International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 3, 507-517, 2020
https://doi.org/10.33889/IJMEMS.2020.5.3.042

On the Calculation of Functional Safety Parameters of Technical Systems

Igor B. Shubinskiy
R & D Complex for Train Safety Ensuring and Station Processes Automation Systems,
Research and Design Institute for Information, Automation and Communication in Railway Transport,
Moscow, Russia.
Corresponding author: igor-shubinsky@yandex.ru

Leonid A. Baranov
Department of Information Management and Protection,
Russian University of Transport (MIIT), Moscow, Russia.
E-mail: baranov.miit@gmail.com

Aleksey M. Zamyshliaev
R&D Complex for Train Safety Ensuring and Station Processes Automation Systems,
Research and Design Institute for Information, Automation and Communication in Railway Transport,
Moscow, Russia.
E-mail: A.Zamyshlaev@vniias.ru

(Received September 4, 2019; Accepted February 13, 2020)

Abstract
Now the scientific methodology is created, the theory and practice of the analysis and synthesis of functional safety of responsible electronic programmable devices and systems at all stages of their life cycle are developed. The basics of the methodology are fixed by standards. Methods of analysis and synthesis of functional safety are strictly formalized. They are based on the calculations of functional safety indicators with respect to failures of constituent elements and, especially, dangerous and protective failures of the system. Known methods of calculation are focused on determining the intensity and probability of dangerous failures. The objective of the proposed method lies in the fact that, in graph form, without resorting to the solution of the system of equations in the operator transformations to establish the distribution function of time until the threat or security failure, or any unhealthy condition of the system. These distribution functions determine all the necessary indicators of mean time (and, if necessary, the variance of this time) to a dangerous or protective failure. The proposed semi-Markov (Markov) operator method allows to solve a number of problems of calculation and prediction of functional safety of critical (responsible) systems. The method is formalized and suitable for subsequent computer implementation. This fact testifies to the expediency of further development of graph methods, convenient for the study of the safety of complex critical systems, devoid of the shortcomings of the proposed method in terms of the complexity of the preparatory work to determine the analytical expressions of transition probabilities in the Laplace - Stieltjes transformations. The given example of using the method has an independent value – it allows you to assess the advantages and disadvantages of ensuring functional safety by building a two-channel system without restarting the channels

Keywords- Of functional safety parameters, Hazardous and protection failures, Markov and semi-Markov stochastic processes, The weight of a path in a graph, The weight of decomposition on the graph.

1. Introduction

The functional safety of safety-critical technical systems has been a focus of attention of experts since the last century (Swir, 1986; Guller, 1991; Braband and Lennartz, 1999). The functional safety of control systems has been investigated in the work of a number of leading scientists (Braband, 2001; Schäbe, 2002; Smith and Simpson, 2004; Gulker and Schäbe, 2006; Bouwman et al., 2009; Kayen and Schäbe, 2009) Critical (dangerous) system faults cause management errors that lead or may lead to fatalities, unacceptable damage to the environment, the economy and the industry's public image. The widespread introduction of information technology, development of safety-critical multi-functional hardware and software control systems eliminated the possibility of manual or even automated identification of all possible causes of dangerous failures. Currently, a scientific methodology, theory and practice of analyzing and synthesizing the functional safety of critical electronic programmable devices and systems at all stages of their life cycle has been developed. Basics of this methodology have been standardized for different branches (IEC 61508-(1-7)-2012), in railway (EN 50126-(1-5):2017, IEC 62278-2098, IEC 62279-2016, IEC 62280-2017, etc), in nuclear energy (IEC 61513- 2011, etc.), industrial networks (IEC 61784-2016, etc) and other industries. The methods of analysis and synthesis of functional safety parameters are strictly formalized. They are based on the calculations of functional safety of technical systems that may be in the following states:

i. *Functioning or defective state* - the state of the system in which all the requirements of technical documentation are provided or at least one of these requirements is not provided, respectively.
ii. *Healthy or unhealthy state* - the state of the system, in which the values of all parameters characterizing the ability to perform specified functions, meet the requirements of technical documentation or not provided the value of at least one parameter, respectively.
iii. *The protective state* - that is, the state of the system in which the performance of all the planned system functions is disabled in case of timely detection of a failure of any control element or a breach of control safety.
iv. *Hazardous state* - i.e. a down state of a system, in which at least one safety function is not performed.
v. *Non-hazardous condition* - the operational or protective state of the system.

These states and their interrelation are illustrated by the images of set theory. Let the complete set of safety states of the system (or software, in the case of its autonomous consideration) is denoted by the symbol *S*. A subset of functioning states -S_h. A subset of the defective -$\overline{S}_h$. Obviously, both of these subsets form a complete set of safety states. A similar observation can be made about a subset of healthy states S_S and unhealthy states $\overline{S}_S$ ($S = S_S \bigcup \overline{S}_S$). The subset of defective states is included in the subset of unhealthy states $\overline{S}_h \subset \overline{S}_S$. In this case, a subset of defective states minus a subset of unhealthy states $(\overline{S}_S \setminus \overline{S_h})$ is part of a subset of healthy states. A subset of unhealthy states $\overline{S}_p$ in turn is divided into two subsets – protective states (S_p) and hazardous states ($\overline{S}_N$) ($S_P = \overline{S}_h \setminus \overline{S}_N$). Subsets of non-hazardous and hazardous system states form a complete set of safety states $S_N = S_h \bigcup S_P;(S_N \bigcup \overline{S}_N = S)$.

Each control system has at least two safe states: normal operation state and shutdown state (the system is off).

It is assumed that a system is free from failures in the normal operating state. A shutdown state is typically a state, in which a system does not perform system functions. A safe shutdown state is to be achieved within a relatively short period of time through the termination of system functions. The termination of system functions can be an active process (an additional function of the system).

2. Problem Definition

It is assumed that the mathematical modeling of functional safety parameters of the system under consideration is carried out using a semi-Markov or Markov random process and a system state graph.

The initial data is as follows:

● *Oriented state graph* $G(S,H)$, where *S* is a finite set of vertices (states) of the system; *H* is a finite set of arcs between vertices *i, j* (states S_i, S_j).

● *Criterion of a dangerous failure* in the form of a set of operable or non-dangerous states $S_N \subset S$, a set of dangerous failure states $\overline{S_н} \subset S$, where $S_N \bigcap \overline{S_N} = \varnothing$, $S_N \bigcup \overline{S_N} = S$, and also the initial state $0 \equiv S_0$ (or $\mathrm{i} \equiv S_i$), where $S_i \subset S_N$.

● *Protective failure criterion* in the form of a set of protective states $S_P \subset S_N$, a set of operational or non-dangerous and unsafe states $\overline{S_P} \subset S_N$, where $S_P \bigcap \overline{S_P} = \varnothing$, $S_P \bigcup \overline{S_P} = S_N$, and also the initial state $0 \equiv S_0$ (or $\mathrm{i} \equiv S_P$), where $S_i \subset \overline{S_P}$.

● *Square matrix* $(F_{ij}(t))$ of conditional distribution functions of the time a system is in specific states (vertices) of the graph, the adjacency matrix and the distribution vector of initial probabilities for the ergodic or transient states. If the behavior of a system is described by a Markov random process, it suffices to set the matrix of transition intensities between adjacent vertices (λ_{ij}), where λ_{ij} is the rate of failures and recoveries of one element of the system in the *i*-th state, as a result of which it goes into the adjacent *j*-th state.

The problem consists in finding formulas that allow using standard procedures for finding paths and contours to calculate a number of indicators that are essential for the rational design of safe systems: mean time to dangerous failure T_D; mean time to protective failure T_P; dispersion of time to dangerous failure D_D or protective failure D_P (if required for the study).

The list above does not include the indicators of the rate and probability of hazardous failures set forth in standards (IEC 61508-(1-7)-2012). They can be identified using the above safety indicators.

It is assumed that the processes of occurrence and elimination of hazardous and protection failures can be simulated using the mathematics of random Markov or, more generally, semi-Markov random processes. Due to the large number of states of the systems under study and, consequently, the increasing number of equations, it is known that the solution of large systems of equations is in many cases complicated. It is preferable to determine the desired indicators of safety and dependability of systems directly on the state graph. The well-known Markov and semi-Markov graph methods (Shubinsky,1985; Rinske and Ushakov, 1988; Shubinsky and Zamyshlyaev, 2012; Pronevich and Shved, 2018) have great advantages in terms of solution technique, since it suffices to once perform well-formalized procedures for finding paths and contours on graphs to identify the dependability indicators of a complex system. However, these methods are not geared towards solving problems of functional safety and, in addition, are not universal enough for a wide class of technical systems.

3. The Method of Solving the Problem

In some problems of calculating the safety and reliability indicators of systems, there is a practical possibility of moving from the description of Markov or semi-Markov random processes of system behavior using differential equations to the description of system behavior using operator Laplace - Stieltjes transformations (Korolyuk, 1965; Kashtanov and Kondrashova, 2012; Viktorova and Stepanyants, 2014; Schäbe and Shubinsky, 2016). The objective of the proposed method is to establish in graph form, without resorting to solving a system of equations in operational transformations, the time distribution functions to a dangerous or protective failure or to any non-working state of the system. Using such distribution functions, all safety indicators listed in clause 2 above are in operator form. To do this, the following input data is to be specified:

- oriented state graph $G(S,H)$, where S is a finite set of vertices (states) of the system; H is a finite set of arcs between vertices i, j (states S_i, S_j).
- dangerous failure criterion in the form of a set of up or non-hazardous states $S_N \subset S$, set of wrong-side failure states $\overline{S_N} \subset S$, where $S_N \cap \overline{S_N} = \varnothing$, and the initial state $0 \equiv S_0$ (or $i \equiv S_i$), where $S_i \subset S_N$.
- criterion of protective failure in the form of a set of safe states $S_P \subset S_N$, a set of operational or non-hazardous and non-safe states $\overline{S_S} \subset S_H$, where $S_S \cap \overline{S_S} = \varnothing$, $S_S \cup \overline{S_S} = S_H$, and the initial state $0 \equiv S_0$ (or $i \equiv S_S$), where $S_i \subset \overline{S_S}$.
- criterion of system failure in the form of a set of functional states $S_1 \subset S$, set of down states $\overline{S_1} \subset S$, where $S_1 \cap \overline{S_1} = \varnothing$, $S_1 \cup \overline{S_1} = S$.
- square matrix ($F_{ij}(t)$) of conditional distribution functions of the time of the system being in particular states (vertices) of the graph, the adjacency matrix and the distribution vector of initial probabilities for the ergodic or irrevocable states.

Theorem. The distribution function of time to dangerous failure of a system, the behavior of which is described by a semi-Markov random process, in the Laplace-Stieltjes transforms at the *i*-th initial state ($i \in S_N, S_N \cap \overline{S_N} \neq \varnothing, S_N \cup \overline{S_N} = S$) is defined by the expression

$$\tilde{\Phi}_i(z) = \frac{\sum\limits_{j \in \overline{S_H}} \sum\limits_{k} \tilde{l}_k^{ij}(z) \Delta \tilde{G}_k^j(z)}{\Delta \tilde{G}_{\overline{S_N}}(z)},$$

where, $\tilde{l}_k^{ij}(z)$ is the *k*-th path in the Laplace-Stieltjes transforms leading from the initial or non-hazardous state of a graph $i \in S_N$ to a hazardous state $j \in \overline{S_N}$.

$\Delta\tilde{G}_k^j(z)$ is the weight of the graph decomposition in the Laplace-Stieltjes transforms without the j-th vertex and vertices of the graph on the *k*-th path;

$\Delta\tilde{G}_{\overline{S_N}}(z)$ is the weight of the decomposition of a graph without vertices of the set of states of a dangerous failure.

The weights of the graph decomposition are determined by the Mason formula widely used in the theory of automatic control

$$\Delta\tilde{G}(z)=1-\sum_j C_j(z)+\sum_{jr} C_j(z)\cdot C_r(z)-\sum_{jrk} C_j(z)\cdot C_r(z)\cdot C_k(z)+\ldots$$

where, $C_j(z)$; $C_r(z)$; $C_k(z)$, etc. are the weights of independent contours on a graph in Laplace-Stieltjes transforms.

Proof. In, Korolyuk (1965), it is shown that the distribution function of the time a system is in a fixed set of states S_N in the Laplace-Stieltjes transforms can be obtained from the equation

$$\tilde{\Phi}_i(z)-\sum_{j\in S_N}\tilde{Q}_{ij}(z)\tilde{\Phi}_j(z)=\sum_{l=\overline{S_N}}\tilde{Q}_{il}(z).$$

We transform this equation into the matrix form, bearing in mind that the right side of the equation is a column vector of free terms of semi-Markov transition probabilities in one step from vertices $i, j,\ldots,r\in S_N$ to vertices $\in\overline{S_N}$

$$\tilde{\Phi}(z)-\tilde{Q}(z)\tilde{\Phi}(z)=\tilde{Q}^*(z)$$

where, $\tilde{Q}(z)=(\tilde{Q}_{ij}(z))$ is the matrix of semi-Markov probabilities; $\tilde{Q}^*(z)=(\tilde{Q}_{il}(z))$ is the column vector.

In the system of equations, the elements of the column vector are unknown. After grouping them on the left side we obtain:

$$\tilde{\Phi}(z)\left[I-\tilde{Q}(z)\right]=\tilde{Q}^*(z).$$

Then, according to the Cramer rule, we find $\tilde{\Phi}_i(z)=\frac{\Delta_i(z)}{\Delta(z)}$, where $\Delta(z)=\left|I-\tilde{Q}(z)\right|$, while $\Delta_i(z)$ is the determinant resulting from the replacement of the *i*-th column in the matrix $I-\tilde{Q}(z)$ with a column vector of free terms $\tilde{Q}^*(z)$, provided that $\Delta_i(z)$ and $\Delta(z)$ are not zero.

Determinant $\Delta_i(z)$ differs from determinant $\Delta(z) = \Delta G_{\overline{S_H}}$ in that in column *i* element $\tilde{p}_{ij}(z)$ is replaced by element $\tilde{p}_{il}(z)$, where $i, j \in S_H$, while $l \in \overline{S_H}$. As a result, we obtain

$$\Delta_i(z) = \Delta G^{i}_{\overline{S_N}} = \sum_{l \in \overline{S_N}} \sum_{k} \tilde{l}_k^{il}(z) \Delta G_k^{l}(z)$$

Therefore,

$$\tilde{\Phi}_i(z) = \frac{\sum_{j \in \overline{S_N}} \sum_{k} \tilde{l}_k^{ij}(z) \Delta \tilde{G}_k^{j}(z)}{\Delta \tilde{G}_{\overline{S_N}}(z)}$$

and when we replace index *l* with *j*, we obtain the desired result. The theorem is proved.

Corollary 1. The functions of the distribution of time to protective failure ($\tilde{\Phi}_S(z)$) or to any down state ($\tilde{\Phi}_1(z)$) in the Laplace-Stieltjes transforms are identified based on this theorem by replacing subsets of states $\overline{S_N}$ with subsets of states S_P or $\overline{S_1}$, respectively.

Corollary 2. Based on theorem and corollary 1, the following indicators of safety, protective and reliability of the system are determined:

- mean time to dangerous failure

$$\bar{t}_D = -\frac{\partial \tilde{\Phi}_D(z)}{\partial z}\Big|_{Z=0};$$

- dispersion of time to dangerous failure:

$$D_D = -\frac{\partial^2 \tilde{\Phi}_D(z)}{\partial z^2}\Big|_{Z=0} - \left[\frac{\partial \tilde{\Phi}_D(z)}{\partial z}\right]^2_{Z=0};$$

- mean time to protective failure

$$\bar{t}_P = -\frac{\partial \tilde{\Phi}_P(z)}{\partial z}\Big|_{Z=0};$$

- dispersion of time to protective failure

$$D_P = -\frac{\partial^2 \tilde{\Phi}_P(z)}{\partial z^2}\Big|_{Z=0} - \left[\frac{\partial \tilde{\Phi}_P(z)}{\partial z}\right]^2\Big|_{Z=0};$$

- mean time to failure (any down state)

$$\bar{t}_1 = -\frac{\partial \tilde{\Phi}_{0_1}(z)}{\partial z}\Big|_{Z=0};$$

- dispersion of time to failure

$$D_1 = -\frac{\partial^2 \tilde{\Phi}_{0_1}(z)}{\partial z^2}\Big|_{Z=0} - \left[\frac{\partial \tilde{\Phi}_{0i\,1}(z)}{\partial z}\right]^2\Big|_{Z=0}.$$

4. Example of Calculation

Let us illustrate the analytical findings with an example of calculation of the average time to dangerous failure. The system contains two identical and independent data processing channels, as well as diagnostic facilities that test the status of each channel and compare their outputs with a periodicity less than the allowable time of detection of single failures. Information is read, if the channel outputs match. Channel failure is asymmetrical. If the diagnostic facilities are operable, the fact of failure of any one channel is identified, upon which the system is put in the state of protective failure. In the event of failure of the diagnostic facilities, a non-dangerous failure occurs. The following channel failure causes the dangerous failure of the system. A dangerous failure can also occur if the diagnostic facilities ignore a channel failure. The graph of the safety states of a two-channel system with in-built diagnostic facilities is shown in Figure 1. The states are as follows: 0: operable state; 1: failure of diagnostic facilities; 2: protective failure initiated by the user or an automatic circuit in case of detection of a failure of any one of the channels by standard diagnostic facilities with the probability of ν; 3: undetected failure of a channel due to failure or insufficient effectiveness of diagnostic facilities (dangerous failure).

The sets of non-hazardous or protective states, respectively $S_{\bar{N}} = \{S_{0,}S_1, S_2\}; S_P = S_2$.

It is assumed that the failure and recovery flows, as well as the one channel failure detection flow are the simplest ones with rates λ, λ_h, μ . The events of failure of complex technical facilities are mutually independent. The recovery is carried out in the state 2 of protective failure. In the event of a failure, the channels are not reset and the system enters the state of right-side failure.

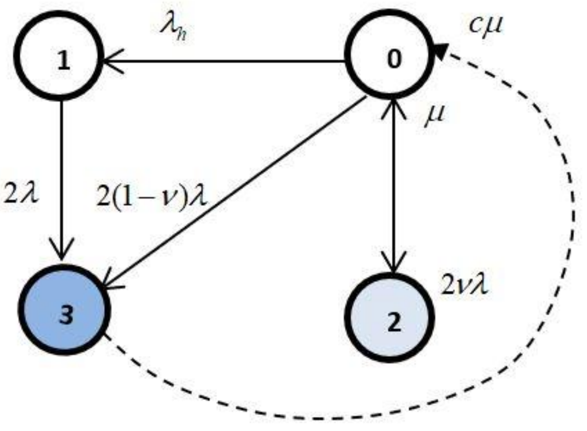

Figure 1. Safety state graph of a two-channel system

In Figure 1, the edges of the graph are marked with the following parameters: λ_h, failure rate of the diagnostic facilities; 2λ, failure rate of two same-type information processing channels; μ, recovery rate after failures of the channel in the case of single maintenance crew.

The functional safety model of the two-channel system in Figure 1 involves the following logic of operation: 0 is the initial state (all elements of the system are correct). If the diagnostic facilities fail, the system goes into state 1. If anyone channel (state 2) has failed and the channel failure was timely detected with probability ν, the system goes into a protective failure state (the system does not function, the channel is under maintenance). In case of hidden channel failure with probability $\bar{\nu} = 1 - \nu$ or one channel failure upon failure of diagnostic facilities (path 0 – 1 – 3), the system is put into state 3 of dangerous failure.

The solution of this model will consist in the analytical definition of the indicator of mean time of wrong-side failure of such two-channel system. Given the above, the behavior of the system is described with a Markov random process. For the solution of the problem involves the preliminary definition of the distribution functions of the unconditional time of the system being in the specific states of the graph and in the Laplace-Stieltjes transforms source parameters - transition probabilities.

The distribution functions of the time of the system being in the graph states in Figure 1,

$$F_0(t) = 1 - \exp[-(\lambda_d + 2\lambda)];\ F_1(t) = 1 - \exp(-2\lambda);\ F_2(t) = 1 - \exp(-\mu);\ F_3(t) = 1 - \exp(-c\mu).$$

The transition to the initial state 0 from the absorbing state 3 of wrong-side failure is shown with a dashed line. This imaginary edge (3-0) of the graph is marked with parameter $c\mu$ (rate of elimination of a wrong-side failure), where $0 < c \leq 1$. If the elimination of a wrong-side failure does not require the modification of the device, then c = 1 and the rate of elimination of a wrong-side failure is equal to the rate of recovery of the device. If the device requires a modification, then, depending on the duration τ of modification, this coefficient will be $c = 1/\tau$ that is much less than 1.

The transition probabilities in the Laplace-Stieltjes transforms for this example are defined by the following expression:

$$\tilde{p}_{ij}(z) = \frac{\lambda_{ij}}{\sum_i \lambda_{ij}} \int_0^\infty e^{-zt} dF_i(t).$$

They have the following form

$$\tilde{p}_{01}(z) = \frac{\lambda_h}{\lambda_h + 2\lambda + z};\ \tilde{p}_{02}(z) = \frac{2\nu\lambda}{\lambda_h + 2\lambda + z};\ \tilde{p}_{03}(z) = \frac{2(1-\nu)\lambda}{\lambda_h + 2\lambda + z};$$

$$\tilde{p}_{12}(z) = \frac{2\lambda}{2\lambda + z};\ \tilde{p}_{20}(z) = \frac{\mu}{\mu + z};\ \tilde{p}_{30}(z) = \frac{c\mu}{c\mu + z}.$$

Based on the established theorem, the distribution functions of time to the dangerous and protective failure are defined in the Laplace-Stieltjes transforms

$$\tilde{\Phi}_D(z) = \frac{\tilde{l}_1^{03}(z) + \tilde{l}_2^{03}(z)}{1 - \tilde{C}(z)};\ \tilde{\Phi}_P(z) = \tilde{l}_1^{02}(z),$$

where,

$$\tilde{l}_1^{03}(z) = \tilde{p}_{01}(z) \cdot \tilde{p}_{12}(z) = \frac{\lambda_h 2\lambda}{(\lambda_h + 2\lambda + z)(2\lambda + z)};\ \tilde{l}_2^{03}(z) = \tilde{p}_{03}(z) = \frac{2(1-\nu)\lambda}{\lambda_h + 2\lambda + z};$$

$$\tilde{l}_1^{02}(z) = \frac{2\nu\lambda}{\lambda_h + 2\lambda + z};\ \tilde{C}(z) = \tilde{l}_1^{02}(z)\tilde{l}_1^{20}(z) = \tilde{p}_1^{02}(z)\tilde{p}_1^{20}(z) = \frac{2\nu\lambda \cdot \mu}{(\lambda_h + 2\lambda + z)(\mu + z)}.$$

Therefore,

$$\tilde{\Phi}_D(z) = \frac{\left[2\lambda\lambda_h + 2\bar{\nu}\lambda(2\lambda + z)\right](\mu + z)}{\left[(2\lambda + \lambda_h + z)(\mu + z) - 2\nu\lambda\mu\right](2\lambda + z)}$$

(1)

and the mean time to dangerous failure is

$$\bar{t}_D = -\frac{\partial\tilde{\Phi}_D(z)}{\partial z}\Big|_{Z=0} = \frac{2\lambda(\mu + 2\nu\lambda) + \lambda_h\mu}{2\lambda\mu[2\lambda(1-\nu) + \lambda_h]} \qquad (2)$$

If we take into account the fact that, in practice, in control systems $\lambda << \mu$; $\frac{\lambda_d}{\lambda} = k$, then, with an error of less than the first order of smallness, an approximate expression of the mean time to wrong-side failure is:

$$\bar{t}_D \approx \frac{2+k}{2\lambda(2\bar{\nu}+k)} \tag{3}$$

By differentiating the distribution function $\tilde{\Phi}_p(z)$ (1) under $z = 0$ the mean time to protective failure is found:

$$\bar{t}_p = \frac{2\nu\lambda}{(\lambda_d + 2\lambda)^2} = \frac{2\nu}{k\lambda(k+2+4/k)} \tag{4}$$

Since, in reality, $4/k >> (k+2)$ and $k+2$ in the denominator can be neglected, then, with an error of less than the first order of smallness, a simplified expression of the formula (4) of the average time to a dangerous failure is valid

$$\bar{t}_p \approx \frac{\nu}{2\lambda} \tag{5}$$

The analysis of expression (3) in the example above demonstrates the feasibility provided the diagnostic facilities have the dependability of $\left(\frac{\lambda_h}{\lambda} = k << 1\right)$ and efficiency of $(\bar{\nu} << 1)$ of a mean time to wrong-side failure ten or more times higher as compared to the same parameter of the information processing channel. However, as follows from the expression (5), the mean time to right-side failure is lower than the mean time to failure of the information processing channel, which can lead to significant system downtime.

5. Conclusion

The proposed semi-Markov (Markov) operator graph method allows to solve a number of problems related to the calculation and prediction of functional safety parameters of critical systems. The method is formalized and suitable for subsequent computer implementation. This indicates the expediency of further development of graph methods, convenient for the study of the safety of complex critical systems, devoid of the shortcomings of the proposed method in terms of time-consuming preparation, involving the definition of analytical expressions of transition probabilities in Laplace-Stiltjes transformations. The above example of the method has its own significance. This allows you to evaluate the advantages and disadvantages of providing functional security through a dual-channel system without restarting the channels.

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgements

The authors would like to express their sincere thanks to the editor and anonymous reviews for their time and valuable suggestions.

References

Bouwman, R., Schäbe, H., & Vis, H. (2009). Application of safety principles–for a guidance system in public transport. In *2009 ESREL Proceedings Reliability, Risk and Safety*, (Vol. 3, pp. 2275-2278).

Braband, J. (2001). A practical guide to safety analysis methods. *Signal+Draht*, *93*(9), 41-44.

Braband, J., & Lennartz, A. (1999). Systematic process for the definition of safety targets for railway signalling applications. *Signal + Draht*, *9*, 53-57.

Gulker, J., & Schäbe, H. (2006). Physical principles of safety. In *ESREL Proceedings Safety Reliability and Risk analysis* (Vol. 2, pp. 1045 -1050). Rotterdam: Balkema.

Guller, W.J. (1991). Safety-critical control systems. *Computer and Control Engineering Journal*, *2*(5), 201-210.

Kashtanov, V.A., & Kondrashova, E.V. (2012). Analysis of input flow controlled by Markov chain. *Dependability*, *1*, 38-52.

Kayen, I.T., & Schäbe, H. (2009). Incorrect and correct understanding of the principles of functional safety. *Dependability*, *4*, 63-74.

Korolyuk, V.S. (1965). The residence time of a semi-Markov process in a fixed set of states. *Ukrainian Mathematical Journal*, *17*(3), 123-128.

Pronevich, O.B., & Shved, V.E. (2018). Algorithm of calculation and forecasting of functional safety indicators of railway power supply systems. *Dependability*, *3*, 46-55.

Rinske, K., & Ushakov, I.A. (1988). Reliability of systems with the use of graphs. In: Ushakov, I.A (ed) *Radio and Communication*. Moscow.

Schäbe, H. (2002). The safety philosophy behind CENELEC rails standings. In *ESREL 2002, European Safety and Reliability Conference* (pp. 788-790). Lyon.

Schäbe, H., & Shubinskiy, I.B. (2016). Limit reliability of structural redundancy. *Dependability*, *16*(1), 3-13.

Shubinskiy, I.B., & Zamyshlyaev, A.M. (2012). Topological semi-Markov method for calculation of stationary parameters of reliability and functional safety of technical systems. *Reliability: Theory & Applications*, 12-22.

Shubinsky, I.B. (1985). A topological method for calculating the reliability of complex technical systems: Handbook. In: Ushakov, I.A (ed) *Radio and Communications*. pp. 490-495.

Smith, D.J., & Simpson, K.L.G. (2004). Functional safety. In: Shubinskiy, I.B. (ed) *A Simple Guide to the Application of IEC 61508 and Related Standards*. Moscow: Technologies.

Swir, V. (1986). Reliability of electronic circuits in signaling systems. *World Railways*, *1*, 59-67.

Viktorova, V.S., & Stepanyants, A.S. (2014). Dependability indices of mean time type. *Dependability*, *3*, 37-47.