcid.org/0000-0001-7303-6360*

Vadim Kharchenko, *Forensic Expert, Individual entrepreneur "Kharchenko V. V.", Kamianske, Ukraine, ORCID: https://orcid.org/0009-0003-0345-9116*

✉*Corresponding author*