UDC.718:519.217 **doi:10.32620/reks.2022.2.12**

Leonid OZIRKOVSKYY[1,2], Bohdan VOLOCHIY[1,2], Oleksandr SHKILIUK[1], Mykhailo ZMYSNYI[1], Pavlo KAZAN[2]

[1] ***Lviv Polytechnic National University, Lviv, Ukraine***
[2] ***Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine***

FUNCTIONAL SAFETY ANALYSIS OF SAFETY-CRITICAL SYSTEM USING STATE TRANSITION DIAGRAM

The subject of research *is to determine the functional safety indicators of a fault-tolerant safety-critical system, namely, the minimal cut sets' probability for a given duration of the system's operation, using the state transition diagram (STD).* ***The aim*** *is to create a new method for analyzing the functional safety of a fault-tolerant safety-critical system. This method is based on the methodology of developing models of operational reliability behavior in the form of STD. This methodology provides a detailed representation of inoperable states and their relation with pre-failure (inoperable critical) states.* ***The task*** *is to propose a new classification for inoperable states of the STD to obtain all possible emergencies in the same space of inoperable states. This approach allows consideration the correlations between the failures, that it is impossible to use the fault trees. Since the space of inoperable states can reach hundreds and thousands of states, a method is proposed for their automated determination according to the classification.* ***The state space method*** *was used to conduct the validation of the method of functional safety analysis. The following* ***results*** *were obtained: the system of Chapman-Kolmogorov differential equations is formed in accordance with the STD and it provides the dependence of the functional safety indicator – the minimal cut sets' probability as a function of the operational duration of the fault-tolerant safety-critical system. This dependence is called the emergency function. The method for determining the emergency function is based on the usage of the emergency mask. Note that the proposed model of operational reliability behavior in the form of STD provides the possibility to conduct both the functional safety and the reliability indicators. The value of the minimal cut sets' probability for a given duration of operation is determined using the fault tree for the validation of the proposed method of functional safety analysis. The fault tree was built by Reliasoft BlockSim software. The obtained value coincides with the value of the minimal cut sets' probability, which was defined by the emergency function for the same operational duration. Thus, the designer can comprehensively analyze the feasibility of introducing redundancy (structural, temporal, functional).* ***Conclusions****: the scientific novelty of the obtained results is the following: the new method for determining safe, critical and catastrophic states in the set of inoperable states is used in the methodology of the STD developing to obtain the stochastic model of operational reliability behavior of fault-tolerant safety-critical system. This technique ensures an automated defining of emergency function by using an improved structural-automatic model.*

Keywords: *functional safety; safety-critical system; reliability engineering; safety engineering; minimal cut sets; fault tree analysis; Markov analysis.*

1. Introduction

The majority of modern electronic information systems belong to the class of critical systems. A detailed overview and classification of such systems is presented in the paper [1].

A Safety-Critical System (SCS) is a software and hardware system and its inoperability results in an emergency at a site where it is installed. The emergency at the site poses a threat to human life or health, an environment or other systems [1 – 3]. Examples of SCS are control systems for complex technical objects such as (telecommunications systems, transport (aviation, railways, pipelines)), medical and robotic systems, energy systems, military equipment, technological lines, etc. [1, 4]. For designing such systems firstly, along with the reliability indicators, the requirements are set for ensuring a given level of functional safety. The required level of SCS functional safety is set at the stage of its system design. At other stages of the system's life cycle, safety can be maintained only through the stability of technological processes, maintenance and proper operation.

According to IEC 61508 and ISO 26262, safety is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment. Functional safety is part of the overall

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

safety that depends on a system or equipment operating correctly in response to its inputs. Safety can be determined as an absence of unacceptable risk due to hazards caused by mal-functional behavior of electrical and/or electronic systems and the interactions of these systems. A characteristic feature of SCS is the ability to actively respond to potentially dangerous situations and minimize its consequences [5]. To do this, additional means of ensuring functional safety are introduced into the structure of the SCS, which reduces its reliability.

Therefore, the problem of ensuring a given level of functional safety of SCS without reducing its reliability is relevant for system design. So, it is needed to identify the "weaknesses" of the system and to introduce some kind of redundancy. It is possible to check the efficiency of such solutions either at the stage of field tests, or by modeling the operational behavior of systems in case of failure. As the cost of unsuccessful solutions due to potential consequences for SCS is very high, so the checking should be done only at the stage of system design. For this, it is necessary to have appropriate models, methods and software that allow to consider several options for design solutions for limited time of the system design stage and reject the unsuccessful ones. This approach allows not only to ensure the necessary reliability and functional safety, but also to reduce the amount of field tests.

2. State-of-the-Art of obtaining functional safety indicators

To quantify the functional safety indicator, namely the risk of SCS operation, the minimal cut sets' probability is used. The development of the fault tree (FT) is carried out to obtain this indicator that allows identifying critical sections of the system in terms of functional safety [6, 7].

Minimal cut sets (MCS) are combinations of the minimum number of failures of system elements that lead to an emergency [6]. Removing at least one defective element of the system from the combination of the minimum number of failures of the elements of this system prevents an emergency [7]. Using minimal cut sets give us the possibility to assess the impact of failures of elements sets on the occurrence of a system emergency and to identify critical elements of the system ("weaknesses of the system"), in terms of the risk of its operation [8]. The indicator "the probability of MCS" is the quantitative assessment of the risk of operation of fault-tolerant SCS, which considers the loss of performance of its elements [6 – 8].

Another indicator for assessing functional safety is the risk factor – RPN (Risk Priority Number), which is determined using FMEA/FMECA analysis technology [9, 10]. The key point in this technology is to obtain the MCS, the probability of which is the quantitative indicator of the risk of system's operation [11]. And considering its value, the indicator is determined as the average value of the frequency of emergencies (Occurrence), which is part of the RPN [12].

Minimal cut sets are obtained by transforming the logical structure of a fault tree by Boolean algebra [7]. As a result of transformations, a new tree is logically equivalented to the original, which consists of a top-level event "accident", a logical element "OR" and minimum sections as basic events, combined with logical elements "AND" [6, 7].

However, the existing method of obtaining MCS has a number of significant shortcomings, which reduces the feasibility of its use at the stage of system design of SCS [13]:

– the probability of MCS is determined only for one (fixed) value of the duration of system's continuous operation (operational duration);

– it is problematic in the fault trees to consider the sequence of events that occur after the failure of separate subsystems or modules. For example: backup system connection, repair and replacement of faulty subsystems or modules, etc. Therefore, the value of the probability of MCS differs significantly from the real value;

– fault-tolerant configurations, in particular sliding reserve, combined structural reserve, etc., are incorrectly implemented using fault trees, which leads to overestimation or underestimation of the probability of an emergency;

– when making changes to the structure or algorithm of the system, the fault tree should be rebuilt. And this requires a lot of labor and time resources.

These shortcomings are partially eliminated in the methodology of development of dynamic fault trees (DFT) [14 – 16]. The main differences between DFT and conventional FT are the introduction of new dynamic types of logical elements or dynamic vertices (operators) [15], which are implemented by, Petri nets, Bayesian networks [14], Markov models [16].

However, a significant part of the shortcomings characteristic of FT are remained for DFT. For example, it is difficult to consider the operational reliability of the system in the presence of functional redundancy, it is impossible to display correctly the limited number of repairs and it is impossible to consider the downtime of the system during maintenance. In addition, DFT does not allow considering the influence of means of control, diagnosis and switching on the value of the probability of MCS.

The use of DFTs at the stage of system design is limited due to their construction is not automated, so it requires a lot of expertise and manual steps. Therefore, it is an expensive procedure both for money and time

required to build DFT. This is especially noticeable when considering modifications of the system's structure and the corresponding restructuring of the fault tree.

Binary decision diagram [17, 18] is a powerful tool for MCS carrying out. This tool allows quick and accurate determining of probability of system emergency.

Based on the analysis, the task of development the method for obtaining the values of probability of MCS, which considers both operational and reliability behavior of the system is relevant with various ways to increase its reliability due to fault tolerance (different types of redundancy, maintenance and repair) and functional safety (control and diagnostics). Therefore, the credibility of the values of the probability of the MCS should be increased. However, the method should have high degree of formalization and be suitable for automated use for elimination of the main limitations of FT and DFT, namely a manual construction of tree. And this is especially relevant for a multivariate analysis of fault-tolerant software and hardware SCS at the stage of their system design.

3. Application of the state space method for the analysis of functional safety indicators

Safety-critical systems during their operation may be in certain states. Changing the mode of operation or values of system's parameters determines the transition from one state to another, and the duration of staying in each state is a random variable. Therefore, the model of SCS behavior is discrete-continuous stochastic model, and the method used to conduct the research is called the state space method [19 – 21].

The state space method is widely used at the stage of system design of various complex systems, including SCS [22]. The model formed by this method is presented in the form of a system of Chapman-Kolmogorov linear differential equations, and allows an adequate representation of all features of the structure and operation algorithm of fault-tolerant SCS:

$$\frac{d\bar{P}(t)}{dt} = A \cdot \bar{P}(t), \qquad (1)$$

where $\bar{P}(t)$ – vector-column of probabilities of SCS staying in states;

A – matrix of intensities of transitions from state to state.

As a result of solving the system of differential equations (1) we obtain the dependences of the distribution of the probability of staying in the states of the graph on the duration of SCS operation and the average values of the duration of SCS being in each state:

$$P_1(t),\ P_2(t),\ ...,\ P_i(t),\ ...;\ \bar{T}_1,\ \bar{T}_2,\ ...,\ \bar{T}_i,\ ...; \qquad (2)$$

where Pi(t) – probability of SCS in the i-th state;

i=1…s, s – number of states;

$\bar{T}_i$ – average value of the duration of being in the i-th state.

From the obtained probability distribution, it is possible to form expressions of both standardized and non-standardized performance indicators by summing the probabilities of being in the appropriate states. It is important that a developer receives the value of these indicators at the stage of system design.

The use of the state space method is regulated by a number of international (FIDES, MIL-HDBK-217, Telcordia SR-332, MIL 217 Plus, IEC TR 62380) and Ukrainian (DSTU 2861-94) standards. However, at the stage of system design, the practical use of the state space method is quite limited due to the complexity of developing models whose phase space is 10^2 - 10^5 states and, accordingly, the system of differential equations has the same order. And considering the need to solve the problem of synthesis through multivariate analysis, in most cases it is performed using typical simplified models [23, 24].

The technique of using the state space method is partially implemented in a number of well-known software products such as ReliaSoft Synthesis Master Suite (ReliaSoft USA), RAM Commander (ALD, Israel), Reliability Workbench (Isograph, USA, UK), PTC Windchill Quality Solutions (PTC, USA), Item Toolkit (Item Software, USA, UK). However, in these software products, models in the form of state transition diagram (STD) are built manually with the subsequent automated solution of the system of differential equations of the form (1) and obtaining reliability indicators.

In paper [25] the improvement of the technique of using the method of state space is shown. As a result of improvement, the construction of the STD is carried out automatically. Automated construction of the STD is based on a structural-automatic model [25]. Structural-automatic model (SAM) is a formalized representation of the structure and algorithm of SCS behavior in the form of three data sets: state vector, reliability and functionality of fault-tolerant SCS components and tree of rules for modification of state vector components.

The algorithm for automated graphing of STDs is implemented in the software ASNA [26]. Basing on the structural-automatic model, ASNA software automates the construction of the STD and forms an analytical model in the form of a system of Chapman-Kolmogorov linear differential equations.

The state space method is not used to assess functional safety indicators. On the one hand, in the known methods of obtaining the STD, all inoperable

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

states which lead to an emergency are combined into one absorbing state. For the reliability analysis of SCS failure, the consequences of the failure itself are not considered.

On the other hand, if inoperable states are not combined, the total number of states increases by 2 or more times. In the case of manual construction, the time spent on obtaining STD can significantly exceed the duration of the stage of SCS system design. The method that ensures the obtaining of MCS directly from the STD was not found during the informational search.

4. Separation of inoperable states into safe, critical and catastrophic states

In order to analyze the functional safety indicators of SCS, in contrast to the analysis of reliability indicators, it is necessary to have a distribution of the probability of the system being inoperable. Moreover, it is important not only to separate the space of states into operable and inoperable states, but also to classify inoperable states into states that directly lead to an accident and that lead to an accident after passing through several intermediate states.

It should be noted that the improved state space method is described in the monograph [25] and does not involve the selection of types of disabled states, as it was focused on the analysis of the reliability of fault-tolerant SCS.

The scheme of construction of the general model of SCS functioning with considering various groups of reasons of failures and division of failures into safe and dangerous is resulted in work [27].

Thus, to obtain the values of the probabilities of MCS with STD, it is necessary to correctly separate all possible inoperable conditions in which the system can be, into the following groups:

– inoperable safe states are states that the system enters after failure of subsystems or modules. However, from these states the system does not directly fall into an emergency;

– critical (pre-emergency) states are the states that the system enters and that precede the emergency. The next step is for the facility where the SCS is installed to be in an emergency;

– catastrophic (emergency) conditions are conditions that correspond to the actual emergency for the site where the SCS is installed.

This classification of conditions makes it possible to compose formulas for determining the functional safety indicator directly from the STD from the distribution of probabilities of being in inoperable safe, critical and catastrophic conditions. At the same time, formulas for determining reliability indicators are compiled from the same STD, on the basis of operational states, and accordingly, it is possible to study the influence of increasing functional safety on the reliability of the system.

The block diagram of the method of separation of disabled states is shown in Fig. 1, and the method itself is described in work [28]. For the practical implementation of this method, an improvement of the structural-automatic model was carried out, that is given in paper [29].

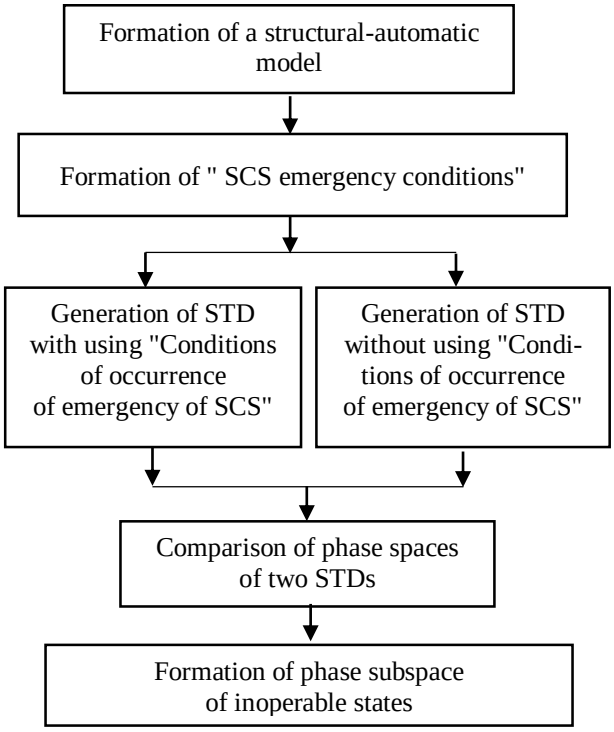

Fig. 1. Block diagram of the method for formation inoperable safe, critical and catastrophic conditions

Thus, from the state transition diagram (Fig. 2), the values of both functional safety indicators (from classified inoperable states) and the values of system reliability indicators (from operational states) can be got. Such structural-automatic model is called a comprehensive model of SCS.

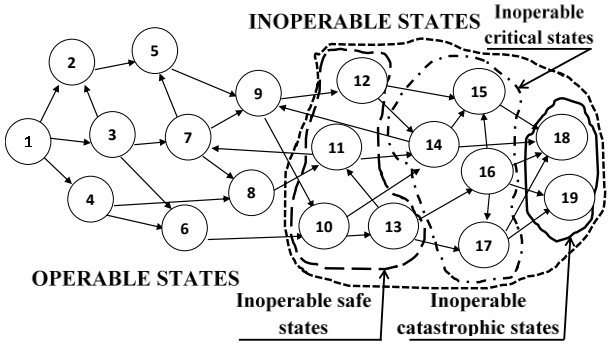

Fig. 2. State transition diagram with separate space of inoperable states for emergency function determining

We note as well that the comprehensive model (STD) allows us to study the dependences of the impact of reliability tools on the value of the safety indicator and safety tools on the value of the reliability indicator.

With such model it is possible not only to determine the indicators of functional safety and reliability, but also to study the impact on the safety of the introduction of fault-tolerant configurations, the application of certain maintenance, recovery strategies and more.

To represent emergencies by the relevant group of incapacitated conditions, it is necessary to form a logical expression "SCS emergency conditions" for each emergency situation of the SCS.

The logical expression "SCS emergency conditions" is formed from the components of the state vector (SV), connected by logical operations. This expression is necessary for the selection from the STD the states that are included in the set of inoperable states corresponding to the emergency situation.

Considering the affiliation of a certain part of the inoperable states of the STD to two or more aggregates (groups) of emergency situations, it is necessary to minimize the logical expression "SCS emergency condition", using the rules of Boolean algebra. This gives the possibility to consider the interdependence of emergencies and get rid of the significant shortcoming of FT and DFT when it is considered (assumed) that all emergencies are independent.

The division of the array of inoperable states of the SCS is performed in the following sequence:

1) the minimized "SCS emergency condition" is introduced into the structural-automatic model of fault-tolerant SCS. "SCS emergency condition" is a condition of combining all inoperable states into one state. On the basis of such SAM, using ASNA software, the construction of the first STD is carried out. The result is an array of all possible operable states and one state in which all inoperable states are combined;

2) the "SCS emergency condition " is removed from the structural-automatic model. On the basis of this SAM, using ASNA software, the construction of the second STD is carried out. This STD includes in addition to all operable conditions, all inoperable conditions;

3) comparing the states of both STDs it is necessary to remove the operable conditions that are in the first and in the second STD. As a result, we get an array of all inoperable conditions.

5. Formation of the emergency function to assess the functional safety

To assess the functional safety of systems using FTs or other logical-probabilistic methods, the concept of MCS, which is represented in the form of logical functions [6 – 8, 13], is used. However, an approach for determination the probability of MCS using the state space method is not known. By the way, applying our experience of developing models in the form of STD, we suppose that such possibility exists. Moreover, the model in the form of STD makes it possible to obtain dependence of the MCS probability due to the operational duration. We propose to call such dependence as an "emergency function".

Thus, the emergency function (EF) is a dependence of the probability of MCS that lead to an emergency situation within the operational duration of the SCS.

The value of the emergency function is defined as the sum of the probabilities of being in safe, incapacitated, critical and catastrophic states. The transitions between these states show the trajectory of the transition (evolution) of the system from insignificant failure to accident. Moreover, the fewer transitions are from inoperable to catastrophic safety, the worse functional safety of the system is, and accordingly there are fewer opportunities to avoid an emergency.

The value of the emergency function is defined as the sum of the probabilities of being in safe inoperable, critical and catastrophic states. The transitions between these states show the trajectory of the transition (evolution) of the system from insignificant failure to accident. Moreover, the fewer transitions are from inoperable to catastrophic safety, the worse the functional safety of the system is, and accordingly there are fewer opportunities to avoid an emergency.

Properties of the emergency function:

– the emergency function is a non-negative function

$$Q_A(t) = \begin{cases} 0, \ t = 0; \\ f(t), \ 0 < t < \infty; \\ 1, \ t = \infty; \end{cases} \qquad (3)$$

– for a particular system, the number of emergency functions QA(t) is equal to the number of MCS leading to an emergency;

– the value of the emergency function for a specific service life of the system is equal to the MCS probability, which is obtained from FT for the specific operation time of the system;

– the combination of all emergency functions QA(t) corresponds to the probability of emergency QAS(t) for the specific operation time of the system:

$$Q_{AS}(t) = 1 - \prod_{i=1}^{k} (1 - Q_{A_i}(t)), \qquad (4)$$

where $Q_{Ai}(t)$ – the i-th emergency function;

k – number of emergency functions.

The method of determining the emergency function is shown in the following sections.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

5.1. Creating an emergency mask to create an emergency function

To create the expression of EF, it is necessary to establish a set of inoperable conditions that lead to an emergency. Since the same conditions may be part of different EFs, it is necessary to have the ways to unambiguously identify them. It is proposed to use the emergency mask as such a tool.

The emergency mask is a logical expression formed from the components of the state vector. In the case where they take a value equal to 0, this is a necessary and sufficient condition for an emergency. The emergency mask is obtained from the "SCS emergency conditions" by minimizing it according to the rules of logic algebra.

The emergency mask has the following properties:

– if the logical expression that describes the emergency situation for SCS consists of components of the state vector, combined only with the operator "AND", then such SCS is characterized by one emergency function:

$$(V_g = 0) \wedge (V_h = 0) \wedge ... \wedge (V_k = 0),$$

where V_g, V_h, … , V_k – components of the vector states of SCS, which describe state of its modules.

– if the logical expression describing the emergency situation for the SCS consists of N groups of components combined by the operator "OR", and in each group the components of the SV are combined only by the operator "AND", then such SCS has number of N emergency functions:

$$((V_m = 0) \wedge (V_n = 0) \wedge ... \wedge (V_q = 0) \vee ... \vee \vee ((V_s = 0) \wedge (V_t = 0) \wedge (V_y = 0)).$$

For example, if the following logical expression is obtained as a result of minimizing the "SCS emergency condition", consisting of three groups of the SV components connected by the logical operator OR:

$$((V1 = 0) \wedge (V2 = 0) \wedge (V3 = 0)) \vee \vee ((V2 = 0) \wedge (V5 = 0)) \vee ((V1 = 0) \wedge (V5 = 0)).$$

Then in this case there are three emergency functions. The first emergency function is formed by inoperable states of the system, in which the 1st, 2nd and 4th modules are inoperable. The second EF is formed by inoperable states of the system in which the 2nd and 5th modules are inoperable, and the third is formed by inoperable states of the system in which the 1st and 5th modules are inoperable. The emergency function is formed on the basis of the received masks.

5.2. Formation of the emergency function from disabled states

The formation of EF consists of two stages. At the first stage, a group of states corresponding to a specific EF is determined from the set of inoperable states by using the emergency mask. At the second stage expressions are formed from the selected states to calculate the values of array of transition rates (ATR).

Identification of groups of states corresponding to one emergency function. All states in which the components of the SV that correspond to 0 in the emergency mask are selected. If the emergency mask has several components combined by the logical operator OR, then accordingly there is the EF. So, for each EF there is a group of states in the STD.

The input data for the method is a set of inoperable states, which are obtained from the STD. To obtain an array of inoperable conditions, it is necessary to use the method described in papers [28 – 30].

To develop an algorithm for automated determination of ATR, the following statements are proposed:

– at least one emergency function is inherent for any fault-tolerant SCS;

– catastrophic state is a state in which the SCS is in an emergency situation;

– if at least for one component of the SV, which has value of 0 and is included in the ATR, the value of 1 is given in all these inoperable states (transit into working state), then the SCS emergency is not happened.

To find the ATR, it is necessary to organize the array of inoperable states of the SCS on the basis of the smallest number of events that lead to an emergency situation of the system. That is, the minimum number of components of the SV, which is equal to 0. These are those inoperable states into which the transition was made directly from the operable state. As a rule, there are inoperable safe conditions. On the basis of the sorted array of inoperable states of the system, in accordance with the components of the emergency mask find the states of the system, from which some specific EF is formed. The result is an ATR.

Sorting of emergency masks components. Sorting is performed by comparing two adjacent components of the emergency masks. In the matrix of the components of the emergency mask, you need to swap the components of the mask, i.e. swap the components of the SV.

As a result of moving the components of the emergency mask in the matrix, a sorted matrix of these components is obtained. Sorting is performed by the number of 0 values in the ATR. The first row of the resulting matrix contains the SV with the smallest number of components whose values are equal to 0.

This line corresponds to the component of the emergency mask. The next is the component of the SV mask with the same or more components of the SV, which are equal to 0 and so on until all states are selected for which the value of the component of the SV corresponds to the emergency mask.

Formation of expressions for emergency functions. The result is a matrix which contains four columns: the sequence number N of ATR is recorded in the first column, and the component of the SV and its value is written in the second column, the state numbers of STD, which form the corresponding ATR, is written in the third. The procedure for obtaining the probability values of the corresponding AFs is to sum the values of the probabilities of staying in the STD states, the numbers of which were recorded in the third column of the corresponding EF in the EF array. The result is filled in the fourth column.

Thus, the formula for determining the values of the emergency function is equal to the sum of the probabilities of being in those states that correspond to the mask of the emergency situation.

$$Q_{A_i}(t) = \sum_{j=m}^{q} P_j(t) + \dots, \qquad (5)$$

where $P_j(t)$ is the probability of SCS in the j-th group of inoperable states m…q, in which the value of the component of the SV is 0 in accordance with the i-th emergency mask. The group of inoperable conditions in the simplest case can include all inoperable conditions. For fault-tolerant SCS, there may be several groups of such states in the STD.

For example, if the emergency mask is:

$$(V1 = 0) \wedge (V2 = 0) \wedge (V4 = 0).$$

And it corresponds to the states of STD number 20… 27 and 32… 35, i.e. in these states the SV components V1, V2, V4 are 0, and components V3, V5 are any other value than 0, the expression for EF is defined as:

$$Q_A(t) = \sum_{i=20}^{27} P_i(t) + \sum_{i=32}^{35} P_i(t).$$

6. Validation the developed methods and techniques

Validation of the developed methods and techniques was performed for tested fault-tolerant SCS by comparing the values of the MCS probabilities, which were obtained from a comprehensive model in the form of STD, and the MCS probability, which were obtained from the FT by Reliasoft BlockSim software.

A fault-tolerant system consisting of two different redundant modules was used as a tested fault-tolerant SCS. The structural scheme of reliability of fault-tolerant SCS is presented in fig. 3. Both modules have hot reserve. The first module, as less reliable, has two backup modules, and the second has one backup module. If the main module fails, the backup module is connected instead. Switching devices are considered to be absolutely reliable and fast. The duration of switching is considered infinitesimal. Backup modules can fail regardless of the main ones.

At the first stage of validation, the SAM was built and on the basis of which a STD, which has 32 states, was generated. According to the method [29], the array of inoperable conditions was determined. In the obtained STD, states 1-7, 9-15, 17-23 are operable. Conditions 8, 16, 24-32 are inoperable, so depending on these states the emergency functions are formed.

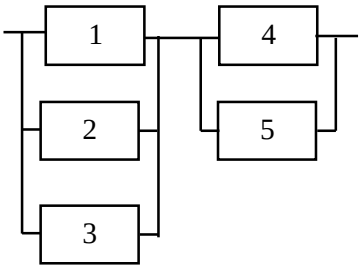

Fig. 3. Reliability block diagram of tested fault-tolerant SCS

For the formation of emergency functions, in accordance with the developed methodology, it is necessary to form emergency masks by minimizing the SCS emergency condition:

$$((V1 = 0) \wedge (V2 = 0) \wedge (V3 = 0)) \vee \vee ((V4 = 0) \wedge (V5 = 0)).$$

The first emergency function has a mask:

$$(V1 = 0) \wedge (V2 = 0) \wedge (V3 = 0)),$$

and the second emergency function has a mask:

$$((V4 = 0) \wedge (V5 = 0)).$$

Therefore, the first emergency function is represented by the sum of the probabilities of staying in states in which components V1, V2 and V3 are 0. These are states 8, 16, 24 and 32:

$$Q_1 = P_8(t) + P_{16} + P_{24}(t) + P_{32}(t).$$

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

The second emergency function is represented by the sum of the probabilities of staying in those states in which components V4 and V5 are 0. These are states from 24 to 32:

$$Q_2(t) = P_{24}(t) + P_{25}(t) + P_{26}(t) + P_{27}(t) + \\ + P_{28}(t) + P_{29}(t) + P_{30}(t) + P_{31}(t) + P_{32}(t).$$

Basing on the obtained STD, ASNA software compiled the system of Chapman-Kolmogorov differential equations, solved it, and obtained the distribution of probabilities of staying in each state. The obtained distribution was exported to Excel spreadsheets and constructed emergency functions $Q_1(t)$, $Q_2(t)$, which are presented in Fig. 4.

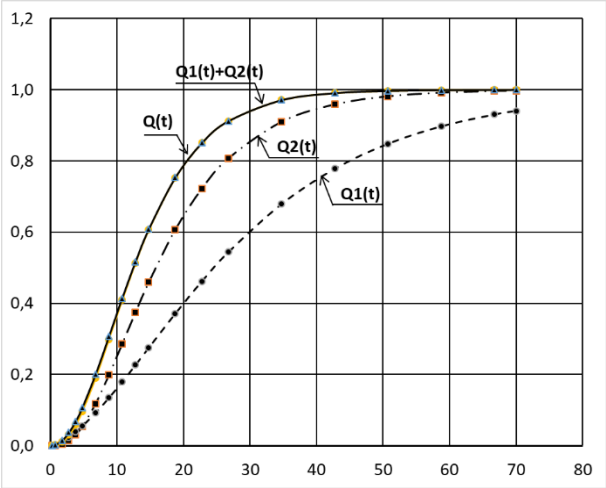

Fig. 4. Emergency functions $Q_1(t)$, $Q_2(t)$ and probability of an emergency Q (t) – curve $Q_1(t)+Q_2(t)$ covered the curve Q(t)

The dependence of the MCS probability due to operational duration as the sum of the probabilities of being in all inoperable conditions is also constructed:

$$Q(t) = P_8(t) + P_{16}(t) + \sum_{i=24}^{32} P_i(t)$$

and as the sum of the emergency functions

$$Q_1(t) + Q_2(t):$$

$$Q(t) = Q_1(t) + Q_2(t) = 1 - (1 - Q_1(t)) \cdot (1 - Q_2(t)).$$

As can be seen from Fig. 4 dependencies of both variants for calculating the probability of an emergency are coincided.

A similar structural reliability block diagram (see Fig. 3) was constructed using ReliaSoft BlockSim graphics editor. The next stage of validation was the transformation of the structural reliability block diagram by tools of ReliaSoft BlockSim into the fault tree, which is presented in Fig. 5. The MCS for this FT also were carried out by ReliaSoft BlockSim.

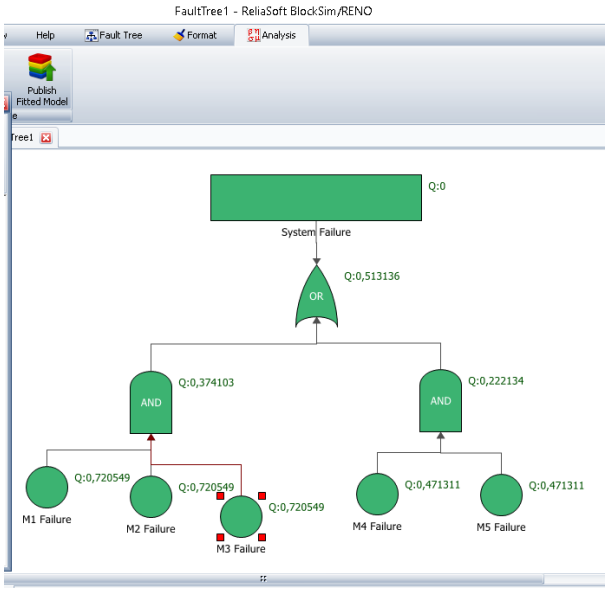

Fig. 5. The fault tree obtained from ReliaSoft BlockSim software

The MCS probabilities of the tested SCS at the same service life were calculated as the emergency function and obtained results were compared with the provided ones by ReliaSoft BlockSim. As it can be seen from Fig. 6 the values of the emergency function Q1(t) and the values of the minimal cut sets' probability MCS1fta are completely coincided. Similarly, the values of the emergency function Q2(t) and the values of the minimal cut sets' probability MCS2fta also are coincided.

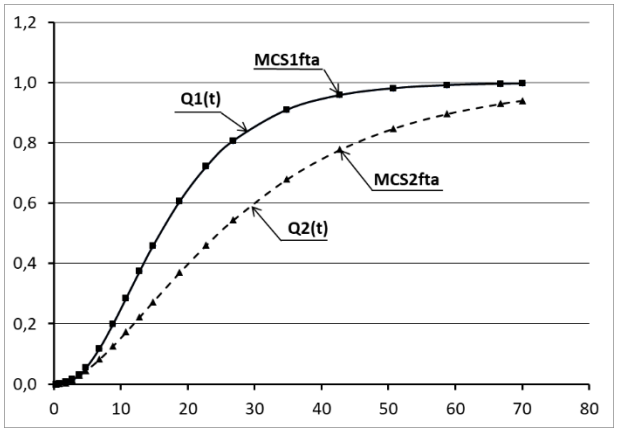

Fig. 6. The value of the emergency function $Q_1(t)$ and $Q_2(t)$ and the value of the minimal cut sets' probabilities MCS_1fta and MCS_2fta

Based on the analysis, the following conclusions can be drawn:

1) developed methods and techniques for determining the value of the minimal cut sets' probability from the STD give reliable results;

2) indicator of functional safety of operation of fault-tolerant SCS, which are still obtained on the basis of the developed fault tree, can be obtained by using the model of operational behavior of fault-tolerant SCS in the form of STD.

7. Conclusions

To overcome the contradiction between the introduction of means for ensuring functional safety and reducing the reliability of SCS, an approach for building the comprehensive model in the form of STD is proposed. This model provides the definition of both reliability and functional safety indicators. For this purpose, a new classification of inoperable states was introduced, which made it possible to obtain the values of the minimal cut sets' probability from the STD without constructing a fault tree. Reliability indicators can also be obtained from the same STD.

1. The comprehensive model in the form of STD provides determination not only of the minimal cut sets probability for a given operational duration without constructing a fault tree, but also to obtain the dependence of the minimal cut sets' probability due to the operational duration.

2. For the practical construction of a comprehensive model of SCS in the form of the STD, a new method was developed for determining safe, critical and catastrophic states in a set of inoperable states. The method is based on the generalized structure of the state vector with a representation of the state of each SCS module and an additional description of its features: maintenance; operational reliability behavior; performance of means of SCS control, diagnostics and switching.

3. To quantify the impact of fault tolerance on safety and the impact of functional safety on reliability, the term of emergency function is introduced. The values of the emergency function for any service life of the SCS are coincided with the values of the minimal cut sets' probabilities obtained for the same service life using the fault tree. The term "emergency mask" is introduced to select the inoperable states that form the expression of the emergency function.

4. The emergency function provides determination of the operational duration of the fault-tolerant SCS, in which the value of the indicator "the minimal cut sets' probability" does not exceed the specified value – the probability of an emergency at the site due to loss of serviceability of the fault-tolerant SCS.

5. The proposed modification of the structural-automatic model provides the automated acquisition of the emergency function. This allows us to provide the multivariate analysis of methods to ensure the functional safety of SCS operation without excessive time, which is crucial for the system design phase. In comparison with the known methods of functional safety analysis, the time spent on obtaining functional safety indicators for one variant of the system is commensurate. However, if it is necessary to analyze changes in the structure of fault-tolerant SCS, in the algorithm of its operation or in the maintenance strategy, the developed methods give a gain in time spent on each new version of the analysis in two or more times.

6. Further research should show the usage of the "emergency function" in the design of fault-tolerant safety-critical systems and the usage of the "emergency function" to analyze the functional safety of critical infrastructure, for which there are contradictions: safety means reduce reliability; or reliability enhancers do not provide the expected increase in functional safety.

Contribution of authors: development of conceptual research provisions, development of mathematical models and analysis of research results, development of methods – **Leonid Ozirkovskyy**; formulation of the goals and objectives of the research, formulation of conclusions – **Bohdan Volochiy**; selection and use of software and hardware for modeling and presentation of results – **Oleksandr Shkiliuk**; validation of developed methods and techniques – **Mykhailo Zmysnyi**; review and analysis of information sources – **Pavlo Kazan**. All authors have read and agreed to the published version of the manuscript.

References (GOST 7.1:2006)

1. Maurya, A. Reliability of safety-critical systems: A state-of-the-art review [Text] / A. Maurya, D. Kumar // Quality and Reliability Engineering International. – 2020. – Vol. 36, iss.7. – P. 2547-2568. DOI: 10.1002/qre.2715.

2. Knight, J. C. Safety critical systems: challenges and directions [Text] / J. C. Knight // Proceedings of the 24th International Conference on Software Engineering ICSE. – 2002. – P. 547-550.

3. Kumar, P. Performance evaluation of safety-critical systems of nuclear power plant systems [Text] / P. Kumar, L. K. Singh, C. Kumar // Nuclear Engineering and Technology. – 2020. – Vol. 52, iss. 3. – P. 560-567. DOI: 10.1016/j.net.2019.08.018.

4. Rausand, M. Reliability of Safety-Critical Systems: Theory and Applications [Text] / M. Rausand.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

– John Wiley & Sons, 2014. – 480 p. DOI: 10.1002/9781118776353.

5. IEC 61508-4:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4: Definitions and abbreviations. [Text]. – Geneva: International Electrotechnical Commission. – 2010. – 68 p.

6. Henley, E. Probabilistic Risk Assessment and Management for Engineers and Scientists [Text] / E. Henley, H. Kumamoto. – Wiley-IEEE Press, 2000. – 600 p.

7. Appendix D: Minimal cut set analysis [Text] / Center For Chemical Process Safety // Guidelines for Chemical Process Quantitative Risk Analysis. – Second Edition. – John Wiley & Sons, 2010. – P. 661-670. DOI: 10.1002/9780470935422.app4.

8. Kohda, T. A Simple Method to Derive Minimal Cut Sets for a Non-coherent Fault Tree [Text] / T. Kohda // International Journal of Automation and Computing. – 2006. – Vol. 3, Iss. 3. – P. 151-156. DOI: 10.1007/s11633-006-0151-4.

9. IEC 60812:2018 – Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA and FMECA) [Text]. – Geneva: International Electrotechnical Commission, 2018. – 165 p.

10. MIL-STD-1629A, Military Standard: Procedures For Performing A Failure Mode, Effects, And Criticality Analysis [Text]. – Department of Defense, Washington DC, 1998. – 54 p.

11. Guidance on Failure Modes & Effects Analyses (FMEAs) [Text] / The International Marine Contractors Association, 2019. – M166, rev. 9. – 99 p.

12. Stamatis, D. H. Risk Management Using Failure Mode and Effect Analysis (FMEA) [Text] / D. H. Stamatis. – ASQ Quality Press, 2019. – 118 p.

13. Adequacy Increase of Assessment of Minimal Cut Sets Considering Latent Failures [Text] / L. Ozirkovskyy, B. Volochiy, A. Mashchak, I. Kulyk // Central European Researchers Journal. – 2019. – Vol. 5, iss. 2. – P. 58-66.

14. Dynamic Fault Tree Analysis: State-of-the-Art in Modeling, Analysis, and Tools [Text] / K. Aslansefat, S. Kabir, Y. Gheraibia, Y. Papadopoulos // Reliability Management and Engineering. – 1 Edition: Chapter 4. – CRC Press, 2020. – 40 p. DOI: 10.1201/9780429268922.

15. Čepin, M. A dynamic fault tree [Text] / M. Čepin, B. Mavko // Reliability Engineering & System Safety. – 2002. – Vol. 75, iss. 1. – P. 83-91. DOI: 10.1016/S0951-8320(01)00121-1.

16. Boudali, H. Dynamic Fault Tree Analysis Using Input/Output Interactive Markov Chains [Text] / H. Boudali, P. Crouzen, M. Stoelinga // Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07). – 2007. – P. 708-717. DOI: 10.1109/DSN.2007.37.

17. Kvassay, M. Minimal Cut Sets and Path Set in Binary Decision Diagrams and logical differential calculus [Text] / M. Kvassay, J. Kostolny // Proceedings of the 10th International Conference on Digital Technologies. – Zilina, 2014. – P. 179-186. DOI: 10.1109/DT.2014.6868712.

18. Pedro, F. Binary Decision Diagrams applied to Fault Tree Analysis [Text] / F. Pedro, G. Marquez // Proceedings of the 4th IET International Conference on Railway Condition Monitoring. – Derby, UK, 2008. – P. 1-5. DOI: 10.1049/ic:20080314.

19. Cui, L. Stochastic Models in Reliability Engineering [Text] / L. Cui, I. Frenkel, A. Lisnianski. – CRC Press, 2020. – 478 p. DOI: 10.120/9780429331527.

20. Reliability Evaluation Techniques [Text] / R. Wang, J. Mathew et al. (eds.) // Energy-Efficient Fault-Tolerant Systems. – Springer Science+Business Media. – New York, 2014. – P. 11-97. DOI: 10.1007/978-1-4614-4193-9.

21. Collins, R. Markov Models: Theory, Algorithms and Applications [Text] / R. Collins. – CreateSpace Independent Publishing Platform, 2017. – 58 p.

22. Reliability Assessment of Multi-cascade Redundant Systems Considering Failures of Intermodular and Bridge Communications. Theory and Engineering of Dependable Computer Systems and Networks [Text] / V. Kharchenko, A. Kovalenko, E. Ruchkov, I. Babeshko // DepCoS-RELCOMEX 2021. Advances in Intelligent Systems and Computing. – Vol. 1389. – Springer, Cham, 2021. – P. 179-188 DOI: 10.1007/978-3-030-76773-0_18.

23. Li, H. A cut/tie set method for reliability evaluation of control systems [Text] / H. Li, Q. Zhao // Proceedings of the American Control Conference. – 2005. – Vol. 2. – P. 1048-1053. DOI: 10.1109/ACC.2005.1470099.

24. Geiger, B. C. Information-Preserving Markov Aggregation [Text] / B. C. Geiger, C. Temmel // Proceedings of IEEE Information Theory Workshop. – 2013. – P. 258-262. DOI: 10.48550/arXiv.1304.0920.

25. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем [Текст] : монографія / Ю. Я. Бобало, Б. Ю. Волочій, О. Ю. Лозинський, Б. А. Мандзій, Л. Д. Озірковський,С.В. Щербовських, В.С. Яковина. – Л. : Видавництво Львівської політехніки, 2013. – 300 с.

26. Volochiy, B. Extending the features of software for reliability analysis of fault-tolerant systems [Text] / B. Volochiy, B. Mandziy, L. Ozirkovskyi // Computational Problems of Electrical Engineering. – 2012. – Vol. 2, no. 2. – P. 113-121.

27. Поночовний, Ю. Л. Методологія забезпечення гарантоздатності інформаційно-керуючих систем з використанням багатоцільових стратегій обслуговування [Текст] / Ю. Л. Поночовний, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2020. – № 3. – С. 43-58. DOI: 10.32620/reks.2020.3.05.

28. Volochiy, B. The New Method of Building a Safety Model for Quantitative Risk Assessment of Complex Technical Systems for Critical Application [Text] / B. Volochiy, B. Mandziy, L. Ozirkovskyy // Communications in Computer and Information Science. – 2016. – Vol. 594. – P. 56-70. DOI: 10.1007/978-3-319-30246-1_4.

29. The Automation of the Exploitation Risks Assessment of the Navigation Information System of Air Drones [Text] / L. Ozirkovskyy, Yu. Pashchuk, A. Mashchak, S. Volochiy // Proceedings of the XIIIth International Conference TCSET'2016 Modern Problems of Radio Engineering, Telecommunications, and Computer Science. – Lviv, 2016. – P. 140-144. DOI: 10.1109/TCSET.2016.7451993.

30. Safety estimation of critical NPP I&C systems via state space method [Text] / B. Volochiy, L. Ozirkovskyy, O. Mulyak, S. Volochiy // Proceedings of 2nd International Symposium on Stochastic Models in Reliability Engineering, Life Science, and Operations Management SMRLO 2016. – 2016. – P. 347-356. DOI: 10.1109/SMRLO.2016.63.

References (BSI)

1. Maurya, A., Kumar, D. Reliability of safety-critical systems: A state-of-the-art review. *Quality and Reliability Engineering International*, 2020, vol. 36, iss.7, pp. 2547-2568. DOI: 10.1002/qre.2715.

2. Knight, J. C. Safety critical systems: challenges and directions. *24th International Conference on Software Engineering ICSE 2002*, 2002, pp. 547-550.

3. Kumar, P., Singh, L. K., Kumar, C. Performance evaluation of safety-critical systems of nuclear power plant systems. *Nuclear Engineering and Technology*, 2020, vol. 52, iss. 3, pp. 560-567. DOI: 10.1016/j.net.2019.08.018.

4. Rausand, M. *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley&Sons Publ., 2014. 480 p. DOI:10.1002/9781118776353.

5. *IEC 61508-4:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4: Definitions and abbreviations*. Geneva, International Electrotechnical Commission Publ., 2010. 68 p.

6. Henley, E., Kumamoto, H. *Probabilistic Risk Assessment and Management for Engineers and Scientists*, Wiley-IEEE Press Publ., 2000. 600 p.

7. Center For Chemical Process Safety. *Appendix D: Minimal cut set analysis. Guidelines for Chemical Process Quantitative Risk Analysis*, Second Edition. John Wiley & Sons Publ., 2010, pp. 661-670. DOI: 10.1002/9780470935422.

8. Kohda, T. A Simple Method to Derive Minimal Cut Sets for a Non-coherent Fault Tree. *International Journal of Automation and Computing*, 2006, vol. 3, iss. 3, pp. 151–156. DOI: 10.1007/s11633-006-0151-4.

9. *IEC 60812:2018 – Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*, Geneva, International Electrotechnical Commission Publ., 2018. 165 p.

10. *MIL-STD-1629A, Military Standard: Procedures for Performing A Failure Mode, Effects, And Criticality Analysis*. Department of Defense, Washington DC, 1998. 54 p.

11. *Guidance on Failure Modes & Effects Analyses (FMEAs). M166, rev. 9*. The International Marine Contractors Association, 2019. 99 p.

12. Stamatis, D. H. *Risk Management Using Failure Mode and Effect Analysis (FMEA)*. ASQ Quality Press, 2019. 118 p.

13. Ozirkovskyy, L., Volochiy, B., Mashchak, A., Kulyk, I. Adequacy Increase of Assessment of Minimal Cut Sets Considering Latent Failures. *Central European Researchers Journal*, 2019, vol. 5, iss. 2, pp. 58-66.

14. Aslansefat, K., Kabir, S., Gheraibia, Y., Papadopoulos, Y. *Dynamic Fault Tree Analysis: State-of-the-Art in Modeling, Analysis, and Tools. In Book Reliability Management and Engineering. 1 Edition: Chapter 4.* CRC Press, 2020. 40 p. DOI: 10.1201/9780429268922.

15. Čepin, M., Mavko, B. A dynamic fault tree. *Reliability Engineering & System Safety*, 2002, vol. 75, iss. 1, pp. 83-91. DOI:10.1016/S0951-8320(01)00121-1.

16. Boudali, H., Crouzen, P., Stoelinga, M. Dynamic Fault Tree Analysis Using Input/Output Interactive Markov Chains. *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)*, 2007, pp. 708-717, DOI: 10.1109/DSN.2007.37.

17. Kvassay, M., Kostolny, J. Minimal Cut Sets and Path Sets in Binary Decision Diagrams and logical differential calculus. *10th International Conference on Digital Technologies*, Zilina, 2014, pp. 179-186. DOI: 10.1109/DT.2014.6868712.

18. Pedro, F., Marquez, G. Binary Decision Diagrams applied to Fault Tree Analysis. *4th IET International Conference on Railway Condition Monitoring*, Derby, UK, 2008, pp. 1-5. DOI: 10.1049/ic:20080314.

19. Cui, L., Frenkel, I., Lisnianski, A. *Stochastic Models in Reliability Engineering*. CRC Press, 2020. 478 p. DOI: 10.1201/9780429331527.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

20. Wang, R. Reliability Evaluation Techniques. *Energy-Efficient Fault-Tolerant Systems*, 2014, pp. 11-97. DOI: 10.1007/978-1-4614-4193-9.

21. Collins, R. Markov Models: *Theory, Algorithms and Applications*. CreateSpace Independent Publishing Platform, 2017. 58 p.

22. Kharchenko, V., Kovalenko, A., Ruchkov, E., Babeshko, I. Reliability Assessment of Multi-cascade Redundant Systems Considering Failures of Intermodular and Bridge Communications. *Theory and Engineering of Dependable Computer Systems and Networks. DepCoS-RELCOMEX 2021. Advances in Intelligent Systems and Computing*, 2021, vol. 1389, pp. 179-188. DOI: 10.1007/978-3-030-76773-0_18.

23. Li, H., Zhao, Q. A cut/tie set method for reliability evaluation of control systems. *American Control Conference*, 2005, pp. 1048-1053. DOI: 10.1109/ACC.2005.1470099.

24. Geiger, B., Temmel, C. Information-Preserving Markov Aggregation. *IEEE Information Theory Workshop*, 2013, pp. 258-262. DOI: 10.48550/arXiv.1304.0920.

25. Bobalo, Yu., Volochiy, B., Lozynsky, O., Mandzii, B., Ozirkovskiy, L., Fedasyuk, D., Scherbovskikh, S., Yakovyna, V. *Matematychni modeli ta metody analizu nadiynosti radioelektronnykh, elektrychnykh ta prohramnykh system* [Mathematical models and methods of reliability analysis of radioelectronic, electrical and software systems]. Lviv Polytechnic Publishing House, 2013. 300 p.

26. Volochiy, B., Mandziy, B., Ozirkovskyi, L. Extending the features of software for reliability analysis of fault-tolerant systems. *Computational Problems of Electrical Engineering*, 2012, vol. 2, no. 2, pp. 113-121.

27. Ponochovnyy, Yu. L., Kharchenko, V. S. Metodolohiya zabezpechennya harantozdatnosti informatsiyno-keruyuchykh system z vykorystannyam bahatotsil'ovykh stratehiy obsluhovuvannya [Dependability Assurance Methodology of Information and Control Systems Using Multipurpose Service Strategies]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and Computer Systems*, 2020, no. 3(95), pp. 43-58. DOI: 10.32620/reks.2020.3.05.

28. Volochiy, B., Mandziy, B., Ozirkovskyy, L. The New Method of Building a Safety Model for Quantitative Risk Assessment of Complex Technical Systems for Critical Application. *Communications in Computer and Information Science*, 2016, vol. 594, pp. 56-70. DOI: 10.1007/978-3-319-30246-1_4.

29. Ozirkovskyy, L., Pashchuk, Yu., Mashchak, A., Volochiy, S. The Automation of the Exploitation Risks Assessment of the Navigation Information System of Air Drones. *XIIIth International Conference TCSET'2016 Modern Problems of Radio Engineering, Telecommunications, and Computer Science*, 2016, pp. 140-144. DOI: 10.1109/TCSET.2016.7451993.

30. Volochiy, B., Ozirkovskyy, L., Mulyak, O., Volochiy, S. Safety estimation of critical NPP I&C systems via state space method. *2nd International Symposium on Stochastic Models in Reliability Engineering, Life Science, and Operations Management, SMRLO 2016*, 2016, pp. 347–356. DOI: 10.1109/SMRLO.2016.63.

Надійшла до редакції 14.02.2022, розглянута на редколегії 15.04.2022.

АНАЛІЗ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ВІДМОВОСТІЙКИХ СИСТЕМ ВІДПОВІДАЛЬНОГО ПРИЗНАЧЕННЯ ЗА ДОПОМОГОЮ ГРАФА СТАНІВ І ПЕРЕХОДІВ

Л. Д. Озірковський, Б. Ю. Волочій, О. П. Шкілюк, М. М. Змисний, П. І. Казан

Предметом вивчення в статті є процес визначення показника функційної безпечності відмовостійкої системи відповідального призначення, а саме ймовірності існування мінімальних січень для заданої тривалості її експлуатації, за допомогою графа станів і переходів. **Метою** є створення методу аналізу функційної безпечності відмовостійкої системи відповідального призначення, в основу якого покладено методику розроблення моделі експлуатаційної надійнісної поведінки у вигляді графа станів і переходів, придатного для такої задачі. В графі станів і переходів має бути деталізовано представлено непрацездатні стани та їх зв'язок з передаварійними станами. **Завдання**: запропонувати для непрацездатних станів графа класифікацію, яка дає змогу показати усі можливі аварійні ситуації в одному й тому ж просторі непрацездатних станів. Такий підхід дає змогу враховувати кореляції між аварійними ситуаціями, що є неможливим при використанні дерев відмов. Оскільки простір непрацездатних станів може сягати сотні – тисячі станів, запропонувати метод для їх автоматизованого визначення згідно класифікації. Провести валідацію методу аналізу функційної безпечності. Використано метод простору станів. Отримані такі **результати**. Сформована за графом станів і переходів система диференціальних рівнянь Колмогорова - Чепмена дає змогу визначати залежність значення показника функційної безпечності «ймовірність існування мінімальних січень», як функцію від тривалості експлуатації відмовостійкої системи відповідального

призначення. Цю залежність названо «функція аварійності». Метод визначення функції аварійності базується на використанні маски аварійної ситуації. Слід відзначити, що запропонована модель експлуатаційної надійнісної поведінки у вигляді графа станів і переходів дає змогу визначати як показник функційної безпечності так і показники надійності. Для валідації запропонованого методу аналізу функційної безпечності визначено значення ймовірності існування мінімальних січень для заданої тривалості її експлуатації з використанням дерева відмов. Дерево відмов побудоване за допомогою програмного забезпечення Reliasoft BlockSim. Отримане значення співпадає з значенням ймовірності існування мінімальних січень, яке показує функція аварійності для такої ж тривалості експлуатації. Таким чином проектант отримує можливість комплексно аналізувати доцільність введення надлишковості (структурної, часової, функціональної). **Висновки**. **Наукова новизна** отриманих результатів полягає в наступному: в основу методики розроблення графа станів і переходів для отримання стохастичної моделі експлуатаційної надійнісної поведінки відмовостійкої системи відповідального призначення покладено новий метод визначення безпечних, критичних та катастрофічних станів в множині станів з несправними підсистемами або модулями; для забезпечення автоматизованого отримання функції аварійності удосконалена структурно-автоматна модель експлуатаційної надійнісної поведінки відмовостійкої системи відповідального призначення.

Ключові слова: функційна безпечність; система відповідального призначення; надійнісне проектування; граф станів і переходів; мінімальні січення; дерево відмов; марковська модель.

АНАЛИЗ ФУНКЦИОНАЛЬНОЙ ОТКАЗОБЕЗОПАСНОСТИ ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ ОТВЕТСТВЕННОГО НАЗНАЧЕНИЯ С ПОМОЩЬЮ ГРАФА СОСТОЯНИЙ И ПЕРЕХОДОВ

Л. Д. Озирковский, Б. Ю. Волочий, А. П. Шкилюк,
М. М. Змысный, П. И. Казан

Предметом изучения в статье является процесс определения показателя функциональной отказобезопасности отказоустойчивой системы ответственного назначения, а именно вероятности существования минимальных сечений для заданной продолжительности ее эксплуатации, с использованием графа состояний и переходов. **Целью** является создание метода анализа функциональной отказобезопасности отказоустойчивой системы ответственного назначения, в основу которого положена методика разработки модели эксплуатационного надежностного поведения в виде графа состояний и переходов, пригодного для такой задачи. В графе состояний и переходов должны быть подробно представлены неработоспособные состояния и их связь с предаварийными состояниями. **Задача**: предложить для неработоспособных состояний графа классификацию, позволяющую показать все возможные аварийные ситуации в одном и том же пространстве неработоспособных состояний. Такой подход позволяет учитывать корреляции между аварийными ситуациями, что невозможно при использовании деревьев отказов. Так как пространство неработоспособных состояний может достигать сотни – тысячи состояний, предложить метод их автоматизированного определения согласно классификации. Провести валидацию метода анализа функциональной безопасности. Использован метод пространства сословий. Получены следующие результаты. Составленная согласно графа состояний и переходов система дифференциальных уравнений Колмогорова - Чепмена позволяет определять зависимость значения показателя функциональной безопасности «вероятность существования минимальных сечений» как функцию от длительности эксплуатации отказоустойчивой системы ответственного назначения. Эта зависимость получила название «функция аварийности». Метод определения функции аварийности основан на использовании маски аварийной ситуации. Для валидации предлагаемого метода анализа функциональной безопасности определено значение вероятности существования минимальных сечений для заданной продолжительности ее эксплуатации с использованием дерева отказов. Дерево отказов построено с помощью программного обеспечения Reliasoft BlockSim. Полученное значение совпадает со значением вероятности существования минимальных сечений, которое показывает функция аварийности для такой же продолжительности эксплуатации. Следует отметить, что предложенная модель эксплуатационного надежностного поведения в виде графа состояний и переходов позволяет определять как показатель функциональной безопасности, так и показатели надежности. Таким образом, проектировщик получает возможность комплексно анализировать целесообразность введения избыточности (структурной, временной, функциональной). **Выводы**. **Научная новизна** полученных результатов состоит в следующем: в основу методики разработки графа состояний и переходов для получения стохастической модели эксплуатационного надежного поведения отказоустойчивой системы ответственного назначения положен новый метод определения безопасных, критических и

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

катастрофических состояний во множестве состояний с неисправными подсистемами или модулями; для обеспечения автоматизированного получения функции аварийности усовершенствована структурно-автоматная модель эксплуатационного надежностного поведения отказоустойчивой системы ответственного назначения.

Ключевые слова: функциональная отказобезопасность; система ответственного назначения; надежностное проектирование; граф состояний и переходов; минимальные сечения; дерево отказов; марковская модель.

Озірковський Леонід Деонісійович – д-р техн. наук, доц. каф. теоретичної радіотехніки та радіовимірювань, Національний університет «Львівська політехніка», Львів; Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна.

Волочій Богдан Юрійович – д-р техн. наук, проф. каф. теоретичної радіотехніки та радіовимірювань, Національний університет «Львівська політехніка», Львів; Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна.

Шкілюк Олександр Петрович – канд. техн. наук, старш. викл. каф. теоретичної радіотехніки та радіовимірювань, Національний університет «Львівська політехніка», Львів, Україна.

Змисний Михайло Михайлович – канд. техн. наук, старш. викл. каф. теоретичної радіотехніки та радіовимірювань, Національний університет «Львівська політехніка», Львів, Україна

Казан Павло Іванович – канд. техн. наук, нач. відділу наукового центру, Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна.

Leonid Ozirkovskyy – DSc. Eng., Associate Professor, Department of Theoretical Radio Engineering and Radio Measurements, Lviv Polytechnic National University, Lviv; Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine,
e-mail: leonid.d.ozirkovskyi@lpnu.ua, ORCID: 0000-0003-0012-2908, Scopus Author ID: 8373567100,
https://scholar.google.com/citations?hl=uk&user=tcBEWZMAAAAJ.

Bohdan Volochiy – DSc. Eng., Professor, Department of Theoretical Radio Engineering and Radio Measurements, Lviv Polytechnic National University, Lviv; Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine,
e-mail: bohdan.y.volochii@lpnu.ua, ORCID: 0000-0001-5230-9921, Scopus Author ID: 8373567400,
https://scholar.google.com/citations?hl=en&user=diFQal8AAAAJ

Oleksandr Shkiliuk – PhD Eng., Senior Lecturer, Department of Theoretical Radio Engineering and Radio Measurements, Lviv Polytechnic National University, Lviv, Ukraine,
e-mail: oleksandr.p.shkiliuk@lpnu.ua, ORCID: 0000-0001-9237-4808, Scopus Author ID: 55225971400,
https://scholar.google.com/citations?hl=en&user=dMkGkOUAAAAJ

Mykhailo Zmysnyi – PhD Eng., Senior Lecturer, Department of Theoretical Radio Engineering and Radio Measurements, Lviv Polytechnic National University, Lviv, Ukraine,
e-mail: mykhailo.m.zmysnyi@lpnu.ua, ORCID: 0000-0002-3384-6139, Scopus Author ID: 35868199600.

Pavlo Kazan – PhD Eng., Head of the Research Center Department, Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine,
e-mail: pavlokua@ukr.net, ORCID: 0000-0001-5929-0469,
https://scholar.google.com/citations?hl=en&user=e8zQzPsAAAAJ.