THE JOURNAL IS INCLUDED IN THE LIST OF THE LEADING JOURNALS AND EDITIONS OF THE HIGHER ATTESTATION COMMISSION (VAK)

ISSN 1729-2646
e-ISSN 2500-3909

THE JOURNAL PROMOTER:
"Journal "Reliability" Ltd

It is registered in the Russian Ministry of Press, Broadcasting and Mass Communications. Registration certificate ПИ 77-9782, September, 11, 2001.

Official organ of the Russian Academy of Reliability

Publisher of the journal
LLC Journal "Dependability"
Director
I. Kalinina
The address: 109029, Moscow,
Str. Nizhegorodskaya, 27,
Building 1, office 209
Ltd Journal "Dependability"
www.dependability.ru
Printed by JSC "Regional printing house,
Printing place" 432049, Ulyanovsk,
Pushkarev str., 27. Circulation: 500 copies.
Printing order
Papers are reviewed. Signed print ,
Volume , Format 60x90/8, Paper gloss

Papers are reviewed.

THE JOURNAL IS PUBLISHED WITH THE PARTICIPATION AND SUPPORT OF THE JOINT-STOCK COMPANY «RESEARCH AND DESIGN INSTITUTE OF INFORMATISATION, AUTOMATION AND COMMUNICATION ON RAILWAY TRANSPORT» (JSC «NIIAS») AND LLC PUBLISHING HOUSE «TECHNOLOGY»

CONTENTS

Regarding the planning of testing scope for new equipment samples

Alexander V. Antonov, *chair of automation systems, Obninsk Institute for Nuclear Power engineering (Branch of National Research Nuclear University MEPhI), Russia, Obninsk, e-mail: antonov@iate.obninsk.ru*
Valery A. Chepurko, *chair of automation systems, Obninsk Institute for Nuclear Power engineering (Branch of National Research Nuclear University MEPhI), Russia, Obninsk, e-mail: chepurko@iate.obninsk.ru*
Vladimir E. Chekhovich, *JSC State scientific center of the Russian Federation – Institute for Physics and Power Engineering named after A. I. Leypunsky, e-mail: 89158916216@rambler.ru*
Vladimir F. Ukraintsev, *JSC State scientific center of the Russian Federation – Institute for Physics and Power Engineering named after A. I. Leypunsky, e-mail: ukraintsev@mail.ru*


Alexander V. Antonov


Valery A. Chepurko


Vladimir E. Chekhovich


Vladimir F. Ukraintsev

Abstract. Purpose. *This article describes the issues of planning testing scope for high-reliable objects. The development and manufacture of new samples of equipment is accompanied by a task to define their reliability characteristics. It is based on the fact that there are requirements related to the necessity to specify the above mentioned characteristics in certificates and technical descriptions of the products supplied to the market. The most objective way to define reliability characteristics of the products is a field test. But under the manufacture of complex expensive objects there is no opportunity to introduce a batch with lots of finished products for testing. Thus there is a task to define the duration of field testing and scope of products to be tested, provided there are requirements for the accuracy of estimations related to the objects' reliability characteristics obtained as the result of testing. Planning of the scope is based on the requirements of a manufacturer related to a necessity to confirm the value of lower bound of reliable operation probability with a predefined confidence level. Two tasks are solved in this work. The first task is to define the scope of testing of a batch with finished products N_0 for a time moment t_0, for which a customer's requirement would be fulfilled related to the achievement of the lower bound of probability of reliable operation, specified with a confidence probability 1 – . This task is solved using a non-parametric approach. The second task is to define a required scope of test N_{t1} of the equipment of this type for the time moment different from the moment of first studies $t_1 \neq t_0$. Here one solves the question: how are N_{t0} and N_{t1} correlated? The scope of tests N_{t1} is defined based on the determination of confidence levels providing with the same accuracy of indices as in point t_0. This task is solved with a semiparametric approach. When solving the second task, the parameterization of mean time to failure distribution is used. Three types of distribution are studied: exponential law, Weibull distribution and distribution with linear function of a failure rate. The considered types of distribution laws help to study the behavior of the objects with a decreasing, constant and increasing function of failure rate.* **Methods.** *The formulas for calculation of test scope for different durations of a test-run are derived. Dependence of scope on the duration of a test-run and on a real level of probability of reliable operation is studied as well. Scope planning and respective studies are carried out for different behavior models of a failure rate of the product.* **Conclusion.** *Obtained results give the basis for a well-reasoned approach to the planning of scope of tests of high-reliable objects. The study results showed that the longer a test-run is, the fewer objects are required to be introduced for a test. Dependence is non-linear; it is specified by the parameterization of the failure rate function. Analogous dependence was also obtained for the probability of reliable operation: the higher the PRO is, the fewer objects are required to be tested.*

Keywords: *planning of scope of tests, duration of a test-run, probability of reliable operation, failure rate, lower bound of probability of reliable operation, confidence probability level.*

Citation format: *Antonov A.V., Chepurko V.A., Chekhovich V.E., Ukraintsev V.F.. Regarding the planning of testing scope of the new equipment samples // Dependability. 2016. No.3. P. 3-7. DOI: 10.21683/1729-2640-2016-16-3-3-7*

Introduction

The development and manufacture of new samples of equipment is accompanied by a task to define their reliability characteristics. It is based on the fact that there are requirements related to the necessity to specify the above mentioned characteristics in the certificates and technical descriptions of the products supplied to the market. The most objective way to define reliability characteristics of the products is a field test. But it should be noted that under the manufacture of complex expensive objects there is no opportunity to introduce a batch with lots of finished products for testing. Thus there is a task to define the duration of field testing and scope of products to be tested, provided there are requirements to the accuracy of estimations related to the objects' reliability characteristics obtained as the result of testing.

Before proceeding with a task definition it is necessary to consider the behavior of indices to be used for the definition. Let us take probability of reliable operation (PRO) – $P(t)$ as an index to be defined. Accuracy of non-parametric estimation of this index is specified by a dispersion calculated by formula:

$$D\left(\hat{P}(T)\right) = \frac{P(t)\left(1-P(t)\right)}{N},$$

where N is scope of tests during which a PRO is estimated. Therefore, we will get a dispersion value depending on the test scope and a PRO value. The higher the PRO value is, the lower the dispersion is. The dispersion gets its maximum value at the PRO level equal to 0.5. Then, as the level is less than 0.5, the dispersion is getting lower again.

The dispersion of the estimation of PRO index is related to another characteristic of accuracy – a lower confidence estimation of PRO calculated with a specified confidence probability 1–α. As there is a task to estimate the objects' reliability characteristics, it is implied that a researcher does not have any a priori information about these indices. A production manufacturer expects that the equipment supplied to the market must be high-reliable. He assigns a task for a researcher about the timing and scope of tests which may ensure a certain level of the equipment reliability. A task can be defined based on the following considerations. A manufacturer formulates some requirements to the lower confidence estimation of PRO ($\underline{P}_0$), which should be provided with a specified confidence probability 1–α, i.e.

$$\Pr(P(t_0)\geq \underline{P}_0)=1-\alpha.$$

This value will be a lower critical value. *Initial value of the lower confidence level of PRO is estimated by the methods of calculation of a structural reliability* [1, 2]. We will define a required number of the objects N_0 to be tested based on this value of the lower confidence estimation of PRO. A required scope of tests that was derived when solving this task, N_0 will ensure the achievement of the specified PRO levels – $[\underline{P}_0,1]$ with confidence probability 1 – α.

If during the tests it turned out that the object's reliability is higher than it was expected by the customer – $\underline{P}_0^* \geq \underline{P}_0$, it means that based on the predefined scope N_0, the reliability index to be estimated is obtained with a higher accuracy – $\underline{P}_0^*$. In this case to achieve the result with a predefined accuracy $\underline{P}_0$, fewer tests N_0^* are required.

Task definition

Therefore, having familiarized with this reasoning one can set the first task of the study which is to define the scope of tests of the batch with finished products N_0 so that for any value $\underline{P}_0^* \geq \underline{P}_0$, predefined with a confidence probability 1–α, a correlation for the required scope of tests $N_0^* \leq N_0$ shall be fulfilled.

When solving the task let us assume that a failure rate function is defined by one of the formulas [1]:

$$\lambda(t) = \lambda; \quad (1)$$

$$\lambda(t) = \lambda_1+\lambda_2 t; \quad (2)$$

$$\lambda(t) = \lambda_1 t^{\lambda 2}. \quad (3)$$

Expression (1) (a rate is constant) is common with an exponential distribution of mean time to failure, formula (2) is basic for a distribution with linear failure rate and function (3) is basic for Weibull distribution.

To simplify calculations let us transform the model under consideration to the following form:

$$\lambda(t) = \lambda g(t), \quad (4)$$

where g(t)=1 corresponds to the exponential distribution,

g(t)=a+bt corresponds to the distribution with linear function of the failure rate, (5)

g(t)=t^a corresponds to the Weibull distribution. (6)

Function of the failure rate g(t) must satisfy two basic requirements:

$$g(t)\geq 0,$$

$$G(t) = \int_0^t g(\tau)d\tau \to \infty \text{ with } t\to\infty.$$

Besides we shall assume that coefficients in (5), (6) a, b are known, the one which is unknown and estimated by the sampling is λ.

Planning of scope of tests in non-parametric statement

Let us proceed with a task solving now. We shall solve the task in non-parametric statement. We know [5] that for any t the number of products that have not failed up to the moment t is distributed by a binomial law

$$N\hat{P}(t) = \mu_N(t) \sim Bin\left(N, P(t)\left(1-P(t)\right)\right)$$

$$\Pr\left(\hat{P}(t) \geq \underline{P}\right) = \sum_{i=k}^{N} C_N^i P^i(t)\left(1-P(t)\right)^{N-i} = I_{P(t)}(k, N-k+1),$$

where $I_x(a,b)$ is an incomplete beta-function, $k = \lceil N\underline{P} \rceil$ is an expression $N\underline{P}$ rounded to the larger one. It is not possible to find an accurate analytical solution of equation

$$I_{P(t)}(k, N-k+1) = 1-\alpha$$

because it contains two unknown variables N and $P(t)$. Let us study approximate ways of the task solving.

If to use a central limit theorem, we shall obtain a normal law for the PRO estimation at the limit:

$$\hat{P}(t) \sim Norm\left(P(t); \frac{P(t)\left(1-P(t)\right)}{N}\right). \quad (7)$$

This makes it possible to form a one-sided confidence set:

$$\Pr\left(\hat{P}(t) \geq \underline{P}\right) = 1-\Phi\left(\frac{\underline{P}-P(t)}{\sqrt{P(t)\left(1-P(t)\right)}}\sqrt{N}\right) = \alpha,$$

where $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} \exp\left(-u^2/2\right)du$ is the function of distribution of the standard normal law – $Norm(0;1)$.

Therefore, estimation of the required scope of tests that would guarantee the fulfilment of the predefined requirements shall be defined by formula

$$N_{t_0} = \frac{P_0 \cdot \left(1-P_0\right) \cdot u_{1-\alpha}^2}{\left(\underline{P}_0 - P_0\right)^2}, \quad (8)$$

where $u_{1-\alpha}$ is a quantile of standard normal distribution $Norm(0;1)$ of level $1-\alpha$.

Variable P_0 is unspecified in expression (8). Let us estimate it based on the following considerations. It was noted earlier that PRO distribution can be approximate by the normal law (7). Thus, for an approximate estimation for P_0 we can offer a point in the middle of interval $[\underline{P}_0, 1]$. Therefore

$$P_0 = \left(1+\underline{P}_0\right)/2.$$

And finally we can write down

$$N_{t_0} = \frac{\left(1-\underline{P}_0\right)\left(1+\underline{P}_0\right)u_{1-\alpha}^2}{\left(1-\underline{P}_0\right)^2} = \frac{\left(1+\underline{P}_0\right)u_{1-\alpha}^2}{1-\underline{P}_0}.$$

Due to the fact that under the planning of testing scope a PRO value in point t_0 is unknown, let us study the dependences of the required scope of products to be tested on value P_0. When performing the calculations the following values of model parameters were taken: $\underline{P}_0$=0.93; α_0 = 0,1; t_0=360; t=540; k = 0,004. The calculations were performed for a linear model of the failure rate (2). The graph of change of the required scope of observations depending on the PRO estimation is shown in Fig. 1. Based on the results shown in the graph we can make the following conclusion: the higher the product's reliability is, the fewer products are required to be introduced for testing to confirm the PRO value. And the dependence is explicitly non-linear.

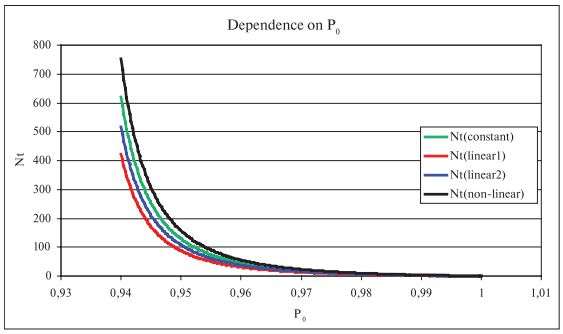


Fig. 1. Dependences of testing scope on P_0.

Semiparametric method of planning of testing scope in point $t_1 \neq t_0$

Let us solve the other task now. We shall define the required scope of tests of the equipment of a given type for another moment of time $t_1 \neq t_0$. Let us denote the required scope of tests as N_{t_1}. And besides let us answer the question: how are N_{t_0} and N_{t_1} correlated? Scope of tests N_{t_1} shall be defined based on the specified confidence bounds that ensure the same accuracy of indices as in point t_0.

Estimation of the number of tests at an arbitrary moment of time t N_t is defined by the formula similar to (8)

$$N_t = \frac{P(t) \cdot \left(1-P(t)\right) \cdot u_{1-\alpha}^2}{\left(\underline{P}(t) - P(t)\right)^2}. \quad (9)$$

Let us notice that in (9) values of the variable $\underline{P}(t)$ and $P(t)$ are unknown. Let us define them. We shall use the opportunity that $\underline{P}(t)$ should belong to the same curve of the lower bound of PRO, estimated as per model (4):

$$\underline{P}_0 = \exp\left(-\underline{\lambda} \cdot G(t_0)\right) \text{ and } \underline{P}(t) = \exp\left(-\underline{\lambda} \cdot G(t)\right).$$

Having taken the logarithm of two equations, getting rid of $\underline{\lambda}$ we obtain the correlation for lower confidence bounds of PRO:

$$\frac{\ln P_0}{\ln P(t)} = \frac{G(t_0)}{G(t)} \text{ or } \underline{P}(t) = \underline{P}_0^{G(t)/G(t_0)}.$$

We shall have the same correlation for PRO estimates

$$P(t) = P_0^{G(t)/G(t_0)}. \qquad (10)$$

If to substitute (10) in (9) and divide by (8) we will get:

$$\frac{N_t}{N_{t_0}} = \frac{P_0^{G(t)/G(t_0)} \cdot \left(1 - P_0^{G(t)/G(t_0)}\right)}{P_0 \cdot (1 - P_0)} \cdot \left(\frac{\underline{P}_0 - P_0}{\underline{P}_0^{G(t)/G(t_0)} - P_0^{G(t)/G(t_0)}}\right)^2,$$

Then we obtain the estimation for the required scope of tests at an arbitrary moment of time t:

$$N_t = \frac{P_0^{G(t)/G(t_0)} \cdot \left(1 - P_0^{G(t)/G(t_0)}\right) \cdot u_{1-\alpha}^2}{\left(\underline{P}_0^{G(t)/G(t_0)} - P_0^{G(t)/G(t_0)}\right)^2}. \qquad (11)$$

If $\lambda G(t)$ is short, then from (11) we will have

$$N_t = \frac{\lambda \cdot u_{1-\alpha}^2}{\left(\lambda - \bar{\lambda}\right)^2} \cdot \frac{1}{G(t)} + o\left(\lambda G(t)\right).$$

As $\lambda = -\frac{\ln P_0}{G(t_0)}$ and $\bar{\lambda} = -\frac{\ln \underline{P}_0}{G(t_0)}$, then we will asymptotically get the result

$$N_t = \left[\left(\frac{\ln P_0}{\ln P_0 - \ln \underline{P}_0}\right)^2 \frac{u_{1-\varepsilon}^2}{1 - P_0}\right] \cdot \frac{G(t_0)}{G(t)}.$$

This formula could be reduced as follows:

$$\frac{N_{t_1}}{N_{t_0}} = \frac{G(t_0)}{G(t_1)} \text{ or } N_t \cdot G(t) = const.$$

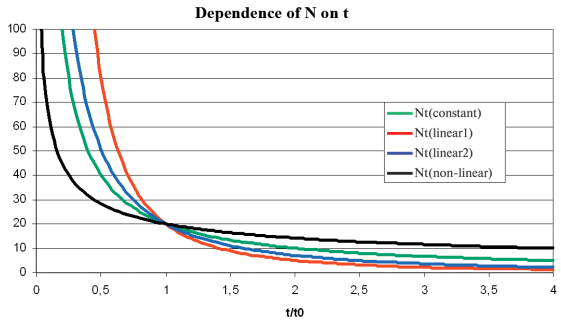


Fig. 2. Dependence of testing scope of the duration of a test-run

We shall study the obtained results. Let us calculate the required scope of tests depending on the duration of a test-run.

Fig. 2 shows the change of testing scope depending on the duration of a test-run in a relative time scale t/t_0. Input parameters of the model along the calculations were taken on the following level: P_0=0.999; $\underline{P}_0$=0.97; α_0 = 0,1; t_0=360.

Green graph corresponds to the case when $g(t)$=1 or $\lambda(t)$=λ (rate is constant). Red graph corresponds to the case when $g(t)$=t or $\lambda(t)$=λt (rate is growing linearly). Blue graph corresponds to the case when $g(t)$=1+kt or $\lambda(t)$= λ(1+kt) (rate is growing linearly from point (0, λ)), with k = 0,004. As a slope ratio k increases, the dependence of scope of observations converges fast to the graph for a linear failure rate. Black graph corresponds to the case when $g(t) = 1/\sqrt{t}$ (rate decreases as per the law $\lambda(t) = \lambda/\sqrt{t}$). The results shown in figure 2 can be illustrated by the calculations. Let us consider the exponential law of mean time to failure distribution ($G(t)$=t). For this model, if with t_0=20 hrs we should perform N_{t_0}=100 tests, then for t_1=200 hrs we will get the testing scope $N_{t_1} = N_{t_0}\frac{t_0}{t_1} = 100 \cdot \frac{20}{200} = 1010$. For a linearly increasing failure rate $\lambda(t)$= λt, respectively $G(t)$=t^2 we will get the result: if for t_0=20 hrs we should perform N_{t_0}=100 tests, then for t_1=200 hrs the number of tests shall be

$$N_{t_1} = N_{t_0}\frac{t_0^2}{t_1^2} = 100 \cdot \frac{20^2}{200^2} = 1.$$

The studies performed for a parametric model of the linear function of a failure rate showed that the increase of probability P_0 in point t_0, under the rest constant input parameters of the model leads to a significant reduction of testing scope N_t (see Fig. 3). Along the calculations input parameters took the following values: $\underline{P}_0$=0.99; α_0 = 0,1; t_0=360; k=0,004. As the result of the performed calculations the result obtained earlier was confirmed: the higher the product's reliability is, the fewer objects are required to be introduced for the tests N_t.

Conclusion

We obtained the results allowing for a well-reasoned approach to the planning of scope of tests of high-reliable objects. The information provided by a manufacturer in relation to the necessity to confirm a lower bound of probability of reliable operation with a predefined confidence probability is used as initial information. The formulas derived in the article made it possible to study the dependence of testing scope on the duration of a test-run and on the probability of reliable operation of the product. The studies showed that the longer a test-run is the fewer products are required to be introduced for testing. And the dependence is non-linear, associated with the parametrization of the failure rate function. Similar dependence was got for the probability of reliable operation as well: the higher the product's PRO is, the fewer objects are required to be tested.

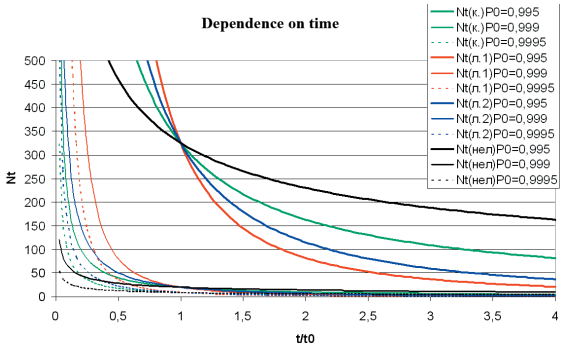


Fig. 3. Dependence of testing scope on time at different P_0

References

1. Antonov A.V. Reliability theory. Statistical models: Study guide/ Antonov A.V., Nikulin M.S, Nikulin A.M., Chepurko V.A. – M.: INFRA-M, 2015 – 576 p.:+Suppl. materials.

2. Antonov A.V. Statistical models in reliability theory: Study guide/ Antonov A.V., Nikulin M.S. – M.: Abris, 2012, – 390 p.

3. Dependability of technical systems: Reference book. Y.K. Belyaev, V. A. Bogatyryov, V. V. Bolotin and others.; Under the editorship of I. A. Ushakov. — M.: Radio i svyaz, 1985.— 608 p, illustr.

4. Reliability determination test. Y.G. Zarenin, I.I. Stoyanova. – M.: Publishing house of Standards, 1978. – 168 p.

5. Kramer G. Mathematical methods of statistics. – M.: Mir, 1975. – 648 p.

6. Antonov A.V. System analysis: College-level Students Book. – M.: High school, 2008. – 454 p.

About the authors

Alexander V. Antonov, Dr.Sci., Professor, Professor of chair of automation systems, Obninsk Institute for Nuclear Power engineering (Branch of National Research Nuclear University MEPhI).

1, Studgorodok, Obninsk, Kaluga Region, 249020, Russia, e-mail: antonov@iate.obninsk.ru

Valery A. Chepurko, Candidate of physical and mathematical sciences, Associate Professor, Associate Professor of chair of automation systems, Obninsk Institute for Nuclear Power engineering (Branch of National Research Nuclear University MEPhI).

1, Studgorodok, Obninsk, Kaluga Region, 249020, Russia, e-mail: chepurko@iate.obninsk.ru

Vladimir E. Chekhovich, Head of Division, JSC State scientific center of the Russian Federation – Institute for Physics and Power Engineering named after A. I. Leypunsky.

1, Bondarenko Square, Obninsk, Kaluga Region, 249033, Russia, e-mail: 89158916216@rambler.ru

Vladimir F. Ukraintsev, Candidate of physical and mathematical sciences, Leading Specialist, JSC State scientific center of the Russian Federation – Institute for Physics and Power Engineering named after A. I. Leypunsky.

1, Bondarenko Square, Obninsk, Kaluga Region, 249033, Russia, e-mail: ukraintsev@mail.ru

Receive on 20.04.2016

Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2640-2016-16-3-8-17*

Simulation model to calculate the indices of reliability of redundant radio electronic systems

Yury G. Zayko, *JSC "SRI "Argon", Moscow, Russia, e-mail: zayko@argon.ru*
Larella N. Iskandarova, *JSC "SRI "Argon", Moscow, Russia*
Alexander V. Trakhtomirov, *Research and production enterprise "Oberon", Kharkiv, Ukraine*

Yury G. Zayko

Larella N. Iskandarova

Alexander V. Trakhtomirov

Abstract. Purpose. *To define quantitative estimates of reliability indices of redundant radio electronic systems, the methods of reliability theory, analytical methods or simulation modeling are applied. This paper describes the application of these methods for systems of diverse complexity, as well as the complex of programs "Dialogue" developed for the calculation of reliability indices.* **Methods.** *The main obstacle for wide application of the simulation modeling method to obtain the reliability indices is high labor intensity of the creation of these models. The current software tools are not very useful. This problem can be solved using the developed complex of programs "Dialogue". This is achieved by creating the simulation models programs automatically on the basis of input initial data. The time of creation of a model is determined by the time of the input. Generating of the simulation models is based on the principle that if the system's behavior in case of failures is determined only by its scope structure, connections between components, failure criteria and redundancy switches, i.e. when the system's response to a failure of its component is uniquely defined in advance, then it will be possible to create models with equal structures for the systems with any configurations. It helps to create the basis for the initial text of the model, common for all simulation models of this type. Such basis forms a permanent part of the model, and the data which define the specifics of failure behavior of the concrete system, are set in form of insertions to the main text.* **Results.** *The complex of programs that is being described is intended to calculate the reliability indices of different technical systems using simulation models, and its consists of the program for the description of system to be simulated "Dialogue-OS", the program for the model synthesis "Dialogue-Synthesis" and special sub-programs combined to a separate library. The complex helps to create specialized simulation models of redundant systems which undergo statistical tests, and based on the obtained results the reliability indices are defined. Using the complex "Dialogue" we can obtain the following reliability indices: 1) probability of reliable operation for a predetermined period of time, 2) failure rate at the end of a predetermined period of time, 3) mean time to failure, 4) data to build a graph of dependence of the probability of reliable operation on time, 5) data to build a graph of dependence of the failure rate on time.* **Conclusion.** *This article provides the results of calculations carried out by theoretical methods, and by the method of simulation modeling that show a good coincidence (relative error is not more than 1%). The complex "Dialogue" makes it possible to calculate the reliability indices of redundant radio-electronic systems of any complexity with accuracy sufficient for practice. It should be noted that the complex "Dialogue" allows for creating the simulation model of reliability for redundant radio-electronic systems, whose reliability characteristics can not be calculated by theoretical methods due to their complexity.*

Keywords*: redundant systems, indices of reliability, reliability theory, simulation modeling, flowchart of the program.*

Citation format*: Zayko Y.G., Iskandarova L.N., Trakhtomirov A.V. Simulation model to calculate the indices of reliability of redundant radio-electronic systems // Dependability. 2016. No.3. P. 8-17. DOI: 10.21683/1729-2640-2016-16-3-8-17*

Theoretical methods of calculation

To improve reliability of radio electronic systems (RES) under the insufficient reliability of the constituent elements, the redundancy is used, i.e. the availability in the system of large number of the elements in comparison to the number necessary to perform the required function (equipment redundancy).

Among the reliability indices which determine RES reliable operation, the following indices are used more often in practice:

- probability of reliable operation (PRO) per the predetermined period of time t – R(t);
- mean time to failure – T_0;
- failure rate per the predetermined period of time t – $\lambda(t)$.

Analytical analysis of the system reliability under redundancy is usually executed with the following restrictive assumptions:

1. Failures of the redundant system elements are the simplest flow of random events.

2. All main and standby elements within one redundant system have equal reliability.

3. Switch devices are not taken into account (implemented in software or accepted as ideally reliable).

4. Redundant system is not performed during its functioning.

5. All elements of the system can exist only in one of two states: operable or non-operable (failure).

Reliability structure diagram (RSD) is a graphic image of operable state of the system. RSD shows a logic connection of operating elements (or units which combine them), necessary for the successful operation of the system. To define quantitative estimates of reliability indices of redundant radio-electronic systems, different methods are applicable. Depending on the RSD type one can use simple Boolean methods, theory of Markov processes and/or the fault tree analysis. Calculations could be performed using theoretical methods or the Monte-Carlo modeling [1] (method of simulation modeling).

The simplest variant is a sequential RSD, in which successful operation (no failure) of each of *m* elements of the diagram (Fig. 1) is required to assure successful functioning of the system. All elements of the diagram are in "on" position, the failure rate of the *i*-th element of the diagram shall be indicated as λ_i (i=1, …, m). RSD input is indicated by symbol I, output is indicated by symbol O.

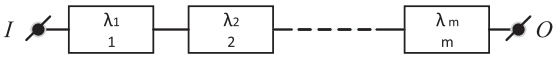


Fig. 1. Sequential RSD with m elements

With the assumptions accepted above the main quantitative characteristics of reliability of a sequential RSD shall be expressed by the following formulas [2]:

$$R_c(t) = e^{-t\sum_{i=1}^{m}\lambda_i}; \quad (1)$$

$$\lambda_c = \sum_{i=1}^{m}\lambda_i; \quad (2)$$

$$T_{0(c)} = \frac{1}{\sum_{i=1}^{m}\lambda_i}. \quad (3)$$

Generally, a parallel RSD may contain *m* of main elements, *l* of hot standby elements and *r* of cold standby elements. In a particular case when all main elements have equal failure rate λ_0, all *l* of hot standby elements have the same value of the failure rate λ_0, all r of cold standby elements are off and have the failure rate λ_p ($0 \le \lambda_p < \lambda_0$) up to the "on" moment, the diagram of this parallel redundancy is given in Fig. 2. Let us indicate the structure of this parallel system (m, *l*, r).

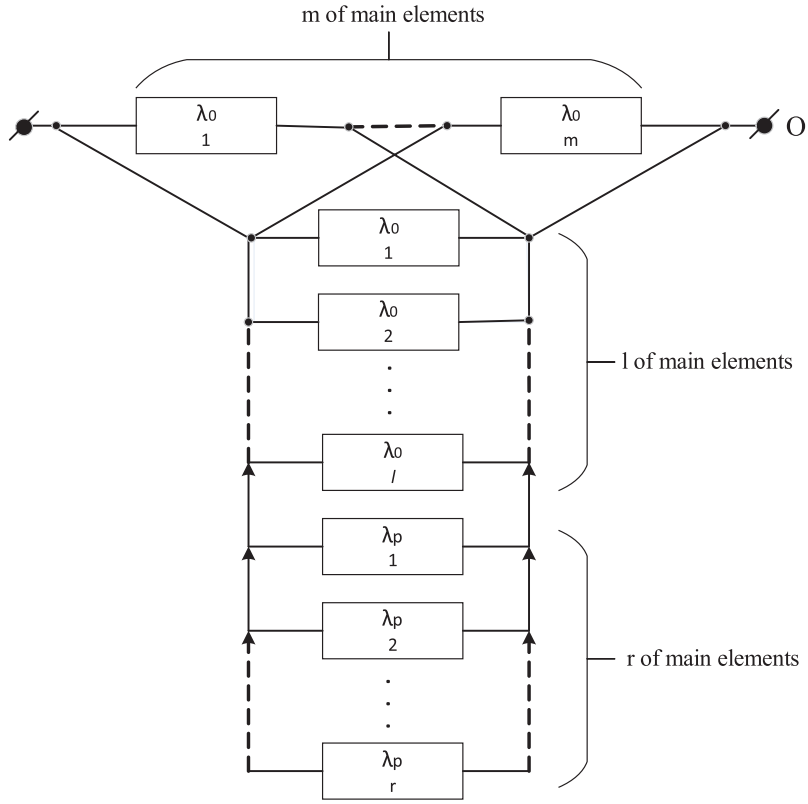


Fig. 2. Parallel RSD with the structure (m, *l*, r)

In a specific case for the structures with equal type of standby (m, *l*, 0) and (m, 0, r) we can obtain a common formula for PRO if the redundant system using the methods of homogeneous Markov processes:

$$R_c(t) = e^{-\lambda_0 t}\cdot\left[\frac{\prod_{j=0}^{n}(m+j\alpha)}{\alpha^n\cdot n!}\sum_{i=0}^{n}(-1)^i\cdot\frac{C_n^i}{m+i\alpha}\cdot e^{-(m-1+i\alpha)\lambda_0 t}\right], \quad (4)$$

where n is the number of standby elements (n = *l* or n= r);
m is the number of main elements (m ≥ 1);

$$\alpha = \frac{\lambda_p}{\lambda_0};$$

$n! = \prod_{k=1}^{n} k$ is a factorial of n;

$C_n^i = \frac{n!}{i!(n-i)!}$ is the number of combinations of n by i.

Mean time to failure is:

$$T_{0(c)} = \int_0^\infty R_c(t)dt = \frac{1}{\lambda_0}\sum_{i=0}^{n}\frac{1}{m+i\alpha}. \quad (5)$$

Rate of failure of the redundant system can be calculated by formula:

$$\lambda_c(t) = -\frac{R'_c(t)}{R_c(t)} = \lambda_0 \frac{\sum_{i=0}^{n}(-1)^i C_n^i e^{-(m+i\alpha)\lambda_0 t}}{\sum_{i=0}^{n}(-1)^i \frac{C_n^i}{m+i\alpha} e^{-(m+i\alpha)\lambda_0 t}}. \quad (6)$$

In a general case for systems with structure (m, *l*, r), which includes hot and cold standby elements, the expression for PRO of the redundant system $R_s(t)$ will depend on the mode of switching cold standby elements to "on" state. In particular, for systems, when cold standby elements turn to "on" state only after the failure of *l* modules from the main scope or from the hot standby, i.e. when the system acquires the structure (m, 0, r), the expression for $R_s(t)$ has rather complex structure [3]. In the simplest case for the redundant system with the structure (1, *l*, 1) the expression for $R_s(t)$ has the following form

$$R_c(t) = \left[1-(1-e^{-\lambda_0 t})^{l+1}\right] + (l+1)\cdot\lambda_0 \cdot e^{-\lambda_0 t}\cdot\sum_{i=0}^{l} C_l^i (-1)^i \times \times \frac{\left[1-e^{-(i+\alpha)\lambda_0 t}\right]}{\lambda_0(i+\alpha)}. \quad (7)$$

Majority redundancy "m of n" often used in practice, is a particular case of the system shown in Fig. 2, if the structure will have the form (m, *l*, 0) (in this case n = m + *l*) or (m, 0, r) (in this case n = m + r).

In practice sequential and parallel diagrams of redundancy are often used. Fig. 3 shows the diagram which consists of a non-redundant element 1, the first parallel redundant group with the structure (1, 2, 0), which consists of elements 2, 3, 4 and the second parallel redundant group with the structure (1, 1, 0) which consists of elements 5 and 6.

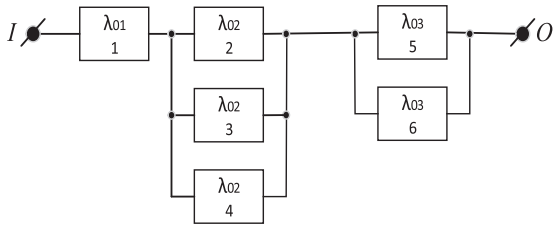


Fig. 3. RSD with sequential and parallel connection of the elements

The example of a more complex diagram with sequential and parallel redundancy is shown in Fig. 4 [1].

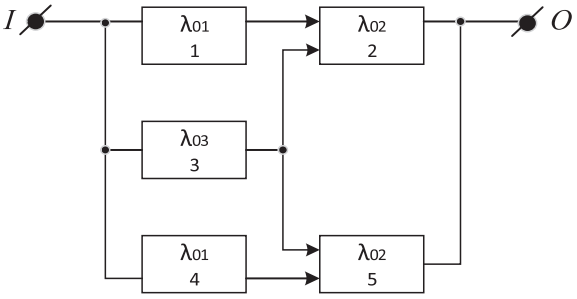


Fig. 4. RSD with sequential and parallel connection of the elements

The figure shows the system of fuel supply to the engines of a light aircraft. Element 1 is a fuel supplier for the engine of the port (element 2), element 4 is a fuel suppler for the engine of the starboard (element 5), and element 3 is a standby supplier for both engines. Failure of this system occurs in case both engines are failed

On the diagram of Fig. 4 elements 1, 3, 4 are control elements, and elements 2, 5 are controlled elements. The connections of control elements with controlled elements are indicated by an arrow.

A more complex diagram with control and controlled elements is shown in Fig. 5 [4].

The diagram consists of control elements C_1, C_2, C_3 and operating elements combined in three lines with sequential and parallel redundancy. Each control element controls its line of operating elements, and a failure of the control element will put the whole line out of operation. Such system of redundancy is used in the unit of optical sensors within the unit of thunderstorm activity registration used within the scope of a spacecraft.

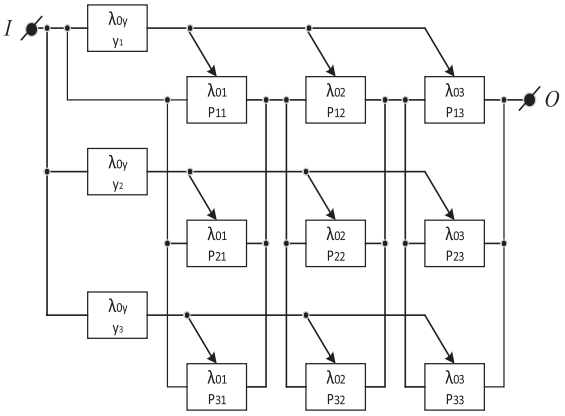


Fig. 5. RSD with control and operating (controlled) redundancy elements

In practice the diagrams with multilevel redundancy can be used (Fig. 6).

On the diagram shown in Fig. 6, at the first level of redundancy a majority diagram "2 of 3" with the structure

(2, 1, 0) is used, at the second level a parallel diagram with cold standby is used.

The analysis shows that for the simplest redundancy diagrams (Fig. 2) there are the formulas to calculate the indices R(t), T_0, λ(t) [1,2]. For the more complex diagrams (Fig. 4, 5) using a fault tree analysis, we can obtain the formulas to calculate the indices R(t) [1, 4], but it is difficult to calculate the indices T_0, λ(t), because such diagrams lose the property of the simplest flow of failures.

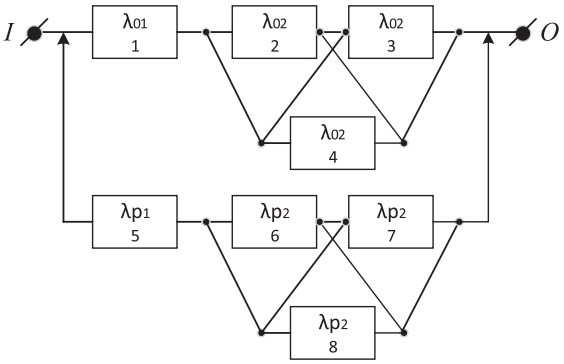


Fig. 6. RSD with two-level redundancy

For the diagram shown in Fig. 6, it is difficult to calculate even the index R(t), as for the diagram of the second level with cold standby it is necessary to know the value of index λ(t) for each line to calculate the index R(t) using the known formulas. Due to the fact that each line contains the redundant diagram of the first level, the flow of failures in the lines is not the simplest any more, and rate of failures of each line can not be calculated using the known formulas.

An alternative to theoretical methods of calculation of reliability indices if the method of simulation modeling which makes it possible to simulate real functioning of the redundant system of any complexity. Below is the description of the complex of programs for simulation modeling used to calculate the reliability indices of redundant systems.

The complex of programs "Dialogue"

The main obstruction of wide application of the simulation modeling method to obtain the reliability indices is a high labor intensity of the creation of these models. The current software tools are not very useful. This problem can be solved using the developed complex of programs "Dialogue". This is achieved by creating the simulation models programs automatically on the basis of input initial data. The time of creation of a model is determined by the time of the input.

Generating of the simulation models is based on the principle that if the system's behavior in case of failures is determined only by its scope structure, connections between components, failure criteria and standby switches, i.e. when the system's response to a failure of its component is uniquely defined in advance, then it will be possible to create models with equal structures for the systems with any configurations..

It helps to create the basis for the initial text of the model, common for all simulation models of this type. Such basis forms a permanent part of the model, and the data which define the specifics of failure behavior of the concrete system, are set in form of insertions to the main text.

Initial data for the synthesis of models are the following information:

- scope of the system and connections between its components;
- failure criteria;
- terms of standby switches;
- rates of failures of the system elements in different modes.

This data is sufficient to reflect the system's failure behavior in the model.

Hereinafter in the text the following terms will be used:

- system is the object of modeling, consisting of elements and units, in relation to which the reliability indices are being determined;
- element is the smallest indivisible part of the system, in which a failure occurs;
- unit is a conditional combination of elements and units;
- system components are elements and units composing the system's scope;
- main scope of the system are the elements and units excluding the switched standby and control components;
- switched standby are the components switched from the standby under the occurrence of special conditions;
- failure criterion – is the state of the component when the failure occurs;
- term of standby switch is the term when the failed component is substituted with a component from standby.

Before starting the program "Dialogue" it is necessary to prepare the part of initial data describing the system scope and connection between its components.

This preparation is based on the assignment of conditional units in the system and giving names to all units and elements.

The following types of units are used for this purpose:

- sequential (SEQ) (Fig.1);
- parallel (PAR) (Fig. 2);
- majority (MAJ), which is a particular case of a parallel unit;
- controlled (CON) (Fig. 5), consisting of control elements (C1, C2, C3) and objects of control (OC) including all operating components (Op_{11},…,Op_{33});
- standby unit (STB) (Fig.2), which is used to assign the cold standby components with any value of m, and to assign the hot standby components with m > 1.

Below is the description of the program "Dialogue", as well as the principles of operation of the simulation model obtained with the help of this program. The program is written in the REXX language using the interpreter Regina 3.6. The complex also includes system files and special sub-programs combined into a library, which are used under translation.

At the first level of the program operation an operator enters initial data describing the system and mode of tests. At the second level, as the result of the processing of the data entered, the synthesis is performed in relation to the model which is the initial text of the computer program Fortran 77, using certain SMPL sub-programs [5].

A flow-chart of the program "Dialogue" is shown in Fig. 7, with the main stages of the program operation.

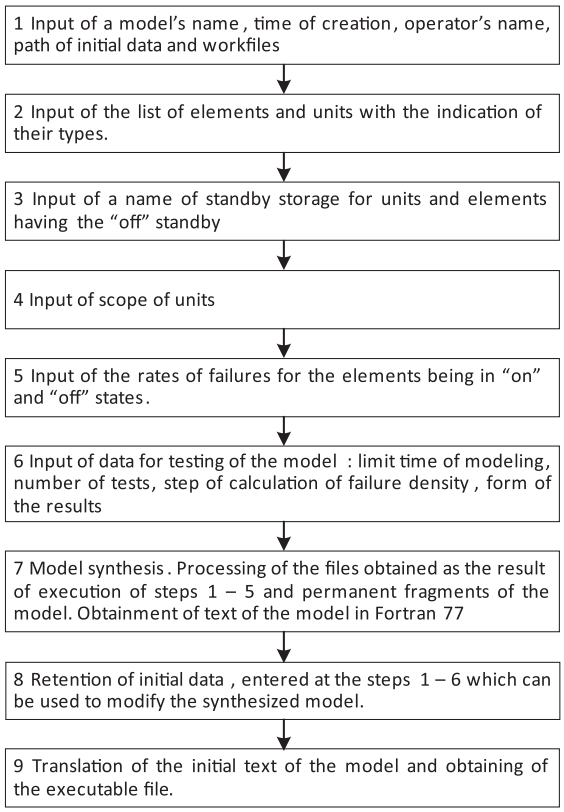


Fig. 7. Flow-chart of the program "Dialogue"

1. Input of the name of the model, time of creation, operator's name and a path of workfiles. The model's name shall be the name of the file with a model entry.

2. Input of the system scope: list of elements and conditional units with the indication of their types.

3. If a unit or an element has an "off" standby, the name of unit where they are stored, is entered.

4. Input of the scope of conditional units is made, including the unit of standby storage.

5. Input of the rates of failures of the elements for "on" and "off" states.

6. Input of data for testing of the model: number of tests, duration of modeling, calculation of failure density. Thus data can be modified on the start of the model's program.

7. Model synthesis. The input data are processed, forming the fragments of text of the model. Permanent parts which form the basis of the model are combined with the formed fragments. The result of combination of the program text in Fortran 77 and operating files.

8. Retention of initial data. To reduce the time of entry of initial data, if it is necessary to test several types of systems, the data entered could be retained, with the possibility to modify them partially and generate a new model.

9. Translation of the formed text of the program and obtaining of the executable file. To start the translation, the installed translator providing for Fortran 77 is required. The choice of this language is based on the fact that after the translation an executable code if formed. This code has a low redundancy in comparison to other languages. Translation and testing of the model can be carried out on another computer.

All obtained models have equal algorithm of operation, they differ only in terms of the parts which describe the system structure. That is why we shall use a generic term "model" for them below in the text.

The obtained models have the following characteristics**:**

– number of components in the system – not more than 100;

– law of distribution of the event to generate – exponential;

– one standby store may serve several components;

– a component can be served only by one standby;

– a standby of the component can be a component of another type, i.e. a standby of the element can be a unit, and vice versa;

– there is no standby for the components which are on standby;

– criterion of standby switch is a failure of the component.

The program "Dialogue" can set the following reliability indices as the results to be obtained:

– value of the probability of reliable operation per the predetermined period of time t – R(t);

– graph of dependence R(t) for the predetermined time interval from $t_{1(R)}$ to $t_{2(R)}$;

– value of mean time to failure – T_0;

– value of the system failure rate per the predetermined period of time t – $\lambda(t)$;

– graph of dependence $\lambda(t)$ for the predetermined time interval from $t_{1(\lambda)}$ to $t_{2(\lambda)}$ (failure density).

Principle of operation of synthesizable models is as follows:

1. On start of the program the time of failure is stochastically generated for each element. If this time is shorter than

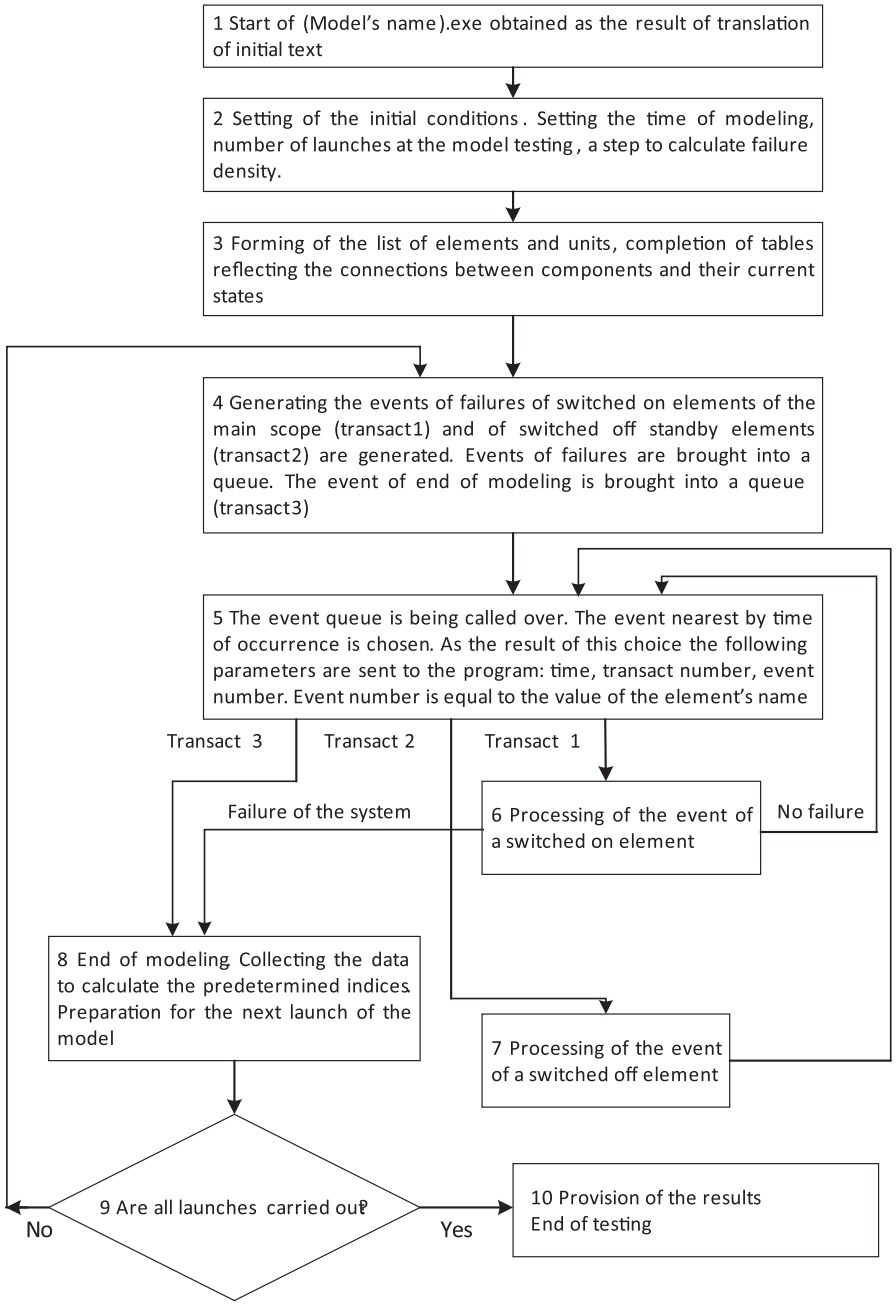


Fig. 8. Flowchart of the program of a simulation model

the predetermined time for the system to end its operation, an event is planned – a failure of the element. As the parameter of the event, the time of occurrence, as well as the name of the respective element are set. Besides there is generation of the event when the model ends its operation with the system ending its operation.

2. Events are brought into a queue and sorted by time.

3. A queue is being called over, and then the event with the shortest time is selected.

4. The selected event (failure of the element) is processed: the system components are being called over, it is necessary to determine whether this failure head to the failure of other components, or to the failure of the system, whether it is possible to switch standby.

5. If a limit time is achieved, or there is a system failure, the model's operation is stopped.

6. If a standby is switched instead of the failed component, the standby is turned on, the events which were generated

```
              MODEL RIS2-1
          RESULTS OF MODELING
      Time of modeling=  1000
       Number of tests=  200000
    Number of failures=  50529
     Number of success=  149471
   Probability of reliable
             operation=.7473550
  Mean time to failure= WAS NOT
                        CALCULATED
                  step=   50
failure rate lambda(t)=.00058785
```

Fig. 9. Results of model testing

```
            MODEL RIS2-1
  MEAN TIME TO FAIULRE WAS CALCULATED
       Time of modeling =  300000
        Number of tests =  200000
      Number of success =       0
    Mean time to failure =  1834,26
```

Fig.10. Results of testing of the model to obtain mean time to failure

DATA OF THE FAILURE RATE GRAPH lambda(t)

step	time	lambda(t)
1	25	0.279248E-05
2	75	0.177235E-04
3	125	0.357058E-04
4	175	0.651742E-04
5	225	0.105678E-03
6	275	0.140588E-03
7	325	0.174245E-03
8	375	0.204881E-03
9	425	0.241084E-03
10	475	0.279565E-03
11	525	0.318051E-03
12	575	0.355583E-03
13	625	0.384560E-03
14	675	0.411543E-03
15	725	0.441098E-03
16	775	0.482188E-03
17	825	0.510980E-03
18	875	0.536080E-03
19	925	0.549788E-03
20	975	0.572966E-03

Fig.11. Data of the failure rate graph lambda(t)

for it earlier are rejected, and new failures are generated for the "on" state.

7. Model is launched for the predetermined number of times, after that the calculation of reliability indices is carried out.

It should be considered that the following split of the events into groups (transacts) is used in the model, in accordance with the type and processing algorithm:

– failures of switched on elements (transact1);

– failures of switched off standby elements (transact2);

DATA OF THE GRAPH OF PROBABILITY OF RELIABLE OPERATION R(t)

step	time	R(t)
1	50	0,999710E+00
2	100	0,999125E+00
3	150	0,997345E+00
4	200	0,994370E+00
5	250	0,989405E+00
6	300	0,981660E+00
7	350	0,973620E+00
8	400	0,963880E+00
9	450	0,951950E+00
10	500	0,939040E+00
11	550	0,924295E+00
12	600	0,907600E+00
13	650	0,890265E+00
14	700	0,872485E+00
15	750	0,853265E+00
16	800	0,833265E+00
17	850	0,811605E+00
18	900	0,790305E+00
19	950	0,768880E+00
20	1000	0,747355E+00

Fig. 12. Data of the graph of probability of reliable operation R(t)

– completion of operation upon achievement of the time of end of modeling (transact3).

The result of the program "Dialogue" is the file (model Name).for with the model written in Fortran. After the translation of this file, an executable file if formed – (model Name).exe. Then it is started, statistical testing is performed.

A flowchart of operation of such models is shown in Fig. 8.

The operation is performed as follows:

1. Start of the executable file obtained after translation.

2. Setting of the initial conditions. It is necessary to set the time of modeling, number of launches at the testing of the model, a step to calculate failure density. This data can be modified under the program execution, and the calculation of failure density could be excluded.

3. The list of elements and conditional units is formed.

The events of failures of switched on elements (transact1) and of switched off standby elements (transact2) are generated. Events of failures are brought into a queue and sorted by the predetermined time of occurrence. The event of end of modeling is brought into a queue (transact3).

The event queue is being called over. The event nearest by time of occurrence is chosen. Depending on the transact number there may be the processing of failures of switched on main elements, the processing of failures of switched off standby elements or the end of modeling.

Processing of the failure of the main components. It is necessary to check whether the failure of this element lead to the system failure. As the element may be present in several conditional units simultaneously, it is neces-

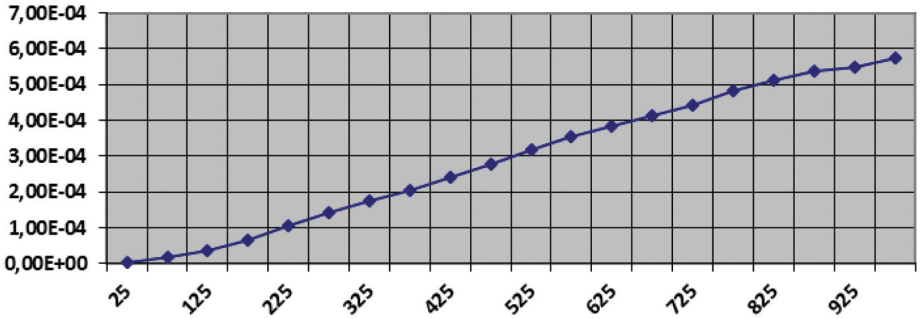


Fig. 13 Graph λ(t)

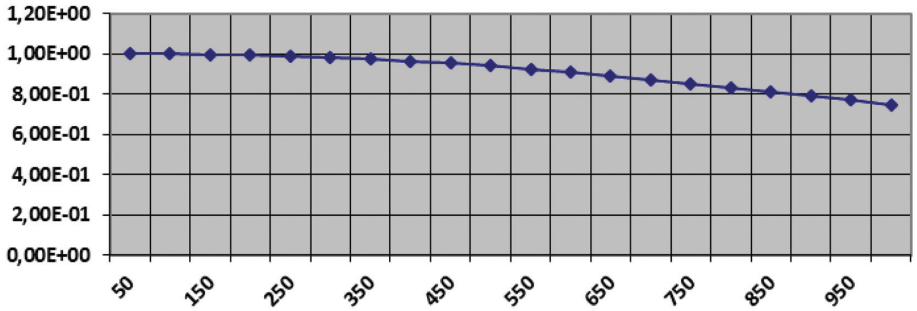


Fig.14 Graph R(t)

Table 1 – Comparative evaluation of the calculation of reliability indices of redundant systems

Examples for calculation			Comparative evaluation of the calculation performed					
			Indices	Calculation method				Relative error, %
				Theoretical		Modeling		
No.	Description of the system	System characteristics		Results	Formulas	Results	The number of tests, step	
1	2	3	4	5	6	7	8	9
1	Fig. 1	m = 3 $\lambda_1 = 40 \cdot 10^{-6}$ $\lambda_2 = 4 \cdot 10^{-6}$ $\lambda_3 = 0{,}4 \cdot 10^{-6}$ t = 8760 h	$R_c(t)$ $T_{0(c)}$ λ_c	0,6777 22522 $44{,}4 \cdot 10^{-6}$	(1) (2) (3)	0,6782 22532 $44{,}22 \cdot 10^{-6}$	200000 100	0,073 0,044 0,405
2	Fig. 2 Structure (1, 2, 0)	$\lambda_0 = 1000 \cdot 10^{-6}$ t = 1000 h	$R_c(t)$ $T_{0(c)}$ $\lambda_c(t)$	0,7474 1833 $590 \cdot 10^{-6}$	(4) (5) (6)	0,7473 1834 $587{,}85 \cdot 10^{-6}$	200000 50	0,013 0,054 0,364
3	Fig. 2 Structure (1, 0, 2)	$\lambda_0 = 1000 \cdot 10^{-6}$ $\lambda_p = 100 \cdot 10^{-6}$ t = 1000 h	$R_c(t)$ $T_{0(c)}$ $\lambda_c(t)$	0,9012 2742 $244 \cdot 10^{-6}$	(4) (5) (6)	0,9021 2745 $243{,}65 \cdot 10^{-6}$	200000 100	0,100 0,109 0,143
4	Fig. 3	$\lambda_{01} = 10 \cdot 10^{-6}$ $\lambda_{02} = 40 \cdot 10^{-6}$ $\lambda_{03} = 100 \cdot 10^{-6}$ t = 8760 h	$R_c(t)$ $T_{0(c)}$ $\lambda_c(t)$	0,5885	(4)	0,5879 12418 $88{,}96 \cdot 10^{-6}$	200000 100	0,102
5	Fig. 4	$\lambda_{01} = 10 \cdot 10^{-6}$ $\lambda_{02} = 100 \cdot 10^{-6}$ $\lambda_{03} = 20 \cdot 10^{-6}$ t = 1000 h	$R_c(t)$ $T_{0(c)}$ $\lambda_c(t)$	0,9909	(8) [1]	0,9892 14535 $21{,}59 \cdot 10^{-6}$	200000 100	0,171

Table 1. Continuation

Examples for calculation			Comparative evaluation of the calculation performed					
			Indices	Calculation method				Relative error, %
				Theoretical		Modeling		
No.	Description of the system	System characteristics		Results	Formulas	Results	The number of tests, step	
1	2	3	4	5	6	7	8	9
6	Fig. 5	$\lambda_{0У} = 10 \cdot 10^{-6}$ $\lambda_{01} = 4 \cdot 10^{-6}$ $\lambda_{02} = 1 \cdot 10^{-6}$ $\lambda_{03} = 0{,}1 \cdot 10^{-6}$ t = 87600 h	$R_c(t)$ $T_{0(c)}$ $\lambda_c(t)$	0,6176	(3) [4]	0,6184 123332 $10{,}30 \cdot 10^{-6}$	200000 100	0,130
7	Fig. 6	$\lambda_{01} = 10 \cdot 10^{-6}$ $\lambda_{02} = 40 \cdot 10^{-6}$ $\lambda_{p5} = 1 \cdot 10^{-6}$ $\lambda_{p6} = 4 \cdot 10^{-6}$ t = 8760 h	$R_c(t)$ $T_{0(c)}$ $\lambda_c(t)$			0,9699 34217 $9{,}26 \cdot 10^{-6}$	200000 200	

sary to check what has the failure lead to in these units. The failure of each unit may lead to the failure of other units, etc. till the last unit is achieved. If the failed unit or element has a standby, it is substituted by a standby component. If there is a failure of the system, a failure counter is increased by one and the modeling is stopped. After the failure is processed, the next event is selected from the queue.

Failure of the switched off standby element is processed in the same way as it is described in clause 6, except for the possibility of standby switch and absence of failure.

The modeling ends for two reasons: achievement of limit time under no failure, or the failure of the system.

If the predetermined number of model launches is not achieved, there is a restart in unit 4. Upon each completion of operation the data used to obtain the results of modeling is collected.

If the predetermined number of model launches is achieved, the results are provided.

As the example of operation of the program "Dialogue", below are the results of RSD modeling shown in Fig.2 with the structure (1,2,0).

Example of the results of the model testing is shown in Fig. 9.

To obtain a reliable value of mean time to failure the model testing is carried out with time of modeling that assures the probability of reliable operation close to 0. Normally it is sufficient to set the time equal to $(1/\lambda) \times 20$, where λ is the least value of λ indices for the elements within RSD.

Example of the results of such calculation is shown in Fig.10

Results of testing in form of tables are shown in Figures 11-12.

Graphs of change of the failure rate $\lambda(t)$ and of the probability of reliable operation R(t) are shown in Figures 13-14. The graphы were constructed using the program not belonging to the complex "Dialogue".

Estimation of the obtained results

To certify the results of operation of the complex "Dialogue" a comparative evaluation of the calculation of reliability indices of redundant systems was performed. The calculations were performed based on the theoretical methods using the known formulas, and based on the operation of a simulation model. The calculation results are listed in Table 1.

According to the analysis of the calculation results listed in Table 1, relative error of the results is not more than 1%.

Moreover, the program "Dialogue" makes it possible to calculate the reliability indices of redundant systems in case there are no analytic formulas.

Thus the program "Dialogue" can be used to calculate the reliability indices of redundant radio-electronic systems.

References

1. GOST 51901-14-2007. Risk management. Reliability structure diagram and Boolean methods. M. Standartinform, 2008.

2. Polovko A.M. Basis of reliability theory. M. Science, 1964.

3. Zayko Y.G., Smirnov M.B. Estimating the reliability of a system with combined redundancy. Dependability, No.4 (11), 2004, p. 40-45.

4. Zayko Y.G., Iskandarova L.N. Calculation of reliable operation of redundant systems with control modules. Radio manufacturing, 2013, Issue 4, p. 50-60.

5. Automation of design of computing systems. Languages of modeling and databases. Edited by M. Brayer. Chapter 1 M. McDougal Modeling of the system level. M. Mir, 1979.

About the authors

Yury G. Zayko, PhD engineering, Associate Professor, Senior Researcher, Head of sector in в JSC "SRI "Argon".

Address: 125, Varshavskoye Highway, Moscow, Russia, tel. +7 (495) 319-68-89, tel. +7 -917-576-43-00.

Larella N. Iskandarova, Senior Programmer in JSC "SRI "Argon".

Address: 125, Varshavskoye Highway, Moscow, Russia, tel. +7 (495) 319-68-89, tel. +7 -926-624-64-27.

Alexander V. Trakhtomirov, Director of Research and production enterprise "Oberon", Address: 4, Garshina Str., Kharkiv, Ukraine, tel. +380 57 7004476, +380 68 6088611.

Receive on 07.10.2015

Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2640-2016-16-3-18-22*

Model for forecasting the reliability of nanosized field-effect transistors considering possible influence of cosmic rays

Artyom N. Volkov, *LLC NPO PKRV (Research and production association Software complexes of real time), Russia, Moscow, email: artem.n.volkov@yandex.ru*

Artyom N. Volkov

Abstract. Purpose. *Within the framework of this work the following purposes were set: study of physical mechanisms of degradation of performance of nanosized field-effect transistors caused by interruptions of Si-H; study of possible influence of cosmic rays on the reliability of nanosized field-effect transistors; development of a model to forecast the reliability of nanosized field-effect transistors considering possible influence of cosmic rays. To achieve the above listed purposes it was necessary to analyze: modern models used to forecast the reliability of nanosized field-effect transistors; data of the scope and intensity of cosmic-ray flux depending on energy.* **Results and Conclusion.** *According to the results of work, the most relevant physical model used to forecast reliability is the Bravais model which considers the following mechanisms of degradation of performance of nanosized field-effect transistors: - single Vibration Excitation – SVE, when the interruption of Si-H is initiated by one carrier with enough energy; – electron – Electron Scattering – EES, when the interruption is initiated by the carrier which received some energy from another carrier as the result of collision ionization, and thereafter having enough energy to interrupt the connection; – multi Vibration Excitation – MVE, when the Si-H interruption is initiated by a sequential bombing of connection by the carriers having energy not enough to interrupt the connection. It has been shown that cosmic-ray protons having high initial energy can penetrate through the structure of a field-effect transistor, losing a part of their initial energy by ionization losses, and achieve a Si/SiO2 boundary. When achieving the boundary protons may have energy sufficient for the initiation of dissociation of Si-H connections by two mechanisms: single Vibration Excitation of Si-H affected by a proton – SVEp is when a single proton having enough energy for interruption runs into a hydrogen atom, and initiates the Si-H dissociation; collision ionization by analogy with the electron – electron scattering described in the Bravais model, in this case there may be the Proton-Electron Scattering – PES. The Bravais model served as the basis for the development of the model to forecast the reliability of nanosized field-effect transistors that considers possible influence of cosmic rays, and helps to give a more accurate forecast of reliability of electronic devices based on nanosized field-effect transistors. This work reflects modern ideas of forecasting the reliability of nanosized field-effect transistors, describing main physical mechanisms of degradation of performance of nanosized field-effect transistors. This article shows that the reliability forecasting models developed for field-effect transistors with a long channel are not suited to modern nanosized devices due to differences in degradation mechanisms. Within the frameworks of this work it was shown that there is a probability of cosmic rays influence on degradation. As the result a model was developed to forecast the reliability of nanosized filed-effect transistors that shall consider such influence.*

Keywords: *reliability, degradation of performance, physical mechanisms of degradation, nanosized field-effect transistors, cosmic rays, model to forecast the reliability of nanosized field-effect transistors.*

Citation format: *Volkov A.N. The model to forecast reliability of nanosized field-effect transistors, considering possible influence of cosmic rays // Dependability. 2016. No.3. P. 18-22. DOI: 10.21683/1729-2640-2016-16-3-18-22*

Introduction

Modern technologies that facilitate the reduction of physical sizes and improve performance of field-effect transistors have lead to the creation of nanosized electronic devices. This hopping from the micron size devices that had been the subject of studies for several decades, to nanosized devices, caused the need for new studies in the field of physical mechanisms of degradation and failures of modern electronic devices based on nanosized field-effect transistors. Models used to forecast reliability and degradation of performance, developed and successfully applied in micron sized electronic devices, can not estimate the reliability of modern nanosized devices in a full scope due to the fact that the latter have different physical mechanisms of degradation which is the reason for a parametric failure and loss in reliability.

Application of modern nanosized field-effect transistors in the space related equipment requires considering possible influence of cosmic rays when forecasting the reliability, as this influence becomes more significant in electronic devices based on field-effect transistors.

Up to date the current physical models which describe the mechanisms of degradation of performance of nanosized field-effect transistors and which are used to forecast the reliability, do not consider possible cosmic ray influence on the degradation of performance, and cannot estimate the reliability of space related electronic devices in a full scope. Thus, the development of the model that will be used to forecast the reliability and degradation of performance of nanosized field-effect transistors considering possible influence of cosmic rays is a relevant objective.

Within the framework of this work we set a task to develop the model to forecast the reliability and degradation of performance of nanosized field-effect transistors considering possible influence of cosmic rays.

Physical models to forecast reliability

Up to date there are many empirical and semi-empirical models to forecast the reliability of metal semiconductor oxide transistors (MSOT), describing the degradation of performance caused by the Si-H interruption at the Si/SiO_2 boundary [1, 2]. Most of these models are based on the concept of "lucky electron model". This concept describes the mechanism of Si-H interruption in the transistors with long channel and electronic devices based on them. These devices are defined by high power supply voltage and, as a consequence, by high value of density of lateral electric field in the channel. This electric field is capable of boosting the electrons in the channel making them "hot", i.e. making them having enough energy to initiate the dissociation of Si-H connection. Most electrons boosted by electric field in the channel of a field-effect transistor continue the movement towards the electron sink, but some of them ("lucky") diverge form the movement trajectory and reach the surface of Si/SiO_2 boundary where they initiate the Si-H interruption, or penetrate into the oxide forming surface or three-dimensional traps. This very mechanism formed the basis of the concept of "lucky" electrons and, therefore of the models to forecast the reliability, based on this concept.

In modern nanosized field-effect transistors having lower power supply voltage and, as a consequence, lower value of density of lateral electric field in the channel, based on the concept of "lucky" electrons, the degradation of performance caused by Si-H interruption, should be minimized or there should be no degradation at all. However, despite the fact that this type of degradation is still observed in modern nanosized field-effect transistors and respective electronic devices, being even a more pressing problem in comparison to micron sized devices, which indicates the availability of different physical mechanisms in nanosized field-effect transistors, causing the Si-H interruption and therefore, the degradation of performance [3].

Thus, the concept of "lucky" electrons and the respective reliability forecasting model are not suited to forecast the reliability and describe the degradation of performance of modern nanosized field-effect transistors and the respective electronic devices. Therefore, we need new models that will consider the special aspects of nanosized field-effect transistors and physical processes behind the degradation of performance caused by Si-H interruption.

In paper [3] the author gives the review of modern physical models used to forecast the reliability and degradation of performance caused by Si-H interruption, for nanosized field-effect transistors. These models describe those new physical mechanisms peculiar for nanosized field-effect transistors that were present in the concept of "lucky" electrons:

– connection may be interrupted under the influence of a single carrier with high energy;

– dissociation of the connection may occur as the result of sequential bombing of the connection by several carriers with less energy;

– in nanosized field-effect transistors the electron – electron scattering is dominant in the process of Si-H interruption;

– in nanosized field-effect transistors, starting from a topology rate of 180 nm and lower, a steering force of degradation is the energy contribution by carriers in the channel, not the electric field.

The most successful physical model is the Bravais model, it does not require solving Boltzmann kinetic equation to define the function of energy distribution of electrons, besides, it combines the approaches developed in other models, and means that the degradation caused by Si-H interruption, may develop by three independent mechanisms:

– Single Vibration Excitation – SVE, when the interruption of Si-H is initiated by one carrier with enough energy. This mechanism is described well by the model of "lucky" electrons;

– Electron – Electron Scattering – EES, when the interruption is initiated by the carrier which received some energy from another carrier as the result of collision ionization, and thereafter having enough energy to interrupt the connection. This mechanism is described well within the energy controlled paradigm [3];

– Multi Vibration Excitation – MVE, when the Si-H interruption is initiated by a sequential bombing of connection by the carriers having energy not enough to interrupt the connection. This mechanism was proposed and described well by the Hess model based on a simplified model of harmonic oscillator [3].

By combining these three mechanisms of Si-H interruption, the Bravais model to forecast the reliability and degradation of performance is described by the following equation:

$$R_{it} = \frac{1}{\tau} = C_1 \cdot \left(\frac{I_{ds}}{W}\right)^{a_1} \cdot \left(\frac{I_{bs}}{I_{ds}}\right)^{m} + C_2 \cdot \left(\frac{I_{ds}}{W}\right)^{a_2} \cdot \left(\frac{I_{bs}}{I_{ds}}\right)^{m} + C_3 \cdot V_{ds}^{a_3/2} \cdot \left(\frac{I_{ds}}{W}\right) \cdot \exp\left(\frac{-E_{emi}}{k_B T}\right) \quad (1)$$

where, R_{it} if the rate of occurrence of surface states as the result of Si-H interruption; τ is a lifetime (time to a parametric or critical failure); C_1 (SVE), C_2 (EES) C_3 (MVE), a_1, a_2, a_3, m are empirical parameters obtained from the results of accelerated tests; E_{emi} = 0.26 eV is the energy of hydrogen emission from the last binding energy level (defined in the Bravais model [3]); k_B is the Boltzmann's constant; T is temperature; I_{ds} is a drain current; I_{bs} a base current; V_{ds} is a voltage on drain; W is a width of channel;

Despite the fact that this model is good in describing the mechanisms of occurrence of surface states from the physical point of view, and though it has a great advantage over the obsolete model of "lucky" electrons which is still applied as an industrial one, the Bravais model can be applied to describe the degradation of performance not only in the devices not exposed to external influence, that may affect the occurrence of surface states at the boundary of Si/SiO_2. This external influence may be ionizing radiation of cosmic rays that may affect the reliability and degradation of performance of modern nanosized field-effect transistors used in the space related equipment.

Modelling of cosmic ray influence on the reliability of MSOT

According to papers [4, 5] cosmic rays consist of nuclei of high-energy protons (10^8 – 10^{20} eV) for more than 80 %, and the intensity of cosmic-ray flux, depending on the energy of particles, is described by formula:

$$I_N(E) \approx 1.8 \times 10^4 \left(E/1\,GeV\right)^{-\alpha} \quad (2)$$

where $\alpha\,(\equiv \gamma + 1) = 2,7$; E is the energy of particles.

We can assume that the protons of cosmic rays, which have high initial energy, can penetrate through the structure of a field-effect transistor, losing a part of their initial energy by ionization losses, and achieve a Si/SiO2 boundary. When achieving the boundary protons may have energy sufficient for the initiation of dissociation of Si-H connections by two mechanisms:

– Single Vibration Excitation of Si-H affected by a proton – SVEp is when a single proton having enough energy for interruption runs into a hydrogen atom, and initiates the Si-H dissociation;

– collision ionization by analogy with the electron – electron scattering described in the Braviax (Bravais) model, in this case there may be the Proton-Electron Scattering – PES. The proton having not enough energy to interrupt Si-H connection, pass the necessary amount of energy to the electron of the channel, which will be able to initiate the process of Si-H dissociation.

According to works [3, 6] the rate of occurrence of surface states R_{it}, as the inverse function from the time to the occurrence of a parametric failure $R_{it} = \frac{1}{\tau}$, which is the basis of the Bravais model, is proportional to the integral of product of two functions:

$$R_{it} \propto \int f(E) \cdot S(E) dE \quad (3)$$

where, $f(E)$ is the energy distribution function, $S(E)$ is the reaction cross section.

Thus, in case of calculation of the rate of occurrence of surface states due to the influence of cosmic-ray protons, it is necessary to define the function of energy distribution of protons and cross section of the reaction of interaction of cosmic-ray protons with hydrogen atoms in oxide and with electrons of the channel.

The intensity of cosmic-ray flux, or a differential flux, nothing else but the function of distribution of cosmic-ray protons by energy, described by equation (2). Thus, it is necessary to define the reaction cross section.

According to [7] the reaction cross section can be defined as follows:

$$S(E) = \frac{dn}{jN} \quad (4)$$

where, dn is the number of predefined reactions, j is the density of flux of particles bumping into the target, N is the number of target particles.

According to [8] the intensity of cosmic rays is defined as follows:

$$I = D \cdot E \quad (5)$$

where, I is the intensity of flux, D is the density of flux, E is the energy.

Thus, the density of the flux of cosmic-ray protons required for the calculation of cross section, can be defined by dividing equation (2), that describes the intensity of the cosmic-ray flux, by the energy:

$$j = I_N(E)/E \approx \frac{1,8 \cdot 10^4 \left(E\right)^{-2,7}}{E} \approx 1,8 \cdot 10^4 \left(E\right)^{-3,7} \quad (6)$$

Denoting the cross section of the reaction of interaction of cosmic-ray protons with hydrogen atoms in oxide by function $S_{SVEp}(E)$, accepting that the number of hydrogen atoms in oxide is found as, n is the concentration of hydrogen atoms in oxide (in m^{-3}), L, W, T_{ox} are the length of the channel, width of the channel, thickness of oxide, respectively, and the number of predetermined reactions dn is defined as the number of occurred surface states $dN_{it}(E)$, we shall obtain the following formula to calculate the cross section of the reaction of interaction of cosmic-ray protons with hydrogen atoms in oxide:

$$S_{SVEp}(E) = \frac{dN_{it}(E)}{1,8 \cdot 10^4 \cdot \left(E\right)^{-3,7} \cdot n \cdot L \cdot W \cdot T_{ox}} \quad (7)$$

By combining equation (2), that describes the function of energy distribution of protons, with equation (7), that describes the function of dependence of the cross section on the energy, we shall obtain the expression for the rate of occurrence of surface states in case of SVEp of Si-H dissociation:

$$R_{itSVEp} \propto \int 1,8\times10^{4}\left(E\right)^{-2,7}\cdot\frac{dN_{it}(E)}{1,8\cdot10^{4}\cdot\left(E\right)^{-3,7}\cdot n\cdot L\cdot W\cdot T_{ox}}dE. \quad (8)$$

taking the constants off the integral sign, substituting all known variables and solving the integral, we shall obtain:

$$R_{itSVEp} = C_4\cdot\frac{dN_{it}(E)}{n\cdot L\cdot W\cdot T_{ox}}\cdot\frac{E^2}{2} \quad (9)$$

where, C_4 is a proportionality coefficient obtained empirically; $dN_{it}(E)$ is the number of surface states occurred after the interaction of protons with hydrogen atoms, which depends on the initial energy of protons and intensity of their flux; n is the concentration of hydrogen in oxide; L is the length of the channel; W is the width of the channel; T_{ox} is the thickness of oxyde; E is the energy of cosmic-ray protons.

For the case of proton – electron scattering, denoting the cross section of the reaction of interaction of cosmic-ray protons with electrons in the channel by function $S_{PES}(E)$, assuming that the speed of electrons in the channel is negligibly low in comparison to the speed of cosmic-ray protons, considering them to be equally distributed in the channel, with the concentration which is defined as $N=\frac{I_{sd}}{e}\cdot L\cdot W$, where I_{sd} is the current flowing through the channel from the source to the drain, e is an electron charge, L is the length of the channel; W is the width of the channel, we shall obtain the following formula to calculate the cross section of the reaction of interaction of cosmic-ray protons with electrons of the channel:

$$S_{PES}(E)=\frac{dN_{it}(E)}{1,8\cdot10^{4}\cdot(E)^{-3,7}\cdot\frac{I_{sd}}{e}\cdot L\cdot W}. \quad (10)$$

By analogy with the interaction of cosmic-ray protons with hydrogen atoms in oxide, we shall obtain the expression of the rate of surface states for proton – electron scattering:

$$R_{itPES} = C_5\cdot\frac{dN_{it}(E)}{\frac{I_{sd}}{e}\cdot L\cdot W}\cdot\frac{E^2}{2}, \quad (11)$$

where, C_5 is a proportionality coefficient obtained empirically;

By analogy with the Bravais model, in which all mechanisms of the degradation of performance, caused by Si-H interruption, are independent, considering the contributions to the degradation from the mechanisms described by equations (9) and (11) to be independent as well, let us combine the Bravais model equation (1) with equations (9), (11) and obtain the expression of the expanded Bravais model, physical model to forecast the reliability of nanosized field-effect transistors that considers possible influence of cosmic rays:

$$R_{it}=\frac{1}{\tau}=\left[\begin{array}{l} C_1\cdot\left(\frac{I_{ds}}{W}\right)^{a_1}\cdot\left(\frac{I_{bs}}{I_{ds}}\right)^{m}+C_2\cdot\left(\frac{I_{ds}}{W}\right)^{a_2}\cdot\left(\frac{I_{bs}}{I_{ds}}\right)^{m}+ \\ +C_3\cdot V_{ds}^{a_3/2}\cdot\left(\frac{I_{ds}}{W}\right)^{a_3}\cdot\exp\left(\frac{-E_{emi}}{k_BT}\right) \end{array}\right]+$$

$$+\left\langle C_4\cdot\frac{dN_{it1}(E)}{n\cdot L\cdot W\cdot T_{ox}}\cdot\frac{E_1^{\,2}}{2}+C_5\cdot\frac{dN_{it2}(E)}{\frac{I_{sd}}{e}\cdot L\cdot W}\cdot\frac{E_2^{\,2}}{2}\right\rangle, \quad (12)$$

where, C_1, C_2, C_3, C_4, C_5 are proportionality coefficients obtained empirically for SVE, EES, MVE, SVE_p and PES mechanisms of the occurrence of surface states, respectively; a_1, a_2, a_3, m are empirical parameters obtained forn the results of accelerated tests (were defined within the Bravais model [3], but may require specification for different types of devices); E_{emi} = 0.26 eV is the energy of hydrogen emission from the last binding energy level (defined in the Bravais model [3]); k_B is the Boltzmann's constant; T is temperature; I_{ds} is a drain current; I_{sd} is the current flowing in the channel from the source to the drain; I_{bs} a base current; V_{ds} is a voltage on drain; L is the length of the channel; W is a width of channel; T_{ox} is the thickness of oxide; n is the concentration of hydrogen in oxide; e is an electron charge; $dN_{it1}(E)$ is the number of surface states occurred by SVE_p mechanism, which depends on the initial energy of protons and intensity of their flux, defined by the results of accelerated tests; dN_{it2} is the number of surface states occurred by PES mechanism, which depends on the initial energy of protons and intensity of their flux, defined by the results of accelerated tests; E_1 is the initial energy of cosmic-ray protons able to reach the $Si\text{-}SiO_2$ boundary with final energy sufficient to initiate the occurrence of surface states by SVE_p mechanism, defined by the structural features of devices; E_2 is the initial energy of cosmic-ray protons able to reach the $Si\text{-}SiO_2$ boundary with final energy sufficient to initiate the occurrence of surface states by PEE mechanism, defined by the structural features of devices.

The operand of equation (12), wrapped in square brackets, refers directly to the model developed by Bravais and co-authors [3], whereas the operand операнд, wrapped in triangular brackets, refers to the supplement to the Bravais model, developed within this work and allowing for the consideration of possible cosmic-ray influence on the degradation of performance caused by Si-H interruption.

Conclusion

Within the framework of this work it was shown that modern nanosized field-effect transistors and the respec-

tive electronic devices are still exposed to the degradation of performance caused by Si-H interruption, despite the reduction of power supply voltage and the value of lateral electric field in the channel.

Empirical and semi-empirical models to forecast the reliability and degradation, based on the obsolete model of "lucky" electrons which is still applied, can not estimate the reliability of modern nanosized field-effect transistors and the respective electronic devices in full scope.

Modern physical models, such as, for instance, the Bravais model helps to describe physical mechanisms of the degradation of performance caused by Si-H interruption, which are peculiar for modern nanosized field-effect transistors and able to give a more accurate forecast of reliability of electronic devices based on nanosized field-effect transistors.

The model developed in this article is based on the physical Bravais model. This model expands the Bravais model and considers possible influence of cosmic rays on the degradation of performance of nanosized field-effect transistors, and as the result it gives a more expanded forecast of the reliability of the respective electronic devices which are potentially suited to be applied in the space related equipment.

References

1. Prabhakar M. Characterization and modeling of hot carrier degradation in sub-micron n-MOSFETs/ M. Prabhakar// Master's thesis, Nashville, Tennessee. – 2002. – P. 60.

2. White M. Physics-of-Failure Based Modeling and Lifetime Evaluation/ M. White, J.B. Bernstein// California Institute of Technology. – 2008. – P. 210.

3. Grasser T. Hot Carrier Degradation in Semiconductor Devices/ T. Grasser// Springer International Publishing Switzerland, 2015. – P. 517.

4. Klapdor-Kleingrothaus G.V. Astrophysics of elementary particles/ G.V. Klapdor-Kleingrothaus, K. Tsuber; under the editorship of. V.A. Bednyakov. – M.: editorial office of magazine "Success of physical sciences", 2000. – 496 p.

5. Review of particle physics, Pt. 24: Cosmic Rays/ K. Nakamura et al.// J. Phys. – Vol. 37. – pp. 269 – 277.

6. Rauch S.E. The energy-driven paradigm of n-MOSFET hot carrier effects/ S.E. Rauch, G.L. Rosa// IEEE Transactions on Electron Devices and Materials Reliability. – 2005. – Vol. 5. – №4. – pp. 701 – 705.

7. Shirokov Y.M. Nuclear phusics/Y.M. Shirokov, N.P. Yudin. – M.: Science, 1980. – 728 p.

8. Loshakov I.I. Introduction to dosimetry and protection from ionizing rays: study guide/ I.I. Loshakov. – Peter the Great St. Petersburg Polytechnic University, 2008. – 145 p.

About the authors

Artyom N. Volkov, developer of text documentation of category 2, LLC NPO PKRV (Research and production association Software complexes of real time).

Address: 113, bld. 1546, Zelenograd, Moscow, 124683, Russia. Tel: +7(905) 756 – 97 – 27, e-mail: artem.n.volkov@yandex.ru

Receive on 17.02.2016

Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2640-2016-16-3-23-25*

About the optimization of overhead system maintenance

Vladislav A. Volodarsky, *Chair of Traffic Systems, Krasnoyarsk Institute of Railway Transport, Krasnoyarsk, Russia, e-mail: volodarsky.vladislav@yandex.ru*
Alexey A. Orlenko, *Krasnoyarsk Institute of Railway Transport, Krasnoyarsk, Russia, e-mail: orlenkoai@yandex.ru*

Vladislav A. Volodarsky

Alexey A. Orlenko

Abstract. Purpose *is to propose and study a mathematical model of optimization of maintenance of overhead devices, which considers the scope of recovery of service life.* **Methods.** *The analysis of this issue has proposed a strategy and a mathematical model of optimization of maintenance of overhead system, as a kind of a long length object that may undergo preventive replacements and overhauls with minimum emergency repair in case of failures of the overhead system. Besides, the paper describes several particular cases of the general model when performing only preventive replacements, or only preventive overhauls. To take into account the scope of service life recovery when performing a preventive overhaul, we use the parameter, which means the "age" of a long length object and which is defined as the difference between its pre-repair service life and inter-repair service life, related to the pre-repair service life.* **Results.** *At the given values of the number of preventive overhauls and scope of service life recovery, we obtained the expressions to define the optimal frequency of preventive overhauls and replacements of overhead system, as well as the optimal specific operating expenses. At the given values of the frequency of preventive replacements and scope of service life recovery, we obtained the expression to define the optimal number of preventive overhauls up to the replacement of overhead system.* **Conclusion.** *To take into account the scope of service life recovery after overhaul, it is advisable to use the parameter which is defined as the difference between pre-repair service life and inter-repair service life, related to the pre-repair service life of the overhead system. The proposed mathematical model of optimization of maintenance makes it possible to define the optimal frequency of preventive overhaul and replacements of overhead system, as well as the optimal number of overhaul for the period of the overhead system operating life under the given scope of recovery of service life.*

Keywords: *service life, scope of recovery, repair, replacement, mathematical model, optimization.*

Citation format: *Volodarsky V.A., Orlenko A.A. About the optimization of overhead system maintenance // Dependability. 2016. No.3. P. 23-25. DOI: 10.21683/1729-2640-2016-16-3-23-25*

State of the art

According to [1], let us understand maintenance as a set of measures aimed to maintain and recover an operable condition of equipment, as well as to recover its service life.

Operation of the overhead system (OS) is accompanied by maintenance (M), current repairs (CR) and overhauls (O), as well as by reconstruction equivalent to preventive replacement [2,3]. Under the performance of maintenance by means of examinations, inspections, testing and measurements, only technical condition of OS is defined [3]. Besides, according to [4], when doing CR, only the recovery of operating capability takes place, but when doing overhauls, the recovery up to the certain level of the object's service life is done. Full recovery of service life takes place only in case of replacement of OS equipment.

At present in the reliability theory [5,6] some methodological issues have been developed regarding optimization of preventive replacements (PRpl) with emergency replacements (ERpl), when initial reliability of devices is completely recovered, or PRpl with minimum emergency repairs (MER) in case of failures. The publications mentioned includes only two extreme cases of scope of service life recovery: no update when MER is done and full update when ERpl or PRpl is performed. But they are the intermediate values of scope of recovery of the devices' service life within these two extreme cases which are of practical interest.

Purpose of this article is to propose and study a mathematical model of optimization of overhead system maintenance, characterized by the extent of scope of service life recovery.

Strategy and mathematical model of maintenance optimization

To consider the scope of service life recovery it is proposed to use the parameter a = Tpr – Tir according to [7] which means "age" of the overhead system after the preventive overhaul. Tpr and Tir here are pre-repair and inter-repair service life respectively [7]. In future, when developing mathematical models for maintenance optimization it is advisable to use a dimensionless parameter $\alpha = a/Tpr$ to estimate the scope of service life recovery. If $\alpha = 0$, it means that replacement has been done. If overhaul is done, for example, in ϕ time, then the OS "age" decreases from τ to $\alpha.\tau$.

From the perspective of reliability overhead system is considered to be an extended object with many different elements connected in series. In the process of troubleshoot-

ing only a separate damaged OS section is recovered, and practically, it does not affect the current reliability of OS as a whole. In this regard, let us consider the maintenance strategy under which failures are eliminated by minimum emergency repair, and after n of preventive overhauls the replacement of OS is done.

The change of the failure rate (FR) depending on the operation life under this strategy is shown in fig.1. After minimum emergency repairs the failure rate is not changed. After preventive overhauls (PO) with frequency x and scope of service life recovery α, FR is reduced to λ(α),and after PRpl with frequency xp it decreases to a zero level. At the time of PO and PRpl FR is λ(x+α). Here x and xp are measured in units of service life.

The mathematical model of OS maintenance optimization under this strategy is defined from expression

$$y = (1 + n\gamma + \varepsilon \int_0^{x_p} \lambda(x)dx) \Big/ x_p, \qquad (1)$$

where y is the relative specific operating expenses;

γ is the parameter of overhaul cost;

ε is the parameter of cost of minimum emergency repair;

λ is a failure rate;

The number of failures at $0 - x_p$ interval is defined as follows:

$$\int_0^{x_p} \lambda(x)dx = \int_0^{\alpha} \lambda(x)dx + (n+1)\int_{\alpha}^{x+\alpha} \lambda(x)dx = \\ = n\ln P(\alpha) - (n+1)\ln P(x+\alpha), \qquad (2)$$

Here P is the probability of reliable operation.

Substituting the values $\int_0^{x_p} \lambda(x)dx$ from (2) to (1), and keeping in mind that $x_p = \alpha + (n+1)x$, we shall get the following mathematical model

$$y = \frac{1 + n\gamma + \varepsilon\left(n\ln P(\alpha) - (n+1)\ln P(x+\alpha)\right)}{\alpha + (n+1)x}. \qquad (3)$$

Let us consider two particular cases of the model (3):

with $n = 0$, when $\alpha = 0$ (there are only replacements that completely recover the initial service life) we obtain the following mathematical model

$$y = (1 - \varepsilon \ln P(x)) \Big/ x,$$

that is known as the model of preventive replacements with minimum emergency repair in case o failure [5];

with $n \to \infty$ (there are only overhauls that partly recover the initial service life) after we revealed the indeterminacy in (3) we shall obtain the following mathematical model

$$y = (\gamma - \varepsilon(\ln P(x+\alpha) - \ln P(\alpha))) \Big/ x,$$

that is known as the model of preventive overhauls with minimum emergency repair in case of failure [7].

Using expression (3) with given values of n and α, the optimal frequency of preventive overhaul x_0 and minimum specific operating expenses y_0 could be defined from the condition $\partial y / \partial x = 0$ as

$$\left(\alpha + (n+1)x_0\right)\lambda(x_0+\alpha) + (n+1)\ln P(x_0+\alpha) - \\ -n\ln P(\alpha) = \frac{(1+n\gamma)}{\varepsilon};$$

$$y_0 = \varepsilon\lambda(x_0+\alpha).$$

Frequency of O can be defined from the expression

$$x = (x_p - \alpha)/(n+1). \qquad (4)$$

$$\text{Then } x + \alpha = (x_p + n\alpha)/(n+1). \qquad (5)$$

Substituting the obtained values of x and $x + \alpha$ from (4) and (5) to expression (3), we shall transform it to the following form

$$y = \left(1 + n\gamma + \varepsilon\left(n\ln P(\alpha) - (n+1)\ln P\left(\frac{x_p + n\alpha}{n+1}\right)\right)\right) \Big/ x_p \qquad (6)$$

Using expression (6) with given values of n and α, the optimal frequency of preventive replacements x_{p0} and minimum specific operating expenses could be defined from the condition $\partial y / \partial x_p = 0$ as

$$x_{p0}\lambda\left(\frac{x_{p0} + n\alpha}{n+1}\right) + (n+1)\ln P\left(\frac{x_{p0} + n\alpha}{n+1}\right) - \\ -n\ln P(\alpha) = (1+n\gamma) \Big/ \varepsilon;$$

$$y_0 = \varepsilon\lambda\left(\frac{x_{p0} + n\alpha}{n+1}\right).$$

Using the expression (6) with given values of x_p and α, the optimal number of overhauls n_0 could be defined from the condition $\partial y / \partial n = 0$ as

$$\frac{x_p - \alpha}{n_0 + 1}\lambda\left(\frac{x_p + n_0\alpha}{n_0+1}\right) + \ln P\left(\frac{x_p + n_0\alpha}{n_0+1}\right) - \ln P(\alpha) = \gamma \Big/ \varepsilon.$$

Conclusion

To take into account the scope of service life recovery after overhaul, it is advisable to use the parameter which is defined as the difference between pre-repair service life and inter-repair service life, related to the pre-repair service life of the overhead system.

The proposed mathematical model of optimization of maintenance makes it possible to define optimal frequency of preventive overhaul and replacements of overhead system, as well as optimal number of overhaul for the period of the

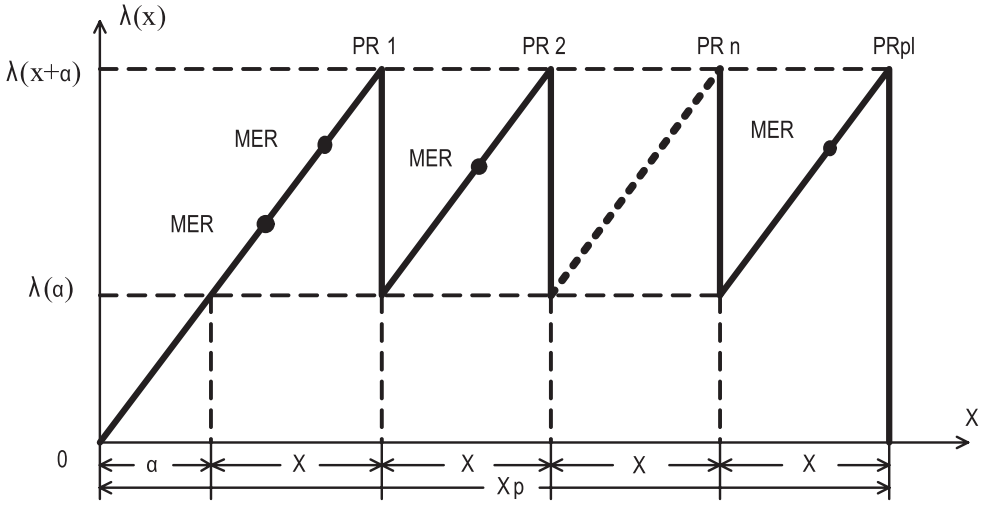


Fig. 1. Change of failure rate due to preventive OR and replacement with minimum emergency repairs

overhead system operating life under the given scope of recovery of service life.

References

1. GOST 32192 – 2013. Dependability in railway technics. General concepts. Terms and definitions.

2. STO RZD 1.12.001 – 2007. The devices for electrification and power supply. Maintenance and repair. Basic requirements.

3. Rules of construction and technical operation of the overhead system of electrified railways (ЦЭ – 868). – M.: Transizdat, 2002. -184 p.

4. GOST 18322 Equipment maintenance and repair system. Terms and definitions.

5. Barlow, R., Proshan, F.: Mathematical theory of reliability. – M.: Soviet radio, 1961. – 488 p.

6. Beichelt F, Franken P. Reliability and maintenance: Mathematical method. M: Radio I Svyaz Press; 1988. – 392 p.

7. Volodarsky V.A. About optimization of preventive replacements and repairs of technical devices // Dependability. – 2011.- No. 2. – P. 49-59.

About the authors

Vladislav A. Volodarsky, PhD Engineering, Professor, Senior Research Assistant of Chair of Traffic Systems, Krasnoyarsk Institute of Railway Transport, Krasnoyarsk, Russia, tel.: +7 (391) 221-60-72 e-mail: volodarsky.vladislav@yandex.ru

Alexey I. Orlenko, PhD Engineering, Associate Professor, Krasnoyarsk Institute of Railway Transport, Krasnoyarsk, Russia, tel.: +7 (391) 271 67 40, e-mail: orlenkoai@yandex.ru

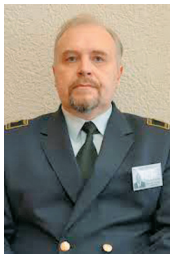
Receive on 29.02.2016

Original article
Надежность № 3 2016 DOI: 10.21683/1729-2640-2016-16-3-26-34
Dependability no.3 2016 UDK 681.3.06+519(076.1)

Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy (part 2)

Gennady N. Cherkesov, *Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia, e-mail: gennady.cherkesov@gmail.com*
Alexey O. Nedosekin, *National Mineral Resources University "Gorny", St. Petersburg, Russia, e-mail: apostolfoma@gmail.com*

Gennady N. Cherkesov



Alexey O. Nedosekin

Abstract. Purpose. *The paper describes main concepts and definitions, survivability indices, methods used to estimate survivability in different external and internal conditions of application of technical systems, including the studies in the field of structural survivability obtained 30 years ago within the frames of the Soviet school of sciences. An attempt is made to overcome different understanding of technical survivability, which has been formed by now in a number of industrial directions – shipping, aviation, communication networks, energy systems, in industries of defense. Besides, the problem is discussed in relation to the establishing of the continuity between technical survivability and global system resilience. Technical survivability is understood in two basic meanings: a) as a property of a system to resist to negative impacts; b) as a property of a system to recover its operability after a failure or accident caused by external reasons. This article also describes the relation between structural survivability, when the logic of system operability is binary and described by a logical function of operability, and functional survivability, when the system operation is described by a criterion of functional efficiency. Thus, a system failure is a fall in the level of its efficiency lower than the value predetermined in advance.* **Methods.** *Technical system is considered as a controlled cybernetic system installed with specialized survivability aids (SA). Logical and probabilistic methods and results of combinatorial theory of random placements are used in the analysis. It is supposed that: a) negative external impacts (NI) are occasional and single-shot (one impact affects one element); b) each element of the system has binary logic (operability – failure) and zero resistance, i.e. it is for sure affected by one impact. Henceforth this assumption is generalized for the r-time NI and L-resistant elements.*
Besides, the work describes the variants of non-point models when a system's part or entire system are exposed to a group specialized affection. It runs about the variants of combination of reliability and survivability, when both external and internal failures are analyzed. **Results.** *Different variants of affection and functions of survivability of technical systems are reproduced. It has been educed that these distributions are based on simple and generalized Morgan numbers, as well as Stirling numbers of the second kind that can be reestablished on the basis of simplest recurrence relations. If the allowances of a mathematical model are generalized for the case when there are n of r-time negative external impacts and L- resistant elements, the generalized Morgan numbers which participate in the estimate of the affection law, are defined based o nthe theory of random placements, in the course of n-tuple differentiation of a generator polynomial. In this case it is not possible to establish recurrence relation among generalized Morgan numbers. It is shown that, under uniform allowances for a survivability model (equally resistant elements of the system, equally probable negative external impacts) in the core of relations for the function of system survivability, regardless of the affection law, there is a vector of structure redundancy F(u), where u is the number of affected elements, F(u) is the number of operable states of the technical system under u failures.* **Conclusion.** *Point survivability models are a perfect tool to perform an express-analysis of structural complex systems and to obtain approximate estimates of survivability functions. Simplest allowances of structural survivability can be generalized for the case when the logic of system operability is not binary, but is specified by the level of the system efficiency. In this case we should speak about functional survivability. Computational complexity PNP of the task of survivability estimation does not make it possible to solve it by the simplest enumeration of states of the technical system and variants of negative external impacts, it is necessary to look for the ways to egress from the blind enumeration, by transformation of the system operability function and its decomposition, as well. Development and implementation of survivability property into a technical system should be conducted with consideration of the property which is assured in biological and social systems.*

PART 2. Multivariate calculations

This paper is a closing article to the first one [1] and it reproduces multivariate calculations by the procedure described in the references. Computational complexity of the task of survivability

estimation and the ways to overcome this problem are discussed. We also deal with a passing from structural survivability to the tasks of functional survivability, establishing a conceptual joint between technical survivability and mobilization resilience in economy.

Keywords: *survivability, vitality, resilience, risk, negative impact, survivability margin, law of vulnerability, function of survivability.*

Citation format: *Cherkesov G.N., Nedosekin A.O. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy (part 2) // Dependability. 2016. No.3. P. 26-34. DOI: 10.21683/1729-2640-2016-16-3-26-34*

1. Introduction

In part [1] we gave a general definition to technical survivability, classified the main approaches to the analysis of survivability, proposed the simplest models and methods of the analysis, based on the theory of axiological probabilities, random placements and logical functions of operability. In the second part we shall discuss four main issues:

- computational complexity of tasks of survivability;
- multivariate calculations of survivability of the systems with complex structure;
- functional survivability and its relation to structural survivability;
- connection between technical survivability and mobilization economic resilience.

2. Computational complexity of survivability tasks and ways how to overcome it

A task of survivability is set and solved on a Cartesian product of two logical and probabilistic spaces: space of negative impacts (NI) and space of states of technical systems. In the simplest case, both these spaces are discrete. In accordance with the terminology of classic paper [2], the task of distribution of NI over the system elements is a *P*-complete or a *P*-difficult, i.e. the number of calculations and the time of calculations are in proportion to N^n, where n is the number of impacts, and N is the number of system elements. It has long been known that for modern computers *P*-completeness represents no difficulty, let even n be estimated by hundreds and thousands which is impossible in reality. A different matter is the assignment of a complete group of possibly operable states, when from 1 to N-1 elements are sequentially taken out from the system of N elements. Due to the fact that in the task of structural survivability an element may be in one of the states – operability or a failure (binary logic), the total number of states of the system to be enumerated is 2^N, computational complexity corresponds to the same number. Thus, the survivability task becomes *NP*-difficult and has its fixed range.

When logical and probabilistic methods of analysis were pushing their way into science (in 1980s), when the most common computers in the USSR were USEC of different modifications, certain experiments established a limit number of the system elements, exceeding of which did not make it possible to solve the task of survivability analysis for observable time. This number was $N = 27$. All attempts to increase this number failed, until several approaches were found to assure the pass from direct enumeration of states to **intent** enumeration. As the result, the work of the school of Prof. A.S. Mozhaev and his followers [3 – 5] led to the situation when it turned to be possible to decompose the graph of complex system into a main graph and its sub-graphs (joint openings), as well as to develop logical schemes of intent enumeration in the space of states. As the result the limit number of elements in the main graph today is 400, and in a sub-graph – 100 (data according to software complex "ARBITR").

Therefore, overcoming a "bane of limit number" in relation to the tasks of structural survivability happened. But we have won only the first position war, because when passing from structural survivability to functional survivability, the space of states of the technical system ceases to be numerable, and a "bane of limit number" comes back, but in a frightening form. This feature is described in more detail in section 5 of this work. In a similar way solution of the task of structural survivability is becomes complicated, if the frequency of impacts is r, and the element resistance is L (or a discrete resistance in a model is substituted with a probabilistic function of resistance).

Let us now describe the simplest examples of survivability analysis (these solutions were originally demonstrated in [6], including all figures and tables of section 3). All examples are well estimated by hand and can serve as tests for new algorithms of analysis, as degenerated cases.

3. Calculation of structural survivability by the system state for the simplest structures

3.1. System with bridge structure of five elements

A system with bridge structure (Fig. 1) is exposed to repeated point negative impacts. It is necessary to estimate survivability by the system state supposing that the affection

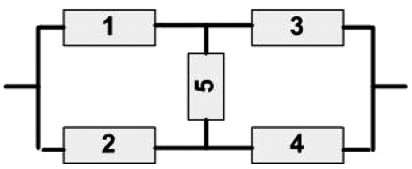


Fig. 1. System with bridge structure

of elements under a single NI is equally probable, and the resistance of elements in relation to the intensity of NI of high accuracy is negligibly low.

Logical function of operability in an orthogonal disjunctive normal form (ODNF) is as follows [7, chapter 4]:

$$F = x_1x_3 \vee x_1'x_2x_4 \vee x_1x_2x_3'x_4 \vee x_2'x_3'x_1x_4x_5 \vee x_1'x_4'x_2x_3x_5. \quad (1)$$

Let us take formulas (31) and (32) from [1], setting $m = 5$, $s_1 = 2$, $N = 5$, $s_2 = 3$, $s_3 = 4$, $s_4 = s_5 = 5$, and we will obtain

$$R(n) = (1 - s_1 / N)^n + \sum_{k=2}^{3}\sum_{i=1}^{n} C_n^j N^{-i}(1 - s_k / N)^{n-i} +$$

$$+2N^{-n}\sum_{i=1}^{n-1} C_n^i = 2(0,6)^n + 2(0,4)^n - 5(0,2)^n. \quad (2)$$

Values $R(n)$ with $n \le 5$ are given in Table 1.

Table 1. Function $R(n)$

n	1	2	3	4	5	6	7
$R(n)$	1	0,84	0,52	0,3024	0,1744	0,1012	0,0592

Let us now take formulas (33) – (37) from [1] to define $R(n)$. For this purpose we shall use formula (37) to draw up a table of coefficients L_{nk} (Table 2) and note that it does not depend on the system characteristics (structure and number of elements). That is why it can be used as a common table to calculate survivability of any systems. Table 3 shows the values of coefficients B_{ki} for nine operable structures obtained from the basic structure by means of removal of one, two or three elements (Fig. 2).

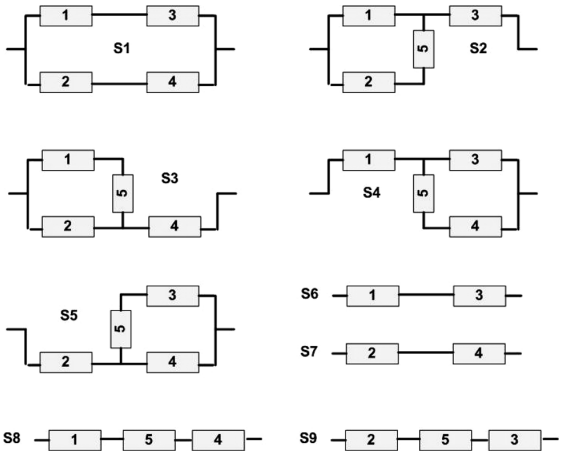


Fig. 2. Operable structures obtained from the basic bridge structure

Multiplying the lines of matrix $||L_{nk}||$ by the columns of matrix $||B_{ki}||$, we shall get the matrix of coefficients r_{ni}, expressing the number of ways which may be used to pass form basic structure S_0 to structure S_i under n-tuple NI (Table 4). Putting the elements of one line together we

Table 2. Numbers L_{nk}

n	L_{nk}						
	k= 1	k= 2	k= 3	k= 4	k= 5	k= 6	k=7
1	1	0	0	0	0	0	0
2	1	2	0	0	0	0	0
3	1	6	6	0	0	0	0
4	1	14	36	24	0	0	0
5	1	30	150	240	120	0	0
6	1	62	540	1560	1800	720	0
7	1	126	1806	8400	16800	15120	5040

Table 3. Numbers B_{ki}

k	B_{ki}								
	i=1	i=2	i=3	i=4	i=5	i=6	i=7	i=8	i=9
1	1	1	1	1	1	0	0	0	0
2	0	0	0	0	0	3	3	1	1
3	0	0	0	0	0	1	1	0	0

will find the number of different disjoint events which lead to an operable structure under n-tuple NI. It is easy to show that values $R(n) = r_n/N^n$ coincide with the values listed in Table 4.

Using formula (5) from [1] and formula (2), we shall find the average number of NI leading to loss of operability:

$$\bar{\omega} = \sum_{n=0}^{\infty} R(n) = 1 +$$

$$+\sum_{n=1}^{\infty}\left\{2(0,6)^n + 2(0,4)^n - (0,2)^{n-1}\right\} = 4,083 \quad (3)$$

Table 4. Numbers r_{ni}

n	r_{ni}					r_n	N^n
	i=1..5	i=6	i=7	i=8	i=9		
1	1	0	0	0	0	5	5
2	1	6	6	2	2	21	25
3	1	24	24	6	6	65	125
4	1	78	78	14	14	189	625
5	1	240	240	30	30	545	3125
6	1	726	726	62	62	1581	15625
7	1	2184	2184	126	126	4625	78125

Average survivability margin $\bar{d} = 3,083$. Significantly, for this structure $d = 2$, and $m = 3$. Therefore, average survivability margin is more than the maximum number of elements that can be removed without loss of operability, more than m-survivability. This effect is explained by the fact that certain elements appear in the field of NI for several times.

The system of calculation of this paragraph which is based on Stirling numbers of the second kind, was completely described in [6] and [10].

3.2. Electric power system with bridge structure of eight elements

Electric power system consists of generating power units 1 and 2, main distribution boards 3 and 4, jumper straps 8, cables 5 and 6, distribution board7 (Fig. 3). It is necessary to estimate survivability by the system state after repeated NI, supposing that at each NI one element of the system becomes non-operable, and the affection of the elements at a single NI is equally probable.

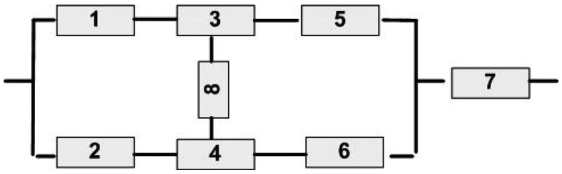


Fig. 3. Structure of electric power system

Logical function of the system operability is as follows:

$$F = x_7(x_1x_3(x_5 \vee x_4x_6x_8) \vee x_2x_4(x_6 \vee x_3x_5x_8) \qquad (4)$$

Orthogonal disjunctive normal form:

$$F = x_1x_3x_5x_7 \vee x_1'x_2x_4x_6x_7 \vee x_1x_2x_3'x_4x_6x_7 \vee$$
$$\vee x_1x_2x_3x_4x_5'x_6x_7 \vee x_1x_2'x_3x_4x_5'x_6x_7x_8 \vee$$
$$\vee x_1'x_2x_3x_4x_5x_6'x_7x_8. \qquad (5)$$

Thus, the logical function of the system operability contains 6 implicants in total, including one implicant without negation, three with one negation and two with two negations. Probabilities

$$P(Q_1 = 1 / A_n) = 2^{-n};$$
$$P(Q_l = 1 / A_n) = \sum_{j=1}^{n} C_n^j N^j (1 - s_1 / N)^{n-j},$$
$$l = 2, 3, 4;\ s_2 = 5,\ s_3 = 6,\ s_4 = 7$$
$$P(Q_l = 1 \mid A_n) = \sum_{j=1}^{n-1} C_n^j N^{-n},\ N = 8,\ s_5 = s_6 = 8. \qquad (6)$$

According to (1) we have:

$$\sum_{l=1}^{6} P(Q_l = 1 \mid A_n) = 2^{-n} + 8^{-n}(4^n + 2^{n+1} - 5) =$$
$$= 2^{-n+1} + 2^{-2n+1} - 5 \times 2^{-3n}. \qquad (7)$$

Table 5. Function of survivability *R*(*n*)

n	1	2	3	4	5	6
***R*(*n*)**	7/8	35/64	139/ 5122	539/ 4096	2107/ 32768	8315/ 262144
R(*n*)**	7/8	1/2	8/56	1/35	0	0

The results of calculations by formula (7) are listed in **Table 5.**

The last line indicates the data of calculations by strategy 2, when the affected elements are excluded from the next affection.

Average number of NI

$$\bar{\omega} = 1 + \sum_{n=1}^{\infty} \left\{2(0,5)^n + 2(0,25)^n - 5(0,125)^n\right\} = 2,9524$$

Average survivability margin $\bar{d} = 1,9524$. It is substantially less than *m*-survivability (here $m = 4$). Survival rate of the system is found using formulas (33) – (37) from **[1]**. We take into account that except a basic structure, the system may have nine more different operable decomposed structures (i=1…9). Let us define coefficients B_{ki} first (Table 6).

Table 6. Numbers B_{ki}

k	B_{ki}				
	***i*=1…5**	***i*=6**	***i*=7**	***i*=8**	***i*=9**
1	1	1	1	0	0
2	0	6	6	1	1
3	0	4	4	0	0
4	0	1	1	0	0

Structures $S_1 \ldots S_5$ occurs at the loss of only one element ($k = 1$), i.e.: 1, 2, 5, 6, 8. Structure S_6 (1357) may occur at the loss of one (4), two (24, 26, 46, 82, 84, 86), three (246, 248, 268, 468) or four (2, 4, 6, 8) elements. Similarly, structure S_7 (2467) occurs at the loss of 1, 2, 3 or 4 elements. Their number is the same as for structure S_6. Structure S_8 (operable elements 138467) occurs at the loss of two elements (25), and S_9 (248357) occurs at the loss of two elements: 1 and 6.

Using the data of tables 2 and 6, we shall define r_{ni}. Results are listed in Table 7.

Table 7. Numbers r_{ni}

n	r_{ni}					r_n	N^n	R_n
	***i*=1…5**	***i*=6**	***i*=7**	***i*=8**	***i*=9**			
1	1	1	1	0	0	7	8	0,875
2	1	13	13	2	2	35	64	0,546875
3	1	61	61	6	6	139	512	0,271484
4	1	253	253	14	14	539	4096	0,131592
5	1	1021	1021	30	30	2107	32768	0,064301

We see that the results in tables 5 and 7 coincide. The analysis of data of Table 7 makes it possible to determine an interesting consistency. Relation r_{ni}/r_n expresses a conditional probability that structure S_i, is saved after *n*-tuple NI provided the system remained operable. As it is shown from the calculation results (Table 8), only for one type of structure (S_6 and S_7) a conditional probability grows at

the increase of the number of NI, and this structure is non-redundant having the least number of elements. Even with $n = 5$ for the share of structures S_6 and S_7 there are 97% of all cases when the system ensures operability.

Table 8. Conditional probabilities

n	$\mathbf{r_{ni}}$ / $\mathbf{r_n}$		
	***i* = 1…5**	***i*= 6,7**	***i*= 8,9**
1	0,1429	0,1429	0
2	0,0286	0,3714	0,0571
3	0,0072	0,4388	0,0432
4	0,0019	0,4694	0,0260
5	0,0005	0,4846	0,0142

Under strategy 2, when the affected elements are excluded from the field of the next NI, and equally probable affection of the remained operable elements, the function of survivability is calculated by the formula:

$$R^*(n) = \sum_{i=1}^{l} C_{N-s_i}^{n-k_i} / C_N^n, \quad (8)$$

where l is the number of implicants in ODNF, s_i is the number of letters in the implicant, k_i is the number of negations. The results of calculations are listed in Table 8. We see that the function of survivability is falling much faster that in the scheme of independent NI (under a "passive strategy"). The average number of NI before affection $\overline{\omega}$ = 2,547. It is less that under strategy 1.

In general we can speak about the existence of a vector of numbers of operable states of the system $F_N(u)$, $u = 0…N$, where u is the number of the elements removed from the system at one moment. Formula

$$f(u) = F_N(u) / C_N^u \quad (9)$$

is a conditional probability that under many-fold affection of u elements in the system of N elements, this system shall keep operability. Then (8) is rewritten in the form

$$R^*(n) = f(n) \quad (10)$$

Vector $F_N(u)$ specifies **structural redundancy** in the system and its profile. And occurrence of this redundancy in the interests of survivability is kept under aby distribution of NI probabilities. This very redundancy equally works on reliability as well. For instance, probability of reliable operation of non-recoverable system with complex structure of homogeneous elements

$$P(t) = F_N(0)*p(t)^N + F_N(1)*p(t)^{N-1}(1-p(t)) + \\ +… + F_N(N\text{-}1)*p(t)(1-p(t))^{N-1}, \quad (11)$$

where $p(t)$ is the probability of reliable operation of one system element. Reliability of such system is the higher, the higher $F_N(u)$ is. It is described in detail in **[**14**]**.

We can pass from the estimating the survivability by state to estimating the survivability by the result of task execution. This work was carried out in **[**6**],** where the same structures were the basis: bridge of five elements and electric power structure of eight elements. Estimate of survivability in this assignment makes it possible to hybridize separate properties of survivability and reliability, getting new complex properties of NI-reliability, NI-safety, etc. **[**11, 12**].**

Structural survivability of multipolar technical systems

Let us consider the variants of constructing a multipolar technical system, when the system can be expressed by a multipolar graph, in which the nodes (without violation of entity) are unexposed to NI, and these are only connections in a graph, which are exposed to impacts. One of possible criteria of non-operability of such system is the occurrence of isolated nodes or separated sub-graphs.

An example is the communication network with the nodes effectively protected from NI and from the line destruction. If any node (or group of nodes) has no connection, the system will lose a critical source of information or a function of control. In practice, it will fall into several subsystems, each of which will start to function independently; and this event is accepted as a fact of loss of survivability.

With no violation of entity let us assume that the branches of the graph of a multipolar system break out one after another, i.e. they are excluded from the field of affection of new NI. Then our task is to form a vector of the system redundancy $F_N(u)$, and then to use formulas (9) – (10) to estimate its probability of survival with n of single NI.

Let us consider two multipolar systems, sequentially in four and five nodes (Fig. 4), in two configurations – non-redundant, when the nodes are closed into a circle, and full-redundant, when the nodes are connected under the principle "each with each one".

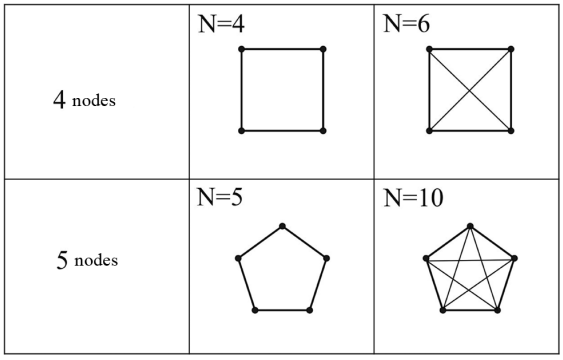


Fig. 4. Different configurations of multipolar systems

Four-polar network, non-redundant system (*N*=4). It is easy to see that the first NI under the active strategy does not put the system out of operation (the same is valid for the structures with more poles). At the same time, any

second NI automatically makes the system non-operable. Therefore:

$$R(n) = 1 \text{ with } n \le 1 \text{ and } R(n) = 0 \text{ with } n \ge 2.$$

And the function of survivability becomes threshold, and it means there is no survivability at all, and it is determined by its non-redundancy.

Four-polar network, full-redundant system (N=6). Here we can see that the system of N=6 connections keeps its operability under any double NI (in all cases the system keeps connectivity). And there are even four scenarios of the system survival under 3-time impact (from 20 possible scenarios). Therefore, the results of estimation of the survivability function are listed in Table 9.

Table 9. Function of survivability for a full-redundant system on 4 nodes

n	$F_6(n)$	C_6^n	$R^*(n) = f(n)$
0	1	1	1
1	6	6	1
2	15	15	1
3	4	20	0,2
≥ 4	0		0

Here the element of a smooth degradation occurs, but nevertheless it leaves much to be desired. Smoothness occurs when additional branches occur (for instance, channels based on another principle of coding and transfer of informationи) alongside with main branches in a graph of multipolar system. Roughly, when digital communication fails there is the possibility of using classical radio communication.

Five-polar network, non-redundant system (N=5). Similarly to non-redundant four-polar network we see that the first NI under the active strategy does not put the system out of operation, and each second one does. Thus, again we deal with a threshold function of survivability:

$$R(n) = 1 \text{ with } n \le 1 \text{ and } R(n) = 0 \text{ with } n \ge 2.$$

Five-polar network, full-redundant system (N=10). System keeps its operability under a three time NI of any direction. With n = 4 the first scenarios of degradation occur (it becomes possible to isolate one of five nodes). With n = 7 and more the system will fail for sure. Therefore, the results of estimation of the function of survivability are listed in Table 10.

Here we really have a slow degradation of survivability. And the more N is, the smoother this degradation is realized with the increase of n.

Table 10. Function of survivability for a full-redundant system on 5 nodes

n	$F_{10}(n)$	C_{10}^n	$R^*(n) = f(n)$
0	1	1	1,0
1	10	10	1,0
2	45	45	1,0
3	120	120	1,0
4	205	210	0,976
5	222	252	0,881
6	5	210	0,024
≥ 7	0		0

Similar results can be obtained if to make NI HB r-tuple and assign the branches in a graph with the resistance level L (analog of the system of channel redundancy). In this case we should use the formula from **[8]**. But it will not change the basic principle: the higher is the redundancy level measured by vector F, the higher is the level of system survivability in respect to NI of wide spectrum.

Functional survivability and principles of analysis

A qualitative leap from structural survivability to the functional one is made as a consequence of substitution of a binary function of operability in the tasks of structural survivability by the level of tolerable loss of efficiency. Let the system be specified by a basic property which defines its performance (for example: in electric power systems this property is available power, in gas systems it is the capacity of a gas pipeline system). Then we can fix the level ε, in percentage of a maximum value of emergence, when we say that if the system efficiency becomes lower than ε in percentage as the result of NI, it means that the system lost its survivability.

Therefore, **functional survivability** is the ability of the system to keep its emergence at the level not lower than ε of the maximum value under NI, or to restore the required level quickly after NI. For instance, in the theory of civil defense there is a principle of technological reserved quota ε=30%, when non-core consumers are de-energized, and all the energy is brought for domestic needs of people. There is also the level of emergency reserved quota ε=10%, when not all citizens get electric power, but only separate important centers of consumption (hospitals, maternities, etc.). And a scientific mission of estimating and assuring of functional survivability is to distribute SA and allowable redundancy, to set the algorithms of system configuration in the way which will make it possible to minimize the probability of technological and emergency reserved quotas in cases of NI of wide spectrum. A more detailed description of ε-criterion is given in papers **[**9, 13, 15 – 17**].**

When NI is point, we are in a discrete space of NI states. There is no such space if we estimate the variants

of areal affection, when there is NI of continuum spectrum. Likewise, passing from structural survivability to the functional one, we lose a discrete space of the system states, it becomes continuous and uncountable. Instead of a logical function of operability we deal with the **algorithm** of assurance of survivability under NI. This algorithm is a kind of a black box having a NI model at the entry, and a resulting effect at the exit. If the entry is a continuum spectrum of impacts, the exit is a continuum spectrum of resulting.

The first that comes to mind in this case is trying to simplify the task, to substitute a continuous space of states by a discrete one. For instance, in [17] we note that a single NI takes a certain quantum of allowable capacity form the system, and the task of a large electric power system is to redistribute the loading and make up the occurred deficit. With the increasing NI, the system starts degradation, its reserves of allowable capacity become exhausted, and one day we will occur at the level of technological reserved quota; and it is necessary to estimate the probability of such negative scenario.

Having begun to deal with the task we discovered that we can substitute a continuous space of states by a discrete one, fixing the certain level ε in the analysis. Actually, ε-criterion is similar to the fixed frequency we scan the system at, specifying a complete set of its operable states. Making the enumeration of states space intent (for instance, using the branch and bound method), may significantly reduce the scope of operations; and *NP*-completeness of the task is still here.

Then we can rewrite formulas (9) and (10) as follows:

$$R^*(n, \varepsilon) = f(n) = F_N(n, \varepsilon) / C_N^n, \qquad (12)$$

where $F_N(n, \varepsilon)$ is the number of operable states of the system of N elements, exposed to n-tuple point NI, on the assumption that the survivability of such system is described by ε-criterion. Besides we can easily pass from an active strategy of NI to a passive strategy – it will not change the analysis principle significantly. The main thing is to estimate the level of functional redundancy, which does not depend on the applicable strategy of NI, as it is being formed in the space of discrete system states specified in an algorithmic way. And then the function of survivability can be estimated with consideration of the strategy, based on the formed vector F.

Beautiful formulas represented for the case of equally probable NI crash totally, when it comes to preferring one NI to the other. In this case we have to go back to the model by Gorshkov [18] which used to be very popular, with assigning of axiological probabilities of point NI affecting separate elements by the Firshburn's principle [19], [20, p. 83-84], building the systems of preferring of one NI to the other. By applying the Gorshkov's formula we estimate the function of survivability at a certain hold point. Varying the NI probabilities in narrow scope, we estimate the dimensions of optimality subset in a multidimensional field of probabilistic scenarios, when out SA decisions are the best ones. Thus, we test our decisions related to the survivability assurance, for parametric stability [13]. Indeed, ε-criterion may serve as one of the parameters at the verification of the decision for optimality.

Passing from structural survivability to functional survivability сразу takes us out from the area of traditional approaches to the analysis, making it possible to estimate not only technical survivability, but also system resilience, in a wide range of classes and purposes of these systems. Thus we gradually move to the area of mobilization economic resilience.

Connection between technical survivability and mobilization economic resilience

Economic unit is a strongly connected system intended to generate a complex economic effect and covered by the loops of positive and negative feedbacks [20]. Different shocks serve as NI in relation to such objects. These shocks affect the system from the side of the unit's environment. Under NI a unit starts to degrade down to the level distinguished as negative, when it is referred to a failure of achievement of strategic aims, either by the level, or by the time of achievement. A control supersystem generates decisions aimed at the survival of the economic unit and at the keeping of resilience in negative environment. Such decisions are tainted by mobilization.

There is an apparent similarity between technical survivability and economic resilience, and this similarity is observed within the frameworks of the general theory of cybernetic systems developed starting from Ludwig von Bertalanffy and his group [21]. Watching the survivability and resilience from systemic positions, we come to the idea of **vitality** as a basic prototype property of survivability in a general sense, which generates its projections in systems of different types. The idea of Bertalanffy was that all living systems (or systems pretending to be viable) had the property of **equifinality**, when a system inevitable comes to its final state, in different ways, from different initial states. Actually, equifinality is a dynamic resilience, realized in the course of pursuing the achievement by the system of its final aims, its base purpose – to serve, deliver a current, protect, supply. Survivability is inherited from equifinality to the same extent as from vitality; the system is vital if it is equifinal, and vice versa.

The obtained isomorphism of technical survivability and economic resilience leaves a wide room for a mutual migration of methods, models and approaches from one type of application to other types. For example, mobilization resilience copies the principle of NI ε-criterion from functional survivability, in the terms of continuous spaces of NI and system states. Balanced score card serves as the function operability and functional algorithm in the economic system. In reverse, technical survivability may get improved if it loses itself in the economic context,

when the analysis of efficiency is supported by an expanded analysis of economic and financial sufficiency of technical decisions for survivability. When it a technical system turns out to have a control supersystem, and a supersystem turns out to have economic context and strategic goals which are introduced to the control supersystem of the respective technical system as basic criteria of performance.

Final purpose of equipment is to serve economic and social systems in standard conditions and under NI, as well. In all cases this service should be developed in stipulated to the extent set forth in advance, with clear expectations, in coordination with the objectives of supersystems.

Conclusion of part 2

The theory of technical survivability shall be developed in the following main directions:

Understanding technical survivability as a general scientific discipline that crosses industrial boundaries. Such vision will be developed when survivability will be observed from systemic cybernetic positions, as a projection of vitality;

Analysis of the experience gained as the result of researches of survivability and resilience carried out in the West. Understanding of how western approaches can be applied in Rissia, why "yes" and why "no";

Substitution of probabilistic models of survivability by inexplicitly scenary models which do not need any axiologic hypotheses, but simulate expert experience in the terms of impacts and reactions, with consideration of essential information uncertainty. Logic of system performance in these conditions may also be "soft", it may be estimated with soft computations and measurements in the sense of Zadeh – Dubois – Prada [22, 23];

Passing from the function of survivability to a risk-function. It is necessary to estimate not the survival rate, but risk of failure to achieve a goal;

A more detailed attention to humanitarian aspects of survivability, to a human factor in survivability control. It is necessary to study not only the technical system, but its SA as well;

Development of a conceptual horizontal between technical survivability and resilience. Implementation of economic and financial measures in the tasks of technical survivability. The task of survivability assurance should be considered from the standpoint of investment project development.

References

1. Cherkesov G.N., Nedosekin A.O. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy. Part 1. Basis of the approach // Dependability. – No2. 2016. P. 3-15.

2. Gary, M. and Johnson, D., Computers and Intractability. – M.: Mir, 1982. – On web-site also: http://cmcstuff.esyr.org/vmkbotva-r15/5%20%D0%BA%D1%83%D1%80%D1%81/9%20%D0%A1%D0%B5%D0%BC%D0%B5%D1%81%D1%82%D1%80/%D0%A2%D0%B8%D0%B3%D1%80%D1%8B/NP-Complectness.pdf .

3. Mozhaeva I.A., Nozik A.A., Strukov A.V. Modern tendencies of structure and logical analysis of reliability and cibersecurity of ASCS. – On web-site also: http://www.szma.com/mabr2_2015.pdf .

4. Mozhaeva I.A. Methods of structure and logical modeling of complex systems with network structure // Author's abstract. St. Petersburg. 2015. 19p.

5. Mozhaev A.S., Gromov V.N. Theoretical basis of the generic logical and probabilistic method of computer-aid system modeling. – SPb: VITU, 2000. – 145 c.

6. Cherkesov G.N. Methods and models of estimation of survivability of complex systems. – M.: Znanie, 1987. – 55 p. – On web-site also: http://www.gcherkesov.com/articles/article02.pdf .

7. Cherkesov G.N. Dependability of hardware and software complexes. – SPb: Piter, 2005. – 480 p.

8. Nedosekin A.O. Application of random placement theory on relation to the analysis of survivability of technical systems // Cibernetics of AS USSR. 1991. No.6.

9. Nedosekin A.O. Analysis of survivability of energy systems by combinatorial and probabilistic methods // Izvestiya EAS. Energy. 1992. N3. C.48 – 58.

10. Nedosekin A.O. Analysis of survivability of automation complex based on a point model // Instrumentation and control systems. 1989. N11. P.12-14.

11. Nedosekin A.O. Connection of fault-tolerance and survivability in functional redundant technical systems // Problems of complex automation of marine technical systems / Abstracts. L., NPO «Avrora», 1989. P.208-209.

12. Nedosekin A.O. Comparative analysis of reliability and survivability of technical systems with network structure // Improvement of quality and dependability of industrial products / Abstracts. L., LDNTP, 1989. P.15 -18.

13. Nedosekin A.O. Assuring of functional survivability of communication networks: analysis and decision-making // Ways of improvement of networks and complexes of technical communication means / Abstracts. L., NPO «Krasnaya Zarya», 1989. P.10 – 13.

14. Nedosekin A.O. Survivability as a function of redundancy in communication networks // X-th symposium on redundancy in information systems / Abstracts. Part 2. L., LIAP, 1989. P.178 -181.

15. Nedosekin A.O. Analysis of survivability of EES by combinatorial and probabilistic methods // MVIN BSE. Issue 41. Irkutsk, 1991.

16. Nedosekin A.O. Analysis of survivability of gas pipeline system of West Siberia in respect to power supply // MVIN BSE. Issue 43. Irkutsk, SEI SO RAS, 1992.

17. Nedosekin A.O. Structural analysis of EES survivability based on the example of test calculation model // MVIN BSE. Issue 43. Irkutsk, SEI SO RAS, 1992.

18. Gorshkov V.V. Logical and probabilistic method of calculation of survivability of complex systems //AS UkrSSR, Cybernetics, 1982, NO.1. – P.104-107.

19. Trukhaev R.I. Models of decision-making under uncertainty. – M.: Science, 1981.

20. Abdulaeva Z.I., Nedosekin A.O. Strategic analysis of innovative risks. – SPb: SPbGPU, 2013. – 145 p. – On web-site also: http://an.ifel.ru/docs/InnR_AN.pdf .

21. Bertalanffy L. von. An Outline of General System Theory. // British Journal for the Philosophy of Science. Vol. 1. 1950. P. 134–165.

22. Zadeh L. From computing with numbers to computing with words — from manipulation of measurements to manipulation of perceptions // International Journal of Applied Math and Computer Science, pp. 307–324, vol. 12, no. 3, 2002.

23. DuBois D., Prade H. Fuzzy sets and systems. Theory and applications. – Academic Press, Inc. Orlando, FL, USA. – 1997. – ISBN 0122227506.

About the authors

Gennady N. Cherkesov, Dr. Sci., professor, professor of Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia, e-mail: gennady.cherkesov@gmail.com

Alexey O. Nedosekin, Dr. Sci., Ph.D., academician of the International Academy of Ecology, Man and Nature Protection Sciences, professor of National Mineral Resources University "Gorny", St. Petersburg, Russia, e-mail: apostolfoma@gmail.com

Receive on 30.03.2016

Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2640-2016-16-3-35-38*

Organization features of functional diagnosis of a control computer with improved survivability

Vladimir G. Zarubsky, *Perm Institute of FSIN of Russia, Perm, Russia, e-mail: volen3030@rambler.ru*

Vladimir G. Zarubsky

Abstract. **Purpose.** *Today, the reliability of protection of mission critical objects and objects of increased risk is achieved by applying integrated safety systems, with the integration of subsystems based on control computers. Improvement of survivability of special purpose computers is a critical task that could be solved using the computers with the property of structural stability. Practical realization of such computer is connected with the task of its functional diagnosis and further functional adjustment. This article describes the process of functional diagnosis of structurally stable control computer as a functional system that is fundamentally different from the traditional control of a personal computer made by the known self-checking programs.* **Methods.** *To solve the task of functional diagnosis the article offers a mathematical model of test check that may become the basis of functional diagnosis of a control computer. Besides, based on the proposed mathematical model, possible outcomes of the test are analyzed.* **Results.** *Analysis of the proposed mathematical model defined the variants of how to minimize the risks of categories I and II, i.e. how to transfer faulty functions to a set of fault-free functions (customer's risk) and to transfer fault-free functions to a set of faulty ones (producer's risk), that is achieved by using a diagnosis practice of "promotion" that is standard for computers. The point is to find an operable "core" – a set of basic functions that help to diagnose the remaining functions of the computer's system of commands. I.e. the "core" with any detected defect is not allowed for further functioning, and a fault-free "core" can serve as rather reliable mean of control. When using this practice, the norm of a single test does not guarantee there is no risk of category I, that explains the common practice of check of each function of the command system by a sufficient sequence of test checks, and the risk of category II does not grow.* **Conclusion.** *The proposed model of a functional diagnosis test check made it possible to form the strategy to construct this process for a structurally stable control computer, namely to implement several particular tasks such as: to separate as a specific the task of identification of an operable "core" as a probable cause of risk of category I, that serves as a source of risk of category II; to perform sequential diagnosis of the remaining part of functions as in computing environment with a developed property of slow degradation of functions; to optimize an extending sequence of test checks for each function reducing the risk of category I, irretrievably leading to the growth of time control that is deficit for a pre-staged self-checking; that is also aimed at the adjustment to the current f-state; to proceed with testing in case of negative results using another software implementation to reduce risk of category II; to develop special procedure to substantiate the duration of testing of each function of control computers.*

Keywords: *control computer, survivability, structural stability, functional redundancy, functional diagnosis, accuracy of control, risks of categories I and II.*

Citation format*: Zarubsky V.G. Organization features of the functional diagnosis of a control computer with improved survivability // Dependability. 2016. No.3. P. 35-38. DOI: 10.21683/1729-2640-2016-16-3-35-38*

Introduction

Terrorist activity that has increased dramatically caused strict requirements for a reliable protection of mission critical objects. To solve this task, integrated safety systems (ISS) came into widespread application. The subsystems forming the part of ISS in most cases are integrated on the basis of a control computer (CC) that is represented by a common personal computer (PC), normally of foreign production with a "regular" operating system. Evidently, a failure of the control computer due to deliberate or undeliberate actions will lead to inadmissible changes of the operation of the whole system. In this situation the reliability of protection of mission critical objects becomes rather doubtful. Therefore, the idea to develop a domestic CC with the properties of improved survivability to different threats seems rather crucial.

Such CC can be represented by the computer with the properties of structural stability [1], whose operation is based on functional redundancy of any modern computer. But practical realization of such computer is connected with two particular tasks – functional diagnosis of CC and its functional adjustment.

All modern computers are multilevel devices, and each of these levels has the properties of functional redundancy [2]. That is why this article describes the processes of functional diagnosis on the example of the architecture command level.

Functional diagnosis of structurally stable (StS) CC, as a functional system differs from the traditional process of

PC control made by the known self-checking programs to define the technical condition: "fault-free – faulty", "operable – inoperable". In modern PC, functional diagnosis of the central processing unit is absolutely useless, as a failure to undergo any test makes it unpractical for a PC availability, because the reduced system of commands becomes non-conforming to a special software. That is not the case with common equipment of special digital weapon computer systems that provide a three-edged (three-channel) structure, which is especially effective against failures and their consequences. Here there are the elements of functional diagnosis aimed at the detection of some particular failures, that do not impede the execution of combat missions, but that are definitely eliminated under operational procedures considering the reduction of survivability margins necessary in extreme operating conditions. This category of failures includes inability of a channel to be a master (slave) one in a two-channel structure, inability of majority devices to defend against single errors at the information input, total or partial loss of functions of inter-channel exchange, etc**.** But in this case we deal not with self-checking, but with the determination of technical condition of the devices served to exchange functional features of the central processing unit.

Functional diagnosis of a structurally stable control computer

Functional diagnosis of the central processing unit, typical for the stage of recovery of CC StS availability, is in fact self-diagnosis, i.e. the identification of functional state $\tilde{\rho}^F$ under the conditions of stochastically undetermined splitting of the functional system F up to the classes $\tilde{\rho}^F$ and $\overline{\tilde{\rho}}^F$:

$$F = \tilde{\rho}^F \cup \overline{\tilde{\rho}}^F, \tilde{\rho}^F \cap \overline{\tilde{\rho}}^F = \varnothing, \quad (1)$$

with convergence

$$\tilde{\rho}^F \to \rho_f^F, \overline{\tilde{\rho}}^F \to \overline{\rho}_f^F, \quad (2)$$

where ρ_f^F is the current functional state of CC StS, as well as with the limited duration of the control process

$$t_{fd} \le t_{fd}^{\max}. \quad (3)$$

Expression (2) means that the risks of categories I and II are kept to minimum, i.e. faulty functions are considered as fault-free functions (customer's risk) and fault-free functions are considered as faulty ones (producer's risk).

In general, such task cannot be solved adequately due to certain unreliability of primary self-checking results, and its fast penetration into the further control processes. And the main principle of any process of control is violated here, the principle that requires all objects of control to be of the higher class than the object of this control. This condition is fulfilled in CC StS with a developed property of slow degradation [3, 4], for which the methodology of organization of the self-checking program is chosen as a mean for identification of the current functional state of ECM.

Really, at the first stage of functional diagnosis an operable functionally complete "core" is searched by the procedure that is common for ECM: "promotion" with a declaration of its inoperability by the first failure to undergo a test check. I.e. the "core" with any detected defect is not allowed for further functioning. Fault-free "core" of the PC functional system can serve as rather reliable mean to control single functions form the remaining part of the system of commands. It is facilitated by the developed property of slow degradation of functions implying that for each function to be checked there is a part serving only its part of the equipment that can undergo rather complete sequence of test checks.

Due to the fact that it is not possible to avoid the issue of control reliability at all, we should analyze the terms of its improvement with the reduction of possible consequences in further processes. To do it we need an adequate model of test control process that describes elementary control operations and their structures in relation to the maintenance of the required reliability level.

Let us consider the process of control of an ad hoc command ϑ as the function of the system of commands θ of the digital computer (DC) installed on the self-checking section to solve the alternative

$$\vartheta \in \rho_\phi^F \mid \vartheta \in \overline{\rho}_\phi^F, \quad (4)$$

that in reality transforms into the solution of alternative

$$\vartheta \in \tilde{\rho}^F \mid \vartheta \in \overline{\tilde{\rho}}^F \quad (5)$$

on the set P_F of variants of splitting (1).

Fault-free function of DC ϑ is defined in the finite discrete space of states S of DC, whose components are the cells of memory and general purpose registers taking various values within the limits of their capacity. It means that for any point S' of an arbitrary subset S_ϑ, $|S_\vartheta| \le |X'_\vartheta \cup X''_\vartheta|$, where $X'_\vartheta, X''_\vartheta$ is a set of input and output variables of command ϑ, there is $S'' \in S_\vartheta$, i.e. the following transformation takes place

$$\vartheta : S' \to S'' \quad (6)$$

Each pair (S', S'') can form the basis for a test check that together with the facility of control (OC) ϑ forms an operational system of control, if it has the means that can help to lead the computation process into the point $S' - a'_\vartheta$ (impact on the facility of control ϑ), as well as the means a''_ϑ to estimate the fact

$$\vartheta(S') = S'', \quad (7)$$

i.e. the reaction of the facility of control to the given impact. a'_ϑ adn a''_ϑ are customary to play the role of means of control (MC). In general the test a_ϑ has the following form

$$a_\vartheta = a'_\vartheta(\hat{\rho}^F)\vartheta a''_\vartheta(\hat{\rho}^F) = \\ = \vartheta \notin \tilde{\rho}^F \mid (\vartheta \in \tilde{\rho}^F \mid \vartheta \notin \tilde{\rho}^F) \mid \hat{\rho}^F \cup \vartheta \qquad (8)$$

where $\hat{\rho}^F$ is the state of identification process $\tilde{\rho}^F$ before the test a_ϑ

$$\hat{\rho}^F \subseteq \tilde{\rho}^F. \qquad (9)$$

The result of the process of control of ϑ by test (8) can be the assignment of ϑ to the class $\overline{\tilde{\rho}}^F$ with a failure to undergo the test by feature (7), uncertainty ($\vartheta \in \tilde{\rho}^F \mid \vartheta \notin \tilde{\rho}^F$), if the process of control of ϑ shall be followed by further tests of type (8), or the assignment of ϑ to the class $\tilde{\rho}^F$ and the linking of this function with an identified part of f-state of $\tilde{\rho}^F$, if this test was final one within the process of control of ϑ (Fig. 1).

Despite there are only two outcomes of each separate test check, there are much more internal cases occurring within the process of control (Fig. 2). Let us analyze situations 1-15 that are connected with: – with the reliability of determination of an operable "core" that was taken as initial at the beginning, but then as the current identified part of f-state

$$\hat{\rho}^F := \rho^F_{\text{яη}}. \qquad (2.10)$$

Two variants are possible:

$$\hat{\rho}^F \subset \rho^F_\phi \qquad (2.11)$$

and

$$\hat{\rho}^F \not\subset \rho^F_\phi; \qquad (2.12)$$

- with the reliability of determination of S' initial data predefined by a test check. For case (2.11) the following expression is inevitable

$$a'_\vartheta(\hat{\rho}^F) : \tilde{S}' = S', \qquad (2.13)$$

where $\tilde{S}'$ is an actual result of the execution of part of test a'_ϑ formed on the basis of subset of commands $\tilde{\rho}^F$. For case (2.12) due to test imperfection in addition to the result

$$a'_\vartheta(\hat{\rho}^F) : \tilde{S}' \neq S' \qquad (2.14)$$

the result (2.13) is possible;

- with the uncertainty of state of the object of control ϑ, whose reactions to the initial data S', can be

$$a'_\vartheta(\tilde{S}') : \tilde{S}'' = S'', \qquad (2.15)$$

5 cases in total (1, 2, 4, 5, 8), as well as

$$a'_\vartheta(\tilde{S}') : \tilde{S}'' \neq S'', \qquad (2.16)$$

4 cases (3, 6, 7, 9), where $\tilde{S}''$ is an actual result of command ϑ;

- with the reliability of estimation of the results (2.15), (2.16) by the sequence of commands $a''_\vartheta(\hat{\rho}^F)$ of a test check: N (norm) for 8 variants (1, 2, 4, 6, 8, 10, 12, 14), $\overline{N}$ (no-norm) for 7 variants (3, 5, 7, 9, 11, 13, 15).

Norm situations are split into two groups. The first group (1, 4, 10) corresponds to the case $\vartheta \in \rho^F_f$. They are unified by the lack of growth of category II risk, as a fault-free command is identified as fault-free. The second group (2, 6, 8, 12, 14) corresponds to the case $\vartheta \notin \rho^F_f$ and by confirming the norm it facilitates the growth of category I risk.

No-norm situations are split into two groups as well. The first group (3, 7, 9, 13, 15) corresponds to the case $\vartheta \notin \rho^F_f$. They are unified by the lack of growth of category I risk, as a faulty command is identified as faulty. The second group corresponds to the case $\vartheta \in \rho^F_f$ and by confirming the no-norm it facilitates the growth of category II risk.

Conclusion

Therefore, getting the norm of a single test does not guarantee there is no risk of category I, that explains the common practice of check of each function of the command system by a sufficient sequence of test checks. And the risk of category II does not grow. As norm situations are just a part of whole group of cases 1-15, we can state that risk of category I is getting lower in the sequence of various test checks passing by norm. It is explained by the fact that with each new test, the next variant of the equipment functioning is checked, and the number of unchecked variants is reduced. In case check of all variants of risk of category I after the norm of the last of them is excluded. However, limitation of duration of the check will not bring it to such situation.

Though it was noted above, the risk of category I not eliminated causes the risk of category II in form of a negative result of test of the function under checking under its norm. In this case the terms of f-diagnosis are getting worse. Based on situation 5 of the test outcome, the case could be improved by repeating a test (S', S''), using other commands from the scope of $\tilde{\rho}^F$. A negative result shall confirm the failure of function ϑ, and a positive result will help to pass to a new functional "core".

A model of test check of f-diagnosis will assist to form the strategy of how to develop this process important to CC StS:

1) special attention should be paid to the identification of an operable "core", as at this stage the risk of category I is being originated, serving as a source of category II risk as well;

2) the remaining part of CC functions should be diagnosed one by one as in computing environment with a developed property of slow degradation of functions;

3) extending sequence of test checks for each CC function reduces risk of category I, but at the same time the time spent to control is growing, and it is deficit for a pre-staged self-checking, that is also aimed at the adjustment to the current f-state;

4) to reduce risk of category II, in case of negative results of tests, they should be continued using the same initial data, but another software implementation;

5) substantiation of the duration of testing of each function of CC requires the development of special procedure.

References

1. Zarubsky V.G. Issues of the development of advanced integrated security systems conforming the requirements of improved survivability, based on structurally stable control computers. Reporter of the Perm Institute of FSIN of Russia. Issue 1 (5)/ 2012. P 4-9.

2. Zarubsky V.G., Rybakov A.P. A mathematical model of adjustment of the integrated system control computer to the current functional state. Reporter of the Voronezh Institute of MIA of Russia. Issue 1/2012. P. 170-178.

3. Kharitonov V.A. Foundations of survivability of functionally redundant systems. SPb.: SPIIRAN, 1993. – 60 p.

4. Tyurin S.F. Synthesis of digital equipment adjusted to failures with a redundancy of basic functions / Devices and systems. Operation, control, diagnostics. Issue 1/ 1999. P 36-39.

About the authors

Vladimir G. Zarubsky, PhD Engineering, Associate Professor of the chair, Perm Institute of FSIN of Russia, Perm, Russia, e-mail: volen3030@rambler.ru

Receive on 10.03.2016

Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2640-2016-16-3-39-46*

Estimation of risks related to stop signal passed by shunting loco or passenger train[1]

Igor B. Shubinsky, *JSC IBTrans, Moscow, Russia, e-mail: igor-shubinsky@yandex.ru*
Alexey M. Zamyshlyaev, *JSC NIIAS, Moscow, Russia, e-mail: A.Zamyshlaev@vniias.ru*
Alexey N. Ignatov, *Moscow Aviation Institute, Moscow, Russia, e-mail: alexei.ignatov1@gmail.com*
Yury S. Kan, *Moscow Aviation Institute, faculty of Application mathematics and physics, Moscow, Russia, e-mail: yu_kan@mail.ru*
Andrey I. Kibzun, *Moscow Aviation Institute, Head of Chair, Moscow, Russia, e-mail: kibzun@mail.ru*
Evgeny N. Platonov, *Moscow Aviation Institute, faculty of Application mathematics and physics, Moscow, Russia, e-mail: en.platonov@gmail.com*


Igor B. Shubinsky


Alexey M. Zamyshlyaev


Alexey N. Ignatov


Yury S. Kan


Andrey I. Kibzun


Evgeny N. Platonov

Purpose *is to develop a procedure for estimating risks that occur as the result of a signal passed at danger (SPAD) by a shunting or train locomotive, as well as to develop recommendations for reducing risks of train collisions when performing shunting movement at a station.* **Methods.** *In oder to achieve the stated purpose, it is necessary to define the average number of points burst open by shunting locomotives without derailment, as well the average number of derailments of shunting locomotives per year. The availabile statistics are used to calculate the average amount of damage from one collision, from a point burst open without subsequent derailment, as well as a point burst open with subsequent derailment. To calculate the average number of damage as the result of a certain injury caused by collision, different types of injuries are considered. Injuries are classified by the level of consequences that are calculated in money terms using a minimum wage. To consider the variability in choosing a route, as well as to obtain the probability of a passenger train collision when passing through a station, the formula of total probability is used. To obtain the probabiity of at least one collision per year, the formula of multiplication of probability is used. To obtain the average number of points burst open and derailments, it is necessary to define the total number of points that are crossed by shunting locomotives at a station per point, the formula of multiplication of probability is used. To define the level of risk caused by the respective unfavorable event, it is necessary to construct risk matrices to define whether there is a necessity in immediate actions to reduce a risk level.* **Results.** *We have studied the task of calculation of unfavorable events caused by stop signal violation by a passenger train or a shunting locomotive. It provides the formulas used to calculate the probability of at least one collision of a passenger train at a station per year, the average number of points burst open by a shunting locomotive without subsequent derailment, as well as the average number of derailments per year. It also contains the formulas used to calculate the average damage from unfavorable events. Risk matrices for all unfavorable events have been constructed. The article gives the example of application of the obtained results which is based on hypothetical data, real data and expert analysis.* **Conclusion.** *Using the developed procedure we demonstrated its practical functionality. It was obtained that for the set of input data which were analyzed, there should not be any measures taken to reduce risks occurred as the result of points burst open and derailments at the station under consideration. At the same time the collision risk is in the orange area – the area of undesirable risks, and therefore, the measures on risk reduction should be taken. And a quantitative value of the risk occurred as the result of points burst open turns out to be higher than that of the collision risk. The matter is that in case of collision JSC RZD bears additional reputational expenses, doubled by the fact that a derailment occurs at a station with large numbers of people.*

Keywords: *probability of train collision, bursting open of point, derailment, damage, risk matrix.*

Citation format*: Shubinsky I.B., Zamyshlyaev A.M., Ignatov A.N., Kan Y.S., Kibzun A.I., Platonov E.N. Estimation of risks related to SPAD by shunting loco or passenger trian[1] // Dependability. 2016. No.3. P. 39-46. DOI: 10.21683/1729-2640-2016-16-3-39-46*

[1] The article was prepared with the support of the Russian science foundation (project No.16-11-00062)

Introduction

In case of signal violation by a shunting locomotive several unfavorable events are possible: the collision of a shuntng locomotive with a passanger or freight train, bursting open of a point without a derailment of a shunting locomotive, derailment of a shunting locomotive. Each of these events occurs with a certain rate or probability. And each of these events is specified by a certain damage. That is why it is very important to perform quantitative estimation of risks to maintain their tolerable level [1].

Paper [2] describes the calculation of probability of a side collision of a shunting locomotive with a passenger train, when one of the trains passes a signal at danger on route of a passenger train, where a route is a set of points that are crossed by a passenger train when passing through a station. Isolated switch is a switch at which there could be no collision caused by a signal violation, non-isolated switch is a switch where there could be a collision. However, when passing through a station, a passenger train has several possible routes thay are used with a certain rate.

In this paper the formula of total probability is used to consider the variability in choosing a route, as well as to obtain the probability of at least one passenger train collision when passing through a station. To obtain the probability of at least one collision per year, the formula of multiplication of probability is used. To obtain the average number of points burst open and derailments, it is necessary to define the total number of points that are crossed by shunting locomotives at a station per year, and to define the probability of bursting open of a point and derailment at one crossing of a switch, the formula of multiplication of probability is used.

We consider the accidents at a railway station and it means that at the collision of a passenger train with a shunting locomotive there may be fatalities at a station itself, as well as on a passenger train. That is why in this paper the average damage from one collision of a passenger train with a shunting locomotive is composed of the damage from the defects of railway infrastructure: railway bed, cars and etc., and of the damage from the consequences of fatalities that is quantitatively expressed based on [1]. Damage from bursting open of points and derailments is formed based on the consequences of defects of railway infrastructure, and fatalities here is unlikely, as shunting works are carried out at a low speed. Risk matrices are constructed based on the approach described in [1].

Calculation of probability of at least one collision of a shunting locomotive with a passenger train per year

According to the schedule received from AS Express for a time period under consideration (a year), let us assign the numbers for passenger trains crossing a station under consideration on a first-come basis, i.e. the first coming train is given number 1, the second one is 2, etc. Let us consider the i-th passenger train from this row.

Let A_i be a collision of a passenger train with number i when it is passing through a station, and $P(A_i \mid R_k)$ be a probability of the collision of a passenger train with number i when it is crossing a station by routeR_k, where k=1, …, K, and K is the total number of possible routs for train with number i. Then a probability of the collision of a passenger train with number i when it is passing through a station is [2]

$$P(A_i) = \sum_{k=1}^{K} P(A_i \mid R_k) P(R_k),$$

where $P(R_k)$ is a probability of route R_k that is defined by formula

$$P(R_k) = \frac{m_{R_k}}{n},$$

where m_{R_k} is the number of passenger trains with number i passed by route R_k, and n is the totatl number of passenger trains with number i passed through a station during the period of observation. If there are no data about last passings of a passenger train with number i through the station, and the monitoring of traffic is not possible, then the probability of use of all routes can be equally probable, i.e.

$$P(R_k) = \frac{1}{K}.$$

Probability $P(A_i \mid R_k)$ is defined using the following formula derived in [2],

$$P(A_i \mid R_k) = P(A_{k:1}) + (1 - P(A_{k:1})) \cdot P(A_{k:2}) + \\ + (1 - P(A_{k:1})) \cdot (1 - P(A_{k:2})) \cdot P(A_{k:3}) + ...,$$

where $P(A_{k:j})$ is a probability of collision of the train with number i, passing through the station by route R_k, on the j-th point. Whereas $P(A_{k:j})$ is calculated by formula

$$P(A_{k:j}) = \left(\lambda_{sh} \left(\frac{l_p}{v_p} + \frac{l_{sh}}{v_{sh}} \right) (P_{sh}(1 + P_p) + P_p) + \right. \\ \left. + \lambda_s P_p \tau_s + \lambda_{sh} P_{sh} P_{ps} \tau_{ps} \right) \cdot k_s,$$

where k_s is the coefficient of a switch's isolation (1 if a switch is non-isolated, and 0 if a switch is isolated);

λ_{sh} is the rate of shunting locomotives passing through the j-th switch in the direction under which a side collision is possible (for simplicity we can assume that $\lambda_{sh} = \tilde{\lambda}_{sh} / 4$, where $\tilde{\lambda}_{sh}$ is the total rate of shunting locomotives passing through the j-th switch in all directions);

$\lambda_s$is the rate of shunting groups that stop at the j-th switch, which did not violate safety when passing through the switch;

τ_s is the average time of a shunting group being at the j-th switch, which did not violate safety when passing through a switch, provided there was a stop at a switch;

l_p is the average length of a passenger train;

v_p is the average speed of a passenger train passing through a station;

l_{ch} is the average length of a shunting group;

v_{sh} is the average speed of a shunting group passing through a station;

P_p is the probability of signal violation by a passenger train;

P_{ps} is the probability of stop of a passenger train at a switch;

τ_{ps} is the average time of standing of a passenger train at a switch;

P_{sh} is the probability of signal violation by a shunting locomotive calculated by formula [2]

$$P_{\text{sh}} = P_{two} \cdot P_{sh(two)} + \left(1 - P_{two}\right) \cdot P_{sh(one)},$$

where P_{two} is the probability of assigning a shunting locomotive crew to a driver and his assistant;

$P_{sh(two)}$ is the probability of signal violation by a shunting locomotive driver when working with an assistant driver;

$P_{sh(one)}$ is the probability of signal violation by a shunting locomotive driver when working without an assistant driver ("driver-only operation").

Let I of trains pass through a station per year in different directions. Let us consider the i-th train from this row, i=1, …, I. If it is coordinated with probability $P(A_i)$ of a collision when passing through a station, the probability of collision of at least one train from I trains is [2]

$$P(A_{year}) = P(A_1 + A_2 + \ldots + A_I) = 1 - \prod_{i=1}^{I}(1 - P(A_i)). \quad (1)$$

Calculation of the average number of points burst and derailments of a shunting locomotive per year

Let L be the total number of locomotives working at a station, and N_l is the average number of switches crossed per hour by a shunting locomotive with number l. Then the total number N_{year} of switches that are crossed by shunting locomotives at a station is calculated by formula

$$N_{year} = 365 \cdot 24 \cdot \sum_{l=1}^{L} N_l. \quad (2)$$

Let us consider several accidents: A_{sh} is SPAD by a shunting group, A_{bop} is a point burst open by a shunting group after signal violation, A_{drl} is derailment after a point burst open. Let the following probabilities be known: the probability of a point burst open after SPAD P_{bop} and the probability of derailment after a point burst open P_{drl}. Then the probability of a point burst open with a subsequent derailment of the rolling stock is defined by formula of multiplication of probabilities [3]

$$P_{bop(drl)} = P(A_{sh} A_{bop} A_{drl}) = P_{sh} P_{bop} P_{drl}, \quad (3)$$

and the probability of a point burst open without a subsequent derailment of the rolling stock is defined using the same formula

$$P_{bop(no\ drl)} = P(A_{sh} A_{bop} \bar{A}_{drl}) = P_{sh} P_{bop} (1 - P_{drl}). \quad (4)$$

Due to the fact that at each switch crossing, derailment or bursting open of a point may occur, the number of points burst open without a subsequent derailment is a random variable with a binomial distribution with parameters N_{year} and $P_{bop(no\ drl)}$, and the number of derailed trains is a random variable with a binomial distribution with parameters N_{year} and $P_{bop(drl)}$. That is why the average number of points burst open without a subsequent derailment is defined by multiplicating the number of cheks by the number of "successes", i.e. is defined by formula [3]

$$\bar{N}_{year}^{bop} = N_{year} \cdot P_{bop(no\ drl)}, \quad (5)$$

and the average number of points burst open with a subsequent derailment is defined by formula

$$\bar{N}_{year}^{drl} = N_{year} \cdot P_{bop(drl)}. \quad (6)$$

Determination of the average damage from unfavorable events

Let us firstly consider the damage that occur after derailment. Damage caused by the derailment at the station consists of four parts. The first part is a material damage that occurs as the result of the destruction of cars, tracks, station infrastructure, freight, etc. These types of damage are recorded in the protocols of traffic accidents and they can be calculated as average variables. The second part of damage is a damage connected with possible fatalities or injuries.

Let there be M_{col} of the collision protocols. Then the average material damage calculated by all accidents is defined by formula

$$\bar{C}_1 = \frac{\sum_{i=1}^{M_{col}} C_{col}^i}{M_{col}}, \quad (7)$$

where C_{col}^i is the material damage caused by the collision recorded in the i-th protocol.

Let us define the average damage connected with possible fatalities or injuries. We shall break all injuries occurred in case of an accident, into classes: moderate injuries; serious injuries; fatalities. Let N_{fat}^i is the number of fatalities in the i-th collision, N_{si}^i is the number of people with serious injuries in the i-th collision, N_{mi}^i is the number of people with moderate injuries in the i-th collision, C_{mi} is the damage caused by one moderate injury, C_{si} is the damage caused by one serious injury, C_{fat} is the damage caused by one fatality. Therefore, average damage caused by probable fatalities or injuries at one collision is

$$\bar{C}_2 = C_{fat} \frac{\sum_{i=1}^{M_{col}} N_{fat}^i}{M_{col}} + C_{si} \frac{\sum_{i=1}^{M_{col}} N_{si}^i}{M_{col}} + C_{mi} \frac{\sum_{i=1}^{M_{col}} N_{mi}^i}{M_{col}}.$$

Variables C_{mi}, C_{si}, C_{fat} shall be found based on [1]. A fatality is equated with material damage that is 5000 of minimum wage, a serious injury is equated with material damage that is 1000 of minimum wage, a moderate injury is equated with material damage that is 500 of minimum wage. From January 1, 2016 minimum wage is 6204 RUB. [4]. Therefore,

C_{mi}=6,204·500=3102 kRUB.,

C_{si}=6,204·1000=6204 kRUB.,

C_{fat}=6,204·5000=31020 kRUB.

Therefore,

$$\overline{C}_2 = 3102 \cdot \frac{\sum_{i=1}^{M_{col}} N_{mi}^i}{M_{col}} + 6204 \cdot \frac{\sum_{i=1}^{M_{col}} N_{si}^i}{M_{col}} + 31020 \cdot \frac{\sum_{i=1}^{M_{col}} N_{fat}^i}{M_{col}} =$$

$$= \frac{1}{M_{col}} \left(3102 \cdot \sum_{i=1}^{M_{col}} N_{mi}^i + 6204 \cdot \sum_{i=1}^{M_{col}} N_{si}^i + 31020 \cdot \sum_{i=1}^{M_{col}} N_{fat}^i \right). \quad (8)$$

As the total damage caused by collisions $\overline{C}_{col}$ is composed of the material damage and the damage from injuries then

$$\overline{C}_{col} = \overline{C}_1 + \overline{C}_2 = \frac{\sum_{i=1}^{M_{col}} C_{col}^i}{M_{col}} +$$

$$+ \frac{1}{M_{col}} \left(3102 \cdot \sum_{i=1}^{M_{col}} N_{mi}^i + 6204 \cdot \sum_{i=1}^{M_{col}} N_{si}^i + 31020 \cdot \sum_{i=1}^{M_{col}} N_{fat}^i \right). \quad (9)$$

Let us now consider the damage that occurs in case of bursting open of points and derailments. Let there be M_{bop} of protocols of bursting open of points without derailments that fixed certain damage. Then the average material damage calculated by all accidents is defined by formula

$$\overline{C}_{bop} = \frac{\sum_{i=1}^{M_{bop}} C_{bop}^i}{M_{bop}}, \quad (10)$$

where C_{bop}^i is the material damage caused by bursting open of a point fixed in the *i*-th protocol. Similarly, if there are M_{drl} protocols of bursting open of points with a subsequent derailment, that fixed certain damage, the average material damage calculated by all accidents is defined by formula

$$\overline{C}_{drl} = \frac{\sum_{i=1}^{M_{drl}} C_{drl}^i}{M_{drl}}, \quad (11)$$

where C_{drl}^i is the material damage caused by bursting with derailment fixed in the *i*-th protocol.

Estimating the risk value

To define the level of risk after the analysis of frequencies and analysis of consequences, quantitative and qualitative estimation is performed. Generally, according to [1] the risk is a certain combination of two values – the probability (or frequency) of an undesirable event P(A) and its consequences C(A). In this paper we shall consider a quantitative value of risk as the multiplication of probability (frequency) by the damage. Thus, the risk caused by collisions as the result of signal violation by one of the trains is defined by formula

$$R_{col} = P(A_{year}) \cdot \overline{C}_{col}, \quad (12)$$

where $P(A_{year})$ is calculated by formula (1), and $\overline{C}_{col}$ is calculated by formula (9) respectively. Risks caused by bursting open of a point without a subsequent derailment are defined by formulas

$$R_{bop} = \overline{N}_{year}^{bop} \cdot \overline{C}_{bop}, \quad (13)$$

$$R_{drl} = \overline{N}_{year}^{drl} \cdot \overline{C}_{drl}, \quad (14)$$

where $\overline{N}_{year}^{bop}$, $\overline{N}_{year}^{drl}$, $\overline{C}_{bop}$, $\overline{C}_{drl}$ are defined by formulas (5), (6), (10), (11) respectively.

Constructing risk matrices

The results of risk estimation can be represented using a risk matrix which has a form of cell table that represents the combination of the frequency of an undesirable event and the severity of its consequences (figure 1), and makes it possible to provide authorized decision-makers with visual information on risk levels for event in question. The form (parameters) of a matrix depends on the field of its application.

A risk matrix is constructed as follows:

— on the vertical axis, the frequencies (probabilities) of the event are calculated. They are represented in accordance with an accepted (normally, logarithmic) scale of frequencies;

— on the horizontal axis, the degrees of the event's consequences are calculated. They are represented in accordance with an accepted (normally, logarithmic) scale of severity of consequences;

— the risk level for each matrix cell is defined and rated.

The main problem when constructing the risk matrices is the correct definition of boundaries for the matrix cells. One and the same cell contains the points with different values of risk, and some points refer, for instance, to the field of "tolerable" risk, and some points refer to the field of "undesirable". In the most unfavorable case, a cell may be divided into two segments of equal space, this preventing us from precisely defining what range of risk values most of points allocated inside this cell belong to.

Probability levels	Risk levels			
Frequent	Tolerable	Undesirable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Undesirable	Intolerable
Occasional	Tolerable	Tolerable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Incredible	Negligible	Negligible	Tolerable	Undesirable
	Insignificant	Marginal	Critical	Catastrophic
	Level of severity of consequences			

Fig. 1. Form of risk matrix

Article [5] offers a procedure to define the boundaries for the cells of a risk matrix, which helps to solve this problem.

Standard [1] recommends a scale with 6 levels (gradations) as a typical probability scale. A scale with 4 levels (gradations) is recommended as a typical scale of consequences.

Let us choose the boundaries for the risk matrix cells in accordance with approach described in [1].

Minimum and maximum values of the probability are assumed 0 and 1 from the condition of classifying an accident event. The most unfavorable event (frequent) is set by a boundary 0,5, i.e. a traffic accident rather occurs than does not occur. Boundaries for an improbable and remote event are chosen in the logarithmic scale in such a way, so that they are an order less, i.e. 0,05 and 0,005 respectively. Value 0,05 is the most common for the probability of a random event. Intermediary boundaries between already set values are chosen in the logarithmic scale in such a way, so that these cells are nearly equal. That is why the boundary that indicates a transition from a probable event to an occasional event is set as 0,15 (approx. three times less than 0,5 and three times more than 0,05). The same is for the boundary of transition form a remote event to an improbable event.

Levels of probabilities for collisions are listed in table 1.

If instead of the probability of an undesired event we estimate the average frequency of a dangerous case, Table A.5 in [1] offers the following frequency levels. For our case this variant of choosing the level is often justified as well.

Boundaries for the severity of consequences shall be chosen based on the damage that will be caused by a fatality. According to Table 2 of GOST R 54505, catastrophic risk occurs in case of one or more fatalities, which is 5000 of minimum wage = 30000 kRUB. Two other boundaries are chosen in the logarithmic scale and differ by one and two orders, respectively (table 3).

Table 1 – Levels of probabilities for collisions

Probability levels	Probability of events per year, *P(A)*	Description
Frequent	$P(A)>0,5$	Hazard is permanent
Probable	$0,15\leq P(A)<0,5$	Frequent occurrence of a dangerous event is expected
Occasional	$0,05\leq P(A)<0,15$	Repeated occurrence of a hazardous event is expected
Remote	$0,015\leq P(A)<0,05$	There is a probability that an event will sometimes occur throughout an object's life cycle
Improbable	$0,005\leq P(A)<0,015$	A hazardous event is assumed to occur in exceptional case
Incredible	$P(A)\leq 0,005$	A hazardous event is assumed not to occur

Table 2 – Levels of frequencies

Levels of frequency	Value, $P^*(A)$, 1/per year	Description
Frequent	$P^*(A)\geq 100$	Hazard is permanent
Probable	$40\leq P^*(A)<100$	Frequent occurrence of a hazardous event is expected
Occasional	$15\leq P^*(A)<40$	Repeated occurrence of a hazardous event is expected
Remote	$6\leq P^*(A)<15$	There is a probability that an event will sometimes occur throughout an object's life cycle
Improbable	$2\leq P^*(A)<6$	A hazardous event is assumed to occur in exceptional case
Incredible	$P^*(A)<2$	A hazardous event is assumed not to occur

Table 3 – Levels of severity of consequences

Levels			
Insignificant	**Marginal**	**Critical**	**Catastrophic**
less than 300 kRUB.	from 300 to 3000 kRUB.	from 3000 to 30000 kRUB.	More than 30000 kRUB.

Let us rate the matrix cells. In this regard let us multiple the upper values of frequency and severity of consequences, corresponding to each cell, and, depending on the result, let us assign a category to it (figures 2 and 3).

Example

According to the data of the Automated System of Traffic Safety (ASRB) for the period 2011-2015 there were 64 traffic accidents of collision, with recorded damage (its amounts are listed in Table 4), as well as 78 traffic accidents with no fixed damage.

According to formula (7) we obtain

$$\overline{C}_1 = \frac{\sum_{i=1}^{64} C_{col}^i + \sum_{i=65}^{142} 0}{78+64} \approx 488 \text{ kRUB.}$$

Let $\sum_{i=1}^{142} N_{mi}^i = 23, \sum_{i=1}^{142} N_{si}^i = 10, \sum_{i=1}^{142} N_{fat}^i = 1$, thus, according to formula (8) we obtain

$$\overline{C}_h = \frac{1}{142}(3102 \cdot 23 + 6204 \cdot 10 + 31020 \cdot 1) = 1158 \text{ kRUB.}$$

Therefore, the total damage from a collision calculated by formula (9) is

$$\overline{C}_{col} = \overline{C}_1 + \overline{C}_2 = 488 + 1158 = 1646 \text{ kRUB.}$$

According to the data of the Automated System of Traffic Safety (ASRB) for the period 2013-2015 there were 17 burstings open of a point with fixed damage listed in Table 5.

Using formula (10) we obtain

$$\overline{C}_{bop} = \frac{\sum_{i=1}^{17} C_{bop}^i}{17} = 78 \text{ kRUB.}$$

According to the data of the Automated System of Traffic Safety (ASRB) for the period 2013-2015 there were 221 burstings open of a point with a subsequent derailment with the damage listed in Table 6.

Using formula (11) we obtain

$$\overline{C}_{drl} = \frac{\sum_{i=1}^{221} C_{drl}^i}{221} = 225 \text{ kRUB}$$

Like in work [2] let there be two locomotives working at a station, each of them crosses 36 switches on the average

	Probability levels	Risk levels			
1	Frequent	300	3000	30000	
0,5	Probable	150	1500	15000	
0,15	Occasional	45	450	4500	
0,05	Remote	15	150	1500	
0,015	Improbable	4,5	45	450	
0,005	Incredible	1,5	15	150	
0		Insignificant	Marginal	Critical	Catastrophic
		300 3000 30000 Level of severity of consequences			

Fig. 2. Risk matrix for collisions

	Levels of frequencies, 1/per year	Risk levels			
100	Frequent				
40	Probable	30000	300000	3000000	
15	Occasional	12000	120000	1200000	
6	Remote	4500	45000	450000	
2	Improbable	1800	18000	180000	
0	Incredible	600	6000	60000	
		Insignificant	Marginal	Critical	Catastrophic
		300 3000 30000 Level of severity of consequences			

Fig. 3. Risk matrix for derailments and bursting open of a point

per hour, and the probability of signal violation by a shunting locomotive is $P_{sh}=1,4\cdot10^{-4}$, the probability of a point burst open is equal to the probability of a derailment after a point burst open $P_{drl}=P_{bop}=0,1$, then the probability of a point burst open with subsequent derailment is calculated by formula (3)

$$P_{bop(drl)} = P_{sh}P_{bop}P_{drl} = 1,4\cdot10^{-4}\cdot0,1\cdot0,1 = 1,4\cdot10^{-6},$$

And the probability of a point burst open without subsequent derailment is calculated by formula (4)

$$P_{bop(no\ drl)} = P_{sh}P_{bop}(1-P_{drl}) =$$

$$= 1,4\cdot10^{-4}\cdot0,1\cdot(1-0,1) = 1,26\cdot10^{-5}.$$

Table 4 – Damage from collisions, kRUB. (per each accident)

207,67	19,56	440	156,81	65,17	21,8	76,7	54,1	35,05	445,92
61,31	5,11	1717	149,75	378	65,12	14,46	422,28	74,5	2264,62
226,3	1,3	326,7	645,25	57,86	1067,27	43,64	0,2	3,63	226,28
4,5	1,02	1082,27	1	1,35	21	195,75	923,35	1	2,45
9,44	11,4	800	41,06	2	2,04	4,49	173	19,35	9,9
66,9	393,4	0,9	2332,72	115,87	5,9	5,9	263	85,7	1612
22	42,7	654,38	51139						

Table 5 – Damage from burstings open of a point, kRUB. (per each accident)

8,49	110,88	49,04	1	18,78	102,39	64,39	85,3	21,61	174,11
4,25	389,48	132,01	91,01	2,57	72,04	0,35			

Table 6 – Damage from derailments, kRUB (per each accident)

79	14,8	422,3	158,03	7,66	28,83	3	215	503,67	9,13
328,07	3,86	133,18	3	20,31	573,44	363,42	263,69	261,9	251,7
247,26	27,05	34	180,75	219,6	322,76	262,5	5123,35	266,45	2027,08
59,75	281,74	228,38	193,5	474,3	75,5	33,93	52,9	82,35	38,96
29,13	1,44	68,07	1,38	1	150,62	970,07	33,3	15	117,3
3,2	375,95	200	192,82	45,64	45,3	349,47	28,31	78,9	33,3
579,26	338,46	479,17	13	43,37	152	525,22	920,84	203,77	2411,23
2	88,52	109,31	408,65	1007,25	1,99	10	608,29	137,7	113,24
7	16,63	11,7	102,78	15	15,89	23,6	25	18,97	34
48,74	48,69	2	15	309,05	223,68	66,28	993,66	42,76	30
155,06	163,25	56,06	43,48	73,67	19,28	36,6	67,9	46	112
71,65	149,05	76,7	33,13	12,34	491,8	1460	32,25	220,61	3,2
9,37	19,2	118,53	703,44	72	124,52	7,73	146,78	188,04	150,47
142,3	179,12	306,86	3,6	717,69	29,5	149,7	254,01	94,77	2
34	309,21	116	10	30	93,9	110	40,77	103,85	1147,05
483,05	89,73	12	340	34	420,16	3,6	24	6,49	139,53
899,9	1	31,67	55,27	22,2	106,76	1,68	129,9	118,61	160
150,8	256,63	374,41	29,62	74,8	98,21	20	292,99	80,46	162,72
1446	544,06	37,56	1610,54	55,1	79,77	101	93,46	125	260,3
3,1	46	773,55	24,5	27,03	203	13,92	655,1	72,49	216
303,89	24,47	58,49	256	447,55	41,43	37,9	8,3	247,99	0,52
704,67	26,5	80,74	494,73	174,99	16,15	58,89	154,81	8,56	17,79
62,82									

The total number of switches crossed by shunting locomotives per year is calculated by formula (2)

$$N_{year} = 365 \cdot 24 \cdot \sum_{l=1}^{L} N_l = 365 \cdot 24 \cdot (36 + 36) = 630720.$$

Therefore, the average number of points burst open by formula (5) is

$$\overline{N}_{year}^{bop} = N_{year} \cdot P_{bop(no\ drl)} = 630720 \cdot 1,26 \cdot 10^{-5} = 7,947,$$

And the average number of points burst open with subsequent derailment by formula (6) is

$$\overline{N}_{year}^{drl} = N_{year} \cdot P_{bop(drl)} = 630720 \cdot 1,4 \cdot 10^{-6} = 0,883.$$

Using formula (1) let it be obtained that

$$P(A_{year}) = 0,3.$$

Let us define quantitative values of risks caused by all unfavorable events and the respective risk areas.

Risk caused by collisions is calculated by formula (12) and it is

$$R_{col} = P(A_{year}) \cdot \overline{C}_{col} = 0,3 \cdot 1646 = 493,8 \text{ kRUB}.$$

And we enter orange area – area of undesirable risk. Thus it is necessary to take measures to reduce risk. Among such measures there can be the installation of Shunting Automatic Cab Signalling (MALS system).

Risks caused by bursting open of points and derailments are calculated by formulas (13) and (14)

$$R_{bop} = \overline{N}_{year}^{bop} \cdot \overline{C}_{bop} = 7,947 \cdot 78 = 620 \text{ kRUB},$$

$$R_{drl} = \overline{N}_{year}^{drl} \cdot \overline{C}_{drl} = 0,883 \cdot 225 = 199 \text{ kRUB}.$$

And we enter green area – area of negligible risk. Therefore, no measures to reduce the risks caused by bursting open of points and derailments are required at this station. We shall note that the risk caused by bursting open of points is higher than the risk from derailments. Nevertheless, measures to reduce the risk from derailment are required, and measures to reduce the risk from bursting open of points are not required. The matter is that under the collision JSC RZD bears additional reputational expenses, doubled by the fact that a derailment occurs at a station with large numbers of people.

Conclusion

This paper describes the task of calculation of unfavorable events caused by SPAD by a passenger train or a shunting locomotive. It provides the formulas used to calculate the probability of at least one collision of a passenger train at a station per year, average number of points burst open by a shunting locomotive without a subsequent derailment, as well as the average number of derailments per year. It also contains the formulas used to calculate the average damage from unfavorable events. Risk matrices for all unfavorable events have been constructed. The article gives the example of application of the obtained results which is based on hypothetical data and expert analysis.

References

1. GOST R 54505-2011 Functional safety. Risk management on railway transport

2. Ignatov A.N., Kibzun A.I., Platonov E.N. Estimation of probability of train collision at railway stations based on the Poisson model // *Automatics and telemechanics*, 2016. No.11. (accepted for publication).

3. Kibzun A.I., Goryainova E.R., Naumov A.V. Theory of probability and mathematical statistics. Basic course with examples and tasks – M.: FIZMATLIT, 2014.

4. Article 1 of Federal Law of 14.12.2015 N 376-ФЗ

5. Novozhilov E.O. Guidelines for construction of a risk matrix // Dependability. 2015. No. 3(54), p. 73-86.

About the authors

Igor B. Shubinsky, Dr.Sci., professor, Director of CJSC IB Trans, Moscow, Russia, tel. +7 (495) 786-68-57, e-mail: igor-shubinsky@yandex.ru

Alexey M. Zamyshlyaev, Dr.Sci., Deputy director general of JSC NIIAS, Moscow, Russia, tel. +7 (495) 967-77-02, e-mail: A.Zamyshlaev@gismps.ru

Alexey N. Ignatov, Moscow Aviation Institute, postgraduate student, Moscow, Russia, tel. +7 906 059 50 00, alexei.ignatov1@gmail.com

Yury S. Kan, Doctor of Physical and Mathematical Sciences, professor, Moscow Aviation Institute, faculty of Application mathematics and physics, professor, Moscow, Russia, e-mail: yu_kan@mail.ru

Andrey I. Kibzun, Doctor of Physical and Mathematical Sciences, professor, Moscow Aviation Institute, Head of Chair, Moscow, Russia, e-mail: kibzun@mail.ru

Evgeny N. Platonov, Candidate of Physico-Mathematical Sciences, Associate professor, Moscow Aviation Institute, faculty of Application mathematics and physics, Moscow, Russia, e-mail: en.platonov@gmail.com

Receive on 02.02.2016

Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2640-2016-16-3-47-53*

Genesis of dependability of unique safety critical systems

Yury P. Pokhabov, *Joint Stock Company "NPO PM – Design Bureau" (JSC NPO PM MKB), e-mail: pokhabov_yury@mail.ru*
Oleg K. Valishevsky, *Joint Stock Company "Academician M.F. Reshetnev Information Satellite Systems" (JSC ISS), e-mail: valishevsky@iss-reshetnev.ru*

Yury P. Pokhabov

Oleg K. Valishevsky

Purpose. *This article offers to focus on the genesis of dependability of unique safety critical systems specified by low probability of failures, using the example of transformable structures of spacecrafts, in relation to which just the possibility of failures can question the reasonability of their creation. It describes the stage of the life cycle of unique mission critical systems at which the measures taken to improve reliability are the most effective, and the stages at which it is already late to take any measures at all.* **Methods.** *Neglecting the genesis of unique mission critical systems will inevitably lead to failures at the stage of operation, and the failures are caused by errors in design, engineering, modeling, as well as by different manufacturing deviations. In practice up to 80% of cases are predetermined before the start of operation – "at a drafting machine" and in manufacturing departments, when something was not thought through, taken into account and controlled, making an error or foozling. Reliability of future products depends on the quality of the decisions taken under development, which directly depend on the principles, rules and requirements used under design and engineering. These notions are interrelated, they have a concrete meaning. Principles are used to develop design solutions. Rules are intermedia between theory and practice, they often reflect the gained experience that should be considered in new developments to avoid repeating the errors. Reliability requirements at the stage of engineering are formed as the result of application of goal-oriented procedures and analyses, being established in graphic and text form in design documentation: in technical requirements and on a draft, as well as in technical specification. Satisfying these requirements is finally aimed at undoubted performance by a product of its functional tasks with predetermined reliability.* **Results.** *The aspects described in the article, separate the methods of reliability theory which are based on probabilistic and statistical models, with practical engineering methods aimed at the creation of reliable equipment. The field of reliability theory covers the study of behavior of finished products, proceeding from the information about mathematical models that consider stochastic parameters. Real objects in reliability theory are schematized to the models described by probabilistic dependences and having a sampling that can be used for statistical generalization. In practice though, engineers work having no statistics and concepts of probabilistic behavior of a future product, and the collection of methods and algorithms of its operation makes it possible to influence the reliability of real products.* **Conclusion.** *This paper shows that the stages of a life cycle of unique safety critical systems before the stage of operation are strictly differentiated by the efficiency of reliability measures. At each stage it is necessary to use certain reliability algorithms and methods that are specific to this particular stage, which may increase the effectiveness when solving the tasks of reliability of unique safety critical systems.*

Keywords: *unique safety critical systems, transformable structure, spacecraft, reliability, genesis, life cycle of products.*

Citation format*: Pokhabov Y.P., Valishevsky O.K. Genesis of dependability of unique safety critical systems // Dependability. 2016. No.3. P. 47-53. DOI: 10.21683/1729-2640-2016-16-3-47-53*

Introduction

When creating any technical product the first task is to achieve such output characteristics that a product is capable of performing. But this very achievement does not guarantee that products will always be manufactured serviceable, that they will not lose the functionality after being stored and transported, that they will perform the targets in full scope and will not operate less than it is predetermined.

Inevitable changes of possible states of products under the influence of external factors and internal chemical and physical processes may eventually reduce their output characteristics, as the result of which the expected efficiency may turn out to be unachieved.

Why is it possible? In most cases the modes and conditions of functioning are not properly estimated or considered. Unintentional wrong actions by personnel are not rare during manufacture and operation processes. Sometimes, constructive decisions go ahead of the production technological capabilities, or they are inadequate to the concepts of physical processes that take place under products' operation. In any of the cases the mentioned factors can lead to failures that may turn out to be accidents and catastrophes. If the social and economic losses suffered

by human society in case of products' failures, exceed the acceptable critical level, there is a need to ensure the reliability of these products.

For common equipment ensuring of reliability is normally a secondary task that is often solved as if by the way, because usually failures do not have any serious consequences. Reliability in this case is considered in the context of optimizing the financial costs and costs in public image. But there are technical objects that exclude any failures despite inevitable additional financial expenses on the prevention of such failures, because otherwise it may lead to far more losses at accidents. Examples of such objects are unique safety critical systems (USCS), in relation to which just the possibility of failures can question the reasonability of their creation. Here it is important to understand at which stage of the USCS life cycle the measures taken to improve reliability are the most effective, and at which stages it is already late to take any measures at all.

In this relation it is worth considering the genesis of USCS reliability on the example of transformable structures (TS), whose main task is to enable long functioning of spacecrafts in space environment by single actuation on orbit [1].

What happens to reliability at the stage of operation of transformable structures

According to GOST 25866-83 the operation of products generally includes use as intended, transportation, storage, maintenance and repair. For opening parts of TS, the operation can be arbitrarily limited by the period from the moment of transfer of a product for storage after factory acceptance and to the opening into operating configuration on low earth orbit. While being in operation TS passes the following stages of the life cycle: storage, transportation, maintenance, preparation for launch at a test range, flight within the scope of a rocket vehicle, placing into orbit, preparation for opening and opening into operating configuration [2].

Let us assume that at any moment of operation τ TS may suddenly fail, and it will not be possible to recover or repair it at subsequent moments of time. Let us define the probability $P_f(t)$, with which this structure will perform its functions within the period of operation up to the moment t. If we assume the TS operating capacity to be a sampling of sequential independent tests with probabilities $P_υ(\tau)$, then the probability of its functioning during the time period t will be:

$$P_f(t) = \prod_{\tau=1}^{t} P_υ(\tau). \quad (1)$$

From (1) it appears that in the course of time t the probability of TS functioning can increase, it can decrease, or hold constant on level 1.

Decrease $P_f(t)$ is the result of stochastic changes of the state of TS under the influence of external factors (overloads, impacts, jarring, vibrations, fluctuations of temperature, humidity, aggressive environments, etc.), as a consequence of implementation of the following processes:

– degradation of physical and mechanical properties of materials caused by wear, corrosion, deterioration, embrittlement, etc.;

– change of physical and mechanical properties of materials under the influence of freeze-thaw temperatures;

– non-convertible deformations and destructions (plastic deformations, crumbling of contact surfaces, creeping, fractures, etc.);

– deterioration of tribocoupling;

– expression of structural instabilities in form of displacement of fixed parts, loosening in screw joints, changes of freeplays in actuated parts, violation of adjustment, etc.

The next important aspect is solving the issue of initial level of P_0 at the moment that corresponds to the start of operation.

Let us consider the situation at the moment when TS is on hold being ready for operation, i.e. it has already had the full capability to show reliability properties, because the relative position, interrelation and interoperation of the elements inside TS has already been implemented (TS is ready for operation), and the relative position, interrelation and interoperation of TS in external environment and with other objects is provided and expected. This state of TS is a priori predetermined in engineering documentation (ED) by rated parameters μ_i and respective tolerances $\Delta\mu_i$. And the parameters are random variables (dependent or independent of time), that may change within the limits of nonrandom tolerances:

$$\Delta\mu_i = \mu_{i\max} - \mu_{i\min} \forall i = \overline{(1,n)}. \quad (2)$$

Parameters μ_i set:

$$\mu_i \in R^N. \quad (3)$$

Number of equations N of set (3) corresponds to the number of parameters of the structure, and with the rise of its detalization it may grow, and according to (2) the parameters will always be within the predetermined range:

$$\mu_{i\min} \le \mu_i \le \mu_{i\max}. \quad (4)$$

If there are no bad errors in ED, and therefore it is not necessary to modify ED at the stage of manufacture, it is considered to be a stationary stochastic model of the object represented in a draft and text form [3]. If a random value of parameter $\mu_i(t)$, predetermined in a stationary model of TS, stays within tolerance $\Delta\mu_i$, TS is considered to be fit for operation. Therefore, the object's readiness for operation is determined by the fulfillment of all ED requirements related to predetermined parameters μ_i, and its performance capability is determined by a random entering the tolerance limits (4). If parameters μ_i go out of the tolerance range it is qualified as a failure. Besides, the possibility of a failure lays in the principle of use of

a stationary stochastic model of the object. Due to the fact that the number of equations (3) under the development of ED is always finite with an infinite number of random values, there is a risk of non-consideration of any failure factors.

Thus, before the operation there is always a risk with probability γ, that not all parameters μ_i under engineering will be properly considered, and those parameters predetermined in ED will be within the respective tolerance under operation $\Delta\mu_i$.

Let us assume that all TS parameters are independent in terms of reliability, and non-consideration of any of them, or going out of the range of tolerance will lead to a parameter's failure. The event specifying the readiness of TS to perform without failures shall be indicated as *H*, and the event specifying the occurrence of a failure in case realization of risk with probability γ, shall be indicated as *A*, then:

$$P(H)+P(A)=1,\ P(A)=\gamma,$$
$$P(H)=1-\gamma. \quad (5)$$

According to formula (5) initial reliability of TS before operation $P_0=P(H)$ is always less than one. And after TS functioning during the period *t*, its reliability with consideration of (1) and (5) is:

$$P(t)=P_f(t)\cdot P(H) \quad (6)$$

Formula (6) makes it possible to consider TS reliability not only as the result of performance of its functions without taking into account the genesis of its origin, but also as the result of the process that leads to an occurrence of this reliability. Thus, a value of TS reliability index determined in a technical task (TT) for the development, shall be defined by formula (6), which presumes the consideration of operational conditions, as well as of engineering and manufacturing prerequisites for failures as the result of the following factors:

– imperfections of design and engineering methods, engineering errors, violations of normative technical documentation, violations of engineering rules;

– imperfections and errors of technologies applied;

– defects and errors of manufacture, installation, violations of technological processes of manufacture, running in friction joints and adjustment, deterioration of parameters as the result of the required testing.

Moreover, if in case of readiness to function without failures indicated as event *H*, normal functioning of TS shall be indicated as event *B*, the reliability (6) of TS functioning TK during the period *t* should be interpreted as conditional probability:

$$P(t)=P(B|H).$$

Based on the mentioned above, reliability should be considered and estimated not only at the stages of the life cycle of the product which is ready for operation, but also in the cases when it is under manufacture or exists in form of the models such as:

– information models under design;

– graphical models under engineering;

– models of technological process under preparation of manufacture.

During the course of sequential modeling and manufacture of the product throughout the life cycle, its expected initial reliability at the start of operation tends to decrease due to the impendence of formation of prerequisites to failures, as the result of modeling errors and as the result of different deviations under manufacture.

The correctness of formula (6) is confirmed by the results of studies carried out by Rome Air Development Center in order to improve the standard of US defense department related to reliability MIL-HDBK-217 [4]. The studies were based on the analysis of data about accidents and incidents at 300 American and European spacecrafts related to 2500 facts of failures for the period from early 1960s till January, 1984. The following factors were accepted as the causes of TS failures: engineering errors – 34,4%, underestimate of environmental conditions – 25,3%, defects of components – 10,8%, quality of manufacture – 8,9%, conditions of operation – 6,9%, other – 2,2% and unknown – 11,5%. In fact, not less than in 79,4% of cases, TS failures were predetermined before the start of operation – "at a drafting machine" and in manufacturing departments (when something was not thought through, taken into account and controlled, making an error or foozling).

Thus, the expected TS reliability at the start of operation is generally always less than one with a tendency to decrease during operation. Moreover, engineering and technological causes that predetermine failures before start of operation prevail over the causes of failures occurred as the results of factors affecting during operation.

Formulas (1) and (5) do not contradict with the TS reliability being "close to one" – фактически "zero point nine repeating": 0,(9)=1 in the interval of operation from 0 to *t*. If we suppose that under design, engineering, technological development and manufacture there was no error (i.e. there are no reasons for failures), hypothetically, initial reliability of the object at the start of operation may be maximum possible, that does not contradict with the idea of developing failure-free objects.

What happens to reliability before the start of operation of transformable structures

The product development and launching into manufacture in accordance with GOST R 15.201-2000 consists of the following stages:

1) Elaboration of tactics and technical task for development engineering (DE);

2) Implementation of DE (incl. the development of engineering (ED) and technological (TD) documentation in accordance with GOST 2.103-68 and GOST 3.1102-81, respectively);

3) Launching into manufacture (incl. the preparation and mastering of manufacture, production and qualification tests).

At the stages of product development and launching into manufacture from the point of genesis of reliability, it makes sense to consider the following stages of the product life cycle:

– development of TT – determination of requirements for the output products;

– design (technical proposal, basic design, technical detailed design) – coordination and validation of requirements for products;

– development of ED – implementation of the requirements for the product in technical documentation for its manufacturer;

– development of TD – coordination of ED requirements ED with manufacturing capabilities производства;

– manufacture (product launching into manufacture) – finished product output.

As it was noted in [5], reliability at the stage of the product development and launching into manufacture is expressed as capability. In accordance with this thesis, there is no capability of the future product to express reliability at the moment of start of TT development. If we use the term *"conditional probability of failure-free operation"* of the product, it will be equal to zero (there is nothing to talk about). Under the TT development the requirements are elaborated in relation to the conditions and modes of operation of the future product, under which the product will actually have to express the property of reliabilityв. By this time it is necessary to collect the data about external environment and loads, carry out basic research of characteristics of structure materials, work out the key technologies of manufacture. With correct statistical samplings there is the possibility to deviate from the stochastic dependence of change of the products parameters, by transferring the reliability tasks to a deterministic approach. The most known example is the assuring structural integrity with a use of safety factors. The more justified and accurate these requirements are in TT, the higher the conditional probability of failure-free operation is.

Based on the TT requirements, at the design stage the operating principles of the future product are built, technical decisions are elaborated, the product's characteristics and functioning algorithms are optimized, design models and methods of parameter calculation are specified.

Design stage is the most important in terms of reliability of the future product, as here it is possible to take such technical decisions that allow for choosing rational design-layout schemes, reduce the uncertainties of the product's states and eventually improve reliability. For instance, using thermal isolation in pads of mounting of continuant structures leads to the exclusion of the possibility of distortion of action elements of a clamping system in non-stationary field of freeze-thaw temperatures [6]. Another example may be a shift of weld in a lining tube of metal high-pressure vessel from the area of maximum voltages, that leads to a reduced influence of technological defects in welds (in particular, due to the occurrence of oxide scabs on the surface of weldments), and to the growth and stabilization of safety factors values [7].

The ability of the future product to express reliability changes at the stage of ED development, as well, but the growth of conditional probability of failure-free operation is limited (ED is developed on the basis of technical decisions already taken at the design stage, and it is difficult to correct design errors at engineering). Potentials of reliability improvement are connected with the possibilities to correct and clear out engineering "trifles", occurred as the result of poor attention, incorrect choice of parameters and decisions, incompetence, hit-or-miss working, lack of qualification of design engineers, etc. [8]. Principal results of engineering are clear and accurate requirements for manufacture of products that exclude any understatements, ambiguity of understanding and interpretation. By the moment of completion of ED development the conditional probability of failure-free operation of the product achieves the maximum level possible for this development (it means that a developer should have instilled all his knowledge, skills and experience, i.e. he cannot go as much long way anymore).

Reliability of future products depends on the quality of the decisions taken under development, which directly depend on the principles, guidelines and requirements used under design and engineering. These notions are interrelated, they have a concrete meaning.

A principle is a basic truth, going without saying, which appears from established logic and forms a general strategy of actions. Principles are used to elaborate design solutions to be *"intermediate or final descriptions of a design object, necessary and sufficient for consideration and determination of further direction or completion of a design stage"* [GOST 22487-77, article 7]. Number of principles is limited by key factors each of which expresses physics of any condition affecting reliability. Essence of these conditions is objective and unshakeable, for instance, the number of functional elements should be minimal, during operation the product should not break down, drives should have enough energy to perform predetermined shifts, etc. A principles is a theoretical basis for further reasoning, decisions and actions, it has no specific guidance in relation to the ways of implementation, it just should be like this, and not otherwise. Principles are implemented with a use of rules that flow out of principles. These rules determine the principles and specify their application.

A rule is a consistency that serves as a guidance that is based on stable interrelations between conditions, on prescribed procedures or norms of activity. Principles and rules exist objectively, independently of us. Deviations from principles and rules break the way it is.

Let us consider the example showing the difference between principles and rules. Energy redundancy of TS opening drives is the principle of performance capability of rotating structure under the conditions of uncertain environment, as well as dispersion of physical properties of the

materials and technological tolerances of the components and assembly units of structures. Values of energy redundancy are determined by the rules related to the choice of correlation between the moments of drive forces and the moments of resistance forces in a swivel head for specific types of drives that take into account the current resistances, rate of response of opening structures, combination of the worst factors, etc. [9]. A principle indicates how it should be (necessary to ensure energy redundancy), and a rule specifies how it actually should be performed (for example, correlation between the margin of a drive moment and the moment of resistance forces shall be not less than three to have the worst combination of factors, correlation of the margin of a drive moment should be ensured in any angular location of a swivel, etc.).

It is not possible to build rules without principles. Rules are used to develop design and engineering solutions.

Rules are intermedia between theory and practice, they often reflect the gained experience that should be considered in new developments to avoid repeating the errors. This experience can be applied in form of the wording "our grandfathers used to do it like this", or expressed in the provisions on normative and technical documentation. Unfortunately, it is very difficult to trace how justifiably and effectively the rules are used, they should be at least formalized and written down as, for example, in paper [10], besides, there are no rules for the new developments. In terms of reliability assurance, following the rules is a necessary, though insufficient condition.

Reliability cannot be achieved "by default", it can be assured only as the result of strict fulfillment of the requirements aimed at the stability of the predetermined properties of the objects. Basis to assure reliability is the fulfillment of the requirements as a realized need to observe the conditions that should be strictly followed at the manufacture. A requirement is a need or expectation that is predetermined, normally supposed or is obligatory [GOST ISO 9000-2011, article 3.1.2].

Reliability requirements at the stage of engineering are formed as the result of application of goal-oriented procedures and analyses [11], being established in a graphic and text form in design documentation: in technical requirements and on a draft, as well as in technical specification. Satisfying these requirements is finally aimed at undoubted performance by a product of its functional tasks with predetermined reliability. But the fulfillment of ED requirements when launching the product into manufacture cannot increase the conditional probability of failure-free operation of the product, as nobody sets such goals for production men. And there are enough reasons to derogate from ED requirements under manufacture, violate technological processes and technological discipline, use means and methods of nondestructive control at the manufacture insufficiently or inefficiently, etc., all this inevitably leads to defects.

The task set at the stage of finished-product output is "not to do much harm" to the quality and reliability when embodying a draft and textual model into a finished product, and the maximum task is that a developer, technologist and manufacturer are "on the same page". That is why it is necessary to have ED requirements being expressed in TD without deviations and interpretations, but at the manufacture being fulfilled with tolerable deviations [12]. At the stage of TD development and product launching into manufacture, the conditional probability of failure-free operation of the future product decreases naturally to the values of the initial level of reliability P_0 at the start of operation.

Change of reliability of transformable structures at the life cycle stages

If according to (6) we base on the fact that failure reasons occur, exist and develop starting from the very early stages

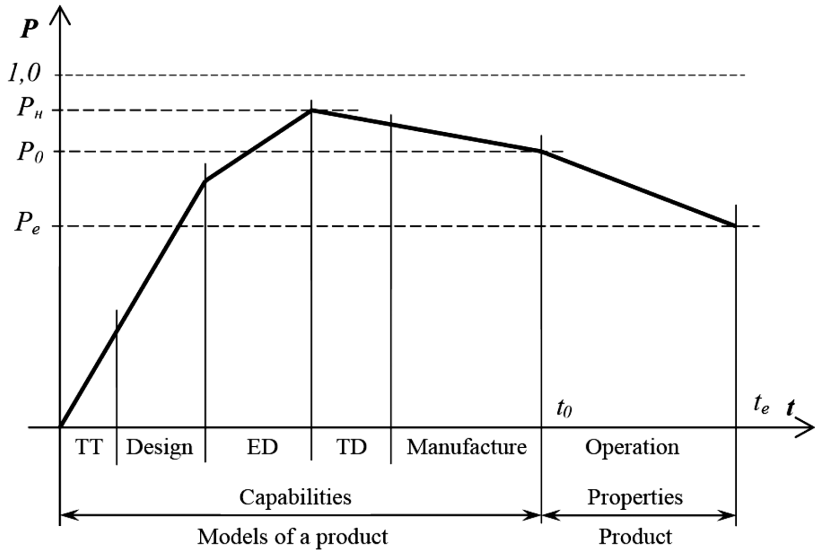


Fig. Graph of change of probability of failure-free operation (conditional probability) of USCS by the life cycle stages

of the TS life cycle, the conditional probability of failures can be represented by the graph given below.

The graph shows that at the end of operation of TS t_e the reliability P_e has the lowest value determined by (1). The product is considered to assure the predetermined reliability P_{prd} if the following equation is fulfilled:

$$P_e > P_{prd}.$$

Drop of the product's reliability within the time interval from t_0 to t_e is consistent with the idea of the behavior of products, based on the widely known U-shaped curve if the product's reliability during its service life [13]. This curve defined the change of the probability of failures under operation. The probability of defect is considered to be high in the initial period of operation due to fundamental errors made under design, manufacture defects or incorrect assembly. Then there comes the period of wear accumulation, during which the failure probability is comparatively low. After the wear achieves a specific level, failures rise sharply again.

For TS there is no long mean time to failure, as well as the respective degradation and deterioration, as it is represented by a classic U-shaped curve, because the operation of TS is performed in the short run during the period of the opening of spacecraft's mechanisms when being under preparation for operation. TS operation totally fits in just with the first section of U-shaped curve. But, as TS refer to USCS specified by low probability of failures, failures at the stage of operation should be minimal, i.e. by the start of operation probabilities of failures caused by design, engineering and manufacture errors should be excluded, or minimized.

According to (6), by the start of operation the initial reliability P_0 is always lower than one, and before the moment of time t_0 the product is specified by the ability to express the property of reliability, and then it specifies this property of reliability. Division of reliability into the ability and property allows for separate consideration of the tasks of practical engineering and the tasks of reliability in the classic presentation of reliability theory.

As it follows from the figure, the ability of the product to express the property of reliability when passing the stages of the life cycle changes significantly. Passing the life cycle stages has different impacts on the initial level of reliability by the start of operation. The graph illustrates the tasks set at different stages of the life cycle under the development and manufacture of TS:

– under the development of TT – to complete fundamental studies of characteristics of structural materials and get all necessary information about external influences and loads;

– under design – to assure the maximum possible level of reliability using efficient technical solutions;

– under the issue of ED – at least not to permit loss of reliability achieved under design, and и, as maximum, to improve reliability by correcting the design errors and setting clear and strict requirements for TS manufacture;

– under the issue of TD – not to alter the reliability requirements in ED;

– under manufacture – not to permit deviations from the requirements in ED and TD.

Conclusion

The aspects related to the genesis of USCS reliability described in the paper, separate the methods of reliability theory with practical engineering methods aimed at the creation of reliable equipment. The field of reliability theory covers the study of behavior of finished products, proceeding from the information about mathematical models that consider stochastic parameters. Real objects in reliability theory are schematized to the models described by probabilistic dependences and having a sampling that can be used for statistical generalization. In practice though, engineers work having no statistics and concepts of probabilistic behavior of a future product, and the collection of methods and algorithms of its operation makes it possible to influence the reliability of real products in a wide range.

This paper uses the example of TS to show that the stages of USCS life cycle are strictly differentiated by the efficiency of reliability measures. At each stage it is necessary to use certain reliability algorithms and methods that are specific to this particular stage, which may increase the effectiveness when solving the tasks of reliability of unique safety critical systems.

References

1. Pokhabov Y.P. Approach to ensuring of dependability of unique safety critical systems examplified by large transformable structures // Dependability. – 2016. – No.1.

2. Chebotarev V.E., Kosenko V.E. Basis of design of spacecrafts of information application. – Krasnoyarsk, SibSAU, 2011. – 488 c.

3. Kurilenko A.M., Ledovsky A.D. Quality of ship control dynamic systems правления. – SPb.: Shipbuilding, 1994. – 176 p.

4. Hecht H., Hecht M. Reliability prediction for spacecraft, Report prepared for Rome Air Development Center, no. RADC-TR-85-229, Dec. 1985. – 156 p.

5. Pokhabov Y.P. About the philosophical aspect of reliability exemplified by unique mission-critical systems // Dependability. – 2015. – No.3. – C. 16-27.

6. Method of fastening of products: pat. 2230945 RF. MPK F16B 1/00 / Y.P. Pokhabov, V.V. Grinevich. – No. 2002113143/11; claimed 18.05.2002; published 20.06.2004. Bul. No. 17.

7. Lepikhin A.M., Moskvichev V.V., Chernyaev A.P., Pokhabov Y.P., Khalimanovich V. I. Experimental estimate of robustness and hermiticity of metal high-pressure vessels // Deformation and damage of material. – 2015. – No. 6. – C. 30-36.

8. Bushuev V.V. Machine construction: reference book. – M.: Machine engineering, 2006. – 448 p.

9. Method of choosing the drive to turn the structure in a pivot unit: pat. 2198387 RF. MPK G 01L 3/00 5/00 / Y.P. Pokhabov – No. 2000129330/28; claimed 23.11.2000; published 10.02.2003. Bul. No. 4.

10. Bowden M.L. Deployment devices // Space Vehicle Mechanisms – Elements of Successful Design, Edited by Peter L. Conley. John Wiley & Sons, Inc., 1998. – P. 495-542.

11. Pokhabov Y.P. About the method of engineering and technological analysis of reliability // Reshetnevsky Readings. – 2015. – Vol. 1. – No. 19. – P. 126-128.

12. Pokhabov Y.P. Ensuring the reliability of large transformable mechanical systems// Reshetnevsky Readings. – 2014. – Vol. 1. – No. 18. – P. 95-97.

13. Clifford M. An engineer's reference book. Mechanical engineering. M.: Publ.house ACB, 2003. 280 p.

About the authors

Yury P. Pokhabov, PhD Engineering, Joint Stock Company "NPO PM – Design Bureau" (JSC NPO PM MKB), Chief of Engineering Innovative Center, tel. +7 913 593 43 89, e-mail: pokhabov_yury@mail.ru

Oleg K. Valishevsky, Joint Stock Company «Academician M.F. Reshetnev Information Satellite Systems» (JSC ISS), leading engineer in the lab of transformable structures, tel. +7 913 582 21 41, e-mail: valishevsky@iss-reshetnev.ru

Receive on 17.03.2016

Надежность № 3 2016 *Original article*
Dependability no.3 2016 *DOI: 10.21683/1729-2640-2016-16-3-54-58*

New international standard for dependability

Viktor A. Netes, *Moscow Technical University of Communication and Informatics, Moscow, Russia, e-mail: vicnet@yandex.ru*

Viktor A. Netes

Abstract. *In 2015 International Electrotechnical Commission adopted a new international standard IEC 60050-192 that specifies the main terms in the field of dependability with their definitions. It was developed by IEC/TC 56 "Dependability" under control of TC 1 "Terminology" and forms Part 192 of International electrotechnical vocabulary. This standard substituted the previous similar standard IEC 60050-191 adopted in 1990. This article is dedicated to IEC 60050-192, acquaintance with which is required for all specialists in the field of dependability. The new standard is compared with the previous IEC 60050-191, and with the similar Russian GOST 27.002–89. In comparison with IEC 60050-191 the new standard contains the modified content and scope, with exclusion of the sections containing the terms related to the quality of services of telecommunication and electric power systems. Based on that, IEC 60050-192 is entitled just with one word "Dependability". Therefore, now it totally corresponds to its status of a horizontal (i.e. inter-industrial, basic) standard. Terminology in the field of dependability is given in respect to a technical item, with analysis of the definitions of this notion, probable structure of the item and the number of terms specifying the types of items. IEC 60050-192 gives a new definition for "dependability": the ability of an item to perform as and when required. This definition was discussed actively, among the IEC experts who took part in the standard development, and among Russian specialists as well. The cluster of features of dependability has also changed: availability, reliability, recoverability, maintainability and maintenance support performance, and in some cases durability, safety and security. A new notion here is "recoverability" defined as ability of an item to recover from a failure, without corrective maintenance. This paper describes the standard's sections dedicated to an item's states and time notions, failures and faults, maintenance and repair, dependability indices, testing, design or engineering, analysis and improvement of dependability. It introduces and explains the most important terms, specifies new terms that were added to the standard, and those excluded from it. The article pays attention to the fact that certain terms have no adequate Russian equivalents. Though the Russian and international dependability terminologies have much in common, there are still significant differences between them. It is explained by the fact that the standardization of dependability terminology in our country that started half a century ago developed for a long time in isolation form similar work world-wide. Due to such differences the creation of a new GOST to be harmonized with IEC 60050-192 is currently not possible. But nevertheless it is necessary to seek to a maximum possible convergence of the Russian and international terminologies.*

Keywords: *dependability, terms and definitions, international standard, International electrotechnical commission.*

Citation format: *Netes V.A. New international standard for dependability // Dependability. 2016. No.3. P. 54-58. DOI: 10.21683/1729-2640-2016-16-3-54-58*

Early in 2015 the International Electrotechnical Commission (IEC) adopted a new international standard (IS) 60050-192, that specifies main terms in the field of dependability with their definitions. It forms Part 192 of International Electrotechnical Vocabulary (IEV). This standard substituted the previous similar standard IEC 60050-191 adopted in 1990, as well as amendments thereto of 1999 and 2002. At first the new standard was supposed to be the second revision of IS 60050-191, but then it was given another number (the reason will be explained later).

IS 60050-192 was prepared by Technical committee (TC) IEC 56 "Dependability" under control of TC 1 "Terminology". The development took quite a long time, progress of this work was reflected in several publications in Russian [1–3], but main purposes of these articles were different and this standard was described in them briefly. This article is especially dedicated to IEC 60050-192, acquaintance with which is required for all specialists in the field of dependability. It should also be mentioned that some notions of this IS are used for the development of the new interstate standard which shall replace GOST 27.002–89, and the work under which is now in well progress.

Of course, one article cannot cover the whole content of IS 60050-192, that is why here we shall consider the most important moments only. The new standard will be compared with the previous IEC 60050-191, and with the similar Russian GOST 27.002–89. In the course of presentation, after first mention of terms we shall give their English equivalents from IS 60050-192 in brackets.

One could get acquainted with IS 60050-192, as well as with other parts of IEV using online version of this

vocabulary which is called “Electropedia” (www.electropedia.org/). Access to this Internet resource is free. Terms of dependability and their definitions are given there in English and French, and only terms (without definitions) are also given in Arabic, German, Spanish, Japanese, Polish, Portuguese and Chinese. Unfortunately, there is no Russian version (for IS 60050-191 there was the Russian version, though it was not provided in“Electropedia”). The complete text of IS in English and in French in electronic form or on paper can be bought through the IEC website (price is 310 CHF).

In comparison with IS 60050-191 the new standard contains the modified content and scope, with exclusion of the sections containing the terms related to the quality of services of telecommunication and electric power systems. Terminology for the quality of telecommunication services is listed in Recommendation E.800 of the International telecommunication union [4], and the terms on reliability and quality of electric power systems shall be described in the special IS 60050-692, which is currently under development. Based on that, IEC 60050-192 is entitled just with one word “Dependability”, whereas IS 60050-191 was called “dependability and quality of service” It was the reason why the standard’s number was changed. Therefore, now IS 60050-192 totally corresponds to its status of a horizontal (i.e. inter-industrial, basic) standard, that should be used by all standardization TCs.

Terminology in the field of dependability is given in respect to a technical item. In IS 60050-191 the definition of this terms just gives different types of items: an individual part, component, device, functional unit, equipment, subsystem, or system that can be considered separately. However, it is hardly a complete list of all possible types of items. That is why the new IS defines an item объект as a subject matter, and the types of items are listed in a note. Then the terms sub item, system and subsystem are defined.

Another note indicates that an item may consist of hardware, software, people or any combination of them. Further the terms “hardware” and “software” are defined. The standard also includes the number of terms specifying different types of software (SW): system software, application software, computer program, firmware, embedded software.

The terms “repaired / non-repaired item” used in the previous IS, are substituted with more precise term “repairable / non-repairable item”. The fact is that a word combination “repaired item” may be understood in two ways: as an item the repair of which is possible, or as an item the repair of which is being carried out at this moment. To exclude the second incorrect meaning the terms were replaced.

In IS 60050-191 the definition of a key term “dependability” is actually reduced to the enumeration of its properties: availability, reliability, maintainability and maintenance support performance. IS 60050-192 gives the new definition of dependability: ability of an item to perform as and when required. This definition was discussed actively, among the IEC experts who took part in the standard development, and among Russian specialists as well. This definition, as well as other definitions of dependability were analyzed in a special article [3] that is why this issue is not described here.

This definition has a note that specifies the properties of dependability. They are availability, reliability, recoverability, maintainability and maintenance support performance, and in some cases durability, safety and security. As it has already been mentioned, availability, reliability, maintainability and maintenance support performance were listed in IS 60050-191. The term “durability” was also mentioned in IS 60050-191, but its relation to dependability was unclear there. Although safety and security are also mentioned in the note as individual terms that have definitions, none of them is mentioned in IS 60050-192.

New term “recoverability” is defined as ability of an item to recover from a failure, without corrective maintenance. Really, recovery is often carried out, for instance, by means of backup switching or SW reloading. These actions cannot be referred to repair, that is why the ability to such recovery is not covered by “maintainability”, and it required the introduction of a new term. A particular case of recovery is self-recoverability when an item has the ability to recover from a failure, without external action to an item. These terms are certainly closely associated with the notion “recovery” that shall be described below.

Speaking about the properties that are the part of dependability let remind that according to GOST 27.002–89 dependability is a complex property which, depending to an item’s designation and terms of application, may include reliability, durability, maintainability and storability, or certain combinations of these properties. There is no well-defined term “availability” in our standard, but there are the factors specifying this property quantitatively: availability factor and operational availability factor. On the other hand, there is no storability in IS.

IS 60050-192 contains no general terms “effectiveness” and “capability” mentioned in the previous IS, because they are considered as not directly referring to dependability.

The new standard, as the previous IS, has a section dedicated to an item’s states. GOST 27.002–89 defines two pairs of states: good – faulty, upstate – down state (a good item is always in the up state, faulty item may be both in the up and down states; an item in the up state may be good and faulty, an item if the down state is always faulty). IS contains no equivalents to good and faulty states, but it has a number of other terms specifying different states of an item. Particularly, there are operating and non-operating states. Being in the first one an item performs a certain required function, being in the second one it does not perform any required function.

For each state the time of being in this state is defined. Then the times related to maintenance and repair

of an item are defined. This intricacy of times could be understood with the help of two figures provided in the standard. Notions of time include useful life, as well as early life failure period, infant mortality period, constant failure intensity period and wear-out failure period. The last three notions are specific to the items with U failure rate curve.

Some terms were excluded from the section about failures. For example, such types of failures as critical and non-critical, sudden and gradual, relevant and non-relevant, degradation, etc. At the same time the following types of failures are kept: complete and partial, primary and secondary, systematic and etc., software failure was added.

Terms "failure cause", "failure mechanism", "common cause failures", "common mode failures" also remain. The first two are quite clear, let us give the definitions for the last two of them. Common cause failures – failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause. Common mode failures – failures of different items characterized by the same failure mode. This term could be understood better with introducing the notion "failure mode" which is defined as manner in which failure occurs. The terms "failure effect" – consequence of a failure, within or beyond the boundary of the failed item and "criticality" – severity of effect with respect to specified evaluation criteria, were also introduced

One of the IS sections is dedicated to the notion that has no direct analogue in the Russian terminology for dependability. In English it is expressed by the term "fault" and defined as follows: inability to perform as required, due to an internal state.

In the Russian version of IS 60050-191 fault is translated as "znachitelnaya neispravnost (Rus.)", in GOST R 27.002–2011 (originally GOST R 53480–2009) – just "neispravnost (Rus.)". But this translation can hardly be admitted a good translation, because by many years of tradition kept in several standards one of which is GOST 27.002–89, "neispravnost (Rus.)" is a short form of the term "neispravnoe sostoyanie (Rus.)". Meanwhile, as per its definition, fault is not a state. By the way, such rendering of the notion "neispravnost (Rus.)" in GOST R 27.002–2011 was criticized hardly by experts [5, 6], because according to our standards "neispravnost (Rus.)" does not at always lead to an inability of an item to perform (that is why when IS 60050-191 was translated into Russian a word "znachitelnaya (Rus.)" was added). We cannot translate "fault" as "otkaz (Rus.)", though these two notions are closely connected as it will be clear from the subsequent. A word "disturbance narushenie (Rus.)" is used in the Russian version of this article as a working Russian equivalent (author will consider other suggestions on this topic with appreciation).

The definition of a fault is supplemented by several notes. The first note says that a fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life cycle, such as specification, design, manufacture or maintenance. The respective words can be used to indicate the cause of a fault: due to the errors occurred at the stage of specification development, design or engineering, manufacturing. Another note says that The type of fault may be associated with the type of associated failure, e.g. wear-out fault and wear-out failure. It is also noted that an item may have one or more faults.

Some terms specifying the types of faults were excluded from this section: critical and non-critical, major and minor, complete and partial and some other terms. The following terms remain though: intermittent, latent, systematic, programme-sensitive. Software and data-sensitive faults were added.

One more IS term having no direct Russian equivalent in GOST 27.002–89, is "maintenance". It can be translated as a word combination "tekhnicheskoe obsluzhivanie i remont" that includes two notions which are separate in the Russian terminology. The word combination "tekhnicheskoe soderzhanie" is proposed in the Russian version of this article as the Russian equivalent to the English "maintenance". This word combination was already mentioned in GOST 32192–2013 Dependability in Railway Techniques – General Concepts – Terms and Definitions.

Maintenance operations are divided into preventive and corrective. The first type operations are carried out to mitigate degradation and reduce the probability of failure, operations of the second type are carried out after fault detection to effect restoration. There are also such types of maintenance as scheduled and unscheduled, deferred; by a state – condition-based, automatic, remote, etc.

A term "Condition monitoring" was added. It deals with obtaining information about physical state or operational parameters of an item. It is used to define the necessity in preventive maintenance operations.

"Repair" is referred to corrective maintenance and is defined as direct action taken to effect restoration. It includes fault localization, fault diagnosis, fault correction and function checkout. During repair there are no technical, administrative and logistics delays.

"Restoration" is defined in IS as event at which the up state is re-established after failure. That is why the duration of the period when an item is in a down state after failure is called "time to restore". GOST 27.002–89 restoration (recovery) is defined as a process when an item is transferred from down state to upstate, which is why a term "restoration time" is used. Each rendering whether it is an event or a process has its pluses and minuses. In particular, IS approach gives a convenient twoness of terms: failure – restoration (both are events), time to failure – time to restore.

In IS 60050-191 a word "restoration" had a synonym word "recovery". But in IS 60050-192 it is introduced as an individual term with somewhat different sense:

restoration without corrective maintenance. It has a special case "self-recovery", a recovery without external intervention.

"Software maintenance" is also a new notion. It is modification for the purposes of software fault removal, adaptation to a new environment, or improvement of performance. It may be corrective, adaptive or perfective.

The sections related to "measures" have not changed significantly. We shall note that in contrast with GOST 27.002–89, IS gives a deeper differentiation for some measures. For instance, there is no general term "availability factor", but there is separate instantaneous availability, mean availability, steady state availability. Three factors of unavailability are defined in the same way.

Inherent availability and operational availability are also distinguished. Inherent availability is provided by the design under ideal conditions of operation and maintenance. Delays associated with maintenance, such as logistic and administrative delays, are excluded. Operational availability is experienced under actual conditions of operation and maintenance. Operational availability is determined considering down time due to failures and associated delays, but excluding external causes.

The sections about "tests: has been extended by supplementing with some new terms. They are: screening test – test carried out to detect and remove non-conforming items, or those susceptible to early life failure; black-box testing – testing in which test cases are chosen using only knowledge of the functional specification of the item under test; white-box testing – testing in which test cases are chosen using knowledge of the internal structure of the item under test; censoring – excluding from a particular assessment, data obtained either after a given duration or a given number of events, etc. Some special terms related to SW tests were added: software alpha test, software beta test, etc. But several terms were excluded. For instance a term "compliance test" remained but "determination test" was excluded.

The section about "design" has also been extended. It contains the remained terms: redundancy, active redundancy, standby redundancy, fail-safe, fault tolerance, fault masking. Some of them were given more exact definitions.

Several terms related to "redundancy", were added, for instance, diverse redundancy and *m* out of *n* redundancy. Some general terms were included: system reconfiguration, fault avoidance, self-checking, self-testing, as well as the terms specific to software: N-version programming, backward recovery, forward recovery. The last two terms mean error recovery in which a system is restored to a previous state, and in which a system is restored to a new state, respectively.

But the section related to the dependability analysis has been reduced. There are no more terms whose sense is clear without definitions, as well as some individual terms. Among the remained terms are prediction, failure modes and effects analysis; failure modes, effects and criticality analysis; fault tree; fault tree analysis; reliability block diagram; state-transition diagram. We shall note that the first two terms had a word "fault" instead of "failure" in the previous IS. The following terms were added into this section: allocation <of dependability requirements>, event tree analysis, life cycle costing.

The section about dependability improvement concepts was also revised in the similar way. Most terms of these sections that were mentioned in the previous IS have been excluded from the new one. Important terms included again: failure reporting, analysis and corrective action system – closed loop process used to improve dependability of current and future designs by feedback of testing, modification and use experience; root cause analysis – systematic process to identify the cause of a fault, failure or undesired event, so that it can be removed by design, process or procedure changes.

In conclusion it should be noted that although the Russian and international terminologies on dependability have much in common, there is still a big difference between them. It is explained by the fact that the standardization of dependability terminology in our country that started half a century ago developed for a long time in isolation form similar work world-wide. Unfortunately, there are still many experts who do not understand the importance of harmonization of the Russian and international standards. Due to such differences the creation of a new GOST to be harmonized with IEC 60050-192 is currently not possible. But nevertheless it is necessary to strive for a maximum possible convergence of the Russian and international terminologies.

To achieve this goal it is necessary not only to make the Russian standards most approximate to international ones, but also to work on the introduction of the accepted Russian terms and notions to IS. It required active participation of the Russian experts in the IS development, that should be not only remote (by correspondence), but also with attendance of meetings and sessions. However, we have to state once again that the contribution of the Russian experts to the development of IS 60050-192 was very low. The Russian experts, in particular the authors of [1], took part in the early stages of this work, but during the last five years there has been no participation, mainly due to the lack of financing.

References

1. Bogdanova G.A., Netes V.A. IEC/TC 56: standardization for dependability // Quality management methods. 2009. No. 5. P. 44–47.

2. Netes V.A., Tarasyev Y.I., Shper V.L. Topical issues of terminology standardization in dependability // Dependability. 2014. No. 2. P. 116–119.

3. Netes V.A., Tarasyev Y.I., Shper V.L. How we should define what "dependability" is // Dependability. 2014. No. 4. P. 3–14.

4. ITU-T Recommendation E.800 (09/08). Definitions of terms related to quality of service.

5. Netes V.A, Rezinovsky A.Y., Tarasyev Y.I., Ushakov I.A., Fishbein F.I., Shper V.L. Деградация вместо гармонизации // Standards and quality. 2011. No. 5.

6. Ushakov I.A. uncalled GOST // Quality management methods. 2011. No. 5.

About the author

Viktor A. Netes, Dr.Sci., Professor of the Moscow Technical University of Communication and Informatics, deputy chairman of Standardization technical committee No.119 "Industrial product dependability", Moscow, Russia, postal address: Aviamotornaya Str., 8a, Moscow, Russia, 111024, e-mail: vicnet@yandex.ru

Receive on 15.08.2016

Надежность № 3 2016
Dependability no.3 2016

Original article
DOI: 10.21683/1729-2640-2016-16-3-59-62
UDK 621.315.23:621.315.98

Simulation model of electromagnetic compatibility of neighboring infrastructure facilities on lines with heavy trains traffic

Valery V. Poliyanov, *Chair "Info-communication systems and information security" Omsk State Transport University, Omsk, Russia, e-mail: PolyanovVV@mail.ru*
Valery E. Mitrokhin, *Chair "Info-communication systems and information security" Omsk State Transport University, Omsk, Russia, e-mail: mitrokhin@list.ru*

Valery V. Poliyanov

Valery E. Mitrokhin

The continuous increase of traffic and traction loads cause the increase of loads on power supply infrastructure that leads to the growth of levels of electromagnetic emission. It results in the growth of probability of emergency functioning of overhead system because of which currents achieve very high levels that may lead to serious accidents in related circuits of signalling and remote control facilities. Such accidents often cause different failures affecting the quality and safety of railway traffic, they lead to equipment damages, as well be a reason for fire. The strongest contribution to the total number of accidents with cable lines is made by electromagnetic influence in case of heavy train movement. And as the result of such train passing along the lines with failed grounding a cable is burnt through. The requirements for EMC of infrastructure facilities are getting stricter, including the requirements for reliability and information security of communication and signalling systems. Existing methods used to define induced currents and voltages do not take into account loads that occur in today's volume of traffic, and do not allow to define the dependence on the parameters of grounding of infrastructure facilities. The parameters of lateral facilities are not taken into account as well. These facilities are located along the track on the whole length of railways. Besides, the grounding parameters change in the course of heavy train moving in different areas. That has become very important to simulate electromagnetic processes in multi-wire systems with consideration of inherent and mutual parameters of lines, as well as ground parameters. But mathematical models of electromagnetic compatibility on railway transport due to its complexity do not always help to obtain the numerical values of induced currents and voltages in the communication circuits and signalling. This article describes an application method of simulation modeling that helps to define the levels of induced currents and voltages in the lateral lines of communication and signalling on the sections of heavy train movement. The paper offers the procedure of simulation modeling, simulation results for a line of heavy train movement and the analysis of the impact of grounding parameters on induced voltages. The simulation results were correlated with the experiment data and admitted to be consistent. The calculations made by the suggested procedure helped to reveal the key dependences of induced currents and voltages on ground parameters, as well as nonlinear dependencies of the induced voltage on ground resistance that forms the basis for further studies and correlation of the obtained data with the statistics accumulated during operation.

Keywords: *electromagnetic compatibility, heavy train movement, simulation modeling.*

Citation format: *Poliyanov V.V., Mitrokhin V.E. Simulation model of electromagnetic compatibility of associated infrastructure facilities on the sections of heavy train movement // Dependability. 2016. No.3. P. 59-62. DOI: 10.21683/1729-2640-2016-16-3-59-62*

Measures to improve reliability on the sections of heavy train movement

Introduction of trains with weight of 6 000 -12 000 t for regular traffic causes the increase of traction loads on power supply system on railway sections by times. Such loads often lead to the defects of equipment and power supply lines and lateral facilities. It is the reason for improvement of traction configuration that includes:

– the creation of power equipment with higher capacity, the extend of cross-section of overhead feeders (up to 5A-185);

– the development of systems of traction power supply with a higher loading capacity;

– the increase of nominal power of a three-phase short circuit at the inputs of traction station up to 1500 MB*A;

– the development and application of effective devices of automation, control and protection of traction stations and overhead equipment from short circuit currents and inadmissible loads (CZAF-3,3kV, CZAF-27,5 kV).

– the application of overhead structures for the sections of heavy train movement including the replacement of contact wires (PBSM-95 on M-120), suspension of line feeders (A-185, 2A-185, M-120) and screening wires.

With consideration of the above listed requirements the overhead system configuration over each main track of open lines consists of [1,2]:

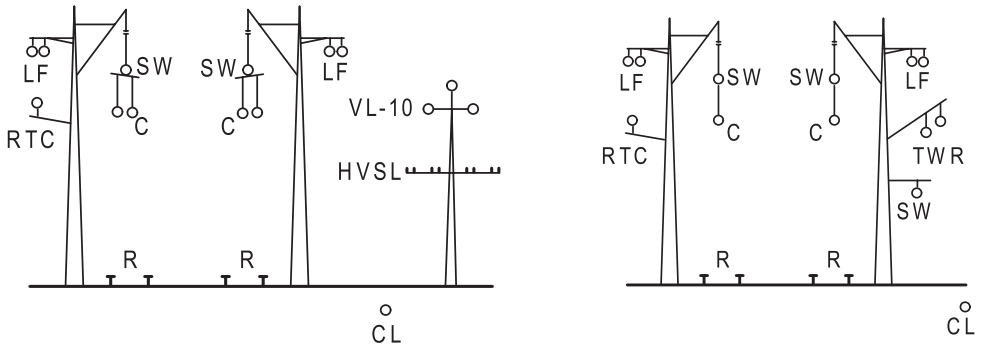


Fig. 1. Schemes of arrangement of linear infrastructure facilities on the sections of heavy train movement, electrified by a) – direct current, b) – alternating current.

– on the sections with direct current – two contact wires with a cross-section not less than 120 mm^2 per each in accordance with GOST 2584-86 [3], one copper span wire with a cross-section not less than 120 mm^2 and two aluminum (aluminum-steel) line feeders with a cross-section not less than 185 mm^2 per each in accordance with GOST 839-80 [4];

– on the sections with alternating current – one contact wire with a cross-section not less than 100 mm^2,], one copper span wire with a cross-section not less than 120 mm^2, one aluminum (aluminum-steel) line feeder with a cross-section not less than 185 mm^2, one aluminum (aluminum-steel) screening wire with a cross-section not less 185 mm^2.

Schemes of arrangement of linear infrastructure facilities on the sections of heavy train movement are shown in figure 1.

The legend of figure 1 is as follows: C – contact wire, SW – span wire, LF – line feeder, R – rails, RTC – guide line of radio train communication 2,13 MHz, VL-10 – overhead line 10kV, HVSL – high-voltage signalling lines, TWR – line "two wires – rail", SW – screening wire, CL – cable line.

The mathematical model that describes the expansion of currents and voltages caused by overhead magnetic interference is represented in each line by the differential equation system whose order depends on the number of the lines forming the part of single electromagnetic system:

$$\begin{cases} -\dfrac{dU_K}{dx} = (R_K + j\omega L_K)\cdot I_K + \sum\limits_{i=1}^{n} I_i \cdot j\omega M_{iK} - j\omega M_{K-кс}\cdot I_{кс}\cdot e^{-\gamma x} \\ -\dfrac{dI_K}{dx} = (G_K + j\omega C_K)\cdot U_K + \sum\limits_{i=1}^{n} (G_{iK} + j\omega C_{iK})(U_i - U_K), \end{cases}$$

where R_k, L_k, G_k, C_k are inherent parameters of the k-th wire,

M_{ik}, G_{ik}, C_{ik} are mutual parameters between the i-th and k-th wires of the system calculated in a frequency spectrum;

$M_{K\text{-кс}}$ is mutual induction between the k-th wire and overhead system,

U_k, I_k, U_i, I_i are currents and voltages in the i-th and k-th wires of the system,

$I_{кс}$ is the overhead current.

With permanent parameters and geometrical relationships in linear infrastructure facilities, the strength of induced currents and voltages depends on boundary conditions defined by the load at the beginning and at the end of the line. That is why an important task is to construct a simulation model to define boundary conditions with consideration of the parameters of grounding of cable lines and ground conductivity on the sections of heavy train movement.

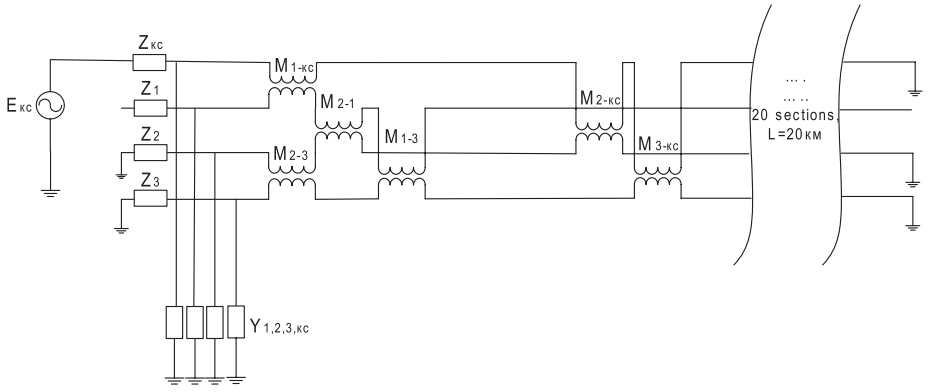


Fig. 2. Simulation modeling scheme

Construction of a simulation model

Simulation modeling of the expansion of currents and voltages in linear facilities was carried out in software environment Simulink (Matlab) in accordance with the scheme as per figure 2.

The modeling was carried out with consideration of linear infrastructure facilities – overhead system, rails, strand and sheath of cable lines.

In accordance with the requirements to heavy train movement [1,2], the railway infrastructure should ensure passing of the group of 3 heavy trains 6300-9000-6300t with the interval of 10 minutes provided there are trains with scheduled weight moving on the adjacent track. In accordance with technical specification of locomotives VL-80 (S,K) [5] under operation in the mode of multiple units maximum current is 110A for a train with scheduled weight, 155A – for a train 6300t, 192A – for a train 9000t. The current of starting of all trains on the section 932 A was accepted as the maximum equivalent current of the overhead system. As the result the values for the currents and voltages at 50Hz frequency were obtained.

Figure 3 shows waveforms of currents and voltages at the end of the cable strand and sheath in case of heavy train movement.

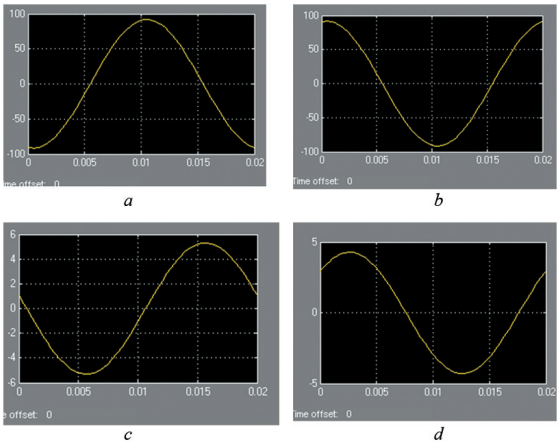


Fig. 3. Waveforms of currents and voltages in case of heavy train movement: a) voltage of the strand at the beginning of the line $U_{S\text{-}B}$; b) voltage of the strand at the end of the line $U_{S\text{-}E}$
c) current of the sheath at the beginning of the line $I_{S\text{-}B}$;
d) current of the sheath at the end of the line $I_{S\text{-}E}$.

Analysis of the influence of grounding parameters on the value of induced voltages

A special feature of heavy train movement sections in the test area of the West Siberian railway is that the bottom in these sections has a higher ground resistance (300-1500 Ohm·m). Besides, heavy traffic is year-around, and during a year the ground parameters change over wide range. Let us perform a simulation for the section of heavy train movement with a length of 20 km, with a total current 932A (50Hz) taking into account the special features of linear facilities grounding.

For calculation we shall take the grounding of metal coatings of the cable in form of four vertical dowel bars sunk into the ground by 5m. For calculation we shall use formulas to define ground resistance. The resistance of current spreading of one vertical ground conductor (bar) [6,7]:

$$R_0 = \frac{\rho_{eqv}}{2\pi L}\left(\ln\left(\frac{2L}{d}\right) + 0,5\ln\left(\frac{4T+L}{4T-L}\right)\right)$$

where – ρ_{eqv} is equivalent ground resistance, Ohm·m;
L is a bar's length, m;
d is a bar's diameter, mm;
T is a distance from the ground surface to the middle of a bar, m.

Digging-in of the horizontal ground conductor can be found by formula [6,7]:

$$T = \left(\frac{L}{2}\right) + t,$$

where t is a digging-in of the vertical ground conductor.

Total resistance of spreading of vertical ground conductors are defined by formula [6,7]:

$$R_0 = 4R_B \cdot \eta$$

η is a demand factor of vertical ground conductors.

Let us obtain a value of induced voltage in the circuit "strand-sheath" ($U_{s\text{-}sh}$) at the beginning of the line under the change of ground resistance (with consideration of the change of the value of mutual induction among the circuits).

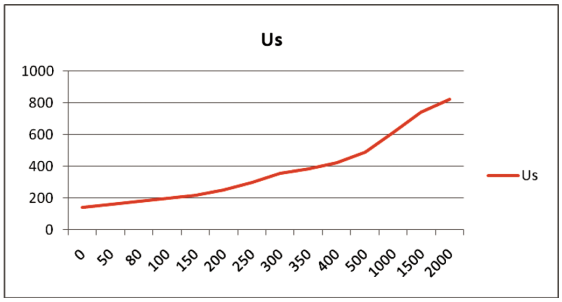


Fig. 4. The graph of dependence of voltage in a cable strand on ground resistance

Apart from fround resistance we need to consider the features of the strcture of the sheath grounding at the place of pulling to buildings. Normative documents [8] regulate the value of resistance of the grounding of a cable line sheath – 4 Ohm, as well as the resistance of metal-on-metal connec-

Table 1 – Dependence of the voltage in a cable strand on ground resistance

ρ, Ом*м	0	50	80	100	150	200	250	300	350	400	500	1000	1500	2000
$U_{s\text{-}sh}$, В	160	210	221	229	259	289	316	343	370	400	438	600	710	783

R_{met}, Ohm	0,1	1	2	3	4	5	10	50	**100**	**1K**	**10Кк**	**100K**	**1M**
$U_{s\text{-}sh}$, В	245	260	277	293	310	325	396	674	776	900	915	919	919

tion of the circuit "metal coatings-GZS-ground" – 0,1 Ohm. The parameters are measured twice a year. However, during a year the value of resistance and metal-on-metal connection may change over wide range. It is connected with climatic factors and electrical and chemical corrosion that accompany the functioning of cable lines. Often the overboost of potentials on cable lines is caused by the damage of conductin parts or bending of metal-on-metal connection.

Let us perform the si,ulation with consideration of the features of cable arrangement. Value $U_{s\text{-}sh}$ was measured at the beginning of the line at the change of resistance of grounding and metal-on-metal connection at the beginning of the line (at the end of the line the value is equal to the norm – 4,1 Ohm).

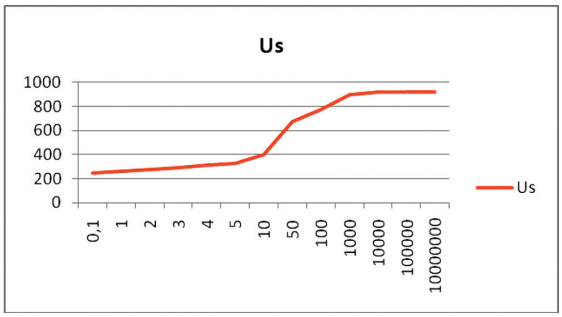


Figure 5. Dependence of the voltage "strand-sheath" on the grounding resistance of cable metal coating

This figure shows that under the growth of ground resistance by higher than 10 Ohm there begins the apparent growth of voltage in the strand ending at 0,9 kV. Very high values of resistence of grounding (higher than 1kOhm) correspond to the cases when grounding conductors or arrangement was damaged or broken.

Conclusion

Based on the constructed simulation model of electromagnetic compatibility, the levels of induced currents and voltages on the sections of heavy train movement are calculated. We have revealed the key dependences of induced currents and voltages on ground parameters of within the range of specific resistance 0 – 2000 Ohm*m with 932A (50Hz) of influencing current. We have performed the simulation depending on the resistance of the ground conductor and metal coatings and determined that the excess of the norm equal to 4 Ohm will lead to nonlinear growth of induced voltage, and the excess of 10 Ohm shall cause a great voltage growth. It helps to form clear requirements to the quality of arrangment and to the parameters of grounding of communication and signaling facilities and to improve the reliability of their functioning.

References

1. Instruction for the handling of cargo trains with increased weight and length on railway tracks of common use. Approved by the order of JSC RZD No.1704p of 28.08.12. Moscow, 2012, 64p.

2. Railway infrastructure on the sections of cargo trains with increased weight and length. Technical requirements. Approved by the order of JSC RZD No.2412p of 25.11.10. Moscow, 2010, 37 p.

3. GOST 2584-86 "Copper and its alloy contact wires. Technical conditions". Moscow, 1997, 9p.

4. GOST 839-80 "Uninsulated wires for aerial power lines. Technical conditions". Moscow, 1981., 26p.

5. Vasko N.M., Kozelsky N.P. Locomotive VL80S. Manual. M.: Transport, 1982., 454 p.

6. Bazelyan E.M. Issues of lightning protection. M.: "IMAG", 2015, 208c.

7. Rudolf Karyakin. Regulations for ground networks. M.: Energoservis, 2006, 360p.

8. Regulations for electric installations. Rev. 7. Approved by the order of Minenergo of Russia No.204 от 08.07.12г. Moscow, 2012.

About the authors

Valery V. Poliyanov, post graduate student, Chair "Info-communication systems and information security" Omsk State Transport University, Omsk, Russia, e-mail: PolyanovVV@mail.ru

Valery E. Mitrokhin, Dr.Sci., professor, Head of Chair "Info-communication systems and information security" Omsk State Transport University, Omsk, Russia, e-mail: mitrokhin@list.ru

Receive on 21.03.2016