electrotechnical systems]. Yekaterinburg: IzdatelstvoUrFU; 2012 [in Russian].

[10]. Fedotova GA. Redundancy as part of the dependability problem in electric-power industry. Dependability 2014;1:60-79 [in Russian].

[11]. GOST R IEC 61508-5-2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 5. Guidelines for methods of the determination of safety integrity levels. Introduction [in Russian].

[12]. Slyshalov VK. Osnovy rascheta nadezhnostisistemelektrosnabzheniya: uchebnoeposobie [Introduction to dependability calculation of power supply systems]. Ivanovo: Ivanovo State Power Engineering University Publishing; 2012 [in Russian].

[13]. Shubinsky IB, Zamyshliaev AM, Pronevich OB. Graph method for evaluation of process safety in railway facilities. Dependability 2017;1:40-45.

[14]. Norman B. The Applicability of Markov Analysis Methods to Reliability, Maintainability, and Safety. Selected Topics in Assurance Related Technologies (START) 2003;10(2).

[15]. Dutuit Y, Innal F, Rauzy AB, Signoret JP. Probabilistic assessments in relationship with safety integrity levels by using Fault Trees. Reliability Engineering & System Safety 2008;93(12):1867-1876.

[16]. Brissaud F, Oliveira LF. Average probability of a hazardous failure on demand: Different modelling methods, similar results. In: Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference & the Annual European Safety and Reliability Conference. Helsinki (Finland); 2012. P. 6073-6082.

[17]. Aho A, Hopcroft J, Ullman J. The Design and Analysis of Computer Algorithms. Mir; 1979.

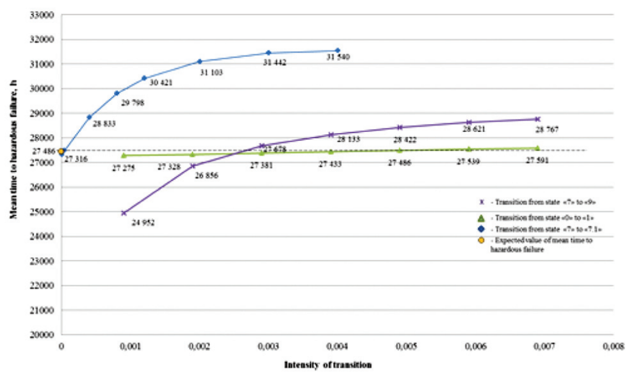
[18]. Babrauskas V. How do electrical wiring faults lead to structure ignitions? In: proceedings of the International Conference on Mathematical Methods in Reliability. San Francisco (USA); 2001. P. 39-50.

About the authors

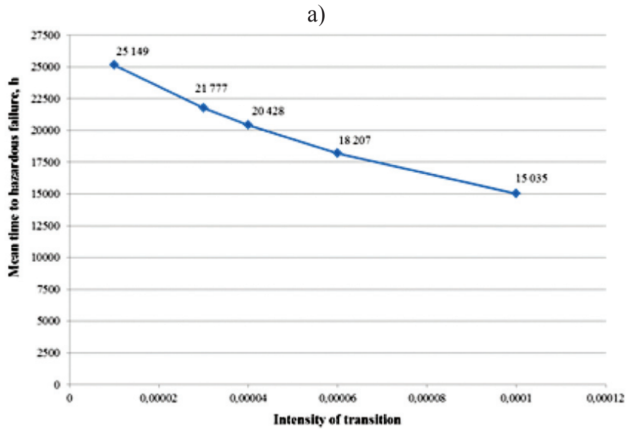
Olga B. Pronevich, Head of Unit, JSC NIIAS, Moscow, Russia, e-mail: o.pronevich@vniias.ru

Viktoria E. Shved, Chief Specialist, JSC NIIAS, Moscow, Russia, e-mail: v.shved@vniias.ru

Received on: 29.03.2018



a)



b)

Figure 6. Graph of dependence of the mean time to hazardous failure and a) rate of transition from states “0→1”, “7→7.1”, “7→9”; b) under decreasing rate of transition into safe state and intensity of transition from state “7→7.1”

Figure 6b) shows the graph of dependence of the mean time to hazardous failure from the intensity of transition from state 7, “PT-1 internal or turn-to-turn short circuit”, into state 7.1, “Detection of actual failure of PT-1”. In this case the value of mean time to hazardous failure expectedly decreases as the intensity of transition into safe state grows.

Thus, the developed algorithm allows predicting the reduction of functional safety indicators and regulating the distribution of efforts aimed at maintaining the system’s operable state,ensuring the redundancy of the system by increasing the intensity of transition into safe state or managing the maintenance and repair system by reducing the intensity of transition between system states.

Conclusion

The paper presents a step-by-step examination of the algorithm of calculation of functional safety indicators of railway PSS based on graph semi-Markovian methods. Using the example of functional safety indicators calculation of a “Railway 110 kV traction substation”, the authors demonstrate the capabilities of the graph method and its universal applicability to systems of any configuration. The stages of system state graph construction and calculation of stationary and non-stationary functional safety indicators are examined in depth, their practical applicability is shown.

The paper also analyses the dependence of the estimated values under changing intensities of transition. The conclusion is made regarding the feasibility of decision-making subject to the values of functional safety indicators.

The method of functional safety indicators calculation considered in the paper has a potentially wide area of practical application, as it does not involve operational calculations, which substantially reduces the threshold of competence required for this method’s application and can be interesting not only to academic, but the engineering community as well.

References

[1]. Gapanovich VA, Shubinsky IB, Zamyshliaev AM. Nekotorye voprosy upravleniya resursami i riskami na zheleznodorozhnom transporte na osnove sostoyaniya ekspluatatsionnoy nadezhnosti i bezopasnosti obektov i protsessov (proekt URRAN) [Some matters of resource and risk management in railway transportation based on the condition of operational dependability and safety of facilities and processes (URRAN project)]. Dependability 2011;1:2-8 [in Russian].

[2]. On the safety of railway infrastructure (Technical guidelines of the Customs Union TR TS 003/2011): approved by order of the Customs Union Commission no. 710 dated 15.07.2011, <http://www.eurasiancommission.org/ru/act/texnreg/deptexreg/tr/Pages/TRVsily.aspx> [in Russian]

[3]. Shubinsky IB. Strukturnoe rezervirovanie v informatsionnykh sistemakh. Predelnyeotsenki[Structural redundancy in information systems. Marginal valuations]. Dependability 2012;1(40): 18-125 [in Russian].

[4]. Chang L, Wu Z, Elnashai AS, Spencer BF. Performance and Reliability of electrical power grids under cascading failures. In: Proceedings of the 14-th World Conference on Earthquake Engineering. Beijing (China); October 12-17, 2008.

[5]. Wu Z, Zhong Q, Zhang Y. State transition graph of cascading electrical power grids. In: proceedings of IEEE Power Engineering Society General Meeting. Tampa (Florida, USA); 2007.

[6]. Shubinsky IB. Funktsionalnayanadezhnost informatsionnykh system.Metodyanaliza[Functional dependability of information systems. Analysis methods]. Ulianovsk: OblastnayatipografiaPechatnydvor, 2012 [in Russian].

[7]. GOST R IEC 61508-2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements. Introduction [in Russian].

[8]. GOST R IEC 61511-1-2015. Functional safety. Safety instrumented systems for the industrial processes. Part 1. Terms, definitions and technical requirements. Introduction [in Russian].

[9]. Oboskalov VP. Strukturnaya nadezhnost elektrotekhnicheskikh sistem [Structural dependability of

series-connected unidirectional edges with the beginning in state i and the end in state j, $G_{\overline{S}_H}$ is the weight of the graph decomposition without the set of non-operable system states (graph vertices) $\overline{S_H}$ and associated edges.

Graph decomposition is a part the graph that does not contain the selected vertices and associated arcs. Graph decomposition is calculated using Mason's formula:

$$\Delta G = 1 - \sum_{j} C_j + \sum_{rj} C_r C_j - \sum_{irj} C_i C_r C_j. \qquad (4)$$

The other stationary functional safety indicators are calculated in the same way. Thus, for instance, the safety coefficient is calculated as follows: according to the algorithm the stationary probabilities of containment of the semi-Markovian model in each of the graph vertices are calculated according to the formula:

$$\pi_i = \frac{\Delta G^i T_i}{\sum_{i \in S} \Delta G^i T_i}. \qquad (5)$$

The advantages of this method include: applicability in calculation of the functional safety indicators of systems with a large number of states; absence of limitations on the structure of the examined system; no requirement to transform the initial state graph; operational calculus is not used.

The graph method also allows determining the strict lower (inf) and upper boundaries (sup) of the non-stationary functional safety indicators of safety-related systems. Values sup $\hat{P}(t)^{\text{haz}}$ and inf $\hat{P}(t)^{\text{haz}}$ are determined on the class of Erlang distribution functions:

$$f(t) = \begin{cases} t^{r-1} \cdot \dfrac{e^{-\frac{t}{T_{MT}^{haz}}}}{(T_{MT}^{haz})^r \, \Gamma(r)}, & t \geq 0, \\ 0, & t < 0. \end{cases} \qquad (6)$$

where$r$ is an integral parameter of distribution.

The failure rate will be within an interval, of which the boundaries are calculated using the formulas given in Table 2. In order to guarantee the specified calculation accuracy 1-ε, iterative calculations are performed, during which at each step Δt the observation interval is reduced up to the case when the following condition is true:

$|\inf\lambda(t) - \inf\lambda(t+\Delta t)| < \varepsilon$, $|\sup\lambda(t) - \sup\lambda(t+\Delta t)| < \varepsilon$,

Documentation and displaying of results

The documentation of results is an important part of the system states analysis. The application of the graph method described in the paper allows, using the results of the preparation stage, calculating a set of stationary and non-stationary functional safety indicators. When making the list of results, the following characteristics should be identified: name of indicator, designation, result of calculation, dimensionality (units of measurement). An example of the list of calculation results is given in Table 3.

The calculation results allow concluding on the high level of functional safety of the 110 kV railway traction substation system that features structural redundancy ensured by backing up the primary component, the power transformer. Indeed, statistically, hazardous failures of the power transformers that disable 110 kV traction substations and cause critical consequences are sufficiently rare as such systems are redundant.

Analysis of the power transformer functional safety indicators

The application of the above algorithms enables variation calculations under different initial values of intensity of transition into the analyzed states. Such research allows making conclusions regarding the expected efficiency of the protection and redundancy systems, as well as the effect of the intermediate state elimination rate on the hazard rate.

Figure 6 shows the results of simulation of the dependence of the intensities of transition between intermediate graph states and the value of mean time to hazardous failure.

As graph 6a) evidently shows, the value of mean time to hazardous failure is most sensitive to changes in the intensity of transition from state 7, "PT-1 internal or turn-to-turn short circuit", into state 9, "PT-1 internal effects protection tripping and transition to PT-2". Also, as the intensity of transition for these states increases, the mean time to hazardous failure grows as well. This is due to the fact that state 1, "Wear of PT-1 insulation", 9, "PT-1 internal effects protection tripping and transition to PT-2", and 7.1, "Detection of actual failure of PT-1" have ways of transition into safe state 0, "PT-1 and PT-2 are operable" with higher intensity than the intensity of transition into hazardous state.

Table 3. Results of system component safety calculation

№	Name of indicator	Notation	Calculation result	Dimension
1	Mean time to hazardous failure	$T_{\text{MT}}^{\text{haz}}$	27 486	hour
2	Mean time between hazardous failures	T_0^{haz}	28 615 933	hour
3	Safety coefficient	C_{S}	1-7·10^{-4}	
4	Probability of hazardous failure	$\hat{Q}(t)^{\text{haz}}$	$\hat{Q}(t)^{\text{haz}} < 3{,}64 \cdot 10^{-5}$	
5	Probability of fault-free operation	$\hat{P}(t)^{\text{haz}}$	$1 - 3{,}64 \cdot 10^{-5} < \hat{P}(T_{\text{MT}}^{\text{haz}})$	
6	Hazardous failure rate	$\hat{\lambda}_C(t)^{haz}$	$3{,}51 \cdot 10^{-4} < \hat{\lambda}_C(T_{MT}^{haz}) < 5{,}11 \cdot 10^{-4}$	

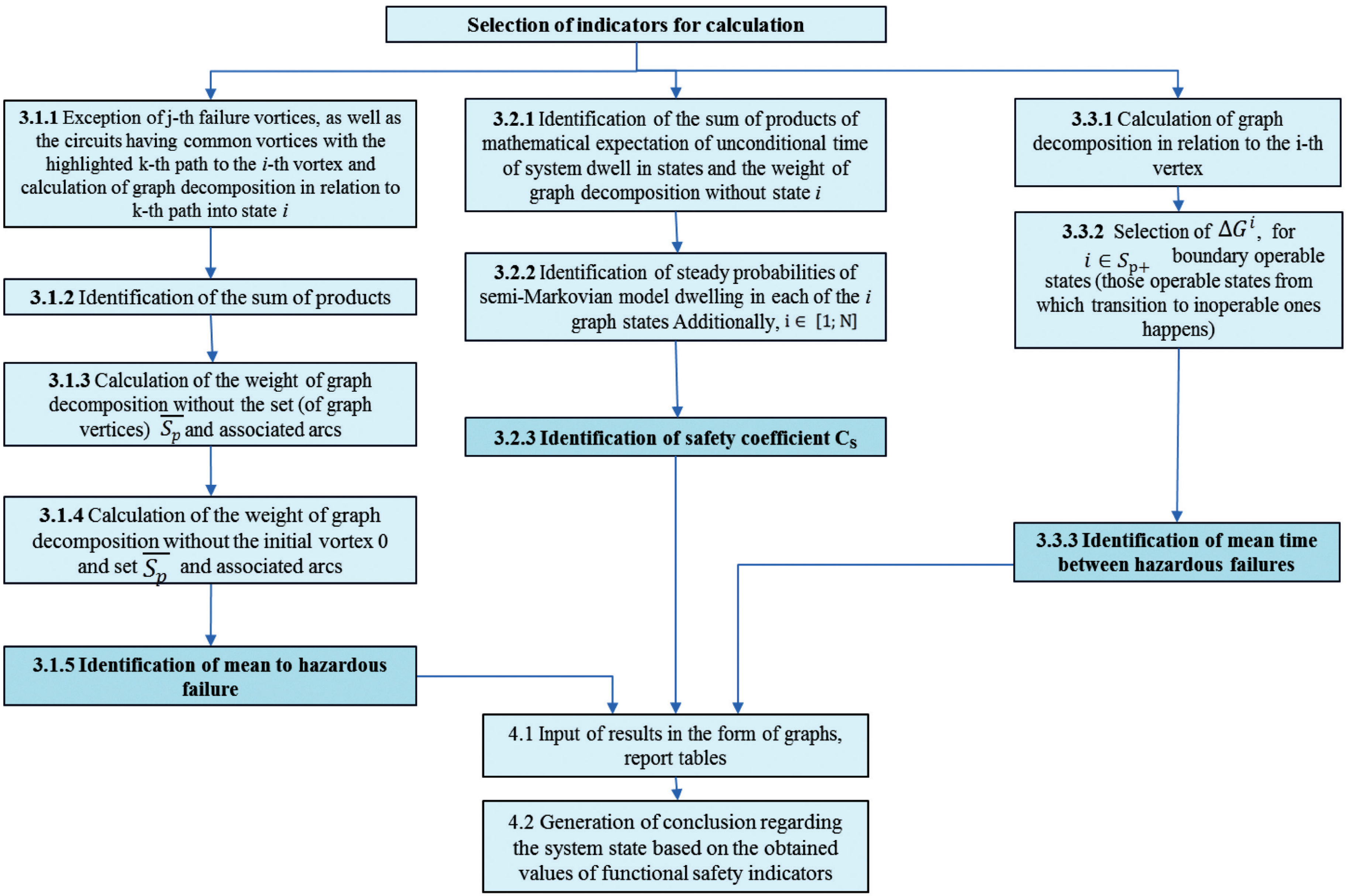


Figure 5. Stages 3 and 4 of the algorithm of calculation of steady functional safety indicators

short circuits or turn-to-turn short circuits. In turn, the state "Short circuit or turn-to-turn short circuits of PT-1" (graph vertex 7) will cause the loss of the capability by the transformer to perform its function. In that case, if the actual failure is discovered in time (graph vertex 7.1), the role of power transformer is taken by the redundant element, i.e. the backup power transformer. Then transition from state 7.1 to state 0 (edge shown in green) occurs. If that does not happen, for example, e.g. due to technical reasons, then the "Railway 110 kV traction substation" experiences a "Hazardous failure. PT-1 and PT-2 are faulty" (graph vertex 10). After the generation of the connections between the vertices, calculations are performed for the weights of the circuits, loops (formula 1) and paths of transition into the vertex (formula 2), as well as the mathematical expectation of the unconditional time of system being in each of the graph vertices (formula 3).

$$C_i = \prod_{i,r \in S} p_{ir} p_{ri} \tag{1}$$

where $p_{ir} p_{ri}$ is the probabilities of transition between neighboring vertices;

$$l_k^{0i} = \prod_{0,i,r \in S_p} p_{or} p_{ri} \tag{2}$$

$$T_i = \frac{1}{\sum_{r=1}^{n} \lambda_{ir}} \tag{3}$$

where λ_{ir} is the intensities of transitions between graph vertices.

Figure 4 shows the state graph of the power transformer. The numbers above the edges characterize the intensities of transition between the states of a system component.

Calculation of stationary and non-stationary functional safety indicators

After the calculation of the graph's topological characteristics, the functional safety indicators are calculated. Let us examine the calculation of one of the stationary indicators in the algorithm, the mean time to hazardous failure. For this system component, using the constructed graph the indicators from Table 2 can be calculated.

The set of non-hazardous states is the key aspect in the calculation of safety indicators. For the calculation of the mean time to hazardous failure of a safety-related system, the system is modeled with a state graph of a semi-Markovian stochastic process and a matrix of intensities of transitions is defined. The value of this indicator reflects the mathematical expectation of the object's time to first hazardous failure with the initial safe state, 0subject to known values of intensity of transition between states.

The proposed algorithm allows consecutively calculating the indicator for any hazardous failure. If this calculation method is used, the system's mean time to hazardous failure is identified according to the formula given in Table 2.

When mean time to hazardous failure is calculated, $G^0_{\overline{S_H}}$ is the weight of decomposition without the initial vertex 0 and the set of non-operable system states (graph vertices) $\overline{S_H}$ and associated edges; l_k^{0i} is the weight of the k-th path from the initial vertex 0to vertex i. A path is a chain of

Table 2. System safety indicators

№	Indicator	Notation	Calculation formula
1	Mean time to hazardous failure	$T^{\text{haz}}_{\text{MT}}$	$T^{\text{haz}}_{\text{MT}} = \frac{\grave{O}_0 \Delta G^0_{\overline{S_H}} + \sum_{(k)} \sum_{0,i} l_k^{0i} \Delta G_k^i T_i}{\Delta G_{\overline{S_H}}}$
2	Mean time between hazardous failures	T^{haz}_0	$T^{\text{haz}}_0 = \frac{\sum_{i \in S_H} \Delta G^i \cdot T_i}{\sum_{i \in S_{H+}} \Delta G^i \cdot \sum_{j \in \overline{S_H}} p_{ij}}$
3	Safety coefficient	C_S	$C_S = \sum_{i \in S_P} \pi_i$
4	Dispersion of time to hazardous failure	$D^{\text{haz}}_{\text{MT}}$	$D^{\text{haz}}_{\text{MT}} = t_0^{-2} - (T^{\text{haz}}_{MT})^2$
5	Probability of hazardous failure	$\hat{Q}(t)^{\text{haz}}$	$\inf \hat{Q}(t)^{\text{haz}} < \hat{Q}(t)^{\text{haz}} < \sup \hat{Q}(t)^{\text{haz}}$
6	Probability of fault-free operation	$\hat{P}(t)^{\text{haz}}$	$1 - \sup \hat{Q}(t)^{\text{haz}} < \hat{P}(t)^{\text{haz}} < 1 - \inf \hat{Q}(t)^{\text{haz}}$
7	Hazardous failure rate	$\hat{\lambda}(t)^{\text{haz}}$	$\hat{\lambda}(t)^{\text{haz}} \in (\frac{-[\sup \hat{P}(t+\Delta t)^{\text{haz}} - \sup \hat{P}(t)^{\text{haz}}]}{\sup \hat{P}(t)^{\text{haz}} \Delta t}; \frac{-[\inf \hat{P}(t+\Delta t)^{\text{haz}} - \inf \hat{P}(t)^{\text{haz}}]}{\inf \hat{P}(t)^{\text{haz}} \Delta t})$

former in a "Traction substation" system entails serious consequences, including the interruption of service and provision of power to third-party users, which will lead to the disruption of business process. In turn, a hazardous failure of such facility may cause the non-fulfillment of the system's safety function, i.e. fire or explosion (for the oil-filled transformer). Such system is the perfect demonstration of the importance of fault-free and safe operation.

An example of the generation of the list of states for the "power transformer" component in accordance with the above definition is given in Table 1. Constructing a graph model requires a list of states (graph vertices). Here and below we will designate the main element, the "power transformers" as "PT-1", and the backup power transformer as "PT-2".

Calculation of the topological characteristics of the graph and temporal indicators of the power supply system

After the identification of the set of possible states, formation of connections between the vertices in the form of a connectivity matrix and matrix of intensities of the system component, the graph of the system component's dependability states is constructed. The result of this stage is the state graph of the system component with transition probabilities. The order of this stage's implementation is given in Figure 3.

Based on the selected states of the power transformer, connections between vertices are built that reflect the transition between states. When connections are built, its is important to remember to take into consideration the structural redundancy (presence of partial homogenous standby) that is normally implemented in the form of a standby power transformer. These connections ensure the transition of the system components into the operable state. Let us give an example of the generation of such connections. The first state of the power transformer is "PT-1 and PT-2 are operable". Later, in the process of operation emerges the state "Wear of PT-1 bushings". This transition is shown with a blue edge in Figure 4. "Wear of PT-1 bushings" can cause heating, flashovers, unequal voltage per phases, etc. The transformer can be in this state during a certain period of time. Some of these states cause mechanical or electrical damages to insulation, wire breaks, cracks. That means the transition into state "Mechanical or electrical damage of PT-1". Further developments may take two different courses: the malfunctions will be discovered and eliminated, i.e. system will return into the previous state or the damage is not eliminated in time, which will cause

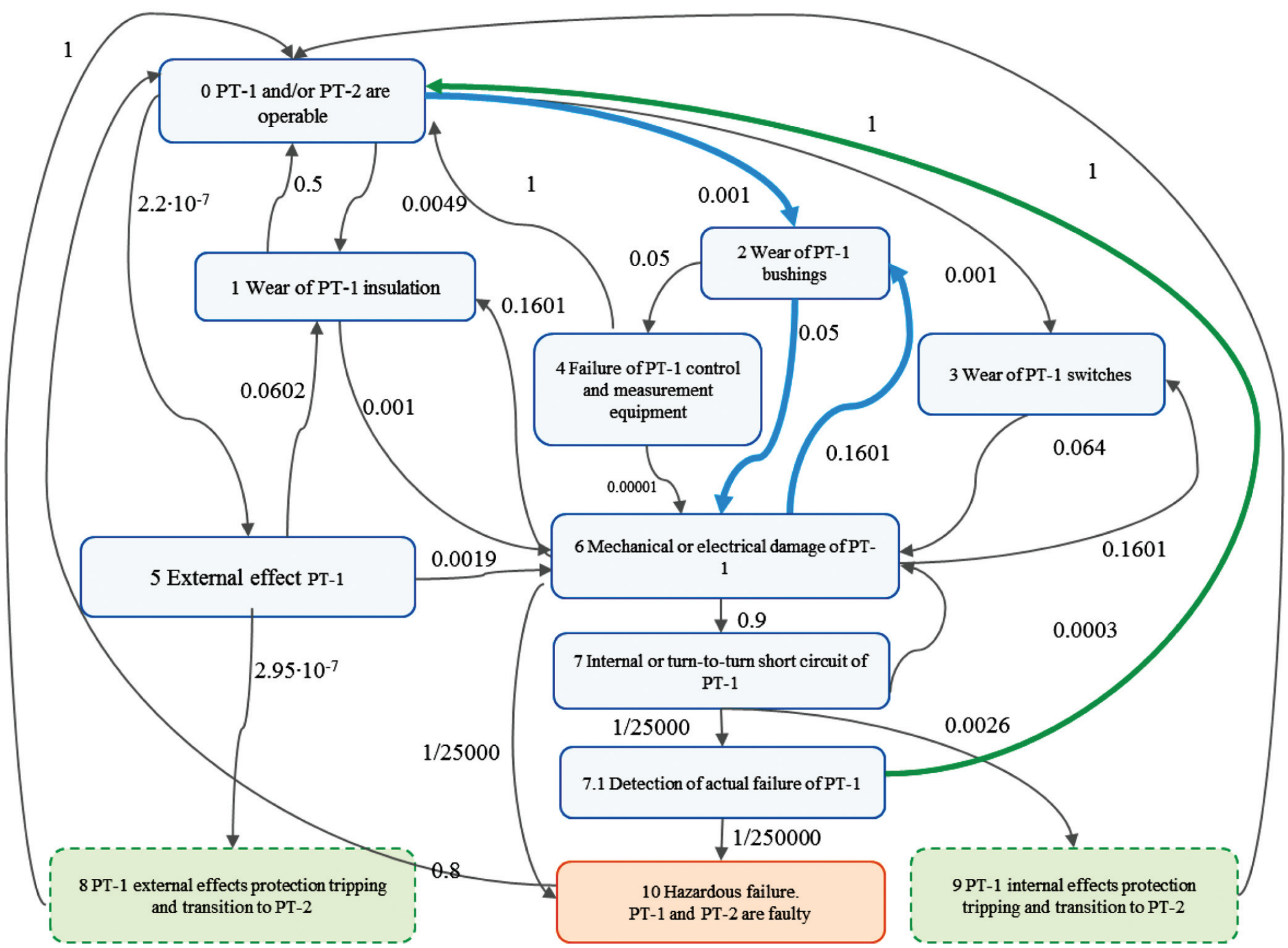


Figure 4. Graph of the sets of states of the component "Power transformer" of the system "Railway 110 kV traction substation"

calculations to be used for evaluation of various indicators, which significantly reduces the time of comprehensive system analysis.

Preparation of application of agraphsemi-Markovian method of calculation of functional safety indicators of power supply systems

The input data for the application of a graph semi-Markovian method is an oriented graph of system states and intensity of transition between states. The implementation of the preparatory stage is shown in Figure 2. Importantly, the application of this method is possible both for the calculation of the indicators of whole system or its individual elements.

At the preparatory stage, the list is made of the system components that affect functional safety, as well as their possible states; the type of sets they are part of is identified. A set of states is understood as a set of significant properties of the system at the current moment of time [13, 17]. The following subsets of states are identified [7, 18]: subset of the operable states S_O, subset of the inoperable states $\overline{S_P}$, subset of the non-hazardous states S_N, subset of hazardous states $\overline{S_H}$ and the subset of safe states S_S. Let us examine each set in more detail.

The set of non-hazardous states of the system (S_N) is the operable or safe state of the system.

The set of safe states of the system (S_S) is the states of the system, in which the process functions are not performed, but all required safety functions are performed.

The set of hazardous states of the system ($\overline{S_H}$) is the non-operable system state, in which at least one safety function is not performed. The set of hazardous system states includes the states, in which safety functions implemented by the consumers are disrupted (e.g. impossibility to implement the functions of automated control of safe train movement).

As an illustration of the method of functional safety indicators using graph semi-Markovian methods this paper cites the "railway 110 kV traction substation" power supply system with partial homogenous standby for the "power transformer" (PT-1) component. Partial homogenous standby in this case is an example of structural redundancy in the from of a standby power transformer (PT-2). The failure of a component like the power trans-

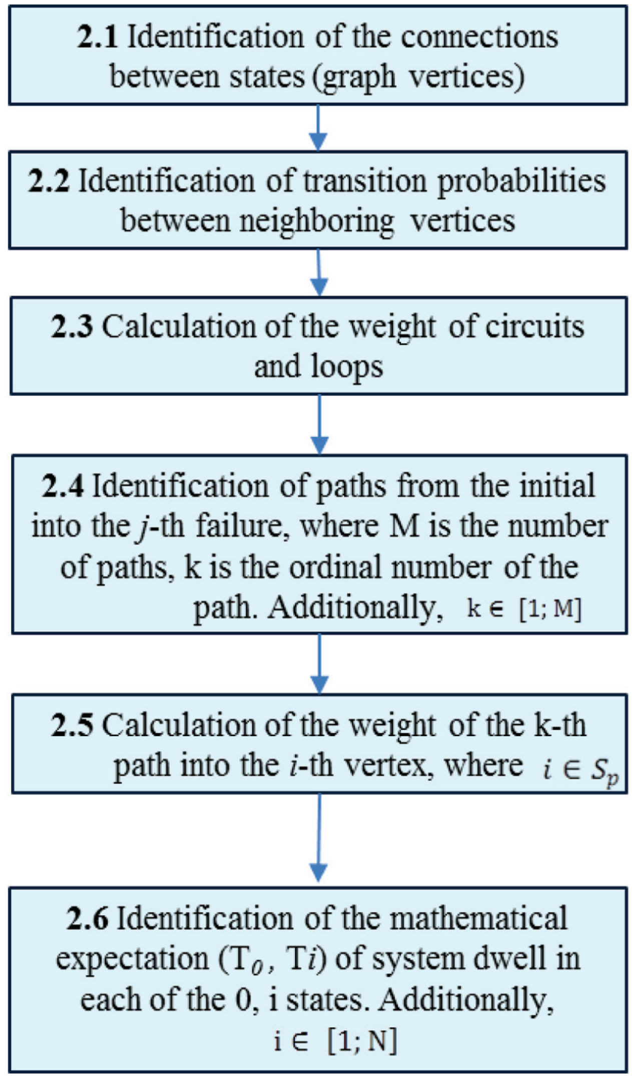


Figure 3. Stage 2 of the algorithm of calculation of functional safety indicators

Table 1. List of the dependability states of power transformer

System component	State of component (graph vertex)	Subset of states
PT-1 and PT-2	PT-1 and PT-2 are operable	S_R, S_N
PT-1	PT-1 insulation wear	S_R, S_N
PT-1	PT-1 bushings wear	S_R, S_N
PT-1	PT-1 switches wear	S_R, S_N
PT-1	PT-1 control equipment failure	S_R, S_N
PT-1	PT-1 external effect	S_R, S_N
PT-1	PT-1 mechanical or electrical damage	S_R, S_N
	PT-1 internal or turn-to-turn short circuit	S_R, S_N
PT-1	Detection of actual failure of PT-1	S_R, S_N
PT-1 and PT-2	PT-1 external effects protection tripping and transition to PT-2	S_P,
PT-1 and PT-2	PT-1 internal effects protection tripping and transition to PT-2	S_P, $\overline{S_P}$
PT-1 and PT-2	Hazardous failure. PT-1 and PT-2 are faulty	$\overline{S_H}$, $\overline{S_P}$

of systems consisting of restorable components as well as the application of this method in the context of PSS. This method is also based on the solution of systems of differential equations using the method of operators. Despite the detailed description of the method, its practical application for the analysis of complex technical systems is limited by the requirement to solve a system of differential equations, of which the number depends on the number of the vertices of the graph that simulates such system.

As the solution of the problem of the large dimensionality of algebraic equations and differential systems, [13] proposes a graph semi-Markovian method based on the decomposition of the initial graph model into component subgraphs that do not contain the identified vortices. The graph semi-Markovian method allows calculating over 10 functional safety indicators using the same pool of initial data and without using operator calculus. Along with the considered scientific studies in this area, the problem of selection of the method of indicators evaluation is also examined in foreign sources. Among the primary methods are the fault tree, Petri net, Markovian and graph semi-Markovian methods [14-16]. The majority of the considered studies come down to the selection of the application of the Markovian and graph semi-Markovian methods.

This paper examines the practical application of graph semi-Markovian methods that enable the evaluation of functional safety indicators taking into account the initial states the system might be in. A hazardous system failure shall be understood as a non-operable system state in which at least one safety function is not performed [7].

Calculation algorithm

For the purpose of calculating system functional safety indicators, it is proposed to use an algorithm (Figure 1) based on a graphsemi-Markovian method that defines the order of the stages of calculation of the primary functional safety indicators.

The algorithm reflects the order of actions associated with the calculation of the system of functional safety indicators, including the stages of generation of the set of states of the evaluated system, construction of the system state graph and procedure of application of formulas for calculation of dependability and safety indicators. The algorithm is designed in such a way as to allow intermediate

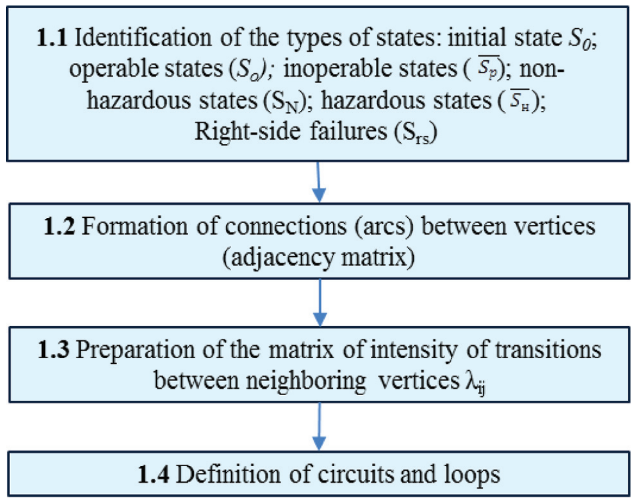


Figure 2. Procedure for implementation of the preparatory stage of calculation of functional safety indicators of complex technical systems using a graphsemi-Markovian method

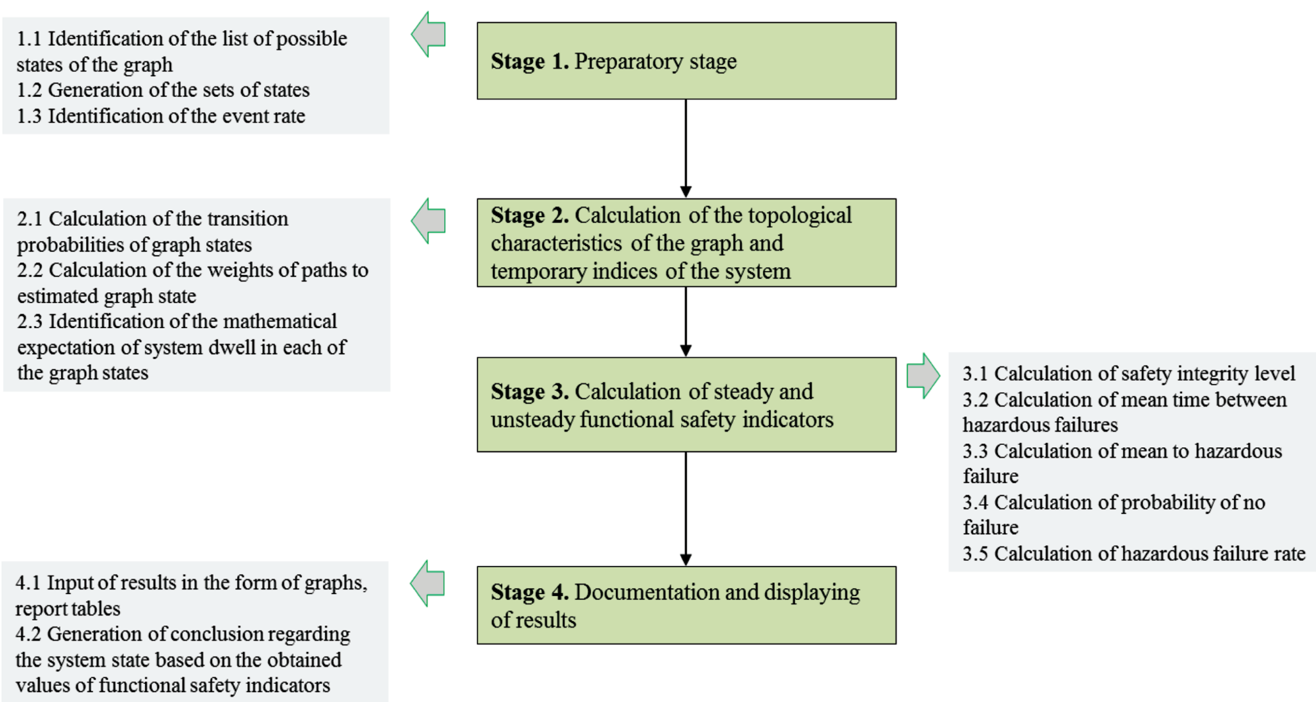


Figure 1. Algorithm of calculation of functional safety indicators of complex technical systems using a graphsemi-Markovian method

Introduction

Functional safety of power supply systems (PSS) is vital to uninterrupted operation of modern cities, as well as to the preparedness, response, recovery and mitigation of the consequences of hazardous events (failures, accidents). This problem is well-known and has its special features from country to country. For example, PSS of the Chinese railway transportation system are characterized by the threats of failure to ensure the dependability and functional safety of PSS under natural disasters (earthquakes) and terrorist attacks [4, 5].

Emergencies and failures of PSS can present danger not only to the workers who operate PSS, but to the environment as well. Interruptions of power supply can disrupt the functions of safety systems that rely on electric power. In railway transportation such systems include transportation safety and traffic safety facilities Another important example are life support systems in hospitals. Functions implemented by such systems are called safety functions. If a PSS failure causes a disruption in the operation of a safety function, such failure should be considered hazardous.

A safety function in this case is understood as a function implemented by a safety-related system or external risk reduction facilities (intruder detection, information security, etc.) designed to guarantee or maintain a safe state with respect to a specific hazardous event [6]. Today's PSS that cater to many consumers are characterized by a complex structure and a large number of tasks and operations that they perform. Increasing system complexity may cause the reduction of the probability of fault-free operation. The problem of ensuring the functional safety of PSS is so pressing, that the European Union has developed a series of standards aiming to establish harmonized approaches to ensuring functional safety of electrical systems. The first standard of these series is dedicated to general requirements for functional safety of electrical, electronic, programmable electronic safety-related systems [7]. Later, corresponding standards were developed for different industries, e.g. the processing industry [8].

Standard [7] establishes the requirement for evaluation of the probability of hazardous failure. Importantly, hazardous failures are sufficiently rare. According to international standards, the rate of hazardous functional failures is 2-4 orders of magnitude lower than the failure rate related to system dependability [6]. This is due to the fact that normally systems incorporate hardware-based dependability feature.

One of the methods of guaranteeing safety and dependability of PSS in railway transportation aimed at avoiding disruptions of traffic is structural redundancy that ensures the performance of safety functions in cases of failure of the backed-up system components. The matter of classification of structural redundancy itself is quite extensive as regards different systems. Depending on the PSS functionality, the following characteristics govern the selection of the type of redundancy: number of backup devices, possibility and parameters of recovery of failed devices; dependability of switching devices; duration of failures before detection by supervision facilities; allowable time of interruption of operation, etc. [9]. Despite the fact that non-fulfillment by a system component of its functions does not necessarily cause the whole system to fail, this event can be considered the failure of a specific component (object) or partial failure of the whole system. Depending on the chosen type of redundancy, in case of failure of one of the components the system may be either non-operable yet not allowing for hazardous failures and complete lasting interruption of operation, or operable in the case if redundancy does not provide for interruption of operation and performs the complete set of system functions. The problem of dependability of PSS is also examined in detail in [10]. Thus, when calculating PSS functional safety indicators, their redundancy and possibility of failure of both basic components performing vital functions, and the components of the system's structural redundancy must be taken into consideration.

The methods of calculation of dependability indicators are well known and examined in many sources. However, the situation with the functional safety evaluation methods is different. Standard [11] regulates 5 methods of defining the requirements for the safety integrity level (ALARP, quantitative method (fault tree), risk graph, layer of protection analysis, hazardous events gravity matrix).

Problem definition and choice of method of calculation of functional safety indicators of supply systems

The main problem in the calculation of functional safety indicators is the selection of the method that would allow calculating the most complete list of indicators based on a single set of initial data. While selecting the calculation methods, it must be taken into consideration that the condition of PSS is defined by the condition of its components, while the condition of the components, in turn, is defined by the effect on the capability by the consumers to perform their functions.

In accordance with [9], using Markovian models conditional probabilities of a system being in one state or another are evaluated by solving differential equations. The search for the equation corresponding to the condition diagram is a problem of its own. The same work allows using different methods for calculation of different indicators and does not demonstrate the potential applications of one method for evaluation of the whole list of required indicators. Among the most important drawbacksof this approach is the complexity of calculation, as well as the iterative collection of initial data required for different models.

[12] sets forth a method of using Markovian processes for identification of the dependability indicators

Original article
DOI: 10.21683/1729-2646-2018-18-3-46-55

Algorithm of calculation and forecasting of functional safety indicators of railway power supply systems

Olga B. Pronevich, *JSC NIIAS, Moscow, Russia*
Viktoria E. Shved, *JSC NIIAS, Moscow, Russia*

Olga B. Pronevich

Viktoria E. Shved

Acknowledgement: *the authors express their personal gratitude to Prof. Igor B. Shubinsky, Doctor of Engineering, for his recommendations regarding the choice of the theoretical background that provided the foundation for the practical research, as well as hisadvice and valuable observations that contributed to this paper.*

Abstract. Aim. *Uninterrupted transportation process is ensured by the highly dependable and safe power supply system of railway transport. In addition, the railway power supply system provides power to external consumers. A risk-oriented approach to railway transportation management requires an infrastructure risk management and safety system. The main purpose of risk management in this area is to improve the dependability and safety of railway infrastructure facilities [1, 2]. Additionally, given the growing numbers of intelligent information systems, as well as automated railway transportation management systems, the task of ensuring functional safety becomes very important. In most cases this problem is solved by introducing redundancy that is understood as an exceeding complexity of the system structure compared to the minimal values required for the performance of the specified task [3]. The simplest way of ensuring redundancy is by creating backup capabilities, particularly standby duplication within the system of functional units and components. In order to evaluate the safety of the railway transportation power supply systems it is required to calculate the functional safety indicators of their components and system as a whole taking into account the factor of redundancy. This approach will enable the optimal redundancy architectures and ensure compliance with the assigned level of general system safety. That requires taking into consideration the complex structure of the evaluated facilities: presence of diagnostics systems, right-side failures, wrong-side failures, as well as their random nature. The paper aims to develop an applied algorithm of calculation and prediction of functional safety indicators using the example of railway power supply systems that can be used in both manual and automated calculation.* **Methods.** *The power supply system evaluated for functional safety indicators is, from the functional point of view, a sequence of function implementations, while the failures of its components are random and some of them cause hazardous events. In this case, system analysis commonly involves Markovian and semi-Markovian methods, as well as graph methods. The advantage of these methods consists in the capability to evaluate the functional safety indicators of complex systems that go into many states, which is also typical for railway power supply systems.* **Result.** *This paper examines the application of graph semi-Markovian methods for calculation of stationary and non-stationary functional safety indicators for components of power supply systems taking into account redundancy and right-side failures. This algorithm allows calculating safety indicators using the example of power supply systems and includes a set of incremental actions aimed at constructing the state graph, calculation of the initial and intermediate graph factors. An example is provided of calculation of the functional safety indicators of a graph of a traction substation power transformer.*

Keywords: *functional safety, power supply systems redundancy, standby, Markovian and semi-Markovian processes, algorithm of calculation of functional safety indicators.*

For citation: *Pronevich OB, Shved VE. Algorithm of calculation and forecasting of functional safety indicators of railway power supply systems. Dependability 2018;3: 46-55. DOI: 10.21683/1729-2646-2018-18-3-46-55*