# Computer System for Evaluation the Reliability of Technological Systems

Kateryna Yalova[a] , Kseniia Yashyna[a] , Leonid Dranishnikov[a] and Abdel-Badeeh M. Salem[b]

[a] *Dniprovsky State Technical University, Dniprobydivska str.2, Kamyanske, 51918, Ukraine*
[b] *Ain Shams University, El-Khalyfa El-Mamoun Street Abbasya, Cairo , Egypt*

### Abstract

The paper presents the results of developing a computer system for evaluation of reliability of technological systems, which uses the logical-graphic method Fault Tree Analysis. Automation of the Fault Tree construction process is aimed at accelerating and improving the accuracy of graphical representation process of the technological system model to assess the level of its reliability and identify the components that most affect the risk of accidents. The paper substantiates the feasibility of using the Fault Tree and describes the algorithm for qualitative and quantitative analysis of Fault Tree data. The architecture of the developed computer system is multi-layered, divided into data layer, user interface layer, and business logic layer. The input for a computer system is a description of a technological system – the object of study – which is defined by a set of interrelated events with a given intensity of occurrence, the combination of which can result in a particular major undesirable event. Based on the entered input data, the Fault Tree is automatically constructed, the probability polynomial is formed, the probabilities of occurrence of intermediate events and the top event are calculated, the list of the minimum emergency combinations and trajectories is developed. The relational database proposes storing data on technological systems, events, types of connections, and graphic notations to implement information actions of inserting, deleting, editing, committing, and exporting data. The adequacy of the implemented design solutions was proved by testing the computer system on the Fault Tree of different complexity from different domain. The results of its application to analyze the reliability of the technological design of brown smoke suppression of metallurgical production in the framework of research work “System analysis and computer modeling of technological processes and information technologies” are presented.

### Keywords [1]

System reliability analysis, fault tree analysis, computer system

## 1. Introduction

It is impossible to achieve absolute safety for systems that use energy. All measures for the safe operation of technological systems must consider the possibility of dangerous, undesirable situations and focus on the relevant risk [1]. Analyzing the reliability of technological equipment has recently become increasingly important. The concept of manufactured risk management emerged when, given the growing number of potentially dangerous facilities and the associated increase in accidents and catastrophes, the question arose as to which strategy to choose to ensure the safety of manufacturing facilities. The tasks of systems reliability evaluation in engineering practice are faced by specialists who perform design and engineering work, developers of plans for localization and elimination of

IntelITSIS’2022: 3rd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 23–25, 2022, Khmelnytskyi, Ukraine
EMAIL: yalovakateryna@gmail.com (K. Yalova); yashinaksenia85@gmail.com (K. Yashyna); dr-leon@ukr.net (L. Dranyshnykov); abmsalem@yahoo.com (A.-B. M. Salem)
ORCID: 0000-0002-2687-5863 (K. Yalova); 0000-0002-8817-8609 (K. Yashyna); 0000-0002-9291-4074 (L. Dranyshnykov); 0000-0003-0268-6539 (A.-B. M. Salem)

emergencies and accidents, developers of safety declarations for high-risk facilities. Risk should be understood as the expected frequency or probability of specific hazards class or the amount of possible damage (loss, damage) from an undesired event or some combination of these values. The application of the concept of risk, thus, allows to translate the danger into the category of measurable categories, where risk is a measure of danger and includes the following quantitative indicators:

- probability of occurrence (frequency of occurrence) of the dangerous factor under consideration;
- the amount of damage from the influence of a dangerous factor;
- uncertainty of losses and probabilities.

The term "risk" is used to analyze the reliability of technological systems, determine the level of hazards and form a set of actions to reduce the risk of an adverse event [2]. Suppose the concept of "risk" is applied to the technosphere. In that case, it should describe the probability of an accident when using the mechanisms or machines of a technological system particular process. The manufactured risk analysis is used to assess the reliability of technological systems, which aims to determine the frequency of adverse events and calculate the probabilities of their occurrence.

In general, the main tasks of risk assessment are related to:

1. Identification of hazards.
2. Analysis of the frequency or probability of adverse events.
3. Assessing the consequences of adverse events.

The generalized assessment of the reliability of technological systems should reflect the state of industrial safety, taking into account the risk indicators of all adverse events that may occur at the hazardous production facility, and based on the results:

- integration of risk indicators of all adverse events (accident scenarios), taking into account their mutual influence;
- analysis of uncertainty and accuracy of the obtained results;
- analysis of operating conditions compliance with industrial safety requirements and acceptable risk criteria.

In modern accidents researching, causation and effect diagrams with a branching structure and called a "tree" (fault tree, event tree), each of which is a branched, finite and connected graph that does not have loops or cycles, have become widespread.

To solve the problems of a quantitative evaluation of reliability and safety of complex technological systems, logical-probabilistic methods, logical-graphic methods [3]: event trees, Fault Tree Analysis (FTA), topological methods have become the most widespread. The first analysis of the reliability of complex technological systems, implemented by FTA, was conducted in the '60s [4]. Today, FTA is effectively used in the aerospace, nuclear energy, chemical and processing industries, pharmaceuticals, petrochemicals, and other high-risk industries [5-7].

Despite the extensive coverage in the scientific and technical literature, experts make some methodological and logical errors in practice, which leads to incorrect results of the technological systems reliability analysis [8]. The urgency of automating the process of technological systems reliability evaluation is associated with the ever-increasing structural complexity and dimensionality of modern technical systems and the need to increase the level of reliability and safety of such systems. Computer systems development and software applications with the function of automatic construction and calculation of the events occurrence probability allows to increase the speed of technological system model construction, simplify the Fault Tree (FT) design process, reduce errors in calculations, get a mechanism for modeling various system states occurrence of adverse events. Currently, there are a lot of commercial and non-commercial software and platforms that allow building the FT and performing analysis of the technological systems reliability in automated mode, such as [9]: OpenFTA, OpenAltaRica platform, ALD Fault Tree Analyzer, DFTCalc, CAFTA, RAM Commander FTA. In addition to opening and advertising software products, scientists Y. Hiraoka, M. Takahashi, A. Majdara, T. Wakabayashi [10,11] describe corporate software development to assess the reliability of specific technological systems. The main disadvantage of commercial software is paying for the purchased license. Free software has some limitations for building a FT, such as restrictions on the number of initiating events or logical operators, the inability to save or reuse the created FT, customization for a specific data domain.

The primary purpose of this work is to present the results of modeling, development, and practical application of non-profit computer system, which provides the ability to design a FT for quantitative and qualitative analysis of a wide range of technological systems reliability.

## 2. Models, methods and technology

System analysis, including the formulation and decomposition of the problem's solution, is used to formalize the process of technological system research, the reliability of which must be evaluated.

FTA is used to evaluate the system's reliability, which is one of the main methods of quantifying the probabilistic component of risk – the frequency of accidents. When constructing a FT, it is necessary to define the conditions for the appearance of the top event; decompose complex prerequisites; identify co-operating factors; exclude feedback between elements specify the reasons for their occurrence; check the validity of all accepted assumptions and initial data. Using the trace-back algorithm allows calculating the probability of events occurrence included in the FT, starting from the bottom level of the tree. The significance of the events leading to the main undesirable event is assessed using the Fussell-Vesely algorithm.

During the computer system design and implementation, the principles of system analysis, function-oriented method of data domain analysis, data normalization rules, principles of relational database design are used. The user interface development was carried out, taking into account the interface's usability.

The methods, principles, and algorithms used in the course of the work make it possible to state that the study results are reasonable and reproducible.

### 2.1. Features of the Fault Tree construction

FTA is a logical-graphical method, which is to build and analyze a model of reliability (safety), that is a model of causal relationships of studied system failures with failures of its elements and other influences, which allows elaborating visually and in detail related elements of infrastructure and events that affect reliability. The advantages of the FT are [12]:

- analysis focuses on finding failures, which allows showing the existing unreliable places of the system;
- provides graphics and presents visual material for those professionals who participate in the maintenance of the system;
- provides an opportunity to perform qualitative or quantitative analysis of system reliability.

The graphical representation of the model uses a highly branched tree data structure, the elements of which reflect the structure of the causal relationships of hazardous situations in reverse so that the root of the tree is the main undesirable event in the technological system probability of which must be established.

The main advantage of the FTA (compared to other methods) is that the analysis is limited to finding only those elements of the system and events that lead to a particular system failure or accident. The main disadvantage of FTA is that the tree has the form of a Boolean algebra diagram, which shows only two states: working and non-working, which makes it impossible to consider the state of partial failure of elements.

The generalized FT construction algorithm can be represented as a set of the following steps:

1. Determining the content of analysis, which establishes the system's boundaries, determines the data for the analysis of its reliability, sets the top adverse event, the risk of which will be analyzed. This fact considers that FT can build both for the whole system and its part.
2. Identify the set of initiating events and states that can lead to the top event. Also, many additional conditions are formed, which in the presence of particular type initiating events can contribute to the development of accidents in an undesirable direction.
3. Establishing logical relationships between established events.
4. Determining the frequency of adverse events.

5. Graphical representation of the failure tree and calculation of intermediate events and top one probabilities.

The main reasons for errors when building a FT are:

- errors of system analysis when describing the composition of the technological system and the set of process events to be analyzed;
- incorrect use of logical symbols;
- incorrect use of statistics on the initiating events probabilities.

The following steps of working with the graphic model data of FT are aimed to conduct a qualitative and quantitative analysis of system reliability.

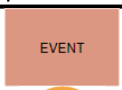
### 2.1.1. Fault tree elements

The FT elements can be divided into three groups: primary failures or initiating, or basic events (conditions in which the technical system usually operates); secondary failures (deviations from process regulations); control failures (equipment does not receive control signals for any reason). A FT includes one top event connected by logical conditions with those intermediate and initial prerequisites, the occurrence of some of which can lead to a specific incident.

The graphical display of the FT uses standardized graphic notations, which makes it possible to clearly define events, logical elements, and types of transmission [4,11]. Event symbols allow setting such events as: “Top Event”, “Intermediate Event”, “Initiating Basic Event”, undeveloped event, external event. The initiating events do not develop further, and the intermediate events are at the output of the elements. The logical gates symbols describe the relationship between input and output events and correspond to classical Boolean logic. Transmission elements are used to connect the inputs and outputs of the corresponding FT, such as the FT of the subsystem in its system. Table 1 shows the basic graphic notations used to build the FT.

**Table 1**

Basic graphic notations of the failure tree

| Graphic notation | Description |
|---|---|
|   | The main element of the FT. It describes the main and intermediate events that can be broken down into components. |
|   | Describes initiating events that are at the lowest level of the hierarchy and have no underlying connections. |
|   | AND gate - sets the logical connection “AND”. Used to describe a situation where an output event occurs if all input events occur simultaneously. |
|   | OR gate - displays the OR connection used to describe the situation when the output Event occurs if any of the input events occur. |

The most commonly used logical elements are AND and OR, but some trees may also use logical operators such as XOR or NAND. For any event to be further analyzed, first look at all possible events that are inputs of operation OR, then that are inputs of operation AND. This scheme is applied to the basic event and all other events whose analysis makes sense to continue.

### 2.1.2. Fault tree analysis

FT can be used for qualitative and quantitative analysis of system reliability. At the qualitative level, it is used to identify possible causes and ways of failure (final event); at the quantitative level – to calculate the probability of a final event based on data on the probabilities of causal events.

Qualitative analysis requires an understanding of the system and the reasons for the failure and a technical understanding of how the system may fail. When conducting the analysis, it is advisable to draw up detailed schemes. It is necessary to set basic events $BE=\{BE_1,\ldots BE_n\}$ and a set of intermediate events $IE=\{IE_1,\ldots IE_n\}$, each of which occurs when a single initiating event or set of initiating events. Boolean algebra is used to describe the relationships between intermediate and initiating events. A complex tree has different sets of initiating events, in which an event is reached at the top; they are called emergency combinations (sections). The minimal cut set is the minor set of initiating events in which an event occurs at the top. The complete set of minimum emergency combinations of a tree represents all variants of combinations of events at which there can be an accident. The minimum trajectory is the smallest group of events in which an accident occurs. Qualitative analysis of the tree is carried out using the selected minimum emergency combinations and trajectories; it compares different routes and initial events to the final and identifies critical (most dangerous) pathways leading to the accident.

Quantitative analysis of the FT calculates the probability of an accident during a given time on all possible routes. The calculation of the probabilities of the intermediate and main events, which are part of the constructed FT, is based on the input statistics of the frequency of occurrence of the initiating events. The following data are used to determine the frequency of occurrence of initiating events:

- statistical data on accidents and reliability of the technological system, the specifics of the hazardous production facility;
- expert assessments by taking into account the opinion of experts in this field;
- analysis of accidents in order to determine the required probability.

The probability of occurrence of events is associated with the intensity of the event by exponential law [13]:

$$P = 1 - \exp(-\lambda t), \tag{1}$$

where $\lambda$ – the intensity of the failure event in the technological system, $t$ – the operating time of the technological system, which determines the intensity of the failure event in the technological system.

In the case of $\lambda t < 0{,}1$ equation (1) turns into:

$$P \approx \lambda t. \tag{2}$$

FT quantitative analysis can be carried out in various ways:

- using structural functions (calculated probability polynomials);
- step-by-step reduction of the FT using trace-back algorithm;
- quantitative assessment of the top event probability using minimal combinations of initial prerequisites.

*Using structural functions*. In this case the problem is to simplify the relations according to the rules of event algebra in order to obtain calculated probability polynomials. The prediction of the probability of a top event is carried out in the following sequence [3]:

1. The analytical model of the process is decompressed into separate blocks;
2. In selected blocks, those subsets of events that are interconnected by conditions AND, OR and have known probabilities are distinguished;
3. For the selected units the probability calculation at the event vertices is performed;
4. The structural function is simplified by replacing each subset of the property with one member having an equivalent probability;
5. The probability of the occurrence of the FT top event is calculated in a similar way.

*Using trace-back algorithm*. If the probabilities of all initiating events are known, the trace-back algorithm to calculate the probabilities of intermediate events and the main undesirable event can be used. The probability of intermediate events depends on the relationship between the events that lead to them. The trace-back algorithm calculates the probability of events that are part of the generated FT by levels, starting from the lowest. $N$ failure tree prerequisites combined by logical condition AND are replaced by one event with equivalent probability of occurrence $P_\cap$ [14]:

$$P_\cap = P_1 \cdot P_2 \cdots P_n = \prod_{i=1}^{N} P_i. \tag{3}$$

$M$ of the FT initial prerequisites, connected by a logical gate OR, are also replaced by one event, and its equivalent probability $P_{\cup}$ is calculated using a formula that estimates the probability of realizing at least one initial event:

$$P_{\cup} = 1 - (1 - P_1)(1 - P_2) \cdots (1 - P_m) = 1 - \prod_{i=1}^{m} (1 - P_i), \tag{4}$$

where $P_i$ – the probability of $i$-th event occurrence.

Also, the probability of a basic event can be determined based on the minimum cut sets as [5]:

$$P(T) = 1 - \prod_{i=1}^{N_c} \left(1 - P(C_i)\right). \tag{5}$$

where $C_i(i=1,..,N_c)$ – is the minimum cut set combination at which a top event occurs.

*Using minimal combinations of initial prerequisites*. This method consists of constructing another tree equivalent to the analyzed FT and including all minimal combinations of one type [15]. The new diagram is also a FT and has only one logical condition: AND if only minimum cut set combinations are used, and OR – when only minimum throughput combinations are used. To calculate the probability $Q$ of incidents, the following expressions are used:

$$Q = 1 - \prod_{i=1}^{a} \left(1 - \prod_{j=1}^{m_i} P_{ij}.\right). \tag{6}$$

$$Q = 1 - \prod_{k=1}^{b} \left[1 - \prod_{l=1}^{n_k} (1 - P_{lk}).\right]$$

where $a$ ,$b$ – the amount of minimum cut set and minimum throughput combination of the FT, $m_i$, $n_k$, the number of initial prerequisites in each of its $i$-th throughput and $k$-th cut set minimum combinations of initial events prerequisites.

Importance indicators are used to determine the contribution of each event or their combination to the occurrence of a system failure. The assessment of the importance of an event is based on the logic of its association with other FT events. It is advisable to use the Fussell-Vesely algorithm to assess the importance of the occurrence of a particular event on the occurrence of the main adverse event. Fussell-Vesely Importance is defined as [16]:

$$I_i^{FV} = \frac{P_{\min cut}(\mathrm{X}_i)}{Q} \tag{7}$$

where $P_{min\ cut}(X_i)$ – is the probability of the $i$-th minimum cut sets leading to the basic event, $Q$ is the probability of the main undesirable event.

## 3. Experiment, Results and Discussions

The analysis of software used to build a FT of complex technological systems made it possible to form functional and non-functional requirements for system software, main of which are:

1. Client-server data processing, with the ability to save data in a database.
2. Implementation of mechanisms for forming a description of the technological process or system in the form of events set with the probabilities of their occurrence.
3. Implementation of probabilistic modeling software mechanisms with automatic calculation of events occurrence probabilities in the system and creation of probability function polynomial.
4. Graphical construction of the FT.
5. Qualitative and quantitative analysis realizing on FT data.

### 3.1. Computing system for automated FTA construction

The computer system is designed as a desktop application in C # as Windows Form Application, does not require an Internet connection, interacts with the user through a standardized interface. The primary functional purpose is the automated design of FT to conduct qualitative and quantitative analysis of the reliability of technological systems.

The system architecture is multi-layered, consisting of a data representation layer, a business logic layer, and a data layer. The scheme of the architecture of the developed computer system is presented in the Figure 1.

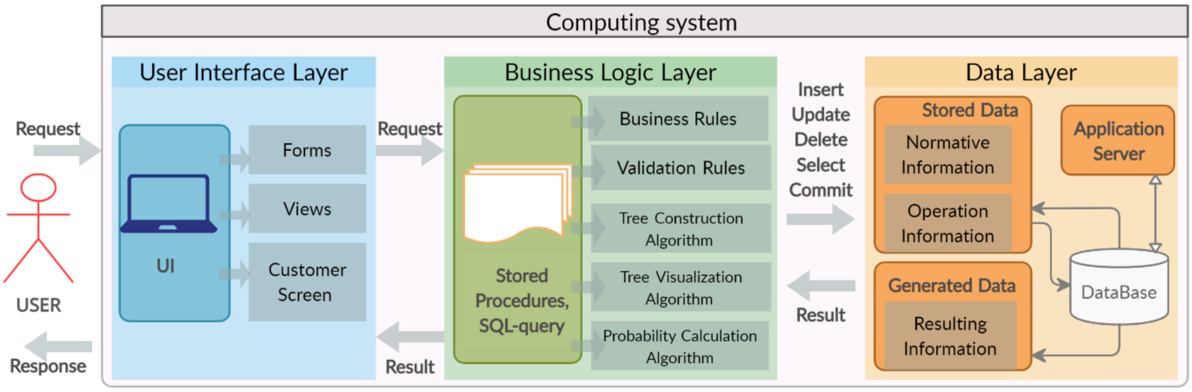



**Figure 1**: Architecture of the developed computer system

The data layer of the system was designed based on the approach described in [17], which implements the division of the data layer into three components: normative, operation, and resulting information. Normative information of the system is conditionally unchanged data, repeatedly used in data entry and the resulting samples formation. Operation information entered by the user is the primary source of data describing changes in the state of the data domain. Obtaining the resulting information is the purpose of the system; it is formed based on the results of queries to the database. The data storage in this system is a relational database, which stores descriptions of technological systems, sets of graphic notations, and types of relationships between events to build a FT, sets of accidents, and the intensity of their occurrence over time.

The business logic layer is designed as a set of software modules:

1. Module for data and descriptions of the technological system input.
2. Module of the FT graphic model construction.
3. Module for calculating and analyzing the data obtained.

Data processing mechanisms were implemented through stored procedures and representations of the database level and software application.

The data representation layer is a user interface developed on the base of the Window – Image – Menu – Pointer (WIMP) graphics standard as a set of screen forms. All graphic forms meet the requirements of unification and standardization and implement the same algorithms to build a dialogue between the user and the software application.

## 3.2. Roles and functions analysis

The developed computer system is user-dependent, i.e., the reliability of input data describing basic and intermediate events sets, the establishment of the main undesirable event, the choice of the logical relationships types of between events, the correctness of initiating events intensity or probability input is the responsibility of system users. The system validates the input data.

During the data domain analysis, two roles of computer system users were identified: the operator and the administrator. The available functions are determined, and the schemes of interaction and support of work with the system are formed considering each user's rights to access information. The system operator is a user-analyst who has sufficient knowledge of the technological system, the reliability analysis of which will be carried out. Table 2 lists the main functions and available operations for the system operator.

**Table 2**
Functions and available actions of the computer system users

| Function | Action |
|---|---|
| Access to the projects stored in the database | Create a new one<br>Open an existing one |
| Working with a new project | Top event, intermediate and initiating events insert<br>Overview of the technological system model current content<br>Deleting, editing the top event, intermediate and initiating events<br>Transactions committing |
| Designing a technological system model | Inserting data on the intensity of the initiating events occurrence<br>Selection of the intermediate i-th event<br>Identification of the events set that cause the i-th event to occur<br>Establishing of the relation type between the events that lead to the i-th event<br>Updating, deleting, committing data on relations between events |
| Graphic representation of a FT | Choice of technological system for FT construction<br>Getting a graphic display<br>Image saving and importing |
| Reliability analysis | Obtaining a probability polynomial<br>Obtaining the values of the intermediate events and the top event probabilities<br>Obtaining a list of minimum emergency combinations and minimum emergency trajectories<br>Obtaining an array of the significance of the initiating and intermediate events estimates |

A system administrator is a user who has access rights to the information stored in a database. In addition to the actions described in Table 2, the administrator has the functions of database management and administration: backup, recovery, data archiving, determination of server connection characteristics, etc.

The functions and actions of users are distributed between screen forms to simplify the dialogue of users with the system, the general scheme of transition between which corresponds to the following logical sequence:

1. Entering data on the technological system, determining the main adverse event.
2. Form a list of initiating events with data entry on the intensity of their occurrence over time and entering data of intermediate events that may affect the technological system reliability and contribute to emergencies.
3. Forming relations between events.
4. Request for automatic construction of the FT and obtaining its graphical model.
5. Request for qualitative and quantitative analysis of the generated FT data.

In addition to the mainline of dialogue with the computer system to implement all the actions described in Table 2, child modal forms are used. The results of confirmed data transactions are displayed in a single relational database.

## 3.3. Data storage

Data and system logic are shared between the database, user interface, and business rule algorithms for implementing information operations with data. According to the proposed system architecture (Figure 1), the normative and operation data are subject to storage in the data storage, implemented in a relational database. The normative information of the system includes:

- set of graphic notations;
- list of developed projects;
- description of technological systems and a set of events.

The input information of the system, which has the properties of dynamism and is entered by operators, is the relationship between events, the intensity of events, the timing of the system, for which it is necessary to calculate the probabilities. The resulting information is a graphical representation of the FT, the formed probability polynomial, the set of calculated probabilities of the base, intermediate and main event, the set of minimum emergency combinations and trajectories. The resulting information is generated by the system automatically according to the input parameters of the calculation.

Database modeling was performed based on the data domain object model with the application of data normalization rules. The specification of the main objects characteristics stored in the database is presented in Table 3.

**Table 3**
Basic entities stored in the database

| Entity | Entity description | Properties | Links to external entities | Relation plurality |
|---|---|---|---|---|
| Tree event | A dynamic entity describing the data of each event included in the tree | The entity is characterized by: name, serial number in the tree, intensity/probability of occurrence, graphical notation. | Event<br>Type<br>Graphic notation | 1:1<br>1:1 |
| Project | Static entity describing the main characteristics of a given data domain | Entity, characterized by the name of the technological system, a description of the main characteristics of the system. | Tree | 1:N |
| Relation | A dynamic entity describing data about the type of relationship between tree events | The entity is characterized by: name, graphic notation, calculation algorithm. | Event<br>Graphic notation | 1:N<br>1:1 |
| Tree | Dynamic entity describing data for system reliability analysis | The entity is characterized by the name, the name of the top event, the date, time of creation. | Event | 1:N |
| Event type | Static entity | The entity is used to determine the type of event: base, intermediate, main | Tree event | 1:1 |
| Graphic notation | Static entity | The entity is used to store and display the type of the project object | | |

Inserting data on the “event” entity, the user is given the opportunity to choose which numerical characteristic will be included in the list of initiating events properties of a particular system: the intensity of occurrence or probability. If the user enters the intensity, the system automatically calculates the probabilities of occurrence for the initiating events for (1) – (2). The obtained probability values are then used to calculate the probabilities of intermediate events and top event probabilities using (3) – (5).

The default calculating period is a calendar year. The user can change this value. If necessary, the user can specify $n$ time calculation periods for which the system will give the results of the probability calculation. Based on the introduced characteristics and calculated probabilities, the system generates minimal cut sets and calculates their contribution to the occurrence of the top event according to (7). Accuracy of probability calculations is $10^{-5}$.

## 3.4. Adequacy substantiation

The adequacy of the implemented design solutions was carried out by checking the manually constructed FTs for different technological systems and the results obtained in the developed system. The data of technological systems were used as a test set:

1. Conveyor system bulk cargo overload in assessing the main undesirable event, “Destruction of the conveyor belt”, data on the intensity of the initiating events, and the results of calculating the probabilities described in the works of A. A. Tverigin.
2. Computer System in estimating the top adverse event “Computer is not functioning” based on A. Saxena and T. Manglani.
3. Filling system in an automotive production line in assessing the main adverse event “Failure in the fluid filling system” based on data from H. Soltanali, M. Khojastehpour, J. T. Farinha, J. E. Pais [5].

Testing the developed software on actual data showed the adequacy of the applied methods, correctness of calculations, and indicators of system reliability. The result of test checks was the conclusion that the implemented design solutions are universal and can be used to calculate the reliability of other technological systems.

# 4. Practical application

After substantiating the adequacy of the implemented software solutions, the developed computer system was used to assess the reliability of the brown smoke suppression system during the release of steel from the blast furnace in the research work “System analysis and computer modeling of technological processes and information technologies” conducted by the team of the Department of Software Systems at Dniprovsky State Technical University. Input data on the technological chain, equipment composition, the intensity of accidents are taken from actual industrial data of technological process logs.

The top event for the analysis and construction of the FT is the emission of brown smoke during the release of steel from the blast furnace.

This event is undesirable because, during the interaction of steel with oxygen, iron oxidizes and partially evaporates, turning into dust, the particles of which rise into the air and form orange (brown) smoke. Emissions of brown smoke reduce the volume of fused steel by 0.0025-0.0075%, significantly pollute the environment, and threaten employees.

The technological system is supplemented by various devices controlled through an automated control system to minimize the formation of brown smoke – the type of automated workplace shown in Figure 2.

The input parameters for building a FT in a given data domain are technological processes set, technological events, and technological equipment, presented in a hierarchical dependence of system states and transitions between them.

The array of input data describing the baseline events was set with the values of the intensity of occurrence and the period $t$ = 1 year. The set of initiating events $BE=\{BE_1,\ldots BE_{11}\}$, their description and intensity are given in Table 4.

The set of intermediate events $IE=\{IE_1,\ldots IE_8\}$, the occurrence of which contributes to the development of the emergency situation consists of 8 events described in Table 5.

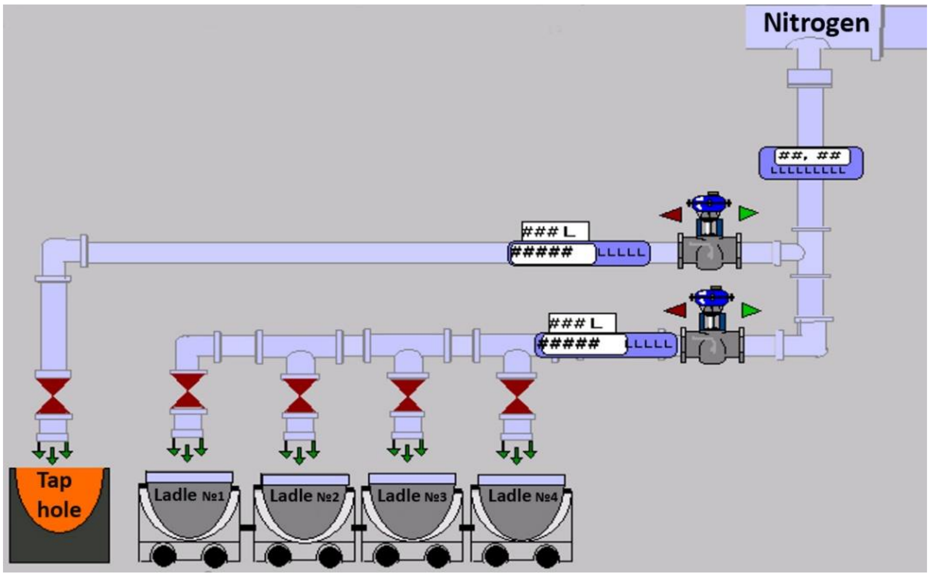


**Figure 2**: The main screen of the automated brown smoke suppression system

**Table 4**
List of initiating events of the brown smoke suppression system

| Event number | Event name | Intensity of occurrence, 1/year |
|---|---|---|
| BE1 | Power plant №1 failed | 0,00500 |
| BE2 | Power plant №2 failed | 0,00500 |
| BE3 | Lack of nitrogen in the tanks | 0,01000 |
| BE4 | Engine failure | 0,02000 |
| BE5 | No engine power | 0,03200 |
| BE6 | No connection to controller | 0,02800 |
| BE7 | Network switch failure | 0,02800 |
| BE8 | The controller power supply burned out | 0,03100 |
| BE9 | The limit switch has failed | 0,03300 |
| BE10 | Damage of electrical power wires | 0,03700 |
| BE11 | Voltage surge | 0,02400 |

**Table 5**
List of intermediate events of the brown smoke suppression system

| Event number | Event name |
|---|---|
| IE1 | There is no electricity |
| IE2 | There is no nitrogen pressure |
| IE3 | The dome of the tap hole does not fall |
| IE4 | The dome of the ladle does not fall |
| IE5 | There is no pressure in the network |
| IE6 | Closed valve |
| IE7 | Pressure sensor failure |
| IE8 | Lack of power to the pressure sensor |

After entering the input data, the user is allowed to view the results of the automatic FT design and analyze the results of automatic calculations. The screen form of the system with the generated tree is shown in Figure 3. The events B9-B14 on Figure 3 are the same as BE3-BE8 respectively. The events B15 B16, B17 are the same as BE9, BE10, BE11 respectively.

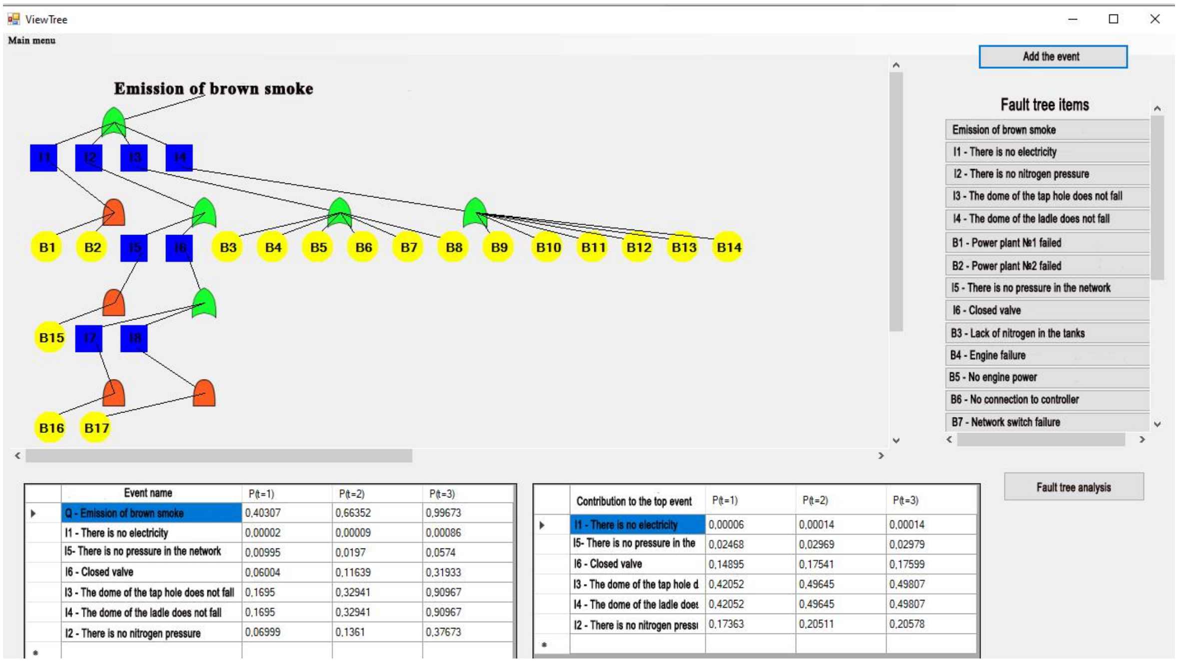


**Figure 3**: Screen form with constructed FT

The screen form of the resulting information is divided into three parts:

1. The area of the FT graphical representation.
2. The area of the output descriptions of the events entering into the FT;
3. The area of calculated data presentation.

Standardized graphical elements for events and logical elements are used to increase the visibility of the displayed FT.

Each event graphic element contains its sequence number in the event list, displayed in an additional area of the screen form.

The top event has the sequence number 0, the base and intermediate events are marked with the sequence number of their set. There are no restrictions on the number of basic, intermediate events and logical elements.

As the size of the FT increases, horizontal and vertical scrolls appear on the screen. The graphic representation of the tree can be exported as a graphic element.

The data generated by the system allows for qualitative and quantitative analysis of the generated FT. The result of the qualitative analysis is the formed set of minimal emergency combinations.

For the case under consideration, $C=\{C_1,..,C_6\}$ and is described as:

$$\begin{gathered} C_1 = BE_1 \cap BE_2, \\ C_2 = BE_3, \\ C_3 = BE_{10} \cup BE_{11}, \\ C_4 = C_5 = BE_4 \cup BE_5 \cup BE_6 \cup BE_7 \cup BE_8 \cup BE_9, \\ C_6 = BE_3 \cup BE_{10} \cup BE_{11}. \end{gathered} \quad (8)$$

The probability $PT$ of the top event occurrence event can be calculated as follow:

$$PT = 1 - [(1 - PC_1)(1 - PC_2)(1 - PC_3)(1 - PC_4)(1 - PC_5)(1 - PC_6)]. \quad (9)$$

where $PC_1,..,PC_6$ is the probability of the $i$-th minimum emergency combination leading to the top event. Quantitative analysis of the tree is performed by the system automatically based on (8) - (9). The results of calculating the probabilities of occurrence of all intermediate events are presented in Table 6. The probabilities of occurrence of the minimum cut sets, and their weight in the occurrence of the main event are shown in table 7.

The estimated probability of occurrence of the main event is 0.40757. Obtained data can be used to identify potential causes of failure, understand co-occurrence events that lead to system failure, establish a list of measures to reduce the probabilities of a “brown smoke emission” event, and increase the reliability of the process as a whole.

**Table 6**
Automatically calculated probabilities of intermediate events

| Event number | Event name | Calculated probability of event occurrence for t=1 year |
|---|---|---|
| IE1 | There is no electricity | 0,00002 |
| IE2 | There is no nitrogen pressure | 0,06854 |
| IE3 | The dome of the tap hole does not fall | 0,16950 |
| IE4 | The dome of the ladle does not fall | 0,16950 |
| IE5 | There is no pressure in the network | 0,00995 |
| IE6 | Closed valve | 0,05918 |
| IE7 | Pressure sensor failure | 0,02371 |
| IE8 | Lack of power to the pressure sensor | 0,03632 |

**Table 7**
Automatically calculated probability of cut sets

| Event number | Probability of occurrence | Contribution to the top event |
|---|---|---|
| C1 | 0,00002 | 0,00006 |
| C2 | 0,00995 | 0,02469 |
| C3 | 0,06004 | 0,14895 |
| C4 | 0,16950 | 0,42053 |
| C5 | 0,16950 | 0,42053 |
| C6 | 0,06999 | 0,17364 |

## 5. Conclusions

Determining the reliability of technological systems is an important task. It allows identifying hazardous parts of the technological system and developing measures to minimize adverse events. One of the ways to quantitatively and qualitatively assess the system's reliability and the probability of occurrence of a particular event is FTA, which allows to visually and mathematically describe a given technological system.

The developed computer system is a unified software tool for creating FTs and risk analysis of technological systems. It is not adapted to a specific data domain or a specific process, expertly dependent at the stage of process description and entering of input parameters of the frequency of occurrence of events included in the FT.

The primary purpose of creating a computer system for FT design is to increase the speed of FT construction, automatic polynomial construction to calculate the probabilities of the intermediate and main event, increase the accuracy of calculation, minimize the impact of skills and accuracy of analysts' calculations. Otherwise, the calculation is performed automatically under the rules for constructing a probabilistic polynomial, changing the incoming system parameters to analyze risks and identify the most vulnerable points in the system. Using trace-back algorithm makes it possible to calculate the probability of FT events occurrence starting from the lowest level. Application of the Fussell-Vesely algorithm allows evaluating the contribution of each event to the probability of the main undesirable event occurrence.

The paper describes main functional requirements for the system, defines the target audience, functions, and available actions depending on the level of data access rights. The system architecture is multi-layered, which ensures the logical and functional independence of the layers. The system data storage is implemented in the form of a relational database that allows storing data on the results of design and analysis of the FT. Testing of the developed system on real industrial data showed the adequacy of the applied methods, correctness of calculations and indicators of system reliability. The practical value of the proposed system is applicability to various data domains, no restrictions on the size of the studied system, the ability to save and export data.

## 6. References


[1] D. Gabriska, Evaluation of the level of reliability in hazardous technological process, Applied Sciences 11 (2021) 1–13. doi: 10.3390/app11010134.

[2] M. Leimeister, A. Kolios, A review of reliability-based methods for rosk analysis and their application in the offshore wind industry, Renewable and Sustainable Energy Reviews 91 (2018) 1065–1076. doi: 10.1016/j.rser.2018.04.004.

[3] N. A. Wessiani, F. Yoshio, Failure mode effect analysis and fault tree analysis as a combined methodology in risk management, in: Proceeding of the International Conference on Industrial and System Engineering, IConISE 2017, IOP Publishing Ltd, Denpasar, Indonesia 2017, pp. 1–11. doi: 10.1088/1757-899X/337/1/012033.

[4] S. Kabir, An overview of fault tree analysis and its application in model based dependability analysis, Expert systems with application 77 (2018) 114–135 doi: 10.1016/j.eswa.2017.01.058.

[5] H. Soltanali, M. Khojastehpour, J. T. Farinha, J. E. Pais, An integrated fuzzy fault tree model with Bayesian network-based maintenance optimization of complex equipment in automotive manufacturing, Energies 14 (2021) 1–22 doi: 10.3390/en14227758.

[6] J. Ignac-Nowicka, T. Krenicky, Fault tree analysis as a tool to increase the level of security in an enterprise, MAPE 1 (2018) 719–725. doi: 10.2478/mape-2018-0091.

[7] N. R. Nurwulan, W. A. Veronica, Implementaion of failure mode and effect analysis and fault tree analysis in paper mill: a case study, Jurnal Rekayasa Sistem Industri 9 (2020) 171–176 doi: 10.26593/jrsi.v9i3.4059.171-176

[8] G.-J. Jiang, Z.-Y. Li, G. Qiao, H.-X. Chen. H.-B. Li, H.-H. Sun, Reliability analysis of dynamic fault tree based on binary decision diagrams for explosive vehicle, Mathematical Problems in Engineering 2021 1–13. doi: 10.1155/2021/5559475.

[9] A. Baklouti, N. Nguyen, J. Choley, F. Mhenni, A. Mlika, Free and open source fault tree analysis tools survey, in: Proceeding of the Annual IEEE International Systems Conference, SysCon 2017, IEEE, Monreal, Canada 2017, pp. 1–8, doi: 10.1109/SYSCON.2017.7934794.

[10] Y. Hiraoka, T. Murakami, K. Yamamoto, Y. Furukawa, Method of computer-aided fault tree analysis for high-reliable and safety design, Transactions on Reliability 65 (2016) 1–17. doi: 10.1109/TR.2015.2513050.

[11] M. Takahashi, Y. Anang, Y. Watanabe, A proposal of fault tree analysis for embedded control software, Information 11(9) (2020) 1–22. doi: 10.3390/info11090402.

[12] G. M. Chodur, X. Zhao, E. Biehl, J. Mitrani-Reiser, R. Neff, Assessing food system vulnerabilities: a fault tree modelling approach, Public Health 18:817 (2018) 1–18. doi: 10.1186/s12889-018-5563-x.

[13] N. A. Zahrin, S. A. Sobri, M. Mohamed, M. F. Mohamed, W. O. Ismail, M. R. Taharin, M. H. Hairi, R. Junid, N. A. Shuaib, Implementation of fault tree analysis (FTA) in manufacruting process: a case study from a wood-based product company, Journal of critical reviews 7 (2020) 3086–3096.

[14] F. Zhang, S. Tan, L. Zhang, Y. Wang, Y. Gao, Fault tree interval analysis of complex systems based on universal grey operation, Complexity (2019) 1–8. doi: 10.1155/2019/1046054.

[15] F. Oshiro, Using quantitative fault tree analysis based on methods of cut sets to predict failure, 2021. URL: https://reliabilityweb.com/articles/entry/using-quantitative-fault-tree-analysis-based-on-method-of-cut-sets-to-predi

[16] A. Saxena, T. Manglani, Enhahcing computer system reliability using fault tree analysis, International Journal of Recent Research and Review 6 (2013) 12–17.

[17] K. Yalova, K. Yashyna, The 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, IEEE, Cracow, Poland 2021, pp. 774–778.