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
Dubrovskaya A.Z.
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.
Papers are published in author's edition. The opinion of members of the editorial board may not coincide with the point of view of authors' publications. The reprint of materials is granted only with the written permission of the editorial board. Manuscripts are not returned.

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

Dear colleagues!

The very hard year of 2016 is over. The Dependability Journal has lost three of its colleagues. G.N. Cherkesov, A.A. Tarasov and E.V. Dzirkal have passed away. They were great scientists and remarkable people. They contributed a lot to the Journals' development.

The losses though did not prevent the members of the Editorial Board and Editorial Team from taking active measures to enhance the Journal's scientific and technical level, promote its publications and get them included in the RSCI index, as well as international databases and citation systems, such as Scopus and Web of Science (WoS), that is expected in the nearest future. According to the Scopus requirements, a bilingual website of the Dependability Journal (www.dependability.ru) has been developed and is now fully operational.

In 2017, Dependability will be published in Russian and English. It is planned to use the website to allow readers conditional access to the electronic versions of the current and previous issues.

The subject matter of the Journal remains largely unchanged: structural and functional reliability of technical and man-machine systems, functional safety of control and safety systems, fail-safety and survivability of systems, standardization and certification in the area of system dependability and safety. The subject matter of the publications is to be extended to functional safety, management of fire, occupational, environmental risks, as well as information security.

The priority is given to items that reflect the results of practical application of advanced technologies, methods and engineering solutions.

The Journal is open for publication of advertisement materials highlighting the latest achievements in the area of design, application and development of technical systems and processes as regards their dependability and safety.

The editorial board calls the authors and readers for active involvement with the Journal. Your observations and proposals will help improve its quality, as well as its scientific and application level.

Best of luck in the year of 2017.

Best regards, I.B. Shubinsky, Professor, Editor-in-Chief

Original article
DOI: 10.21683/1729-2640-2017-17-1-4-10

On the definition of the term “dependability”

Yuri P. Pokhabov, *NPO PM – Maloe konstruktorskoye buro (OAO NPO PM MKB), Zheleznogorsk, Russia, e-mail: pokhabov_yury@mail.ru*

Yuri P. Pokhabov

Aim. *Solving the task of ensuring the dependability of flexible space structures requires an unambiguous interpretation of the term “dependability”, as there is an objective need for considering each and every of the many factors that affect the operating performance. In this case, neither the parametric, nor the functional definitions of dependability given in GOST 27.002 are acceptable. The functional definition of dependability does not require a profound knowledge of the physical principles of flexible structures operation, identification and management of the factors that can cause failures, while the parametric definition of dependability does not allow for a complete parametric description of a product, as the explanation of the term “dependability” states and assumes the presence of factors that are “impossible” or “unnecessary” to characterize based on parameters.* **Methods.** *The contradiction between the parametric and functional definitions of dependability can be resolved by means of the hypothesis of confluence of the parametric and functional approaches to dependability that implies that if all the parameters that characterize the ability of a product to perform the required functions continuously maintain their values in time in specified modes and conditions of operation, maintenance, storage and transportation, then the composite dependability indicator of such product also maintains its values in time in specified modes and conditions of operation, maintenance, storage and transportation. Under the hypothesis of confluence of the parametric and functional approaches to dependability omissions in the parametric description of a product in operation are not allowable. As a consequence, the parametric description must take into consideration not only the parameters, but also the indicators that are not technically measurable, but can be evaluated quantitatively. E.g. the probability of an event can be evaluated within the range from 0 to 1.* **Results.** *The parametric description of a flexible structure based on all parameters and indicators that characterize the ability to perform the require functions allows expressing all values of parameters in different units and all abstract numeric values of indicators numerically to enable the “addition” of the parameters and indicator values. For that purpose, the values of each of the parameters and indicators within the specified limits are evaluated subject to the probability of being with the specified limits over the operation time. Thus found probabilities of the parameters and indicators being within the specified ranges can be reduced to a single generalized dependability indicator by using the method of dependability structure diagram that takes into consideration the functional connection between the operation of elements with a certain reliability in a specific sequence.* **Conclusions.** *The article shows the possibility of a uniform understanding of parametric and functional dependability that are connected in terms of meaning, concepts, definition and methodology. In order to solve the flexible structures dependability tasks when every little detail must be taken into consideration, a parametric definition of the term “dependability” can be used with the addition of just two words to the definition given in GOST 27.002. As a result, the definition of the term “dependability” required and sufficient for the purpose of flexible structures dependability can be as follows: “Dependability is the property of an object to maintain in time and within the set limits the values of all parameters and/or indicators that characterize the ability of the system to perform the required functions in specified modes and conditions of operation, maintenance, storage and transportation”.*

Keywords: *term, dependability, parameter, indicator, probability, flexible structure, spacecraft, probability of no-failure.*

For citation: *Pokhabov Yu.P. On the definition of the term “dependability”. Dependability, 2017, vol. 17, no. 1, pp. 4-10. (in Russian) DOI: 10.21683/1729-2640-2017-17-1-4-10*

Introduction

In 2014, Dependability journal published two articles [1, 2] dedicated to the terminology of dependability, in which the authors, as they phrased it, deliberately avoided to give final recommendations as to the definition of the term "dependability". Meanwhile, solving the task of ensuring the dependability of flexible structures (FS) of spacecraft (SC), that are unique highly vital systems [3], requires an unambiguous interpretation of the term "dependability", as there is an objective need for considering each and every of the many factors that affect the operating performance [4]. In this case neither the parametric, nor the functional definitions of dependability given in GOST 27.002 are acceptable. The functional definition of dependability does not require a profound knowledge of the physical principles of FS operation, identification and management of the factors that can cause failures, while the parametric definition of dependability does not allow for a complete parametric description of a product, as the explanation of the term "dependability" states and assumes the presence of factors that are "impossible" or "unnecessary" to characterize based on parameters.

Contradictions between the parametric and functional definitions of the term "dependability" in the context of flexible structures

FS operation is defined by a sequence of states over the lifecycle and is characterized by the following time intervals:

t_1 – operation in compact stowage in launch position during storage, ground handling, ground operation, SC flight as part of the launch vehicle and preparation to transformation in near-earth orbit (operation in launch position is allowed within several years);

t_2 – programmed activation of the initiator that releases the structures in launch position at a given time upon a external. In fact, this time interval lasts for a few moments ($t_2 \ll t_1$);

t_3 – operation of the retaining device and release of the stowed structures (assigned change of kinematic state of devices) ($t_3 \approx t_2$);

t_4 – performance of specified functions of spatial reconfiguration of folded structures (transformation) that usually takes from several seconds to several minutes within several hours from insertion into intended orbit ($t_2 \ll t_4 \ll t_1$);

t_5 – performance of intended mission of the structure in open position over the active service life. For today's SCs this interval is not less than 12-15 years ($t_5 > t_1$).

The term operation should be understood according to the definition given in the now obsolete GOST 22487, i.e. *execution in the facility (system) of a process (processes) according to the specified algorithm and (or) manifestation of specified properties by the facility*.

FS operation in each of the state and transition from state to state is characterized by certain parameters. In the explanations of the term given in GOST 27.002 it is explicitly stated that *the parameters that characterize the ability to perform the specified functions include kinematic and dynamic parameters, structural strength, functional precision, performance, speed and other characteristics*. [5]. At the same time, the parametric definition of dependability reads that dependability is *the property of an object to maintain in time and within the set limits the values of all parameters that characterize the ability to perform the required functions in specified modes and conditions of operation, maintenance, storage and transportation* [5].

Based on the given definition, [6] concludes that dependability is:

1) a generalized property of a technical system's performance;

2) retention in time of continuous output parameters with the specified limits:

$$X(t) \in [X_l, X_u], \quad (1)$$

where t is the current operation time; X_l and X_u are respectively the lower upper limits of allowable values of the parameter $X(t)$;

3) performance of the required functions in specified modes and conditions of operation (application);

4) observance of operation conditions.

However, during FS operation *«the ability of the system to perform the required functions»* cannot always be characterized by parameters. For instance, during the Soyuz-1 mission in 1967 the left solar array (SA) panel did not deploy which entailed a series of catastrophic failures of onboard systems and ultimately the decision by the State Commission to initiate emergency disorbit of the craft [7]. As it was later found, the design of the spacecraft did not take into consideration the fact that the SA panel rotation function could be disrupted due to the ability of vacuum thermal insulation shields to "inflate" in zero-gravity environment up to the limits of its movement and thus create an obstacle to panel travel which ultimately caused it to catch and fail to deploy. In this case there is no parameter that would characterize the property of ensuring unimpeded movement of the rotating structure along the specified trajectory.

As for this, the explanations of the terms given in GOST 27.002 include an additional functional definition of the term "dependability" as *the property of a facility to retain in time the ability to perform the required functions in specified modes and conditions of application, maintenance, storage and transportation.* This definition *is used when the parametric description is unnecessary (e.g. for the simplest facilities of which the operability is characterized in terms of "yes" or "no") or impossible (e.g. for "machine-operator" systems, i.e. systems not all functions of which can be characterized quantitatively)* [5].

Thus, there is a conflict of methods, i.e. a parametric description of FS operation as a unique highly vital product must take into consideration literally each and every factor that affects the operability, however in reality that is impossible. The parametric definition of dependability does not allow for an adequate management of the multitude of factors that affect the FS operability, while the functional definition of dependability does not enable that at all.

The above factors that are sometimes not only versatile, but also physically different [4], many of which cannot be characterized by parameters, include:

- strength factors (absence of destruction and intolerable irreversible deformation);
- stiffness factors (required level of minimal partial frequencies of proper oscillations in the folded and working positions);
- stress-related factors (permissibility of displacement of the structure's elements in case of deformations under external mechanical forces and thermal factors);
- stability factors (non-permissibility of bifurcations within the range of operational loads, e.g. due to play in kinematic pairs or unauthorized folding of structures in the working position);
- design factors (design errors, deficiencies in design methods);
- process factors (deficiencies or disruptions in the adopted process, process errors, insufficient adjustment and calibration limits, uncontrollable effects of assembly, etc.);
- geometrical factors (gaps in kinematic pairs, free travel in mechanisms and drive springs, etc.);
- tribological factors (choice of tribicoupling materials, consistency of lubricant properties, assignment of the thickness of lubricant solid films, etc.);
- vibration resistance factors (impermissibility of loosening of screw joints, allowable partial frequencies, allowable vibration displacements, etc.);
- thermophysical factors (allowable heat distortions, compatibility of materials in terms of coefficient of linear expansion, use of thermal isolation in fastening and operation, etc.);
- physical and mechanical factors (drive moment margins, allowable deployment speed, required values of actuator impulse for initial move, etc.);
- precision factors (precision and stability of positioning, lack of play in working condition, etc.);
- organizational factors (used redundancy methods, ensuring specified deployment zones, observance of specified order of restraint of deployed sections, etc.);
- anthropogenic factors (elimination of unauthorized actions and negligence of personnel, management of engineering psychology factors that complicate incorrect assembly or use of structures, foolproofing).

The authors believe that one of the difficulties of practical application of parametric or functional definition of dependability [2] consists in the separation of the *function (task) performed by the system and the function performed by its parts and/or elements,* which in the given example causes the following contradictions:

- a parametric description of SA panels failure is impossible, as the panels themselves do not have intrinsic properties that depend on the state of panel structures at the moment of failure;
- the failure occurs independently of the intrinsic properties of the SA panels as a result of interaction with external structures (SC vacuum thermal insulation shields).

In the given example, we are evidently dealing with a failure to perform the target function, i.e. deployment of SA panel into working position. In the context of the sequence of states in operation the failure to perform the target function is the consequence of a partial function failure that occurs during SA panel state change t_4 in operation.

Hypothesis of confluence of the parametric and functional approaches to dependability

The above noted contradiction between the parametric and functional approaches to dependability can be overcome if the property of ensuring unimpeded movement of the rotating structure of SA panels along the specified trajectory is defined with the probability of events that takes into consideration both the intrinsic properties of the facility and its interaction with external structures and the environment. In this case the occurrence of the event A that conditions the performance of the target function of SA panel rotation into the working position can be characterized by one of the dependability indicators [5, 8], i.e. the probability of no-failure (PNF), while the performance of the intermediate state change t_4 in operation can be defined by the probability as the level of confidence in the occurrence of the event B that conditions the transition from one state into another. The PNF of SA panel rotation into the working position is associated with the probability of performance of the intermediate state change function t_4 through a conditional probability as the probability of occurrence of the event A provided that the event B has already occurred:

$$P(t)=P(A|B). \quad (2)$$

Thus, the factor that ensures the operability and that is *"impossible"* to be characterized by a parameter can be characterized by a probability that completely defines the performance of the intermediate state change function in operation and ultimately the performance of the target function.

As it is known, any property of a facility can be *distinguished qualitatively and defined quantitatively* [9]. In addition, *quantitative information can be changed, while qualitative information cannot be changed, but can be evaluated* [10].

As it follows from the above example, each i^{th} event in

the process of operation can be associated with a certain number that is called its probability and representing the measure of this event's occurrence, while it is impossible to technically measure the probability, but it is possible to evaluate the probability of occurrence of such event within the range between 0 and 1:

$$P_i(t) \in [0,1]. \quad (3)$$

The probability is an indicator that integrates certain data that can be the basis for evaluation of occurrence of an event, manifestation of a property, process or phenomenon.

Thus, the functions of individual parts of a facility not subject to parametric description can be quantitatively evaluated using indicators as probabilities of retention of the properties that characterize the ability to perform the required functions in time according to (3).

For facilities of which the operability is characterized in terms of "yes of no" the i^{th} property to perform the required functions can also be defined by the probability of retaining in time the "yes" and "no" characteristics:

$$P_i(t) \in \{[1,1] \vee [0,0]\}. \quad (4)$$

The probability of *"performing the required functions"* by a product in general at a random moment in time $\tau \in [0,t]$ is described by the formula:

$$P(\tau)+Q(\tau)=1, \quad (5)$$

where $P(\tau)$ is the PNF; $Q(\tau)$ is the probability of failure.

Based on (5), the dependability of a facility over the operation time $0 \le \tau \le t$ can change within the limits of the unstrict two-sided inequality:

$$1-Q_{\max} \le P(t) \le 1, \quad (6)$$

where $Q_{\max}$ is the maximum value of the probability of failure within the time interval $0 \le \tau \le t$.

Formula (6) can be brought to the form similar to (1):

$$P(t) \in [P_l, 1], \quad (7)$$

here $P_l=1-Q_{\max}$.

It is obvious that the parametric and functional definitions of dependability lead to the conclusion of the continuous retention within specified limits in time of the values of not only the output parameters of dependability (1), but also its output indicators (7). Failure to account for some parameters or error in determining their previous values inevitably cause the uncertainty of limit values of output dependability indicators which in turn causes the risk of failures. For instance, failure to account for event *B* in formula (2) causes the non-fulfilment of condition (7). Therefore, the output dependability indicators can reliably be within the specified limits only in those cases when the parametric description includes *"within the specified limits the values of all parameters that characterize the system's ability to perform the required functions"*. In this case the parametric and functional approaches to dependability are confluent.

Hypothesis of confluence of the parametric and functional approaches to dependability: ***If all the parameters that characterize the ability of a product to perform the required functions continuously maintain their values in time in specified modes and conditions of operation, maintenance, storage and transportation, then the composite dependability indicator of such product also maintains its values in time in specified modes and conditions of operation, maintenance, storage and transportation.***

Within the hypothesis of confluence of the parametric and functional approaches to dependability the gaps in the parametric description of a product in operation are not tolerable, hence in the above example the performance of the SA panel intermediate state change functions in operation absolutely must be taken into consideration on the parametric description.

The parametric description with regard to (1), (3)–(4) and (7) can be represented with the set of parameters $X_i(t) \in G$ and indicators $P_i(t)=X_i(t) \forall X_i(t) \notin G$ of which the values meet the following condition of $X_i(t)$ being within the range of specified allowable states *D* (here and elsewhere the functional symbol of time *t* is omitted):

$$D=\{X_i | X_i \in [X_{min(i)}, X_{max(i)}]\} \forall i=\overline{(1,n)}. \quad (8)$$

If $n \to \infty$ out of (8) follows the proof of the hypothesis of confluence of the parametric and functional approaches to dependability:

$$\because \{X_i\} \subseteq D \therefore P_i = P\left[X_{\min(i)} \le X_i \le X_{\max(i)}\right] \Rightarrow$$
$$\Rightarrow P = P\left[X_i \in D\right]. \quad (9)$$

where $P[\cdot]$ is the probability of a random event that is described in the square brackets.

Proof (9) enables parametric descriptions using a set that indifferently consist of parameters or indicators of a product's elements. In addition, in the limiting case the parametric description may consist of one composite dependability indicator that characterizes the *"ability to perform the required function"* of the product as a whole.

Thus, parametric description of products using parameters and indicators allows harmonizing the parametric

and functional approaches to dependability, in which the parametric and functional dependability are parts of a whole.

Differentiation of the notions of parameters and indicators

The use of the hypothesis of confluence of the parametric and functional approaches to dependability requires strict differentiation of the notions of parameters and indicators. Up to this day there is no such differentiation:

– according to GOST 27.002, the ability of a system to perform the required functions is equally characterized by the indicators (*structural strength, operational precision, etc.*) and the parameters (*kinematic and dynamic parameters, speed, etc.*) [5];

– A.S. Pronikov, the founder of parametric dependability, classified as **parametric indicators** mechanical and strength indicators, power, precision of operation, motive force, top speed, performance, efficiency, noise level, pressure, fuel consumption, etc. [11];

– according to the generally accepted practice, the dependability of facilities *is quantified using the indicators that are chosen and defined subject to the facility's distinctive features, modes and conditions of its operation and consequences of failures* [12].

Both the parameters and indicators are physical values that characterize some properties of a facility (dependability, strength, rigidity, geometry, setting, dynamics, etc.). Parameters are understood as values, of which the intensity can be directly measured by technical mans or calculated (length, force, moment, etc.), while indicators are understood as calculated summarized data that can be used to evaluate the state of the considered property or parameter (assurance factor, drive moment margin, PNF, probability, etc.). Parameters are always defined by a numerical value and unit of physical quantity as they serve to measure geometrical and physical values of the world around, while the indicators are only defined by an abstract number that is part of the value [13].

Using indicators for quantitative evaluation of properties allows accounting for:

– properties that can only be distinguished qualitatively in "binary" form: "zero-one", "yes-no" or characterized only by dependability indicators, e.g. PNF;

– statistical characteristics for critical elements of structures, if any (mass-produced elements or those manufactured in numbers sufficient for statistical conclusions);

– confidence level of failure risk elimination in case associated design, engineering and process solutions are used, based on objective supervision facilities and methods.

The importance of joint use of parameters and indicators in preparation of parametric description of facilities consists in the following capabilities:

– dependability evaluation not only based on quantitative information (through parameters), but qualitative information (through indicators) as well;

– universal enumeration of parameters and indicators that affect dependability;

– elimination of selectiveness and subjectivity in selecting the parameters for dependability evaluation.

The use of the notions a parameter and indicator in parametric descriptions of facilities allows choosing the properties of values that are convenient for characterization. For example, the following can be used for defining the properties of strength:

– values of actual loads (parameters) if they allow clearly evaluating the stress-strain state (tension, compression, shift, bend, twist, stability);

– values of actual load (parameters) if it is required to distinguish ultimate limit states (general strength, fatigue, longevity, temperature strength, creep flow, etc.);

– margins of safety (indicators) if a combined stress state is under consideration subject to the chosen strength criterion (limit strain-stress state);

– PNF (indicators) if the strength property is considered as a stochastic value.

Results of application of the hypothesis of confluence of the parametric and functional approaches to dependability

It must be noted that the upper and lower allowable limits of values may have different physical meaning. For instance, the margin of safety of the drive moment with respect to the resistive moment expresses the *property of the actuator to be sufficiently powerful to rotate the structure* and defines the lower limit of the value (in case of low drive moment margin the rotating structure may fail to deploy). The upper limit of this value is defined by *the strength of the rotating structure when fixed in the working position caused by the conversion of the kinetic energy of rotation into potential energy of deformation at the moment of sudden stop (in case of large drive moment margins the structure may be destroyed). That means that the indicators quantify the properties of products in discordant dimensionless form, which does not allow converting the multi-parametric description into a single generalized dependability indicator, not to mention that the parameters themselves have different units of measurement.*

The absence of a method for accounting and conversion of multi-parametric models into a generalized dependability indicator is reflected in the basic concepts of parametric dependability *that deals not with product failure, but changes in its output parameters. In practice, in parametric dependability a product's operability is identified by the governing parameter*. The state is considered operable if the value of the governing parameter

of element X that defines the quality of such element in operation does not go beyond the specified *working area* or *tolerance range* [14]:

$$X_{\min} \le X \le X_{\max}. \quad (10)$$

In order to obtain the generalized FS dependability indicator it is required to convert the values of all parameters and indicators that constitute the parametric description to the concordant dimensionless form, i.e. expressing all values of parameters in different units and all abstract numeric values of indicators numerically to enable the "addition" of the parameters and indicators values.

This becomes possible if condition (10) is expressed by the probability of a parameter or indicator being within the allowable range within the time period $\tau \in [0,t]$:

$$P_i(t) = P\left[X_{\min(i)} \le X_i(\tau) \le X_{\max(i)};\ 0 \le \tau \le t\right]. \quad (11)$$

In this case the generalized dependability indicator subject to the parametric description of a product (8) can be obtained using the method of dependability structure diagram that takes into consideration the functional connection between the operation of elements with a certain reliability (11) in a specific sequence. For instance, for products in which all the structural elements are single points of failure, which is typical to FSs, the PNF subject to (11) is found using the formula:

$$P(t) = \prod_{i=1}^{n} P_i(t). \quad (12)$$

Under the hypothesis of confluence of the parametric and functional approaches to dependability formula (11) with regard to (8) and (11) is equivalent to the following:

$$P(t) = P\left\{X_i(\tau) \in D, \tau \in [0,t]\right\}. \quad (13)$$

Formula (13) is nothing short of the dependability function in V.V. Bolotin's general theory of mechanical systems dependability [15].

Conclusion

The article shows the possibility of a uniform understanding of parametric and functional dependability that are connected in terms of meaning, concepts, definition and methodology.

In order to solve the FS dependability tasks when every little detail must be taken into consideration, a parametric definition of the term "dependability" can be used with the addition of just two words to the definition given in GOST 27.002. As the result, the definition of "dependability" sufficiently required for the purpose of FS dependability can be as follows: *"Dependability is the property of an object to maintain in time and within the set limits the values of all parameters* ***and/or indicators*** *that characterize the ability of the system to perform the required functions in specified modes and conditions of operation, maintenance, storage and transportation"*.

References

1. Netes VA, Tarasyev YuI, Shper VL. Aktualnye voprosy standartizatsii terminologii v oblasti nadezhnosti [Topical issues of reliability terminology standardization]. Dependability. 2014; 2: 116 – 119. Russian.

2. Netes VA, Tarasyev YuI, Shper VL. Kak nam opredelit chto takoe "nadezhnost" [How we should define what "dependability" is]. Dependability. 2014; 4: 3 – 14. Russian.

3. Pokhabov YuP, Ushakov IA. O bezavarijnosti funktsionirovaniya unikalnykh vysokootvetstvennykh sistem [On the fail-safety of unique highly vital systems]. Metodi menedzhmenta kachestva [Methods of quality management]. 2014; 11: 50 – 56. Russian.

4. Pokhabov YuP. Podkhod k obespecheniyu nadezhnosti unikalnykh vysokootvetstvennykh sistem na primere krupnogabaritnykh transformiruemykh konstruktsij [Approach to ensuring the dependability of unique safety critical systems exemplified by large flexible structures]. Dependability. 2016; 1: 24 – 36. Russian.

5. GOST 27.002-89. Industrial product dependability. Basic concepts. Terms and definitions. Moscow: Izdatelstvo standartov; 1990.

6. Stepanenko EA. Matematicheskie metody otsenivania nadiozhnosty tekhnicheskikh sistem i tekhnogennogo riska. Ch. 1 [Mathematical methods of evaluation of dependability of technical systems and technology-related risk. Part 1]. Krasnodar: Kuban State University; 2010.

7. Muromov IA. 100 velikikh katastrof [100 great disasters]. Moscow: Veche; 2004.

8. GOST 27.003-90. Industrial product dependability. Dependability requirements: contents and general rules for specifying. Moscow: Standartinform; 2007.

9. On approval of regulations on the units of measurement allowed for use in the RF. Decree of the Government of the RF dated 31.10.2009 no. 879.

10. Korotkov NA. Fenomen virtualnoj realnosti kak obekt nauchnogo analiza i filosofskoj refleksii [Phenomenon of virtual reality as an object of scientific analysis and philosophical reflection] [abstract of thesis]. Saint Petersburg; 2010.

11. Pronikov AS. Parametricheskaya nadiozhnost mashin [Parametric dependability of machines]. Moscow: Bauman MSTU Publishing; 2002.

12. GOST 27.002-83. Industrial product dependability. Terms and definitions. Moscow: Izdatelstvo standartov; 1984.

13. Chertov AG. Fizicheskie velichiny (terminologia, opredelenia, razmernosti, yedinitsy). [Physical values

(terms, definitions, dimensions, units)]. Moscow: Vysshaya Shkola; 1990.

14. Sugak EV, Vasilenko NV, Nazarov GG, Panshin AB, Karkarin AP. Nadiozhnost tekhnicheskikh sistem [Dependability of technical systems]. Krasnoyarsk: NII SUVPT; 2001.

15. Bolotin VV. Prognozirovanie resoursa mashin i konstruktsiy [Lifetime forecasting of machines and structures]. Moscow: Mashinostroenie; 1984.

About the author

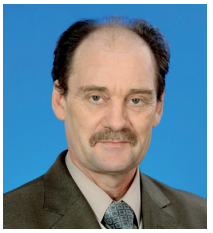
Yuri P. Pokhabov, Candidate of Engineering, NPO PM – Maloe konstruktorskoye buro (OAO NPO PM MKB), Head of Center of Research and Development, 55a Lenina Str., 662972 Zheleznogorsk, Krasnoyarsk Krai, Russia, phone: +7 913 593 43 89, e-mail: pokhabov_yury@mail.ru

Received on 17.08.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-11-16
Dependability, vol. 17 no.1 2017 УДК 62-932.2

Measures to improve the dependability of automated power grid process control equipment

Sergey V. Vendin, *V. Gorin Belgorod State Agricultural University, Belgorod, Russia*
Artiom Yu. Mamontov, *IDGC of Centre, Belgorodenergo, Belgorod, Russia*
Nikolai O. Sharshukov, *Belgorod Shukhov State Technological University, Belgorod, Russia*


Sergey V. Vendin


Artiom Yu. Mamontov


Nikolai O. Sharshukov

Abstract. *Automated control equipment is being progressively integrated into the power grid. Automated process control in the electric power industry involves the ability to control the position of electrical switching devices, monitor their current status, as well as display numeric data on currents, voltages, etc. Disruptions in the automated operations control facilities (AOCF) cause defects in power systems and grid equipment. AOCF failures impair condition monitoring of power grids and operation of switching devices. Due to the impossibility of real-time remote management of power supply installations, the power provider is unable to guarantee continuous power supply. The article analyzes the AOCF equipment currently in operation as part of distributed systems at power substations, looks into the advantages and drawbacks of specific facilities, suggests methods to increase the dependability of equipment operation in the context of a 35-110 kV distributed power supply network. An AOCF equipment certification procedure is proposed. It is also suggested to provide process control documentation for power supply facilities that contain operator process control facilities (OPCF). The documentation is to be stored in maintenance areas as hard copies and at the IT portal as scans. The availability of the documentation at power supply facilities increases labor productivity of engineering personnel that perform operational checks and accident recovery activities. Apart from the mandatory set of substation documents (for the operational, maintenance and RPEA personnel), it is suggested to equip substations with OPCF equipment diagrams. This optimization minimizes time expenditures and errors made during maintenance and repair activities on automated supervisory and process equipment at power supply facilities. That enables remote management of systems operation recovery (power supply, resetting of sensors, controllers, data collection and communication devices, etc.). The efficiency of operational checks by engineering personnel is increased. The absence of emergencies ensures uninterrupted power supply to all categories of consumers and thus increases the overall investment potential of the power supply industry. Therefore, the fail-safe operation of equipment is an obvious factor of Russian technology development as well as complies with the Rosseti regulations regarding the common engineering policy in the integrated power grid.*

Keywords: *AOCF, remote control, electric reliability, distributed networks, integrated power grid.*

For citation: *Vendin S.V., Mamontov A.Yu., Sharshukov N.O. Measures to improve the dependability of automated power grid process control equipment. Dependability, 2017, vol. 17, no. 1, pp. 11-16. (in Russian). DOI: 10.21683/1729-2640-2017-17-1-11-16*

Introduction. Purpose and scope of the research

Today's AOCF equipment is multilevel systems comprising process-specific hardware and customized software. As of now, the AOCF solutions are integrated into the railway, metal, nuclear and energy industries. AOCF systems enable real-time remote control and status monitoring of electrical installations. [1]

Personnel involved in the maintenance of electrical installations have to deal with frequent emergency failures of equipment due to sets of related reasons. That determines the aim of this research, i.e. provision of measures to enable normal AOCF equipment operation. In the context of the aim, the article describes the solutions for the following set of goals.

1. Analyzing AOCF facilities in operation in the 35-110 kV distributed power supply network, identifying the advantages and shortcomings of specific items.
2. Analyzing the primary causes of equipment failures.
3. Proposing the measures to improve the operational dependability of the above equipment.

1. AOCF facilities analysis, advantages and shortcomings

Currently in operation as part of the integrated power grid, there are several hardware and software AOCF solutions intended for collection of data on current position, as well as control of switches.

AOCF systems in operation

1.1. KOMPAS 1.1., supervised remote control station involved in the collection and processing of data. KOM-

PAS is a modular system consisting of a power supply unit, telemetry (TM), remote signalling (RS) reception and telecontrol commands (TC) units. It has a small number of remote signalling and current telemetry signals (8 to 64) and 32 telecontrol commands.

Make-up of the system:

- KTMS-M, modem and addressable module. It is used for interaction with data communication devices;
- KUKP-3, module intended for processing of received remote control data that is also equipped with a port for receiving TM signals;
- MVTS-M, module intended for processing of received telesignalling data that is also equipped with a port for receiving RS signals;
- MVTU, module intended for processing of TC commands that is also equipped with a port for receiving TC signals from direct-point repeater unit (BRP).

In 35-110 kV networks, the supervised station (SS) is connected with top-level devices by means of high-frequency aerial line communication. The significant shortcoming of the SS is the non-availability of synchronization with state-of-the-art communications channels (GPRS, 3G, 4G) which rules out remote connection and interaction with the SS device.

KOMPAS modules architecture is shown in Figure 1.

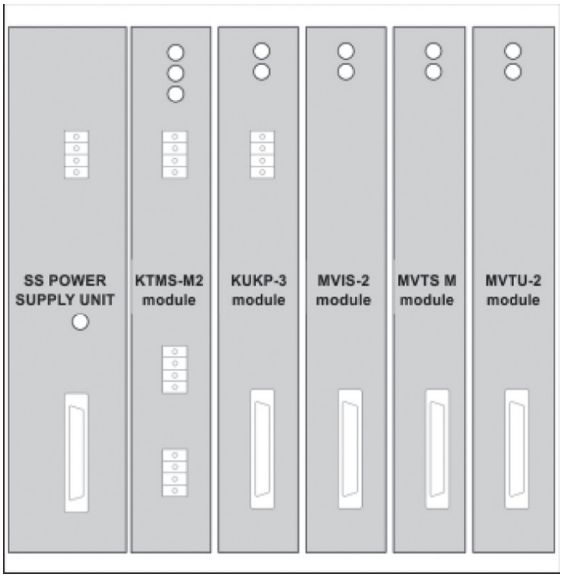


Figure 1. KOMPAS SS modules location diagram

It is not always required to deploy KOMPAS at electricity generation facilities, as in case of aerial line shutdown for maintenance, break or failure of high-frequency equipment channel, the KOMPAS equipment is unable to communicate data to the top level and switching devices monitoring and control is impossible. KOMPAS communications channels are not redundant (in tested conditions). In terms of configuration, technical specifications of electricity generation facilities, KOMPAS 1.1 is obsolete and is frequently replaced with new high-technology solutions.

1.2. MTK-30.KP is the most popular and dependable remote control solution for power distribution networks. The widespread deployment of MTK-30.KP is due to its universality, dependability, wide range of available peripherals and redundancy capability. The MTK-30.KP system is intended for operation as part of remote control solutions that ensure information collection in AOCF systems. The device has a distributed architecture, consists of a set of modules connected with RS 485, CAN and Ethernet buses, interfaces with several RS-232 communications channels by means of a specialized multichannel adaptor, Ethernet interfaces.

MTK-30.KP make-up

The make-up and number of modules is determined by the functionality and information capacity of the MTK-30.kp device. It includes the following primary modules:

- data collection and communication device;
- discrete signals input modules (RS);
- current telemetric input modules (TM);
- interface converter;
- telecontrol modules (TC);
- digital measurement converter (RS 485/232).

Figure 2 shows the layout of remote control modules. The make-up can be extended according to specifications.

1. Current telemetering module (TM) 2. Modem for interaction with data communication devices 3. Remote control cabinet 4. Interface converter 5. Remote signalling module (RS) 6. Main computer 7. Backup power supply module 8. Additional battery module 9. Power and data transmission cable channels

The advantage of the system is the redundancy capability of all components. If due to a combination of causes one of the modules or the main computer fail, the backup module can be activated. It can be observed that the software (SW) including the operational algorithms have been standardized. The software code used by solid-state equipment is adapted to specific operating environment. The monitoring management (SCADA) and personnel working modes undergo improvements, the probability of emergency failures is minimized. AOCF devices exchange data via fiber-optic and wireless channels.

There is also a number of AOCF hardware and software solutions (EKOM TM by OOO Prosoft Sistemy, Syndis SO-5 by OOO NPP Mikronika (Russia, Poland) in operation in the power generation industry. Most of them are comparable with MTK-30.KP in terms of performance, and their overview is unnecessary in the context of the considered tasks.

2. Analysis of the primary causes of equipment failures

Deployment of new technology involves the improvement of maintenance and diagnostics practices. The requirements for the personnel involved in the adjustment

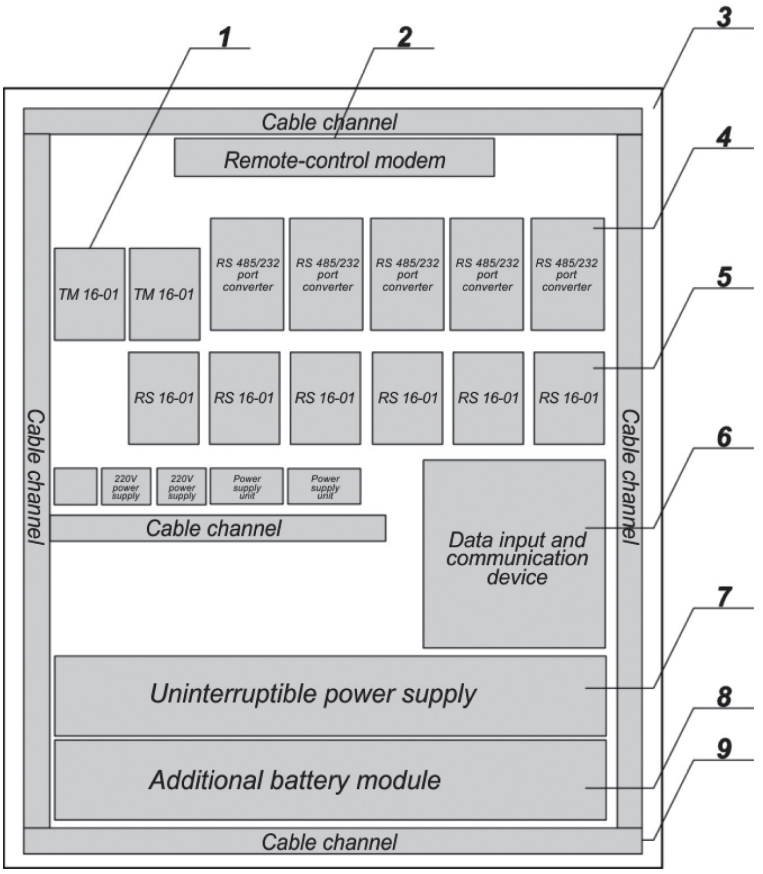


Figure 2. Modules location diagram of MTK-30 supervised station

of complex automated systems also increase. [2] Before commissioning, equipment undergoes numerous simulation tests . Given the commitment to power efficiency and non-interference of personnel in the business process, the probability of emergency failures still remains high. Given below (Figure 3) is a block diagram that indicates the types of process violations, their causes and possible methods of elimination.

3. Measures to improve the operational dependability of the above equipment

3.1 Managerial and engineering activities

3.1.1. Provision of additional redundancy

The review of the systems above leads to the conclusion regarding AOCF devices redundancy. [3] Providing redundancy not only in power supply, but for the switching devices, transformers, data collection and communication devices (DCCD) as well. Each unit in the equipment channel is structured and if one part of the system fails, communication with all remote control and remote signalling facilities is lost. If two devices operate in parallel, the probability of failure is lower, and in case of one or several modules failure the power generation facility remains under dispatcher supervision and control.

3.1.2. Application of stable voltage sources

A stable voltage source enables required power quality in the network and dependable and stable operation of AOCF power supply units. Modern power substations that supply AOCF devices use the Shtyl PS220-14/48-40 uninterruptible power supply (PSU) units that include a considerable number of batteries and a stable voltage source, which prevents abnormal operating modes and failure of AOCF power supply units. Voltage is applied in accordance with the equipment's nameplate data.

3.1.3. Routine inspection and supervision of equipment. Quality installation and setup in accordance with the manufacturer's requirements.

Activities shall comply with the schedule. Provision of equipment supervision for the purpose of identifying

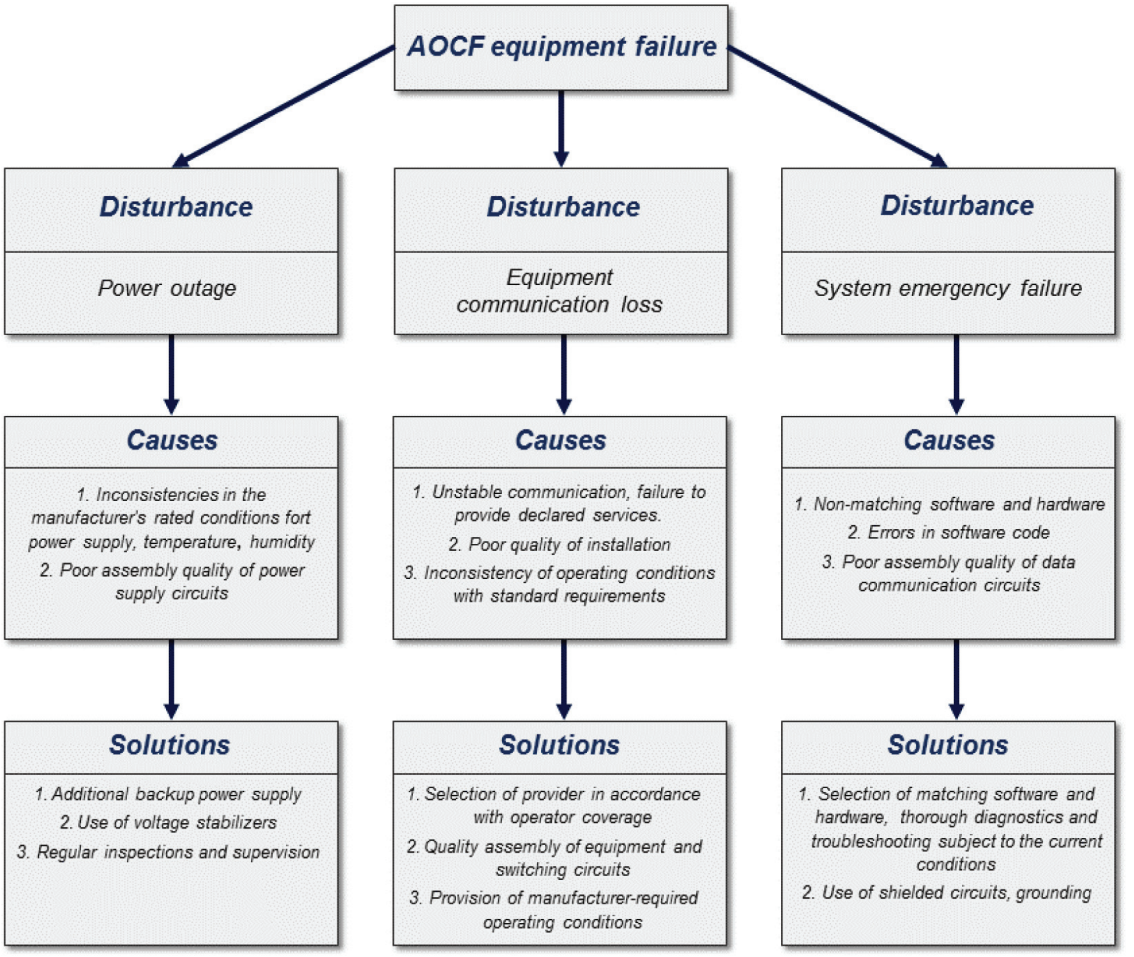


Figure 3. Block diagram of process violations, causes and solutions of AOCF equipment failures

possible defects. Provision of the temperature and humidity in accordance with the manufacturer's requirements. Increased vigilance for the safety of automated equipment, password policy and access to the hardware and software system at power generating facility to prevent accidents and terrorist attacks. While performing inspections, due attention must be given to obsolete equipment that is especially sensitive to the changes of ambient temperature, atmospheric pressure, humidity. The external part of the high-frequency communication channel (high-frequency choke, coupling capacitor, terminal blocks) are prone to contact defects, therefore scheduled inspection of secondary circuits is required. Assembly and setup must be entrusted to well-known companies that specialize in assembly activities and can provide letters of recommendation from Russian and foreign customers. The personnel involved in the assembly, setup, maintenance and operation of AOCF should have certificates issued by the manufacturers (Cisco, ProSoft, etc.) and allowing for the performance of maintenance operations on the given type of equipment.

3.1.4 Selection of provider in accordance with operator coverage

Wireless data communication services (GPRS, 2G, 3G, 4G) in most cases are provided by the mobile telecommunication services provider. The channels may be primary for a number of categories of equipment where deploying broadband wired channels is complicated or unnecessary. E.g. ASKUE equipment, remote-controlled reclosers exchange data with the server via the above channels. [4] [5] Wireless channels (GPRS, 2G, 3G, 4G) are typically used for integration into an existing AOCF solution that supports synchronization with the given communication and its use the redundant feature that runs in parallel with the primary one. Using wireless communication channels is associated with the problem of contracting for data communication services for equipment situated in scarcely-populated areas where there is no mast structures with telecommunication operators' transmit-receive modules. Therefore, in order to optimize the task, while concluding the contract it is required to provide the geographical coordinates of the facility that will use the specific type

of communication. In case of fringe reception in the area where equipment operates another data communication provider may be chosen. [4] [5]

3.2. OPCF facilities certification

It is suggested to provide process control documentation for power supply facilities that contain operator process control facilities (OPCF). The documentation is to be stored in maintenance areas as hard copies and at the IT portal as scans. The availability of the documentation at power supply facilities increases labor productivity of engineering personnel that perform operational checks and accident recovery activities. Apart from the mandatory set of substation documents (for the operational, maintenance and RPEA personnel), it is suggested to equip substations with OPCF equipment diagrams.

It is proposed to classify the lists of documentation per each facility as follows

1. General information on the equipment A set of high-quality photographs of OPCF equipment, general OPCF equipment layout, list of operated equipment with serial/part numbers, battery replacement dates, uninterruptible power supplies (UPS) calibration, etc.

2. AOCF documents. One-line connection diagram of equipment power supply (per each AOCF cabinet), equipment location diagram with branding (per each AOCF cabinet), signal circuit of telemetry information of the facility, functional chart of AOCF facilities with IP addresses. This section should also include copies of documents on the inclusion of new remote signalling and telecontrol facilities, operational check records.

3. Telecommunications equipment documents (TCom). One-line connection diagram of equipment power supply (per each TCom cabinet), equipment location diagram with branding (per each TCom cabinet), functional charts of data communications channels. It is also proposed to complement this section with copies of communication channels redundancy check records.

4. Automated system for fiscal power metering (ASKUE) documents. One-line connection diagram of equipment power supply (per each ASKUE cabinet), equipment location diagram with branding (per each ASKUE cabinet). Metering devices connection diagram at inputs, outgoing lines and received data (real and reactive power).

5. Security and engineering video surveillance documents (SEVS). One-line connection diagram of equipment power supply (per each SEVS cabinet), equipment location diagram with branding (per each SEVS cabinet). Location and power supply diagram of video surveillance cameras.

6. OPCF power supply and grounding documents. It is proposed to include in this section documentation regarding OPCF equipment power supply in the facility, records of earthing bars tests in the facility.

This optimization minimizes the time expenditure and errors made during maintenance and repair activities on automated supervisory and process equipment at power supply facilities. That enables remote management of systems operation recovery (power supply, resetting of sensors, controllers, data collection and communication devices, etc.). The efficiency of operational checks by engineering personnel is increased.

Conclusions. The article reviews the advantages and shortcomings of AOCF equipment operated at 35-110 kV voltage class substations. The authors have analyzed process violations, causes of failures and recovery methods. Efficient AOCF equipment operation methods are suggested. The absence of emergencies ensures uninterrupted power supply to all categories of consumers and thus increases the overall investment potential of the power supply industry. Therefore the fail-safe operation of equipment is an obvious factor of Russian technology development as well as complies with the Rosseti regulations regarding the common engineering policy in the integrated power grid.

References

1. PJSC Rosseti regulations on the common power grid engineering policy. Approved by the PJSC Rosseti Board of Directors (Minutes of Meeting no. 138 dated 23.10.2013).

2. Mamontov AYu, Vinogradov AA, Kaplin AV. Kompiuternaya programma raschota parametrov zhivotnovodcheskoy fermy s biostantsiey [Computer program for parameters calculation of an animal farm with biological research station]. Promyshlennaya energetika [Industrial power systems]. 2016; 5: 46 – 49. Russian.

3. Mamontov AYu, Vinogradov AA, Nedosekov AYu, Sharshukov NO. Gazovaya turbina i gazoporshnevoy dvigatel v sistemakh elekrosnabzhenia agropromyshlennykh predpriyatiy [Gas turbine and gas reciprocating engine in power supply systems of agro-industrial enterprises]. Energobezopasnost i energosberezhenie [Power safety and saving]. 2016; 2: 31 – 35. Russian.

4. Glinkin EI, Chichiov SI, Kalinin VF. Informatsionno-izmeritelnaya sistema elektrosetevoy kompanii [Information and measurement system of a power grid company]. Moscow: Izdatelsky dom Spektr; 2011.

5. Chichiov SI. Modernizatsia avtomatizirovannoy sistemy kontrolia i ouchota elektoenergii regionalnoy setevoy kompanii [Modernization of automated system for electric power control and metering of a regional grid company]. Energobezopasnost i energosberezhenie [Power safety and saving]. 2010; 2: 20 – 24. Russian.

6. Livshits II. Otsenka zashchishchionnosty obiektov toplivno-energeticheskogo kompleksa [Vulnerability evaluation of fuel and energy facilities]. Energobezopasnost i energosberezhenie [Power safety and saving]. 2015; 5: 5 – 11. Russian.

About the authors

Sergey V. Vendin, Doctor of Engineering, Professor, Head of Chair of Electrical Equipment and Electrical Technology in Agro-Industrial Enterprises, V. Gorin Belgorod State Agricultural University, Belgorod, Russia. 1 Vavilova Str., 308503, p. Maysky, Belgorodsky District, Russia

Artiom Yu. Mamontov, Engineer, IDGC of Centre, Belgorodenergo, Belgorod, Russia.
42 Preobrazhenskaya Str, 308012, Belgorod, Russia.

Nikolai O. Sharshukov, Student, Belgorod Shukhov State Technological University, Belgorod, Russia.

Received on 29.06.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-17-21
Dependability, vol. 17 no.1 2017 УДК 621.399

Moving redundancy of tolerant elements

Sergey F. Tyurin, *Perm National Research Polytechnic University, Perm, Russia, e-mail: tyurinsergfeo@yandex.ru.*

Sergey F. Tyurin

Abstract. *Redundancy is one of the primary ways of improving dependability. In particular, structural redundancy is used. In such cases fail-safe operation of elements, devices and systems can be ensured. Fail-safety can enable mitigation of both faults and failures. The paper examines the matter of increasing dependability by means of the so-called sliding redundancy that ensures the health of systems of n elements with m redundant elements that can replace any of the main elements. It is proposed to improve sliding redundancy through recovery of elements out of a number of failed elements that have retained some functionality (basis). For example, the basis of the logical (Boolean) function in terms of Post's theorem is available if such function is not a zero-preserving function, not a one-preserving function, not a self-dual function, not a line function, not a monotone function. Previously, the author proposed the so-called functionally complete tolerant logical functions (FCTF) that do not only possess functional completeness but retain it under the specified failure model. Then even a failed element remains functionally complete, yet with reduced capabilities, e.g. becomes a 2OR-NOT, though the FCTF can be implemented with an element 2AND-2OR-NOT. In this case the recovery of the original function requires several 2OR-NOT elements. However, the diagnostics of such elements and their reconfiguration in case of failure are problematic. This approach can be interpreted with logic recovery of programmable logic devices (PLD) that is based on the so-called Look Up Tables (LUT) that are memory devices based on 16:1 multiplexers. The circuit is a transmitting transistor tree. If they fail, the healthy half of LUT can be used. By means of reconfiguration using standard PLD facilities that contain local and global connections matrix, such "semi-LUTs" can be transformed into LUTs whose functions are equivalent to initial ones. That equals to an increase of the number of redundant elements. Sliding redundancy with recovery of elements out of several failed ones that retained the basis can be used in critical system applications when repair or replacement of elements is impossible. The article proposes a formula that takes such recovery into consideration, analyzes the special features of such redundancy and evaluates the advantages for dependability.*

Keywords: *dependability, redundancy, sliding redundancy, recovery, failures, fault tolerance, failure rate.*

For citation: *Tyurin S.F. Moving redundancy of tolerant elements. Dependability, 2017, vol. 17, no. 1, pp. 17-21. (in Russian) DOI: 10.21683/1729-2640-2017-17-1-17-21*

Introduction

System dependability can be achieved through redundancy. Standby redundancy is often used when the functions of the main element are transferred to the standby element only upon failure of the main one [1]. In case of majority redundancy, a failure or fault is disguised. However, that requires a high level of redundancy. A lesser structure redundancy is typical to adaptive fault tolerance [2, 3, etc.] that includes procedures for supervision, reconfiguration and automatic replacement of failed modules by available redundant ones. In case of sliding redundancy a group of main elements is backed up by one or more redundant elements each of which can replace any of the failed elements of the group [1]. If the number of main elements is n and the number of backup elements is m, sliding redundancy ensures operability if subset of elements R is operational with the power of $|R| \geq n$. Without regard to the complexity and diagnostics and recovery time, for the exponential failure model the probability of no-failure for a system with sliding redundancy is described with the formula:

$$P_{SMR}(n,m,t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot \left[1 - e^{-\lambda\cdot t}\right]^{n+m-i}. \quad (1)$$

In formula (1) P_{SMR} is the probability of no-failure of a system with sliding redundancy (SMR), t is time, hours. Graphs of (1) change in MathCad are given in Fig. 1.

In case of an element's failure, a switch device (SD) enables the remaining backup ones (the so-called reconfiguration is performed); taking into account the SD failure rate λ_{sd} and the assumption of ideality of supervision of the main and backup elements, we deduce:

$$P_{SMR}(n,m,t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot \left[1 - e^{-\lambda\cdot t}\right]^{n+m-i} \cdot e^{-\lambda_{sd}\cdot t}. \quad (2)$$

The graph of dependency of P_{SMR} (2) from the number of backup elements for n =10 if $\lambda = 10^{-5}$ (1/h), $\lambda_{sd} = 10^{-7}$ (1/h) is given in Fig. 2.

Problem definition

Let us not consider the recovery by means of replacement or repair of failed elements. Let us suggest using the

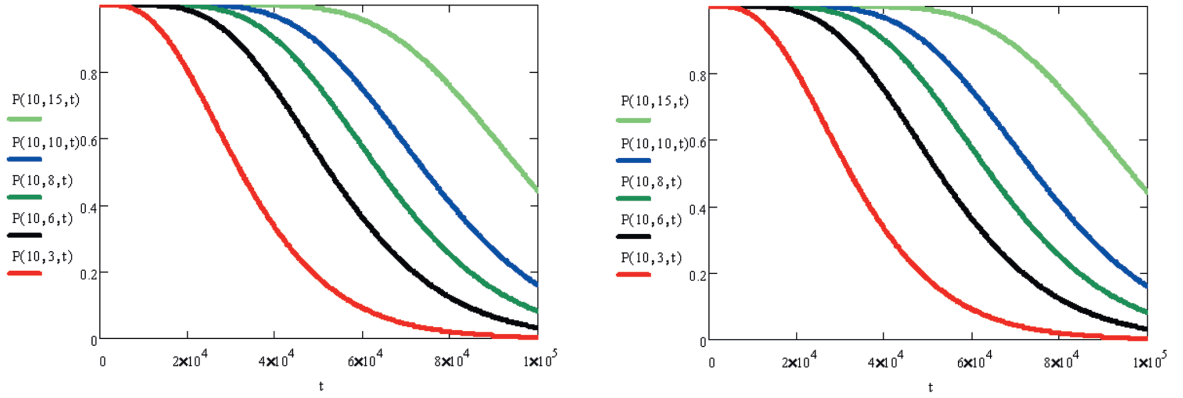


Figure 1. Dependence of P_{SMR} on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) with no regard to failure rate of a switch device

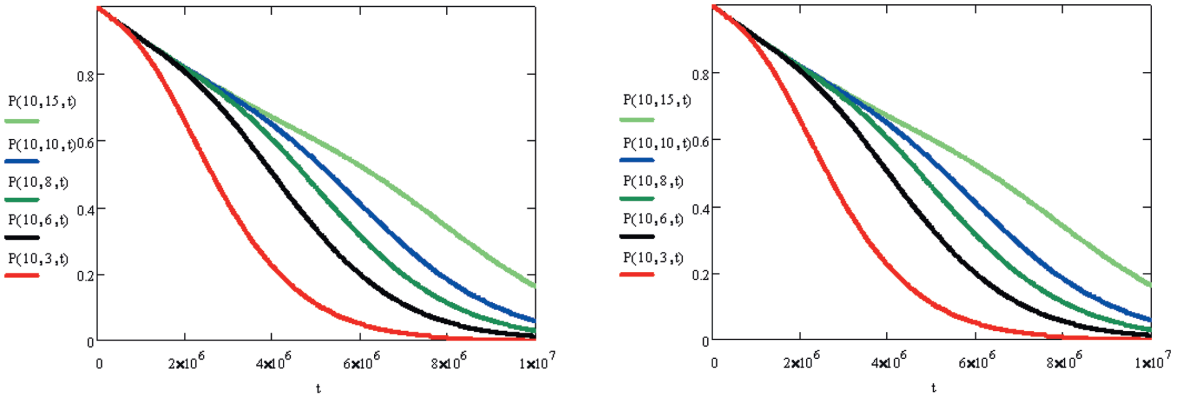


Figure 2. Dependence of P_{SMR} on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) with regard to failure rate of a switch device $\lambda_{sd} = 10^{-7}$ (1/h)

capabilities of the failed elements, i.e. a kind of "internal" redundancy [4]. In this case the failed elements of the system with sliding redundancy remain in backup if they retain at least some functionality (basis) and can be used, but in order to supplement the initial element more than one of them will be required. This concept conforms with state-of-the-art programmable logic devices (PLDs) of the type FPGA (field-programmable gate array) that contain a large number of logical devices (Look Up Table, LUT) [5] in case of single failures of which it is sometimes possible to use a LUT with a smaller number of variables [6-7]. Normally, a PLD does not use all the logical devices (according to some evaluations, 70% or even less). Therefore, the remaining elements can constitute the backup for the sliding redundancy. After proper diagnostics, reconfiguration can be performed remotely (e.g. for a spacecraft, using commands from mission control). However, in case of LUT starvation, the PLD stops being operational. For critical systems in which the PLD cannot be replaced that is not acceptable.

Theoretical part

The recovery of failed main (backup) elements is equivalent to their increase given that they recover as failures occur. However, in order for one element to recover, a number of them must have failed. The premises of the proposed approach to elements recovery out of failed ones lay in the modern trends of introducing built-in diagnostics units into PLDs and systems on a chip, in-built maintenance service with test generators in accordance with the IEEE 1500 standards [8]. Those units can also be backed-up, e.g. according to the technology used by Xilinx in the Virtex PLD [9], which allows assuming the ideality of supervision of main and backup elements.

Let us consider a LUT with two variables that is described with the following formula:

$$z = a\bar{x}_2\bar{x}_1 \vee b\bar{x}_2x_1 \vee cx_2\bar{x}_1 \vee dx_2x_1. \quad (3)$$

If a failure occurs in one half of this LUT, it can for instance be represented with the following formula:

$$z_1 = a\bar{x}_1 \vee bx_1. \quad (4)$$

If there are such «half» elements with functions z_1, z_2, z_3, then the following formula can be recovered from them by means of the required variable (reconfiguration) (3):

$$z = z_3 = (a\bar{x}_1 \vee bx_1 = z_1)\bar{x}_2 \vee (c\bar{x}_1 \vee dx_1 = z_2)x_2. \quad (5)$$

In general, for various abstract bases the following formula will be in place:

$$\nu = \left\lfloor \frac{m}{r} \right\rfloor, \quad (6)$$

where r is the maximum number of failed elements required for recovery of the initial function, $\lfloor \cdot \rfloor$ is the closest lowest whole natural number (ceil). For instance, m=5; r=4; v=1. I.e. a sixth failure can be additionally countered. The remainder will be:

$$w = m - r\left\lfloor \frac{m}{r} \right\rfloor. \quad (7)$$

In our case w=1.

$$1 \le w \le r - 1. \quad (8)$$

The remainders may become useful later when failures occur in the elements out of the number n.

If we do not count the remainders, then the number $v_1 = \left\lfloor \frac{m}{r} \right\rfloor$ is used to counter v_1 failures additionally to m. For instance, m=18; r=4; v=4. That means that if four elements fail, one more element can be recovered from them, i.e. the following number of additional failures will be countered:

$$v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor. \quad (9)$$

In principle, the "nesting" of the fractions can be high, but the number of countered additional failures does not exceed n. We believe that elements that failed more that once do not recover (though in some cases that is possible, e.g. transition of three-element basis into a two-element one). We deduce the following:

$$m;\ v_1 = \left\lfloor \frac{m}{r} \right\rfloor;\ v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor;\ v_3 = \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor}{r} \right\rfloor \ldots \quad (10)$$

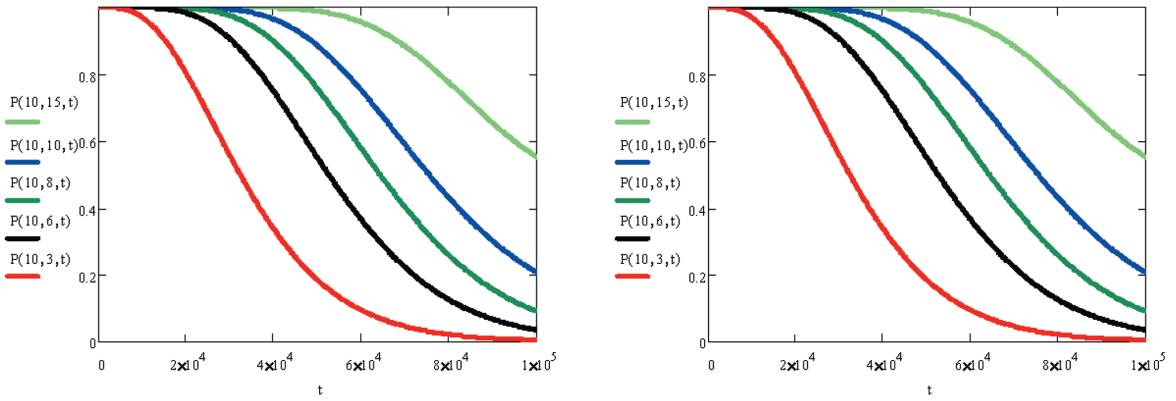


Figure 3. Dependence of P_{SMR} with partial recovery on the time t (h), number of backup elements m, main elements n if $\lambda = 10^{-5}$ (1/h) and r=3 with no regard to failure rate of a switch device

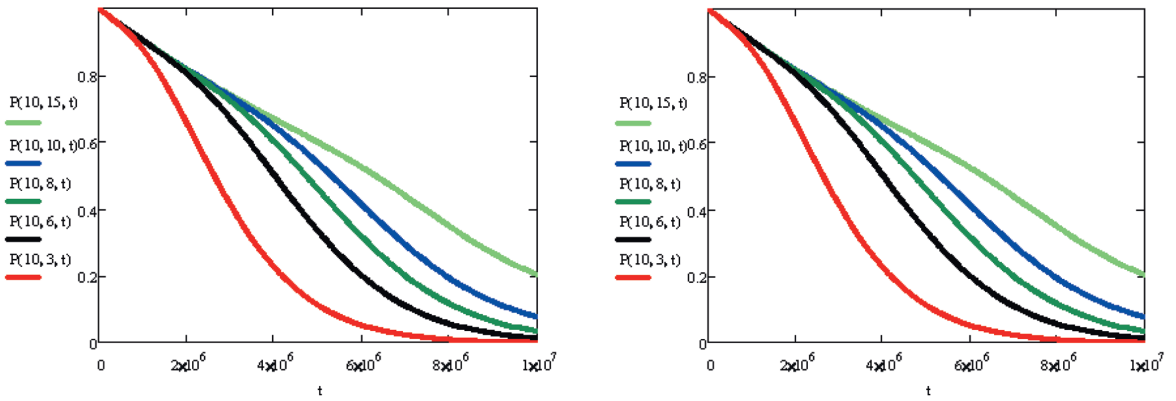


Figure 4. Dependence of P_{SMR} with partial recovery on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) and r=3 with regard to failure rate of a switch device $\lambda_{sd} = 10^{-7}$ (1/h)

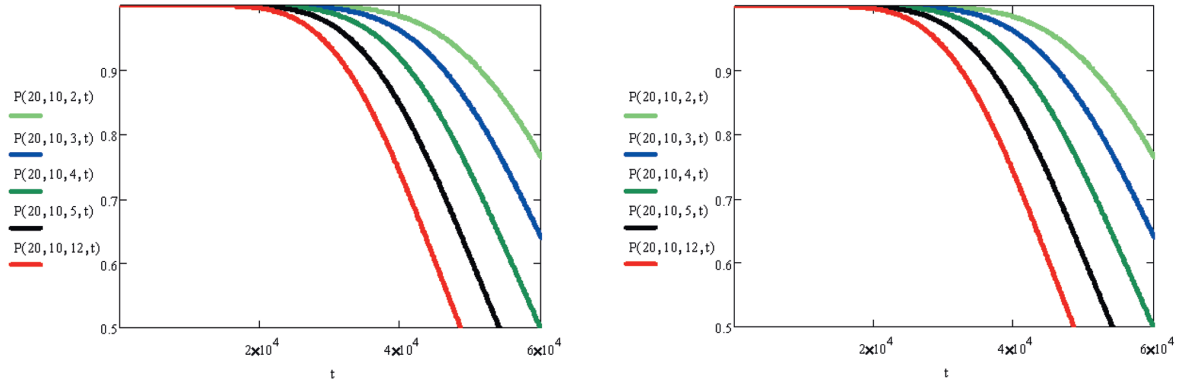


Figure 5. Dependence of P_{SMR} with partial recovery on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) and various r with regard to failure rate of a switch device $\lambda_{sd} = 10^{-7}$ and cost of recovery equipment $\lambda_r = 10^{-8}$ (1/h)

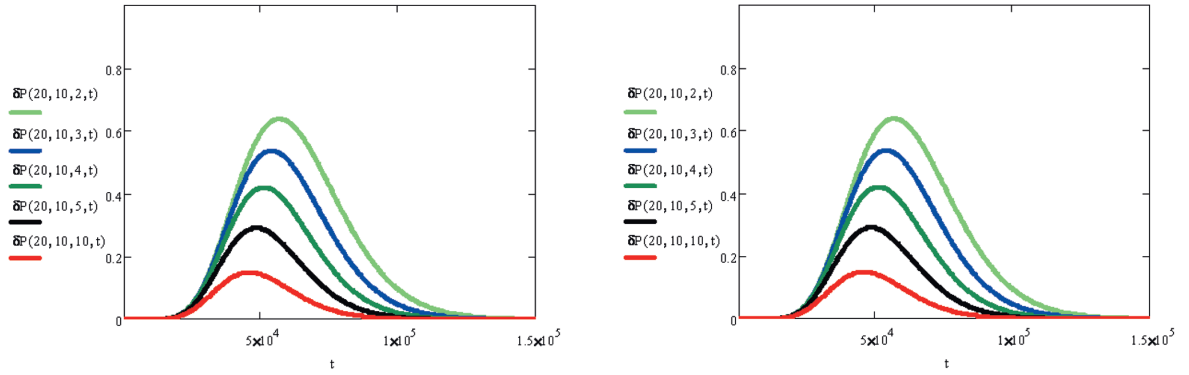


Figure 6. Dependence of $\delta P(n, m, r, t)$ with partial recovery on the number of backup elements m, main elements n, number of failed elements r required for recovery of one element, time t (h) if $\lambda = 10^{-5}$ (1/h) with regard to the failure rate of a switch device $\lambda_{sd} = 10^{-7}$ (1/h), $\lambda_{rec} = 10^{-8}$ (1/h)

This is none other than a geometrical progression, yet with truncation.

$$\sum_i v_i = \theta \le n. \qquad (11)$$

This sum shows the additional number of countered failures with no regard to the "remainders".

If regard is given to the "remainders", then:

$$v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor + m - r\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor;$$

$$v_3 = \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor + \left\lfloor \frac{m}{r} \right\rfloor (1-r) + m - r\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor}{r} \right\rfloor. \qquad (12)$$

Experimental part

As a first approximation (for recovery out of m failed elements of a system) we deduce for v_1:

$$P_{SMR}(t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} \cdot e^{-\lambda_{sd}\cdot t} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda t} (1-e^{-\lambda t})^{m+j} e^{-\lambda_{sd} t}. \qquad (13)$$

Respective (13) graphs without and with regard to failure rates of a switch device are given in Fig. 3 and 4:

In case of additional expenditures for the recovery of the failed λ_{rec} we deduce:

$$P_{SMR}(t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} \cdot e^{-\lambda_{sd}\cdot t} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda t} (1-e^{-\lambda t})^{m+j} e^{-(\lambda_{sd}+\lambda_{rec})t}. \qquad (14)$$

Graphs of change (14) are given in Fig. 5.

We deduce the value of gain δP:

$$\delta P = [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} + \\ + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda t} (1-e^{-\lambda t})^{m+j}] e^{-(\lambda_{my}+\lambda_{e})t} - \\ - [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\lambda t} (1-e^{-\lambda t})^{n+m-i}] e^{-\lambda_{my} t}. \quad (15)$$

The results of calculation of formula (15) in MathCad are given in Fig. 6.

Out of formula (15) let us deduce the conditions of gain under given λ_{rec}. Let us reconstruct (15) in order to identify λ_{rec}:

$$\delta P_{mp} + [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} (1-e^{-\lambda t})^{n+m-i}] e^{-\lambda_{my} t} = \\ = [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} + \\ + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda\cdot t} (1-e^{-\lambda t})^{m-j}] e^{-(\lambda_{my}+\lambda_{e})t}. \quad (16)$$

By dividing the left part of the formula (16) by the right part without the member that takes into consideration λ_{rec} and taking the logarithm we will deduce l_{rec}:

$$-\frac{1}{t} \ln \frac{\{\delta P_{mp} + [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\lambda t} (1-e^{-\lambda t})^{n+m-i}] e^{-\lambda_{my} t}}{\left([\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} + \right.} = \lambda_{e}. \quad (17)$$
$$\left. + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda\cdot t} (1-e^{-\lambda t})^{m+j}] e^{-\lambda_{my} t}\} \right)$$

Conclusion

The proposed sliding redundancy with recovery of elements out of several failed ones that retain the basis ensures a significant growth of dependability. In some cases the probability of no-failure under condition of perfect diagnosis grows 15-20% of the maximum possible gain. This approach can be used for systems in which the maintenance is impossible, e.g. spacecraft in orbit, in flight or in operation on other planets. Later, the matter of recovery time recording should be considered with the use of the mathematical tools of Markov chains, and the matters of supervision and diagnostics should be analyzed in further detail. Recording of slowdown of the elements built out of failed elements is of interest as well.

References

1. GOST 27.002-89. Industrial product dependability. General concepts. Terms and definitions. Moscow: Izdatelstvo standartov; 1990.

2. Shubinsky IB. Nadiozhnye otkazoustoychivye informatsionnye systemy. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016.

3. Vasiliev NP, Shubinsky IB. Analiticheskaya otsenka veroiatnosti ouspeshnoy adaptatsii k otkazam modulnykh vychislitelnykh sistem s mnogourovnevoy aktivnoy zashchitoy [Analytical evaluation of the probability of successful adaptation to failures of modular computer systems with multilevel active protection]. Izvestia vysshykh ouchebnykh zavedeniy. Priborostroenie [Journal of higher educational establishments. Instrument engineering]. 1994; 37: 3 – 4. Russian.

4. Tyurin SF. Problema sokhranenia funktsionalnoy polnoty boulevykh funktsiy pri "otkazakh" argumentov [The problem of maintaining the functional completeness of Boolean functions in case of argument "failure"]. Avtomatika i telemekhanika [Automation and remote control]. 1999; 9: 176 – 186. Russian.

5. Strogonov A, Tsybin S. Programmiruemaia kommutatsia PLIS: vzgliad iznutri [Software switching of FPGA: a look from the inside]. Available from: http://www.kit-e.ru/articles/plis/2010_11_56.php (accessed 16.10.2016).

6. Tyurin SF, Gromov OA. A residual basis search algorithm of fault-tolerant programmable logic integrated circuits. Russian Electrical Engineering. 2013; 84 (11): 647 – 651. DOI: 10.3103/S1068371213110163

7. Tyurin SF, Grekov AV. Functionally Complete Tolerant Elements. International Journal of Applied Engineering Research. 2015; 10 (14): 34433 – 34442.

8. Parfentiy AN, Khakhanov VI, Litvinova EI. Modeli infrastruktury servisnogo obsluzhivania tsifrovykh sistem na kristallakh [Models of infrastructure of digital systems on a chip maintenance service]. ASU i pribory avtomatiki [ACS and automatic devices]. 2007; 138: 83 – 99. Russian.

9. Carmichael C. Triple Module Redundancy Design Techniques for Virtex FPGAs. Available from: https://www.xilinx.com/support/documentation/application_notes/xapp197.pdf (accessed 07.12.2016).

About the author

Sergey F. Tyurin, Doctor of Engineering, Professor, Honored Inventor of the Russian Federation, Professor of Automation and Remote Control, Perm National Research Polytechnic University, Perm, Russia, e-mail: tyurinsergfeo@yandex.ru

Received on 21.11.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-22-26
Dependability, vol. 17 no.1 2017 УДК 620.169.2

Method for calculating gamma-percentile time to failure and failure rate of resistive position sensors of control systems

Anton S. Ishkov, *Radio Technology and Radioelectronic Systems Department, Penza State University, Penza, Russia, e-mail: ishkovanton@mail.ru*
Alexey I. Tsygankov, *JSC NII elektronno-mekhanicheskikh priborov (NIIEMP), Penza, Russia, e-mail: cygankv-aleksejj@rambler.ru*

Anton S. Ishkov

Alexey I. Tsygankov

Abstract. Aim. *Traditionally, the dependability indicators of resistive position sensors based on wire-wound potentiometers used in various control systems are confirmed by means of appropriate dependability tests or tests of comparable products. For cases of non-availability of comparable products test data or significant changes in the product's design and materials, a method for short-term dependability testing and dependability indicators forecasting is required. Calculations of dependability indicators are to be based on statistical information on the variations of properties and parameters over the course of dependability testing along with research findings regarding the physical patterns, descriptions of process kinetics that cause such variations.* **Methods.** *The analysis of physical processes that cause catastrophic changes in resistive position sensors has shown that under electrical loads thermal and electrical fields form that cause electrokinetic, thermoelectric, thermo-diffusion effects. In all cases the rates of physical and chemical processes are functions of material temperature, have temperature dependence and are described with the Arrhenius equation. The conducted research allowed establishing that variations of the position sensors' impedance are largely defined by the processes occurring in the resistive element. The temporal dependence of impedance can be described with a logarithmic, exponential or polynomial dependence.* **Results.** *Mathematical models that describe physical and chemical processes occurring in resistive position sensors in operation allowed developing a scientifically grounded calculation and experimental method for short-term reliability testing. The method includes the description of thermal and electrical modes, durability testing conditions and timing. It is shown that the results of such tests are used in subsequent statistical processing for the purpose of forecasting dependability values. Gamma-percentile time to failure and failure rate are evaluated by means of forecasting the degradation of the acceptance criterion values. The dependence of acceptance criteria values acquired in the course of the tests is approximated by a straight line, exponential curve or a polynomial equation. The form of the approximating line for forecasting the value of gamma-percentile time to failure and failure rate is defined analytically based on the adopted model that describes the physical and chemical processes occurring in potentiometers in operation. The value of acceptability criteria of gamma-percentile time to failure required by the performance specifications and technical regulations is identified through extrapolation of the approximating line as a continuation of the chosen approximating curve (straight line).* **Conclusions.** *The provided test data for short and long-term reliability corresponds to the calculated values of dependability indicators, which confirms the applicability of the developed calculation method. The application of the proposed method allows reducing the scope and duration of costly dependability tests.*

Keywords: *resistive potentiometers, short-term reliability testing, forecasting, gamma-percentile time to failure.*

For citation: *Ishkov A.S., Tsygankov A.I. Method for calculating gamma-percentile time to failure and failure rate of resistive position sensors of control systems. Dependability, 2017, vol. 17, no. 1, pp. 22-26. (in Russian) DOI: 10.21683/1729-2640-2017-17-1-22-26*

Introduction

Resistive (potentiometric) position sensors based on wire-wound potentiometers find wide application in automated guidance, supervision and control systems, and they are primary sources of information for such systems. Currently, despite the availability of digital potentiometers, the interest for wire-wound potentiometers is still high. Among the reasons of their continued popularity are strong accuracy characteristics and high dependability. The durability of some items may reach 5 mil operating cycles. According to regulatory documents, the dependability indicators of potentiometers are the gamma-percentile time to failure ($T\gamma$) and failure rate. In practice, the following methods are used for confirming potentiometers compliance with the specified dependability criteria: experimental based on short and long-term reliability tests, computational and experimental, computational based on the results of comparable

products testing [1]. Normally, short-term reliability tests are conducted at the stage of research and development activities. Based on the obtained test data or comparable product tests, the required potentiometer dependability criteria are confirmed. However, using the test results of comparable products is often complicated due to non-availability of such data or due to significant modifications to product design and used materials.

Obviously, the methods for confirmation of potentiometer compliance with the specified dependability requirements are to combine statistical information on the variations of properties and parameters over the course of dependability testing and research findings regarding the physical patterns, descriptions of process kinetics that cause such variations.

Analysis of physical and chemical processes occurring in products

The correctness of calculation results is defined by the compliance of the adopted model with the actual patterns of physical and chemical processes occurring in the products. Under electrical loads, thermal and electrical fields form within potentiometers that cause electrokinetic, thermoelectric, thermo-diffusion and other effects. The physical and chemical processes cause changes in the electrical parameters of potentiometers.

Under electrical loads, the materials that compose potentiometer elements develop additional fields and physical and chemical processes, primarily:

- thermal field distortion (uneven heating) and associated thermomechanical stress,
- electrical field distortion and field gradient that causes local overheating and ruptures,
- electrolysis, ionization and other localized processes.

Changes in the potentiometer electrical impedance in time are due to processes of oxidation, diffusion, as well as solid body reactions. In all cases the rates of physical and chemical processes in potentiometer materials are functions of material temperature, have a temperature dependence and are described with the Arrhenius equation [2].

$$\tau^{-1} = \nu_0 \cdot \exp\left(\frac{-Q}{kT}\right),$$

where ν_0 is the frequency multiplier, Q is the energy of activation, τ^{-1} is the relaxation rate, k is the Bolzmann constant.

In operation, materials used in potentiometers develop various physical and chemical processes that may cause significant deviations of the potentiometer's electrical impedance from the reference value. As the specific electrical impedance of the frame and coatings is significantly higher than the specific electrical impedance of the resistive element's material, it should be expected that if the electrical impedance of the frame and coatings is subject to significant variations, the overall impedance of the potentiometer accurate to measurement error value will remain constant. Thus, the variation of a potentiometer's overall impedance is defined by the processes occurring in the resistive element.

The passage of electrical current causes a potentiometer to generate heat. The amount of heat generated in unit time is defined by Joule-Lenz's law. Based on the volume of the potentiometer in the steady state, a certain temperature distribution is established that is defined by the resistor design and the current that passes through it. Any process that causes changes in the structure and composition is defined by the displacement of atoms and ions, i.e. the diffusion. The rate of diffusion is defined by the diffusion coefficient that depends on the temperature and energy of activation.

In the case of chemical gas corrosion there is a number of dependencies that describe the variation of the thickness of the oxide film as the function of time. The overall impedance of a potentiometer is a function of the thickness of the oxide film. The growth of the films can be described with:

a) a parabolic equation of the n-th degree [3]:

$h^n = kt + \gamma$;

b) a logarithmic equation [3]:

$h = k\ln(t) + \gamma$,

where k is a coefficient that depends on the temperature, n, γ are constants.

The dependence of the acceptability criteria, e.g. variation of impedance, on the time is represented by the following functional relations:

1) $Z = a\lg(t)$,
2) $Z = at+b$,
3) $Z = t^a$.

The dependence of impedance variation in time on the temperature, load and its starting rate is represented as [4]:

$$Z = Z_0 \cdot e^{\frac{-B}{T}} \cdot P^{\beta} \left(1+\alpha \cdot f\right) \cdot f(\tau),$$

where Z is the acceptance criterion, relative variation of overall impedance, %, Z_0 is the coefficient with the dimension of the acceptance criterion, B is the energy coefficient that characterizes the potentiometer's activation energy, T is the temperature, ^{0}K, P is the electric load, W, f is the starting rate, 1/h, α is the cycling coefficient, $f(\tau)$ is the time parameter.

By means of transformations and introduction of additional designations, this mathematical model is written in the form of linear polynomial with coded explanatory variables [3]:

$$y(x) = b_0 + b_1x_1 + b_2x_2 + b_3x_3.$$

Method for dependability testing of potentiometers

The application of mathematical models that describe physical and chemical processes occurring in resistive

position sensors in operation allows developing a scientifically grounded calculation and experimental method for short-term reliability testing (stage 1). The results of such tests are used in further statistical processing for the purpose of forecasting the values of dependability criteria (stage 2).

Short-term reliability tests of potentiometers (1000 hours) are carried out in two cycles. The first cycle includes 3 stages:

1. Hot soaking under (85+3) °C, direct current and appropriate power of 1 W for 400 h. The accuracy of voltage control is ±5 %.

2. Humidity soaking under increased air humidity according to method 207-2 of GOST 20.57.406 without electric load for 96 h.

3. Wearing tests are conducted with rotation of potentiometer axis within not less than 90 % of the operating angle and rotation speed of 100 revolutions per minute with the number of axis rotations of 41600 for low-resistance potentiometers and 83300 rotations for high-resistance potentiometers.

The second test cycle includes the following stages:

1. Hot soaking (modes as in the first cycle) for 400 h;

2. Soaking in normal environmental conditions under 1 W direct current for 96 hours. The accuracy of voltage control is ±5 %.

3. The wearing test is similar to the one in the first cycle.

Potentiometers are deemed successfully tested for short-term reliability if the relative variation of the overall impedance is not more than ±2% and there is no mechanical damage.

Gamma-percentile time to failure if γ = 95% and failure rate are evaluated by means of forecasting the degradation of the acceptance criterion values (ACP) obtained as the result of short-term reliability tests in the following order.

1. In each i-th ($i = 1, 2, \ldots N$) time cross-section using the measured ACP values (relative variation of impedance) Y_{ij} ($j = 1, 2, \ldots n$) the ACP value in the i-th time cross-sections is identified subject to dispersion Y_i:

$$Y_i = m_i \pm \frac{KS_i}{\sqrt{n}},$$

where m_i is the average ACP value, S_i is the mean square value of ACP in the i-th time cross-section, K is the quantile of Student's t-distribution, of which the values are chosen subject to confidence probability $P = 0{,}95$.

2. The calculated values of Y_i are used as experimental points that are later approximated by one of the following equations:

a) straight line,

b) exponential curve,

c) polynomial equation.

The value of gamma-percentile time to failure is identified by means of extrapolation of approximating lines as a continuation of the chosen curve (straight line) constructed according to the least squares methods.

The values of Y_i can be with one sign (plus or minus) or different signs (plus and minus). In the first case the approximation does not take the sign into consideration, while in the second case the approximation is based on absolute values of ACP deviation. The most satisfactory approximating line is chosen based on the minimal discrepancy between the experimental and calculated values of ACP deviation using the least squares method.

3. Calculation of gamma-percentile operation time for the case of straight line approximation:

$$Y = b_0 + b_1 x.$$

where x is the products testing time, b_0, b_1 are coefficients calculated according to formulas:

$$b_0 = \frac{\sum_{i=1}^{N} y_i \sum_{i=1}^{N} x_i^2 - \sum_{i=1}^{N} y_i x_i \sum_{i=1}^{N} x_i}{N\sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2},$$

$$b_1 = \frac{N\sum_{i=1}^{N} y_i x_i - \sum_{i=1}^{N} y_i \sum_{i=1}^{N} x_i}{N\sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2}.$$

The value Y for the specified value of gamma percentile time to failure x is identified using the formula:

$Y = b_0 + b_1 x$.

In each time cross-section, the value of discrepancy is identified between the experimental values Y_e and the values Y_p identified using the calculated straight line. Accumulated discrepancy is calculated:

$$\sum_{i=1}^{N} S_{SL}{}^2 = \sum_{i=1}^{N} \left(Y_P - Y_e\right)^2.$$

4. Calculation of gamma-percentile operation time for the case of exponential approximation:

$$Y = 1 - e^{-kx},$$

where k is the coefficient that defines the rate of exponential curve growth.

For the last two time cross-sections, the values of coefficients k_1, k_2 are identified:

$$-k_1 = \frac{\ln\left(1 - Y_{1NORM}\right)}{x_1}, -k_2 = \frac{\ln\left(1 - Y_{2NORM}\right)}{x_2},$$

where x_1, x_2 are the last two time cross-sections, Y_{1NORM}, Y_{2NORM} are normalized values of ACP deviation in the second to last (Y_1) and last time cross-sections (Y_2).

The values Y_1, Y_2 are normalized to the maximum allowable ACP deviation (ΔY_{alw}) in accordance with the

values given in the performance specification or technical regulations:

$$Y_{1NORM} = \frac{Y_1}{\Delta Y_{ALW}},\ Y_{2NORM} = \frac{Y_2}{\Delta Y_{ALW}}.$$

As the calculated value of k, the average of the following coefficients is adopted: $k = \frac{k_1 + k_2}{2}$.

The value Y for the specified value of gamma percentile time to failure x is identified using the formula:

$$Y=(1-e^{-kx})+\Delta Y_{BGN},$$

where ΔY_{BGN} is the ACP value in the first cross-section.

Accumulated discrepancy is calculated: $\sum_{i=1}^{N} S_{exp}^2 = \sum_{i=1}^{N} (Y_P - Y_E)^2$.

5. Calculation of gamma-percentile operation time for the case of polynomial approximation:

$$Y=b_0+b_1x+b_2x^2+b_3x^3,$$

where b_0, b_1, b_2, b_3 are polynomial coefficients.

For the purpose of polynomial coefficient calculation, the matrix of time cross-sections (X) and the ACP values matrix (Y) are constructed:

$$\begin{bmatrix} \sum_{i=1}^{N} Y_i \\ \sum_{i=1}^{N} Y_i x_i \\ \sum_{i=1}^{N} Y_i x_i^2 \\ \sum_{i=1}^{N} Y_i x_i^3 \end{bmatrix} = \begin{bmatrix} N & \sum_{i=1}^{N} x_i & \sum_{i=1}^{N} Y_i x_i^2 & \sum_{i=1}^{N} Y_i x_i^3 \\ \sum_{i=1}^{N} x_i & \sum_{i=1}^{N} Y_i x_i^2 & \sum_{i=1}^{N} Y_i x_i^3 & \sum_{i=1}^{N} Y_i x_i^4 \\ \sum_{i=1}^{N} Y_i x_i^2 & \sum_{i=1}^{N} Y_i x_i^3 & \sum_{i=1}^{n} Y_i x_i^4 & \sum_{i=1}^{N} Y_i x_i^5 \\ \sum_{i=1}^{N} Y_i x_i^3 & \sum_{i=1}^{N} Y_i x_i^4 & \sum_{i=1}^{N} Y_i x_i^5 & \sum_{i=1}^{N} Y_i x_i^6 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

The value Y for the specified value of gamma percentile operation time x is identified using the formula:

$$Y=b_0+b_1x+b_2x^2+b_3x^3.$$

Accumulated discrepancy is calculated: $\sum_{i=1}^{N} S_{POL}^2 = \sum_{i=1}^{N} (Y_i - Y)^2$

6. Values $\sum_{i=1}^{N} S_{SL}^2$, $\sum_{i=1}^{N} S_{EXP}^2$, $\sum_{i=1}^{N} S_{POL}^2$ are compared and the lowest one is identified. The value obtained by means of the approximation formula with the lowest accumulated discrepancy is taken as the calculated value Y for the specified value of gamma-percentile time to failure x (in hours).

7. The calculated value Y is compared with the maximum allowable ACP deviation (ΔY_{ALW}). If the condition $Y < \Delta Y_{ALW}$ is fulfilled, the potentiometers comply with the specified requirement for gamma-percentile time to failure.

8. Calculation results verification in the case of a straight line or polynomial equation approximation of experimental points through calculation of homogeneity of variance using Cochran's Q test, as well as model validity check using Fisher's ratio test.

9. Product failure rate over the gamma percentile time to failure is identified using the formula:

$$\lambda = \frac{1-P}{T_\gamma}.$$

Conclusion

In order to validate the above method, short-term reliability tests were performed on 24 wire-wound potentiometers. According to the results of short-term reliability tests not a single catastrophic or parametric failure was identified, while the electrical parameters of the resistors were within the specified requirements.

As per the proposed method, the gamma percentile evaluation of time to failure was performed that equaled to T_γ = 10000 hours.

As the result of experimental data processing, exponential approximation was chosen for forecasting potentiometer ACP within the time of period of 10000 hours. The ACP value (Y) within the operation time x = 10000 hours was calculated using the formula:

$Y=1-e^{-kx}$= 1,166 %.

The comparison of the calculated value Y = 1,166 % with the maximum allowable ACP deviation ΔY_{ALW} = ±2% shows that the condition $Y < \Delta Y_{ALW}$ is fulfilled, therefore the products comply with the specified requirements in terms of gamma-percentile time to failure if γ = 95 %. The graph of ACP variation over the operation time of 10000 hours is given in Figure 1.

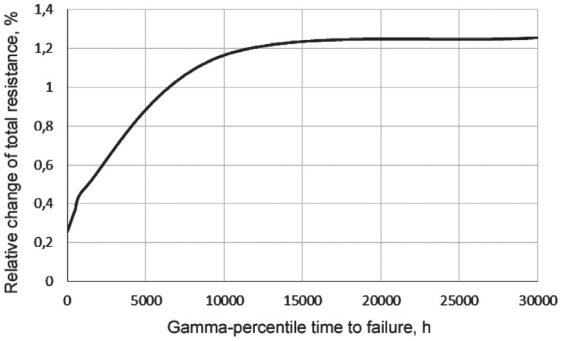


Figure 1. Graph of relative variation of impedance over the operation time of 10000 hours

In order to confirm the calculations of gamma-percentile time to failure, 10000-hour long-term reliability tests were carried out on the same wire-wound potentiometers. Failures were not recorded, the ACP values of the potentiometers did not exceed allowable figures.

References

1. Ishkov AS, Zuev VD. Metodika otsenki gamma-protsentnoy narabotki radioelektronnykh komponentov informatsionno-izmeritelnykh sistem po rezultatam kratkovremennykh ispytaniy [Method of evaluation of gamma-percentile time to failure of information and measurement

systems based on the results of short-term tests]. Dependability. 2015; 2: 82 – 85. Russian.

2. Perrote AI. Osnovy ouskorennykh ispytaniy radioelementov na nadiozhnost [Basic concepts of accelerated dependability testing of radio elements]. Moscow: Sovietskoie radio; 1969. Russian.

3. Demidovich BP, Kudriavtsev VA. Kratki kurs vysshey matematiki. Ucheb. posobie dlya vuzov [Short course on advanced mathematics. Textbook for higher educational institutions.]. Moscow: OOO Izadatelctvo Astrel, OOO Izdatelstvo AST; 2001. Russian.

4. Kauffe K. Reaktsia v tviordykh telakh i na ikh poverkhnosti [Reaction in solid bodies and on their surface]. Moscow: Inostrannaya literatura; 1962.

About the authors

Anton S. Ishkov, Candidate of Engineering, Senior Lecturer in Radio Technology and Radioelectronic Systems, Penza State University, Senior Researcher, JSC NII elektronno-mekhanicheskikh priborov (NIIEMP), Penza, Russia, phone: +7 (841-2) 47-71-19, e-mail: ishkovanton@mail.ru

Alexey I. Tsygankov, Postgraduate, Penza State University, Head of Laboratory, JSC NII elektronno-mekhanicheskikh priborov (NIIEMP), Penza, Russia, phone: +7 (841-2) 47-71-42, e-mail: cygankv-aleksejj@rambler.ru

Received on 08.06.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-27-31
Dependability, vol. 17 no.1 2017 УДК 621.3.019

Identification of dependability indicators of manufactured samples of radioelectronic systems

Boris I. Filippov, *Information Protection Department, Novosibirsk State Technical University, Novosibirsk, Russia, e-mail: filippov-boris@rambler.ru*
Yulia V. Zamiatina, *Information Protection Department, Novosibirsk State Technical University, Novosibirsk, Russia, e-mail: zamiatina.abs323@gmail.com*

Boris I. Filippov

Yulia V. Zamiatina

Abstract. *The article deals with the identification of dependability of manufactured samples of radioelectronic systems. This task belongs to the class of a posteriori analysis. In order to identify the dependability characteristics of equipment, upon production of a pilot batch one performs a posteriori analysis whose first stage is the statistical test (ST). There are a lot of methods for such tests that primarily depend on identifying the time of test completion (r – to failure of r systems, T – upon reaching operation time T, n – to failure of all systems, as well as mixed ones) and the ability to replace failed systems with healthy ones. Such tests are necessary because at the design stage a designer does not possess complete a priori information that would allow identifying the dependability indicators in advance and with a sufficient accuracy. An important source of dependability information is a system for collection of data on product operational performance. There are two primary types of dependability tests. One of them is the determinative test intended for evaluation of dependability indicators. It is typical for mass-produced products. Another type of test is the control test designed to verify the compliance of a system's dependability indicators with the specifications. This paper is dedicated to the first type of tests. It shows the procedure for statistical tests of radioelectronic systems using various procedures. Evaluation of the mean time to failure $\hat{t}^*$ is usually performed by means of the method of maximum likelihood. The essence of the method is that in the process of statistical data processing the likelihood function is found, while the required parameter ($\hat{t}^*$ is the evaluation of parameter t^*) equals to the argument value under which the likelihood function is maximal. The evaluation of the mean time to failure $\hat{t}^*$ is a point estimate of the initial parameter t^*, which in turn is a random value and within a specific test can take any positive value from 0 to ∞. Therefore, in addition to the point estimation an interval estimation of the measured parameter is usually performed. That means that estimation $\hat{t}^*$ identifies the confidence interval $(\hat{t}^*_L, \hat{t}^*_U)$ in which the value of the measured parameter t^* with a specified probability is found. Here $\hat{t}^*_L, \hat{t}^*_U$ are respectively the lower and upper limits of a confidence interval. The article considers two procedures of testing pilot batches of radioelectronic systems, and for each of them the following dependability indicators are defined: evaluation of mean time to failure; confidence interval of mean time to failure. It is shown that for the purpose of identifying the mean time to failure, test procedure [n, V, r] is more efficient than procedure [n, B, r].*

Keywords: *radioelectronic system, time to failure, test duration.*

For citation: *Filippov B.I., Zamiatina Yu.V. Identification of dependability indicators of manufactured samples of radioelectronic systems. Dependability, 2017, vol. 17, no. 1, pp. 27-31. (in Russian) DOI: 10.21683/1729-2640-2017-17-1-27-31*

Introduction

At the current stage of the society's development when the concept of information technology has become ingrained in many people's minds everyone now depends on the security of personal information. If valuable information is communicated with a delay or is inaccurate, a person, company or nation as a whole may face serious consequences. For that reason the requirements for the dependability and availability of radioelectronic systems of information communication and processing are becoming more demanding.

The dependability characteristics of radioelectronic systems (RES) are identified in two stages: a priori analysis that consists in approximate calculation of system dependability based on known quantitative (probabilistic) characteristics of its elements' dependability, as well as a posteriori analysis upon production of a pilot batch of equipment [1-5]. A posteriori analysis provides more accurate results for a specific manufactured batch [6], therefore this stage is of importance as regards the manufacturing process.

Problem definition and solution

In order to identify the dependability characteristics of equipment, upon production of a pilot batch one performs a posteriori analysis whose first stage is the statistical test (ST). There are a lot of methods for such tests that primarily depend on identifying the time of test completion (r – to failure of r systems, T – upon reaching operation time T, n – to failure of all systems, as well as

Figure 1. Instants of failure and failure cycle

mixed ones) and the ability to replace failed systems with healthy ones. [7].

Upon completion of statistical data processing, the calculated characteristics are validated against the specifications and requirements of regulatory documents by public authorities as required.

Identification of dependability characteristics based on testing of pilot batches of RES according to [n, B, r] procedure

1. Problem specification

It is assumed that tests are performed on a pilot batch of 100 (n = 100) RESs without replacement of failed systems to 20 (r = 20) failures. The resulting sample must correspond to the theoretical failure flow model, i.e. the probability density function (PDF) of the failure cycle must correspond to the model as follows

$$w(y_i) = \lambda(n-i+1)e^{-\lambda(n-i+1)y_i} \quad (1)$$

where $\lambda=1/t^*$ is the failure rate of one system, t^* *is* the mean time to failure of one system, *(n – i + 1)* is the number of systems involved in the tests inclusive of the failed ones.

Such sample can be acquired out of the value x evenly distributed over the interval (0; 1) according to formula

$$y_i = -\frac{1}{\lambda(n-i+1)}\ln(x).$$

Let the mean time to failure of one system be 1000 hours.

As the result, we get the failure pattern shown in Figure 1.

2. Estimation of mean time to failure of a pilot batch

Estimation of mean time to failure $\hat{t}^*$ is usually performed by means of the method of maximum likelihood. The essence of the method is that in the process of statistical data processing the likelihood function is found, while the required parameter ($\hat{t}^*$ is the evaluation of parameter t^*) equals to the argument value under which the likelihood function is maximal (Fig. 2).

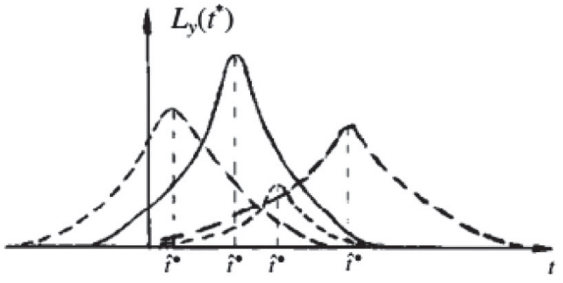


Figure 2. Possible formula for the likelihood function

The likelihood function equals to the joint probability density of intervals y_i subject to their independence

$$L_y(t^*) = \prod_{i=1}^{r} w(y_i) \quad (2)$$

Then, the estimation of mean time to failure will equal to the extremum of the likelihood function

$$\hat{t}^* = \hat{t}^*_{MП} = \arg\max L_y(t^*).$$

In order to find the extremum of the likelihood function, the following equation must be solved

$$\frac{\partial L_y(t^*)}{\partial t^*} = 0.$$

As any monotone function of likelihood function is also a likelihood function, then in order to simplify the solution we can use the equation

$$\frac{\partial \ln L_y(t^*)}{\partial t^*} = 0.$$

Given (1) and (2) we deduce:

$$L_y(t^*) = \prod_{i=1}^{r} w(y_i) = \prod_{i=1}^{r} \lambda(n-i+1)e^{-\lambda(n-i+1)y_i} = e^{-\sum_{i=1}^{r}\lambda(n-i+1)y_i}\prod_{i=1}^{r}\frac{1}{t^*}(n-i+1),$$

$$\ln L_i(t^*) = \sum_{i=1}^{r}\left[\ln(n-i+1) - \ln t^* - \lambda(n-i+1)y_i\right]. \quad (3)$$

If we replace $\lambda = 1/t^*$ and differentiate:

$$\frac{\partial \ln L_y(t^*)}{\partial t^*} = \sum_{i=1}^{r}\left[-\frac{1}{t^*} + \frac{n-i+1}{t^*}y_i\right].$$

As a result, we obtain an evaluation of mean time to failure that in our case equals to:

$$\hat{t}^* = \hat{t}^*_{MП} = \frac{1}{r}\left[\sum_{i=1}^{r}(n-i+1)y_i\right] = 952{,}39 \text{ (hours)} \quad (4)$$

3. Total operation time of all systems to the r^{th} failure

Expression (4) shall be rearranged to time points:

$$\hat{t}^* = \frac{1}{r}\left[\sum_{i=1}^{r}(n-i+1)(t_i - t_{i-1})\right] = \frac{1}{r}\sum_{i=1}^{r}(n-i+1)t_i - \frac{1}{r}\sum_{i=1}^{r}(n-i+1)t_{i-1} = \frac{1}{r}\left[\sum_{i=1}^{r}t_i + (n-r)t_r\right], \quad (5)$$

where $(n–r)t_r$=(100–20)·203,43=16274,4 (hours) is the total operation time of non-failed systems;

$\sum_{i=1}^{r} t_i = 2366{,}6$ (hours) is the total time of no-failure of all failed systems;

$\sum_{i=1}^{r} t_i + (n-r)t_r = 18641$ (hours) is the total operation time of all systems to the r^{th} failure.

4. Confidence interval of mean time to failure

The estimation of mean time to failure $\hat{t}^{\cdot}$ is a point estimate of the initial parameter t^*, which in turn is a random value and within a specific test can take any positive value from 0 to ∞. Therefore, in addition to the point estimation, an interval estimation of the measured parameter is usually performed. That means that estimation $\hat{t}^{\cdot}$ identifies the confidence interval $(\hat{t}_L^{\cdot}, \hat{t}_U^{\cdot})$ in which the true value of the measured parameter t^* with a specified probability is found

$$P\left\{\hat{t}_L^{\cdot} < t^* < \hat{t}_U^{\cdot}\right\} = \gamma, \tag{6}$$

where γ is the confident probability (or confidence coefficient), $\hat{t}_L^{\cdot}, \hat{t}_U^{\cdot}$ are respectively the lower and upper limits of the confidence interval.

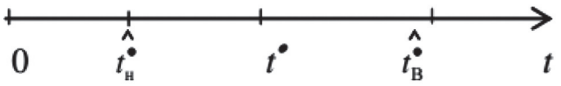


Figure 3. Confidence interval

In order to identify the confidence interval, we need to know the distribution function of estimation probability. For that purpose, we must transform formula (6) in such a way as to use normalized quantities

$\hat{t}_L^{\cdot} = \hat{t}^{\cdot}(1-\varepsilon_1)$
$\hat{t}_U^{\cdot} = \hat{t}^{\cdot}(1+\varepsilon_2)$, where $\hat{t}_U^{\cdot} - \hat{t}_L^{\cdot} = \hat{t}^{\cdot}(\varepsilon_1 + \varepsilon_2)$ is the length of the interval.

Then, (6) rewrites as

$$P\left\{\hat{t}^{\cdot}(1-\varepsilon_1) < t^* < \hat{t}^{\cdot}(1+\varepsilon_2)\right\} = \gamma \tag{7}$$

Given that

$$\begin{matrix} t^* > \hat{t}^{\cdot}(1-\varepsilon_1) \\ t^* < \hat{t}^{\cdot}(1+\varepsilon_2) \end{matrix} \text{ or } \begin{matrix} \hat{t}^{\cdot} < \dfrac{t^*}{1-\varepsilon_1} \\ \hat{t}^{\cdot} > \dfrac{t^*}{1+\varepsilon_2} \end{matrix},$$

formula (7) is as follows

$$P\left\{\frac{t^*}{1+\varepsilon_2} < \hat{t}^{\cdot} < \frac{t^*}{1-\varepsilon_1}\right\} = \gamma,$$

$$\text{or } P\left\{\frac{1}{1+\varepsilon_2} < \frac{\hat{t}^{\cdot}}{t^*} < \frac{1}{1-\varepsilon_1}\right\} = \gamma. \tag{8}$$

Thus, we need to find the PDF of the value $\dfrac{\hat{t}^{\cdot}}{t^*}$.

Out of (5) we can deduce that the total time to failure equals to

$$t_\Sigma = \hat{t}^{\cdot} r = \sum_{i=1}^{r}(n-i+1)y_i = 18844,43 \text{ (hours)}. \tag{9}$$

The probability density function of intervals y_i is known (1). In this law, the variable must be replaced in order to deduce the standard probability density with the variance equal to 1.

Let us denote by

$$z_i = \frac{n-i+1}{t^*} \cdot 2y_i; \frac{\partial y_i}{\partial z_i} = \frac{t^*}{2(n-i+1)}. \tag{10}$$

Then $w(z_i) = \dfrac{1}{2} e^{\frac{z_i}{2}}$ is the exponential density with unit variance.

It is known that in this case $\sqrt{z_i}$ has a Gaussian distribution, while $\sum_{i=1}^{r} z_i$ is distributed over $\chi^2(2r)$ with $2r = 40$ degrees of freedom, which is commonly used in statistics for processing of experimental data.

Given (9) and (10)

$$\sum_{i=1}^{r} z_i = \frac{2t_\Sigma}{t^*}.$$

Let us introduce the variable

$$\tau = \sum_{i=1}^{r} z_i = \frac{2t_\Sigma}{t^*} = \frac{2\hat{t}^{\cdot} r}{t^*},$$

τ is distributed over $\chi^2(2r)$ with $2r$ degrees of freedom; r is the number of failures.

The distributions $\chi^2(2r)$ are tabulated. For a large number of degrees of freedom this distribution tends to normal.

Let $\dfrac{1}{1+\varepsilon_2} = \alpha_2$ & $\dfrac{1}{1-\varepsilon_1} = \alpha_1$, then formula (8) for the confidence interval works out to

$$P\left\{2r\alpha_2 < \tau < 2r\alpha_1\right\} = \gamma. \tag{11}$$

Fig. 4 shows the PDF χ^2, the crosshatched area under the curve is the confident probability γ (the whole area under the PDF, as we know, equals to one). As shown in Fig. 4, the confidence interval can be plotted on the axis τ differently, i.e. the solution is ambiguous.

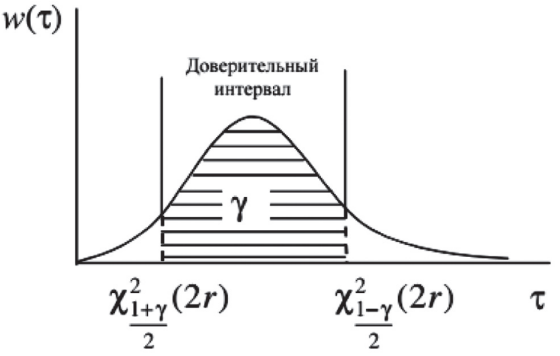


Figure 4. Probability density function χ^2

That is usually done to make the interval limits cut on the right and left identical areas under the curve equal to $\dfrac{1-\gamma}{2}$.

Then, the lower limit of the confidence interval $\chi^2_{\frac{1-\gamma}{2}}(2r)$ is $\left(\frac{1-\gamma}{2}\right)\%^{th}$ distribution point $\chi^2(2r)$, while the upper limit of the confidence interval $\chi^2_{\frac{1-\gamma}{2}}(2r)$ is $\left(\frac{1-\gamma}{2}\right)\%^{th}$ distribution point $\chi^2(2r)$, of which the values are identified in accordance with the $\chi^2(2r)$ inverse distribution tables.

Further, based on (11),

$$P\left\{\chi^2_{\frac{1+\gamma}{2}}(2r) < \tau < \chi^2_{\frac{1-\gamma}{2}}(2r)\right\} = \gamma,$$

or

$$P\left\{\chi^2_{\frac{1+\gamma}{2}}(2r) < \frac{2\hat{t}^{\cdot}r}{t^*} < \chi^2_{\frac{1-\gamma}{2}}(2r)\right\} = \gamma, \quad (12)$$

or

$$P\left\{\frac{2\hat{t}^{\cdot}r}{\chi^2_{\frac{1-\gamma}{2}}(2r)} < t^* < \frac{2\hat{t}^{\cdot}r}{\chi^2_{\frac{1+\gamma}{2}}(2r)}\right\} = \gamma.$$

From (12) it is seen that the lower limit of the confidence interval is equal to

$$t^* > \frac{2\hat{t}^{\cdot}r}{\chi^2_{\frac{1-\gamma}{2}}(2r)} = \hat{t}^{\cdot}_L,$$

while the upper limit is respectively equal to

$$t^* > \frac{2\hat{t}^{\cdot}r}{\chi^2_{\frac{1-\gamma}{2}}(2r)} = \hat{t}^{\cdot}_U.$$

Thus it can be established that for our tested radiotechnical system under a confident probability of 80% the true value of t^* lies in the range from $\hat{t}^{\cdot}_L = \frac{2\hat{t}^{\cdot}r}{\chi^2_{\frac{1-\gamma}{2}}(2r)} = 735{,}3\ (hours)$ to $\hat{t}^{\cdot}_U = \frac{2\hat{t}^{\cdot}r}{\chi^2_{\frac{1-\gamma}{2}}(2r)} = 735{,}3\ (hours)$.

5. Test duration

The duration of test corresponds with the moment of the r^{th} failure when the test stops. For the [n, B, r] procedure this value is random and it is important to evaluate it both for the contractor and the customer.

The PDF of this value is hard to find, as $T = t_r = \sum_{i=1}^{r} y_i$, while the values y_i are heterogeneous (depend on i (1)). So, let us just identify the average value (expectation) and variance.

Average test duration

$$m(T) = m(t_r) = \sum_{i=1}^{r} m\{y_i\} = \hat{t}^{\cdot}\sum_{i=1}^{r}\frac{1}{n-i+1}. \quad (13)$$

Let us write (13) as a series $m(t_r) = \hat{t}^{\cdot}\sum_{k=n-r+1}^{n}\frac{1}{k}$, where $k=n-i+1$.

Let us denote $\phi(m) = \sum_{k=1}^{m}\frac{1}{k}$,

then $m(t_r) = \hat{t}^{\cdot}\left[\phi(m) - \phi(n-r)\right]$

It is known that if $m>>1$, the function $\phi(m) \approx \ln m$.

Then if $r>>1$, the average test duration

$$m(t_r) \approx \hat{t}^{\cdot}\ln\frac{n}{n-r}.$$

If $n = r$, then $m(t_r) = \hat{t}^{\cdot}\phi(n) = \hat{t}^{\cdot}\ln n = 4385{,}93$ (hours).

The variance of test duration equals to

$$D(t_r) = \hat{t}^{\cdot 2}\sum_{i=1}^{r}\frac{1}{(n-i+1)^2}. \quad (14)$$

Let us denote $\phi(m) = \sum_{k=1}^{m}\frac{1}{k^2}$, then

$$D(t_r) = \hat{t}^{\cdot 2}\left[\phi(n) - \phi(n-r)\right].$$

If $n \to r$, then $D(t_r) \to \hat{t}^{\cdot 2}\cdot\frac{\pi^2}{6}$.

I.e. the variance of test duration decreases as r grows, but tends not to zero, but a constant number, therefore this procedure is not very efficient.

Identification of dependability indicators based on the results of test of a specific pilot batch of RESs according to the [n, V, r] procedure

1. Problem specification

It is assumed that the conditions of this problem are comparable with those of the above one. As a result of the test, a sample of instants of failure was obtained.

The failure model for one system is

$$w(t) = \lambda e^{-\lambda t}, t > 0, \lambda > 0,$$

or

$$w(t) = \frac{1}{t^*}e^{-\frac{t}{t^*}}, t > 0,$$

where t^* is the average time to failure.

The sample of intervals $y_i = t_i - t_{i-1}$ is homogenous and is governed by probability density

$$w(y_i) = n\lambda e^{-n\lambda y_i},$$

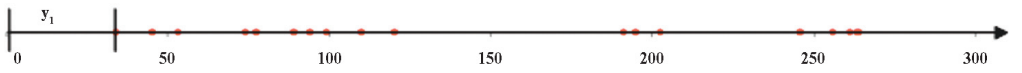


Figure 5. Instants of failure and failure cycle

where $n\lambda$ is the collective failure rate of the systems involved in the test.

2. Identification of mean time to failure

The estimation of the mean time to failure $\hat{t}^*$ can also be performed by means of the maximum likelihood method.

For the purpose of the current task, the likelihood function represents the PDF of the intervals y under the given value of the parameter t^*

$$L_y\left(t^*\right)=\prod_{k=1}^{r} w\left(y_k\right)=\left(\frac{n}{t^*}\right)^r \cdot e^{-\sum_{k=1}^{r}\frac{-n}{t^*}y_k}.$$

The maximum likelihood estimation of $\hat{t}^*$ is defined as the parameter that corresponds to the maximum of the likelihood function

$$\frac{\partial \ln L_y\left(t^*\right)}{\partial t^*}=\frac{-r}{t^*}-\frac{n}{t^{*r}}\cdot\sum_{k=1}^{r} y_k=0.$$

Then the estimation is

$$\hat{t}^*=\frac{n}{r}\sum_{k=1}^{r} y_k=\frac{n\cdot t_r}{r}=1319{,}85 \text{ (hours)},$$

where $n\cdot t_r = t_\Sigma = 26397$ (hours) is the total time to failure shared by both test plans. It implies that $\hat{t}^*=\frac{t_\Sigma}{r}$, and the quality of estimation is identical to that of the procedure [n, B, r] under identical t_Σ and r.

3. Average duration of test

$$m\left\{t_r\right\}=\sum_{k=1}^{r} m\left\{y_k\right\}=\frac{r}{n}t^*.$$

If $n = r$, then $m\left\{t_r\right\}=t^*=1319{,}85$ (hours), which is less than under the procedure [n, B, r].

Variance of the duration of test

$$D\left\{t_r\right\}=\sum_{k=1}^{r} D\left\{y_k\right\}=\frac{r}{n^2}\left(t^*\right)^2.$$

If $n = r$, then $D\left\{t_r\right\}=\frac{\left(t^*\right)^2}{n}$ and tends to zero if n increases. Therefore, this test procedure is more efficient compared to [n, B, r].

Conclusions

The article examined two procedures for testing pilot batches of radioelectronic systems and for each of them the following dependability indicators were identified:

- estimation of mean time to failure;
- confidence interval of mean time to failure;
- it is shown that for the purpose of identifying the mean time to failure test procedure [n, V, r] is more efficient than procedure [n, B, r].

References

1. Zhadnov VV, Polesky SN. Proektnaya otsenka nadiozhnosti radiotekhnicheskikh sistem [Engineering estimate of dependability of radiotechnical systems]. Yurkov NK, editor. Nadiozhnost i kachestvo, tr. Mezhdunar. simpoz.: v 2 t., Vol. 1 [Dependability and quality, Third International symposium: in 2 vol., Volume 1]; 2006; Penza, Russia. Penza: Penza State University Publishing; 2006. Russian

2. Zhadnov VV, Sarafanov AV. Oupravlenie kachestvom pri proektirovanii teplonagruzhennykh radioelektronnykh sredstv [Quality management in the design of thermally loaded radiolectronics facilities]. Moscow: Solon-Press; 2004. Russian.

3. Artiukhova MA, Zhadnov VV, Polessky SN. Metod uchyota vliyaniya sistemy menedzhmenta nadyozhnosti predpriyatiya pri raschyotnoj otsenke pokazatelej nadyozhnosti ehlektronnykh sredstv [Method for accounting of the impact of enterprise dependability management system in estimation of dependability indicators of electronic facilities]. Radioelekpronika, informatika, ouparvlinnia [Radioelectronics, information technology, control]. 2013; 2:48 – 53. Russian.

4. Filippov BI. Apriornyj analiz nadyozhnosti radiotekhnicheskikh sistem bez vosstanovleniya [A priori dependability analysis of radiotechnical facilities without recovery]. Izvestia VolgGTU, seria Elektronika, izmeritelnaya tekhnika, radiotekhnika i sviaz [Journal of the Volgograd State Technical University, Electronics, Measurement Technology, Radio Technology and Communication Series]. 2015; 11 (176): 97 – 111. Russian.

5. Filippov BI. Aposteriornyj analiz nadyozhnosti radioelektronnykh sistem [A posteriori dependability analysis of radiotechnical facilities]. Vestnik AGTU, seria Oupravlenie, vychislitelnaya tekhnika i informatika [Journal of the Astrakhan State Technical University, Control, Computer and Information Technology Series]. 2015; 9: 81 – 91. Russian.

6. Nadiozhnost ERI: Spravochnik [Dependability of electronic components: Reference book]. Moscow: Ministry of Defense Press; 2006.

7. Levin BR. Teoria nadiozhnosty radiotekhnicheskikh sistem [Dependability theory of radiotechnical systems]. Moscow: Sov. radio; 1978. Russian.

About the authors

Boris I. Filippov, Candidate of Engineering, Assistant Professor, Senior Lecturer in Information Protection, Novosibirsk State Technical University. Russia, 630099, Novosibirsk, Uritskogo Str., 17, app. 13, phone: +7 (923) 225 67 21, e-mail: Fillippov-boris@rambler.ru

Yulia V. Zamiatina, student, Information Protection Department, Novosibirsk State Technical University. Russia, 630017, Novosibirsk, B. Bogatkova Str., 192/5, app. 183, phone: +7 (913) 209 46 56, e-mail: e-zamiatina.abs323@gmail.com

Received on 24.11.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-32-39
Dependability, vol. 17 no.1 2017 УДК: 004.056.53

Method for risk evaluation of functional instability of hardware and software systems under external information technology interference

Sergey G. Antonov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Russia, Korolyov, e-mail: sergey_antonov_1960@mail.ru.*
Sergey M. Klimov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Russia, Korolyov, e-mail: klimov.serg2012@yandex.ru*

Sergey G. Antonov

Sergey M. Klimov

Abstract. *The aim of the article is to develop a method that would allow for a quantitative evaluation of stability risks of hardware and software systems under simulated information technology interference and simulation of real management process cycle. The article shows the relevance and importance of the methods for risk evaluation of hardware and software systems stability in the context of targeted and coordinated information technology interference. Information technology interference is understood as targeted and coordinated hardware and software, as well as software actions aimed at temporary disruption of operation or logical defeat of hardware and software systems. Successful information technology interference is conditioned by the presence of vulnerabilities in the hardware and software systems that include IP and MAC addresses and communication equipment ports available to the intruder. The method presented in the article is based on the following: risk evaluation is performed using a test bed or active facilities with the involvement of respectively a fixed and portable information technology measures simulation system. The risk of destabilization of hardware and software systems is evaluated experimentally as the combination of frequency and consequences of successful information technology interference. The preliminary risk evaluation allows choosing the solution for information protection in order to eliminate potential vulnerabilities. The residual risk is evaluated based on the ability of hardware and software systems to eliminate the consequences of information technology interference through various inbuilt resilience features. The research resulted in the proposed method of evaluation hardware and software system security risks under information technology interference as a logical sequence of steps: risk analysis of information technology interference; identification of vulnerabilities, simulation of system operation processes under information technology interference at the trial facility; selection of the best information protection and system fault tolerance facilities; preliminary an final evaluation of system stability risks. As part of the method, probability and temporal indicators of hardware and software systems stability risk evaluation were developed that enable analysis of recovery from threats of combined information technology interference, selection of rational information protection and fault tolerance measures. As part of the method, it is proposed to use a cubic analysis scheme of elimination of vulnerabilities of critical elements of hardware and software systems that allows identifying the levels of tolerable risk and levels of reference model of interaction of open systems required for elimination of vulnerability subject to the frequency of information technology interference. Additionally, a certificate of evaluation of stability risks of hardware and software systems subject to the frequency of successful interferences was developed. In the conclusion it is noted that the developed method allows using the knowledge regarding potential vulnerabilities and experimental studies to identify the probabilistic values of security risks in order to determine the most hazardous threats and adoption of respective information protection measures.*

Keywords: *hardware and software systems, information technology interference, stability risks, information protection and fault tolerance facilities.*

For citation: *Antonov S.G., Klimov S.M. Method for evaluation of risks of functional instability of hardware and software systems under external information technology interference. Dependability, 2017, vol. 17, no. 1, pp. 32-39. (in Russian). DOI: 10.21683/1729-2640-2017-17-1-32-39*

Introduction

A number of nations, as well as the hacker community are actively involved in the development of software designed for preparation, delivery and secret introduction of information technology interference (ITI) code (computer attacks) against automated process control systems in transportation, energy, telecommunications and other industries [4]. The basic elements of the above automated systems are hardware and software systems (HSSs) interconnected by communications equipment and distributed computer networks.

Currently, HSSs represent sets of information management facilities designed for real-time collection, processing, output of control information and information interaction

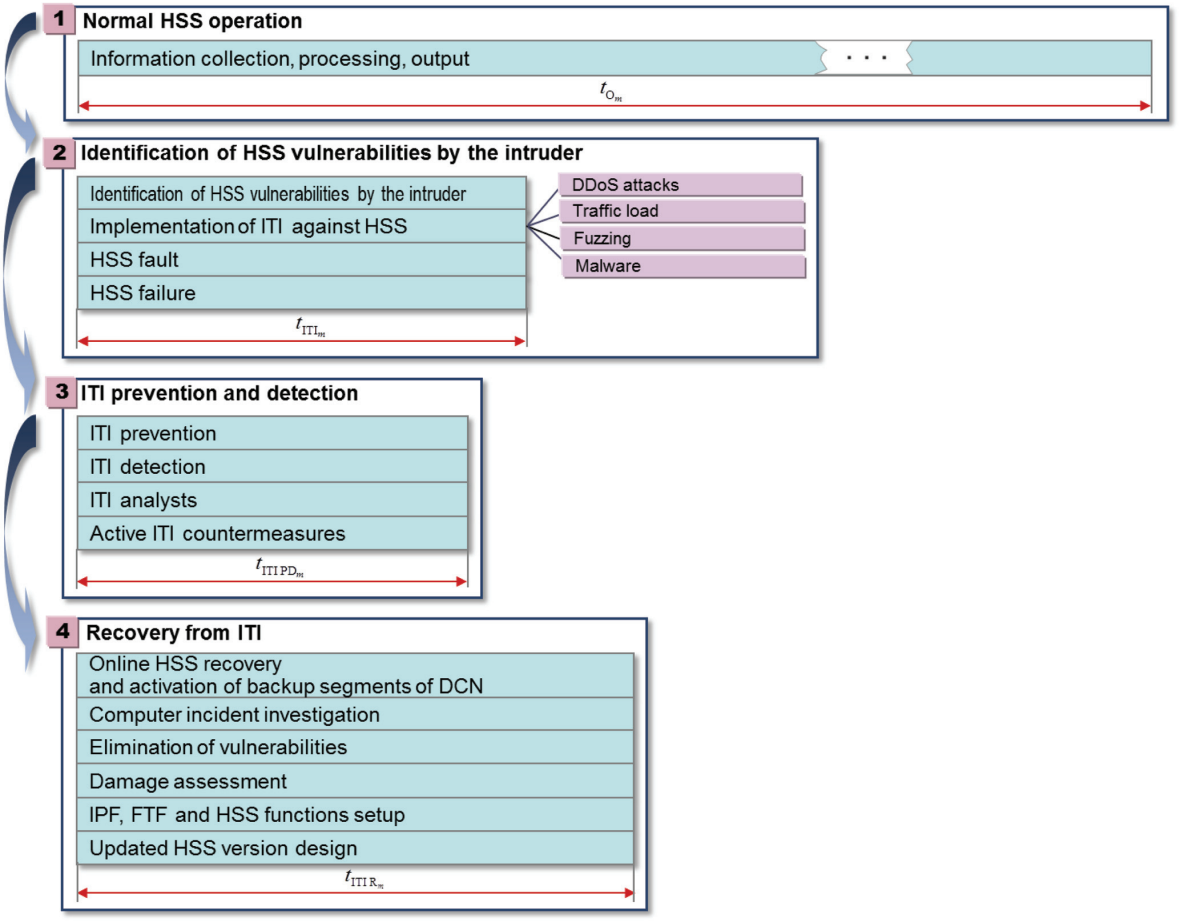


Figure 1. Time picture of HSS-based DCN operation processes under ITI

between control elements and data management centers. In this article H SSs are primarily regarded as complex and multifunctional sets of programs, while the technical equipment is regarded as the processing resource required for the execution of such programs.

HSS-based distributed computer networks (DCNs) are essentially critical distributed information management systems that can be targeted by intruders' ITIs.

ITIs are understood as targeted and coordinated hardware and software, as well as software actions aimed at temporary disruption of operation or logical defeat of HSSs. The above interferences can be considered a variety of malicious remote computer attacks against software, control processes, computer and telecommunications equipment of a HSS network [1].

The HSS components vulnerable to ITIs are accessible IP, MAC addresses and port numbers of communication equipment. The potential vulnerabilities of the considered HSSs are due to the following:

a) use of public TCP/IP data communication protocols; foreign-made backbone link equipment with potential undocumented capabilities and remote programmed control; untrusted hardware and software platforms (imported servers, e-mail software, self-updating operating systems or kernels);

b) possible unauthorized actions of internal intruders aimed at intentional or unintentional ITI;

c) uncoordinated and inadequate operation of diverse elements of information protection facilities (IPF).

As the above vulnerabilities condition the potential possibility of implementation of ITIs that could cause disruptions in HSS operation, the development of a method that would allow for a quantitative evaluation of HSS stability risks under simulated ITIs is of relevance.

Problem definition

The research is based on the following premises:

- risk assessment can be done on a test bed or active facilities using respectively fixed and portable ITI simulation systems;
- risk is evaluated experimentally based on the frequency of successful ITIs;
- preliminary risk assessment allows choosing an IPF solution to address potential vulnerabilities;

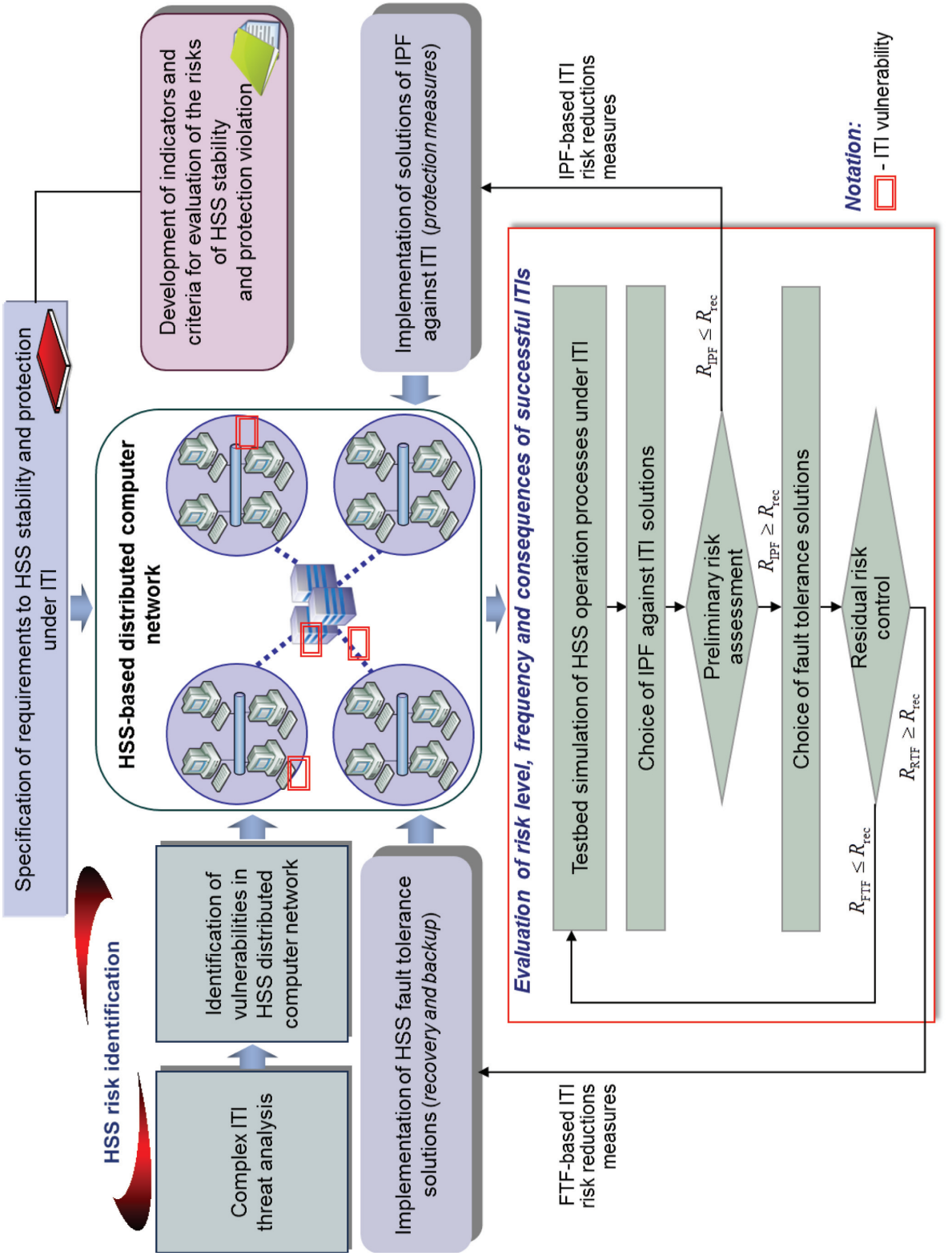


Figure 2. Evaluation scheme of HSS security risks under ITI

- the residual risk is evaluated by the ability of HSS to eliminate the consequences of ITI by means of fault tolerance facilities (FTF), i.e. HSS functions and elements recovery and backup facilities.

Figure 1 shows the time picture of the HSS-based DCN operation processes under ITI that are represented in seven standard periods.

The particular feature of ensuring operational stability of HSS under ITI consists in the fact that, in theory, a multitude of ITIs is supposed to be countered by the IPF. At the same time, in practice the IPF only record ITIs against HSS at best, while the task of ensuring the operability and restorability of the disrupted system remain unsolved. It should be noted that state-of-the-art ITIs, the so-called targeted computer attacks, are primarily intended for incapacitating HSSs by disrupting the probabilistic and temporal characteristics of their information processing policy. The consequences of a successful ITI against an HSS consist in short-time faults (from several seconds to 30 minutes) and failures (up to several hours) of HSSs.

The time taken to execute the information management functions of the HSS' special software (SSW) under ITI is the primary parameter of its operational stability.

The notations for Figure 1 are as follows:

t_{O_m} is the operation time of DCN with HSS; t_{ITI_m} is the duration of the intruder's ITI; $t_{PD\ ITI_m}$ is the time taken to prevent and detect the intruder's ITI; $t_{R\ ITI_m}$ is the time of ITI recovery.

Therefore, the total time of the control process cycle (CPC) of DCN with HSS under ITI can be defined with the formula:

$$t_{CPC} = \sum_{m=1}^{N} [t_{O_m} - (t_{ITI_m} + t_{PD\ ITI_m} + t_{R\ ITI_m})], \quad (1)$$

where $m=\{1, 2, \ldots, N\}$ is the natural integers.

An assessment of HSS risks under ITI involves the following:

1. Choice of assessed HSSs and definition of the detail of their characteristics evaluation within the CPC.
2. Simulation of a set of ITIs against HSS.
3. Identification of known and unknown ITIs in the context of the dynamic HSS operation process.
4. ITI analysis (parametric identification, cataloguing of signatures and updating of ITI database).
5. Choice of solutions for protection of information against ITI (ITI countermeasures) and HSS fault tolerance (recovery and backup).

While using state-of-the-art ITI counter-strategies and critical information systems risk management methods [1–3, 5–7], let us represent the method for evaluation of HSS security risks under ITI as the following sequence of steps (Figure 2):

1. Complex ITI threat analysis.
2. Identification of vulnerabilities of DCN with HSS.
3. Testbed simulation of HSS operation processes under ITI.
4. Choice of solutions for protection of information against ITI.
5. Preliminary assessment of the risk to HSS stability with the chosen IPFs (under the optimal solution for protection of information against ITI).
6. Choice of HSS fault tolerance solutions.
7. Residual risk control (final assessment) subject to the chosen HSS fault tolerance solution.

Table 1. Standard HSS vulnerabilities certificate

HSS vulnerability description elements	HSS vulnerability description
1. Name of vulnerability	Operator HSS vulnerability
2. Vulnerability identifier	HSS-2016-00007
3. Brief description of vulnerability	Vulnerability allows malicious HSS takeover
4. Vulnerability class	Windows OS vulnerability
5. Name of vulnerable element and its version	Version 10 e-mail modules
6. HSS data communication protocol	Data communication protocol, direct access to HSS controls
7. HSS hardware and software design details	Hardware and software platform is based on the client/server, hypervisor and software virtualization technologies, data communication protocol TCP/IP v.6, special software version 1.1
8. Type of defect	Operator authentication defects
9. Location of occurrence (manifestation) of vulnerability	Vulnerability exists due to the absence of legitimacy test of the source of HSS control
10. Defect type identifier	No data
11. Date of vulnerability detection	1.11.2016
12. Author of information on detected vulnerability	Information security unit
13. Means (rule) of vulnerability detection	Execution of step-by-step instructions
14. Vulnerability hazard criteria	Exceeding of specified risk probability value
15. Hazard level of vulnerability	High
16. Possible vulnerability elimination measures	Improvements to information protection facilities and HSS information interaction protocols
17. Additional information	A Juniper router is used in the network

Table 2. Certificate of evaluation of HSS stability risks under ITI

ITM frequency	ITM risk evaluation			ITM hazard rate
	I variant *CADPF functions minimal*	II variant *CADPF functions medium*	III variant *CADPF functions maximal*	
Incredible event $P_{ITI} \leq 10^{-8}$ 1/h	Low	Low	Low	Minor
	Score: 3	Score: 3	Score: 3	Total score: 9
Possible event $P_{ITI} \leq 10^{-7}$ 1/h	Low	Medium	High	Tolerable
	Score: 3	Score: 5	Score: 7	Total score: 15
Probable event $P_{ITI} \leq 10^{-6}$ 1/h	Medium	High	High	Undesirable
	Score: 5	Score: 7	Score: 7	Total score: 19
Probability of event is high $P_{ITI} \leq 10^{-5}$ 1/h	Medium	High	Very high	Significant
	Score: 5	Score: 7	Score: 10	Total score: 22
Probability of event is very high $P_{ITI} \leq 10^{-4}$ 1/h	High	High	Very high	Intolerable
	Score: 7	Score: 7	Score: 10	Total score: 24
The event will certainly happen $P_{ITI} \leq 10^{-3}$ 1/h	High	Very high	Very high	Critical
	Score: 7	Score: 10	Score: 10	Total score: 27

The complex ITI threats to HSS include the following simulated effects:

- distributed denial of service (DDoS attacks);
- traffic load with data batches (multiple streams with standard data batches);
- fuzzing, i.e. exposure to non-standard (with distorted fields) data batches;
- secretly inserted and self-propagating malware.

Step 1. It is suggested to analyze complex ITI threats using a classification similar to the one suggested in [1], i.e. in terms of classification criterion of ITI effect on HSS. According to the above classification criterion let us identify ITIs of five types:

- functional disruption (fault or failure) of HSS;
- link disconnections in data communication channels;
- insertion of false information (distortion of information);
- information overloading of HSS;
- identification of zero day ITI vulnerabilities by means of fuzzing (multiple streams of semantically distorted data batches).

Step 2. Let us identify the vulnerabilities of DCN with HSS for the purpose of developing the ITI simulation model by using GOST R 56546-2015 "Information security. Vulnerabilities of information systems. Classification of vulnerabilities of information systems" and designing a standard HSS vulnerabilities certificate (Table 1).

The method assumes the presence of potential zero day vulnerabilities in the software design of data communication protocols, communications equipment, operating systems, device drivers and other HSS-based DCS components within 3-5% of all possible IP, MAC addresses and port numbers.

Step 3. Simulation of HSS operation processes under ITI involves using the specially equipped test bed to experimentally reproduce interrelated processes:

- normal operation of a segment of a distributed computer network with HSS;
- simulation of an intruder's ITI system;
- ITI counteractions based on various applications of IPF and FTF.

Modelling the above processes should allow experimental research and analysis of HSS network security under ITI. HSS network security is analyzed per seven levels of the reference model of interaction of open systems (RM IOS) by verifying the implementation of DCN security functions at each level. The most important aspect of evaluation of HSS security under ITI is to verify the access control to network services at the transport, session and network levels of RM IOS.

The level of detail of the HSS, ITI, IPF and FTF simulation models is to ensure reproduction of the main functions of risk objects, performance of a sufficient number of tests and generation of statistical data for risk assessment.

Step 4. To an array of chosen IPFs against ITI we'll ascribe the following:

- computer attack detection and prevention facilities (CADPF);
- firewalls (FW);
- false network information objects (FNIO);
- virus protection facilities (VPF);

- automated trusted loading modules (ATLM), identification and authentication of operators.

Let us assume that a DCN with HSS carries restricted access information. Then let us define that the proposed method considers IPF classes that ensure protection of restricted access information in DCN.

Step 5. Preliminary evaluation of risks of HSS stability with chosen IPFs.

The choice of measures and means of information protection against ITI must involve vulnerability diagnostics of network configuration and software, each of the IPFs for compliance with regulatory documents, as well as a general assessment. The input data for preliminary assessment of the risk to HSS stability with the chosen IPFs under ITI are as follows:

1. The probability of detection and identification of complex ITIs can take minimum (0,2–0,4), medium (0,5) and maximum values (0,7–0,9).

2. The probability of implementation of ITI against HSS can take minimum (0,2–0,4), medium (0,5) and maximum values (0,7–0,9).

3. The options of measures and means of information protection against ITI are finite (3 – 5 solutions) and are defined by the certified IPFs that can be used as part of HSS (subject to the nature of its hardware and software platform).

The control of the required level of HSS information protection under ITI is ensured by maintaining the value of probability of CPC performance over a given time (for near-rel-time systems) under ITI not lower than required (for instance, R_{rec}=0,95).

Complex ITIs disrupt HSS protection and primarily jeopardize the availability and integrity of information, data batch routing logic. An intruder carries out interference only if an HSS has vulnerabilities.

A preliminary assessment of the risk of HSS security violation involves experimental verification of the capability to ensure HSS and IPF elements functional stability against faults and failures under ITI.

It is assumed that ITI processes are independent and exponentially distributed. The probability of successful ITI conditions the risk of HSS faults and failures.

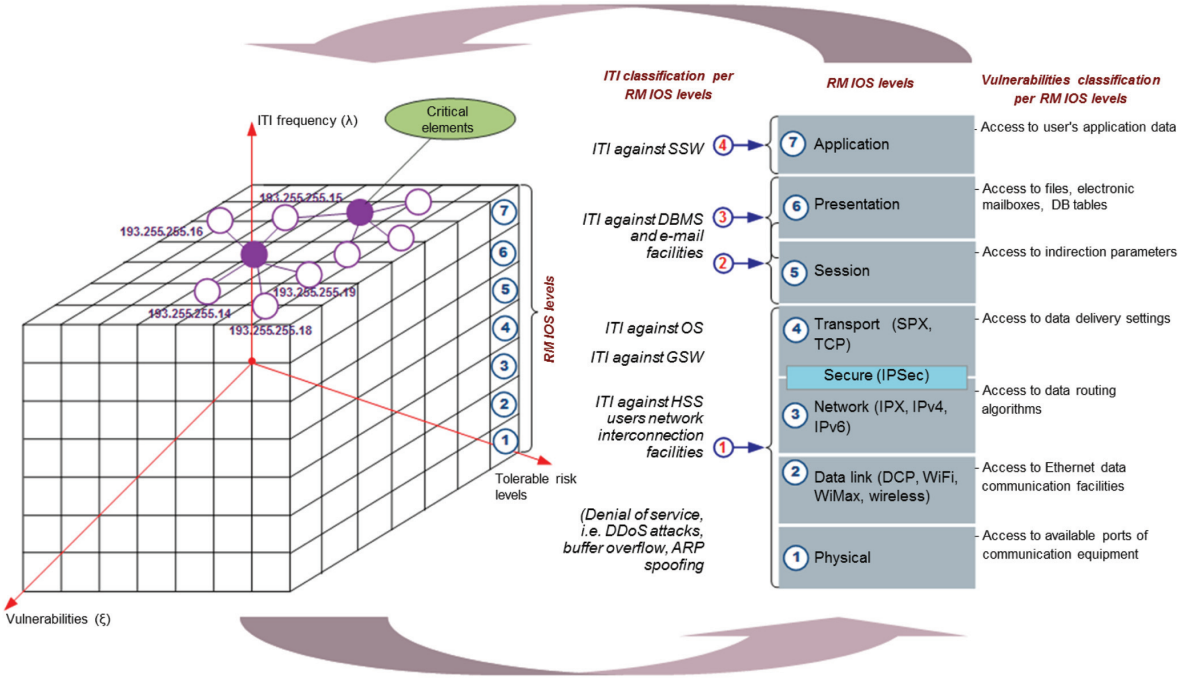
A preliminary assessment of HSS risks under ITI includes the following:

a) development of indicators for risk evaluation:

- probability (frequency) of successful ITI (according to Table 2), P_{ITI};
- probability of successful ITI countermeasures, P_{SCM};
- expected damage (levels of ITI consequences, Table 2) – Υ_i;
- the value of risk of HSS security violation due to ITI equals to the product of the probability of successful ITI ant the expected damage, R_{ITI_j};

b) choice of confidence interval (tolerability limits) of successful HSS-based ITI [5]:

- identification of confident probability:



Notations: *special software (SSW), database management system (DBMS), operating system (OS), general software (GSW), data communication protocol (DCP).*

Figure 3. Cubic analysis scheme of elimination of vulnerabilities of critical elements of HSS

$P_{ITI}(\varepsilon)=\beta=0,95$ is the maximum achievable value for HSSs of complex systems [2], where ε is a half of the length of the confidence interval;

- identification of HSS failure rate as a result of successful ITI:

$$\lambda_{ITI_i}=\sum_{i=1}^{m}\frac{n_{D\ HSS_i}}{N_{HSS_i}t_{ITI_i}}, \quad (2)$$

where λ_{ITI_i} is the average number of successful ITIs per time unit; $n_{D\ HSS_i}$ is the number of disrupted HSSs in DCN; N_{HSS_i} is the total number of HSSs in DCN; t_{HSS_i} is the duration of ITI; m is the number of tests;

c) identification of a potential risk value for HSS solution per correlation (of fault and failure rate as a result of successful ITI):

$$R_{HTB_i}^{ITTP}\left(t_{HTB_i}\right)=\left[\prod_{i=1}^{k}\left(1-e^{-\lambda_{HTB_i}t_{HTB_i}}\right)\right]\gamma_i, \quad (3)$$

where i is the HSS solution; γ_i is the magnitude of damage caused by ITI (identified from the total score in Table 2).

Calculating R_{ITI_j} follows the principle of the risk being as low as practically possible.

Step 6. Choice of HSS fault tolerance solutions based on redundancy (structural and functional redundancy) and recovery (time redundancy of process control cycles of DCN with HSS) using [1–3]:

a) the HSS fault tolerance based on recovery facilities (assuming that FTF ensures elimination of ITI consequences by recovering HSS) will be defined with the formula for probability of recovery:

$$P_{rec}^{FTF}\left(t_{rec}\right)=\frac{\mu_{R_i}}{\lambda_{ITI_i}+\mu_{R_i}}+\frac{\lambda_{ITI_i}}{\lambda_{ITI_i}+\mu_{R_i}}e^{-(\lambda_{ITI}+\mu_R)t_{rec}}, \quad (4)$$

where under condition of exponential law of distribution of ITI frequency and HSS elements recovery, μ_{R_i} is the HSS recovery rate based on the i^{th} HSS;

b) the HSS fault tolerance based on redundancy will be defined with the formula for availability factor:

$$K_{A_i}^{HSS}=\frac{1}{1+m\dfrac{\lambda_{ITI_i}}{\mu_{R_i}}}P_{adap}, \quad (5)$$

where m is the number of backup HSS elements in DCN; P_{adap}>0,85-0,90 is the probability of successful HSS adaptation to faults and failures after occurrence of ITI.

Step 7. Residual risk control (final evaluation) subject to the chosen HSS fault tolerance solution consist in the fact that for the chosen solutions and IPF against ITI, additional risk evaluations are performed that allow confirming that said measures and IPF allow reducing the risk to the tolerable level (as practically achievable).

The condition of minimization of residual risk of the chosen solution for HSS fault tolerance under ITI is considered the elimination of vulnerabilities that can be exploited for accomplishing the interference or the neutralization of ITI by means of coordinated application of IPF and FTF.

Figure 3 shows the proposed cubic analysis scheme of elimination of vulnerabilities of critical elements of HSS that allows identifying the levels of tolerable risk and levels of RM IOS required for elimination of vulnerability subject to the frequency of ITI.

The cubic scheme is used as follows:

a) one of the seven RM IOS levels is chosen (as an example, in the scheme the seventh level is chosen), at which the critical HSS elements are considered;

b) using Table 1, the facts of elimination or non-elimination of HSS vulnerabilities are established;

c) on the right-hand side of Figure 3 (ITI types corresponding to available network services at RM IOS levels) the possible ITIs for the respective level are chosen;

d) based on experimental data and Table 2, ITI frequencies are identified;

e) the tolerable risk for critical HSS elements is defined based on the mathematics:

$$R_{ITI_j}^{TR}\left(t_{ITI_j}\right)=\gamma_{HSS_j}\prod_{j=1}^{N_E}\left[1-P_{vul_j}\left(t_{ITI_j}\right)P_{ITI_j}\left(t_{ITI_j}\right)\right], \quad (6)$$

where t_{ITI_j} is the period of time of the j^{th} ITI implementation by the intruder; γ_{HSS_j} is the damage caused by the fault (failure) of a critical HSS element during the j^{th} ITI; N_E is the number of experiments; $P_{vul_j}\left(t_{ITI_j}\right)$ is the probability of vulnerability exploits over time t_{ITI_j}, identified by means of expertise or based on statistical data of HSS-based DCN operation; $P_{ITI}\left(t_{ITI_j}\right)$ is the probability of successful implementation of the j^{th} ITI over time t_{ITI_j} against a critical HSS element.

Let us evaluate the minimal possible risk of HSS destabilization under ITI using the Savage test:

$$R_{HSS}(t_{CPC})=\max_i \min_j R_{ITI_{ij}}(t_{CPC}), \quad (7)$$

where i is the fault tolerant DNS with HSS solution based on IPF and FTF; j is the successful ITI against HSS.

Conclusion

As the result of examination of HSS-based DNSs that can be targeted by ITIs, the article proposes a method to be used to evaluate actual level of protection of HSSs against ITIs that allows using the knowledge regarding potential vulnerabilities and experimental studies to identify the probabilistic values of security risks in order to determine the most hazardous threats and adopt respective information protection measures.

References

1. Klimov SM, Astrakhov AV, Sychiov MP. Tekhnologicheskiye osnovy protivodeystvia kompiuternim atakam. Elektronnoe ouchebnoe izdanie [Basic processes of computer attack reaction. Electronic study guide]. Moscow: Bauman MSTU; 2013. Russian.

2. Klimov SM., Astrakhov AV, Sychiov MP. Metodicheskie osnovy protivodeystvia kompiuternim atakam.

Elektronnoe ouchebnoe izdanie [Basic methods of computer attack reaction. Electronic study guide]. Moscow, Bauman MSTU; 2013. Russian.

3. Klimov SM, Astrakhov AV, Sychiov MP. Eksperimentalnaia otsenka protivodeystvia kompiuternim atakam. Elektronnoe ouchebnoe izdanie [Experimental evaluation of computer attack reaction. Electronic study guide]. Moscow: Bauman MSTU; 2013. Russian.

4. Ovchinsky VS. Novaya strategia kiberbezopasnosti SShA [The new US cyber security strategy]. Mezhdunarodny nauchno-analiticheskiy zhurnal Strategicheskie prioritety [Strategic Priorities International Scientific and Analytical Journal]. 2015; 4 (8): 41 – 48. Russian

5. Shubinsky IB. Strukturnaya nadiozhnost informatsionnykh system. Metody analiza [Structural dependability of information systems. Analysis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2012. Russian.

6. Shubinsky IB. Funktsionalnaia nadiozhnost informatsionnykh system. Metody analiza [Functional reliability of information systems. Analysis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2012. Russian.

7. Shubinsky IB. Nadiozhnie otkazoustoychivie informatsionnie systemi. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016. Russian.

About the authors

Sergey G. Antonov, Head of unit, 4th Central Research and Design Institute of the Ministry of Defence of Russia. 38/2 M.K. Tikhonravova Str., app. 176, 141092 mkr. Yubileyny, Korolyov, Moscow Oblast, Russia, phone: +7 (916) 788-57-92, e-mail: sergey_antonov_1960@mail.ru.

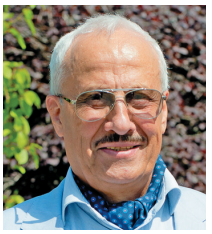
Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4th Central Research and Design Institute of the Ministry of Defence of Russia. 12 B. Komitetskaya Str., app. 105, 141092 mkr. Yubileyny, Korolyov, Moscow Oblast, Russia, phone: +7 (985) 928-13-55, e-mail: klimov.serg2012@yandex.ru.

Received on 22.12.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-40-45

Graph method for evaluation of process safety in railway facilities

Igor B. Shubinsky, *ZAO IBTrans, Moscow, Russia, e-mail: igor-shubinsky@yandex.ru*
Alexey M. Zamyshlyaev, *JSC NIIAS, Moscow, Russia, e-mail: A.Zamyshlyaev@vniias.ru*
Olga B. Pronevich, *JSC NIIAS, Moscow, Russia, e-mail: O.Pronevich@vniias.ru*


Igor B. Shubinsky


Alexey M. Zamyshlyaev


Olga B. Pronevich

Aim. *Industrial safety (OS) is the state of protection of operating personnel from harmful effects of manufacturing processes, energy, equipment, objects, conditions and schedule of work [1]. The most efficient evaluation of OS in railway transportation is ensured by composite indicators, one of which is the risk assessment indicator. That is also reflected in the Russian legislation that stipulates the requirement to evaluate fire, occupational and other types of risks that affect industrial safety. According to the definition set forth in GOST 33433-2015 [2] risk is a combination of the probability and consequences of an event. The most complicated task related to risk assessment is the choice of the evaluation model for the probability of an undesired event. The model must enable practical applicability of evaluation results for planning of risk compensation measures. Currently, there are a large number of probability evaluation methods that can be divided into two large groups, i.e. expert and quantitative. Expert methods have several well-known shortcomings. The quantitative methods require the construction of a system of equations or an analytical model. In the context of railway facilities the construction of analytical models of probability evaluation is of principal interest due to the possibility of demonstration of the factors that are taken into consideration by the model. The aim of the article is to formalize the analytical method for evaluation of the probability of railway facility transfer into a hazardous state (in the context of industrial safety).* **Methods.** *Undesirable events that cause industrial safety incidents in railway facilities are random; they can be represented as a random process. A random system development process, including objects transition from a safe state into hazardous (undesirable) states, i.e. system state change in time, can under some assumptions be described with a semi-Markov process. In general, the construction and solution of semi-Markov models comes down to building a system of homogenous differential equations. This procedure always involves mathematical difficulties. [3] shows the possibility of representation and solution of semi-Markov models with a coupled graph model. Such models are highly visual, and allow formalizing the wanted system states, as well as paths of transition from safe into hazardous states. The main problem of modelling random processes of industrial safety state changes is the requirement to identify the complete list of hazardous states and preceding non-hazardous or pre-hazardous states. The processes typical to railway facilities are characterized by a multitude of states that cause various events. The concept of "state" usually characterizes an instantaneous image, a "cross-section" of a system. Thus, at the first stage of construction and solution of a model of random process of a system's industrial safety state change, the finite sets of safe and hazardous states of the railway facility under consideration are identified in accordance with the known hazardous state criterion [4]. As the process of state change of a system's industrial safety in railway transportation is random in time, in this article system operation is described with a semi-Markov process with the assumption that the discrete process is described with an embedded Markov chain. The set of system states and their connections are represented with a directed state graph with defined topological concepts [3]. For a constructed model, the article provides the proof of the theorem identifying the probability of system transition from an initial non-hazardous into a hazardous state, as well as the formula for calculation of such probability.* **Results.** *The graph method for evaluation of industrial safety in railway facilities developed in this article includes both the rules of construction of a system's safety states graph and the tool for evaluation of the probability of system transition into a specific hazardous state. The graph is the basis of the practical method for calculation and forecasting of industrial safety incidents. The article provides the proof of the theorem identifying the probability of system transition from an initial non-hazardous into a hazardous state, as well as an example of application of graph method for evaluation of probability of fire in a fixed facility. The proposed probability evaluation method can be used in planning of industrial safety measures in terms of specification of new states or rules of transition into associated states.*

For citation: *Shubinsky I.B., Zamyshlyaev A.M., Pronevich O.B. Graph method for evaluation of process safety in railway facilities. Dependability. 2017, vol. 17, no. 1, pp. 40-45. (in Russian) DOI: 10.21683/1729-2640-2017-17-1-40-45*

Introduction

The industrial safety indicators are divided into two types, i.e. actual and calculated (planned). Among the actual indicators are occupational injuries frequency factors, size of insurance payouts, fire frequencies, charges for negative environmental effects, etc. The actual indicators can be represented in either absolute or relative values that are defined by means of direct measurements. The calculated indicators of industrial safety normally fall into the category of composite or integrated indicators. According to the Russian and global experience, the most efficient calculated indicator is the composite indicator that combines quantitative and qualitative evaluations, i.e. the indicator of risk. The risk matrix is widely used for risk evaluation [2, 5]. The consequences of a risk event are always negative. Those typical to operated railway facilities are well known. GOST 33433-2015 recommends standard gravity levels for railway transportation. Calculations of the probability of an undesired event involve the problem on choosing the method of calculation. Currently, there are a large number of probability evaluation methods that are divided into two large groups, i.e. expert and quantitative. The most important aspect of choosing the method for evaluation of the probability of undesired events is ensuring the practical applicability of the results, which means that the evaluation model must take into consideration the states of the system's controlled parameters. A system that allows managing the probabilities of hazardous events and accidents must be based on the information on the processes implemented in railway facilities and states that are associated with accident and undesired events. The approach proposed in this paper aims to create a demonstrable and well formalized method to identify the probability of system transition into hazardous state.

Subsets of states of railway facilities

A distinctive feature of a complex system, such as a railway facility, is its property to maintain the overall state of operability in case of failure of individual elements or even whole subsystems [1]. Such system states in many cases reduce its operational efficiency. This property of railway facilities significantly affects the specification and solution of the safety task. For instance, in terms of fire safety, the states of "violation of the Fire prevention rules (FPR)" and "development of fire due to violation of the FPR" are two different system states. The probabilistic characteristics of such states also differ. From the point of view of facility fire safety management, not only the probability of violation, but the probability of its timely elimination should be evaluated. This approach forms additional relations among various states. Let us formalize the concept of "safety state" in terms of the theory of sets:

State of operability S_{op} is state of a system under which the values of all parameters that characterize the ability to perform the specified functions comply with the requirements of technical documentation.

State of nonoperability $\bar{S}_{op}$ is state of a system under which the value of at least one parameter that characterizes the ability to perform the specified functions does not comply with the requirements of technical documentation.

Set of non-hazardous industrial states S_I is the system states under which safety of property, life, health of employees and third parties is ensured in accordance with regula-

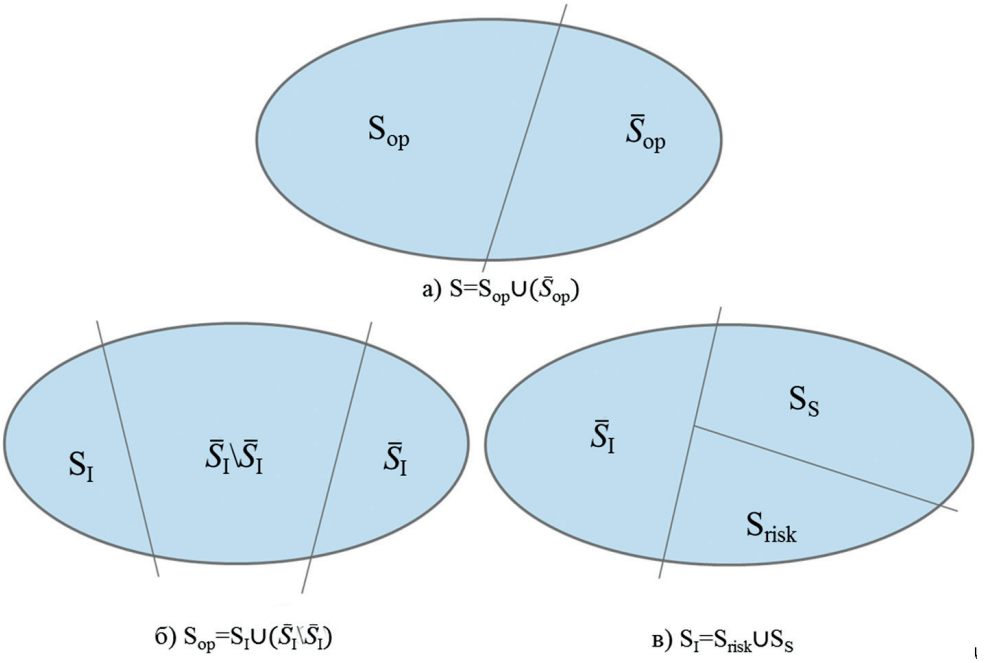


Figure 1. Safety states of system

tory documents [1]. This set includes the sets of safety and pre-hazardous system states.

Set of safety states S_S is the system states under which safety of property, life, health of employees and third parties is ensured in accordance with technical, process control documentation, operational conditions.

Set of pre-hazardous states S_{risk} is such states of operability under which the system approaches the limits of the specified hazardous state criterion at such speed that it can pass into a hazardous state before the next maintenance inspection or repair.

Set of hazardous states $\overline{S}_I$ is the state that may cause harm to property, health and life of employees, as well as third parties.

Figure 1 shows diagrams of sets of safety states of system.

In this article we focus our attention on states S_I, S_{risk}, $\overline{S}_I$

Safe system states graph

Events of fire, accidents with environmental consequences, occupational injuries are random. Let us represent the considered system with the previously designed sets of states as a directed state graph *G(S,H)*, where S is the finite set of system states; H is the finite set of arcs between vertices i,j (states s_i, s_j). System development can be described as follows: if a system is in state s_i, then with probability p_{ij} it can pass into state s_j. The criterion of hazardous event is the system transition into a set of hazardous states $\overline{S}_I$.

System safety graph construction must take into consideration the following requirements:

1) From each state of set S_i there is a possibility of transit into state of set S_{risk} or $\overline{S}_I$.

2) From each state of set S_{risk} the system transits either into state S_i, or state $\overline{S}_I$.

Let us give an example of state graph description of fire safety in premises of a fixed facility (see Table 1):

S is the complete set of object states, S=*{S0, S1, S2, S3, S4, S5};*

S_I is the subset of non-hazardous states, SI=*{S0};*

S_{risk} is the subset of pre-hazardous states, SP=*{S1, S2, S3};*

$\overline{S}_I$ is the subset of hazardous states), $\overline{S}_I$={S4, S5}.

Thus, $S= S_I \cup \overline{S}_I$, $S_{and}=S_{risk} \cup S_S$.

Table 2 shows the values of probabilities of one-step transitions from the i^{th} state to the j (p_{ij}) state. Those probabilities are a priori, they are specified by means of expertise based on the analysis of fire development cases.

Table 2. Transition probabilities matrix

		States						
		0	1	2	3	4	5	∑
S	0	0,7	0,3	0	0	0	0	**1**
t	1	0,5	0	0,3	0,2	0	0	**1**
a	2	0	0	0,7	0	0,3	0	**1**
t	3	0	0	0	0,3	0,2	0,5	**1**
e	4	0	0	0,3	0	0,7	0	**1**
s	5	0	0	0	0	0	1	**1**

Figure 2 shows the state graph

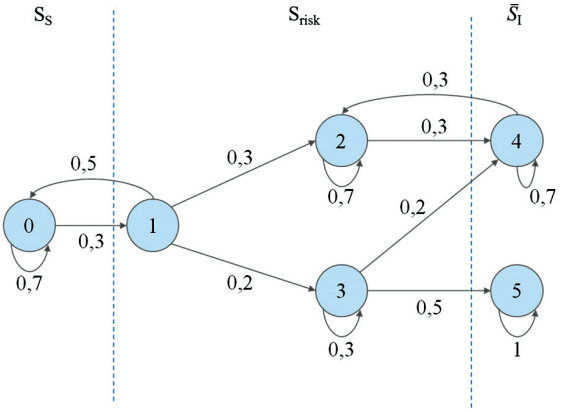


Figure 2. State graph of fire safety in premises of fixed facility

The aim is to identify the probability of system transition from a specific non-hazardous state into any hazardous one. The calculation data must be taken into consideration when taking decisions regarding the changes of transition probabilities through the deployment of fire safety systems, carrying-out of preventive repairs and other accident prevention measures.

The topological concepts used in mathematical simulation:

path, a chain of series-connected unidirectional arcs beginning in state *i* and ending in state *j*, the weight of a path l_k^{ij} is identified with the formula:

Table 1. Set of system states

Set	Subset	№	Notation	Description	Breached regulatory document
S	S_I	0	S_0	Cables/wires not damaged	
	S_{risk}	1	S_1	Open cables/wires (without protective sleeves/pipes/conduits) in places where mechanical damage may occur.	IEC 2.1.47
		2	S_2	Sharp bends, micro-damage (non-visible damage of insulation)	
		3	S_3	Use of cable/wire with visibly damage insulation	FPR 42 a)
	$\overline{S}_I$	4	S_4	Cable heating due to rising transition resistance	
		5	S_5	Short circuit and melting of insulation, sparks due to SC	

$$l_k^{ij} = \prod_{i,r,j \in S} p_{ir} \cdot p_{rj}, \quad (1)$$

where p_{ir} is the probability of one-step transition from state i into state r;

closed circuit is a chain of series-connected unidirectional arcs, in which the output of the final vertex in a circuit is connected to the initial vertex of the circuit. The weight of the j^{th} circuit is identified by the formula:

$$C_j = \prod_{i,j \in S} p_{ij} \cdot p_{ij}; \quad (2);$$

loop is a case of closed circuit, in which the incoming and outgoing arcs merge into one arc, the weight of the loop is $C_j=p_{ij}$;

graph resolution is a part of a graph that does not contain marked vertices and connected arcs; the weight of resolution ΔG_i is calculated subject to exclusion of vertex i and connected arcs from the graph; the weight of resolution $\Delta G_{\overline{S}_i}$ is calculated subject to additional exclusion from the graph of the vertices of set $\overline{S}_I$ and connected arcs; the weight of resolution ΔG_k^f is calculated subject to exclusion from graph of vertex f, as well as the vertices situated on the k^{th} path from the initial vortex into vertex i, as well as the connected arcs;

the weight of resolution (determinant) is found using Mason's formula:

$$\Delta G = 1 - \sum_j C_j + \sum_{rj} C_r \cdot C_j - \sum_{irj} C_i \cdot C_r \cdot C_j + \ldots \quad (3)$$

Theorem

The probability of system transition from the specific i^{th} initial non-hazardous state ($i \in S_I, S_I \cap \overline{S}_I \neq \varnothing, S_I \cup \overline{S}_I = S$) into any hazardous state $f \in \overline{S}_I$ is determined from the formula

$$b_{if} = \frac{\sum_{f \in \overline{S}_I} \sum_k l_k^{if} \Delta G_k^f}{\Delta G_{\overline{S}_I}} \quad (4)$$

where l_k^{if} is the k^{th} path leading from non-hazardous state of graph $i \in \overline{S}_I$ into hazardous state f;

ΔG_k^f is the weight of graph resolution without the f^{th} vertex and graph vertices situated on the k^{th} path:

$\Delta G_{\overline{S}_I}$ is the weight of graph resolution without the vertices of the hazardous state set.

Let us prove the correctness of formula (4). A random system transition from initial non-hazardous state i into any hazardous one is possible as follows:

- by preliminary transition into associated non-hazardous states. That is described with the sum of products of the probabilities of transition from the initial non-hazardous state into another non-hazardous state and the probability of system transition from those non-hazardous states into any hazardous state, i.e. this probability equals to: $\sum_j p_{ij} \cdot b_{if}$. Or, in matrix form, T·V, where T is *nxn* dimension transition probability matrix, while *n* is the number of vertices in the set of non-hazardous states; V is *nx1* dimension column-vector of probability of transition into hazardous state;

- by direct one-step transition into any hazardous state that is described with a column-vector of probabilities of one-step system transitions from state i into any hazardous state f: P=(p_{if}). This column-vector has the size of (nx1), where n is the number of vertices in the set of non-hazardous states.

Thus, the probability of random system transition from initial non-hazardous state i into any hazardous state f can be expressed with the following matrix equation:

$$V=TV+P \quad (5).$$

In this equation, the unknown quantities are the elements of the column-vector V. After their grouping in the left part of the matrix equation we deduce:

$$V(I-T)=P \quad (6)$$

where the right part of the equation is the column-vector of free terms of the probabilities of one-step transitions from vertices $i, j, \ldots, z \in S_I$ into vertex $f \in \overline{S}_I$.

Then, according to Kramer's rule, we deduce $B_i = \Delta_i/\Delta$, where the graph determinant in the set of non-hazardous states $\Delta = |I - \Pi|$, while Δ_i is the determinant deduced by substituting the i^{th} column in the matrix $I - \Pi$ with the free term vector P under the condition that Δ_i and Δ are not equal to 0.

Determinant Δ_i differs from determinant Δ in that in column i element p_{ij} is replaced with element p_{if}. In accordance with [2], let us use the graph form of representation of determinant and minors, as well as graph paths, i.e.:

$$\Delta = \Delta G_{\overline{S}}, \ \Delta_i = \sum_{f \in \overline{S}_I} \sum_k l_k^{if} \Delta G_k^f, \quad (7)$$

where $\Delta G_{\overline{S}_I}$ is the weight of graph resolution without the set of hazardous vertices;

ΔG_k^f *is* the weight of graph resolution without hazardous vertices, as well as the vertices situated on the k^{th} path;

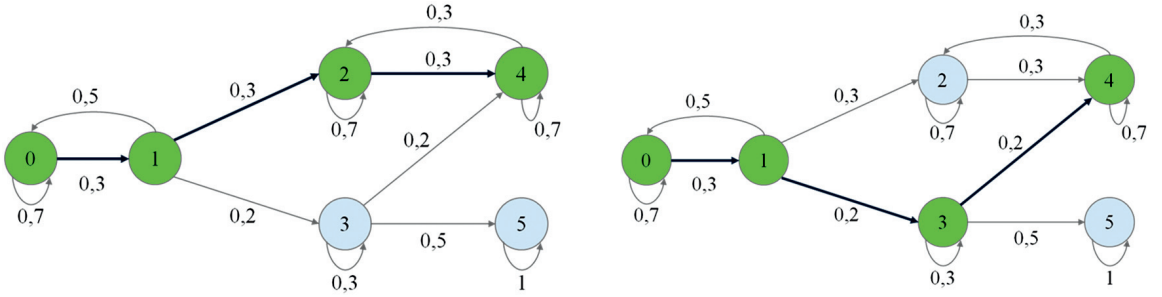
l_k^{if} is the weight of the k^{th} path from the non-hazardous vertex i to the hazardous vertex f.

By substituting formulas (7) into formula (6) we deduce that

$$b_{if} = \frac{\sum_{f \in \overline{S}_I} \sum_k l_k^{if} \Delta G_k^f}{\Delta G_{\overline{S}_I}}.$$

Example of evaluation of probability of cables in a fixed facility passing into fire-hazardous state

For the above system hazard state graph, let us calculate the probability of transition from state S_0 "Cables/wires not damaged" into state S_4 "Cable heating due to rising transition resistance". Figure 3 shows paths of transition into hazardous state S_4.



a) Path to hazardous state No. 1 b) Path to hazardous state No. 2

Figure 3. Paths of transition into hazardous state S_4

Table 3. Path weight calculation

№	Notation	Path	Formula	Path weight calculation	Path weight
1	l_1^{04}	$S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow S_4$	$p_{01} \cdot p_{12} \cdot p_{24}$	0,3·0,3·0,3	0,027
2	l_2^{04}	$S_0 \rightarrow S_1 \rightarrow S_3 \rightarrow S_4$	$p_{01} \cdot p_{13} \cdot p_{34}$	0,3·0,2·0,2	0,012

In accordance with the theorem for evaluation of the probability of system transition from initial non-hazardous state into hazardous state, the probability of system transition from S_0 to S_4 is defined with the formula:

$$b_{04} = \frac{\sum_{f \in \overline{S}_i} \sum_k l_k^{04} \Delta G_k^4}{\Delta G_{\overline{S}_i}}.$$

As it is seen from Figure 3, the number of transition paths from S_0 to S_4 k=2.

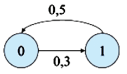
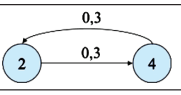
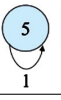
Table 3 shows the calculation of weights of paths from state S_0 to state S_4. Table 4 shows circuit weight calculations.

For the considered case, the weight of graph resolution without the vertices of the hazardous state set equals:

$$\Delta G_{\overline{S}_i} = 1 - (0,7 + 0,15 + 0,7 + 0,3) +$$
$$+ (0,105 + 0,045 + 0,49 + 0,21 + 0,21) -$$
$$- (0,0315 + 0,147) = 0,0315.$$

Then, the probability of transition from state S0 (wires and cables not damaged) into state S4 (heating due to rising transition resistance):

Table 4. Circuit weight calculation

№	Circuit code	Vertices	Form	Formula	Circuit weight, C_i	Circuit with hazardous states
1	C_1	$S_0 \rightarrow S_1 \rightarrow S_0$		$p_{01} \cdot p_{10}$=0,5·0,3	0,15	
2	C_0	$S_0 \rightarrow S_0$		p_{00}=0,7	0,7	
3	C_2	$S_2 \rightarrow S_2$		p_{22}=0,7	0,7	
4	C_4	$S_2 \rightarrow S_4$		$p_{24} \cdot p_{42}$=0,3·0,3	0,09	V
5	C_3	$S_3 \rightarrow S_3$		p_{33}=0,3	0,3	
6	$C_{4.4}$	$S_4 \rightarrow S_4$		p_{44}=0,7	0,7	V
7	C_5	$S_5 \rightarrow S_5$		p_{55}=1	1	V

$$b_{04} = \frac{\sum_{f \in \bar{S}_1} \sum_k l_k^{04} \Delta G_k^4}{\Delta G_{\bar{S}_1}} =$$

$$= \frac{0,027 \cdot 0,7 + 0,012 \cdot 0,3}{0,0315} = \frac{0,0225}{0,0315} = 0,71.$$

In the same way, the probability of transition from state S0 (wires and cables not damaged) into state S5 (Short circuit and melting of insulation, sparks due to short circuit) is calculated.

$$P_{05} = \frac{\sum_{f \in \bar{S}_{op}} \sum_k l_k^{05} \Delta G_k^5}{\Delta G_{\bar{S}_{op}}} = \frac{0,03 \cdot 0,3}{0,0315} = \frac{0,009}{0,0315} = 0,29.$$

Conclusion

It was shown that random events of fire, accidents with environmental consequences, occupational injuries can be evaluated with a model of semi-Markov process on the assumption that transitions between system states are described with a discrete-time embedded Markov chain. A graph model of system fire safety analysis was demonstrated that includes the states of a multitude of hazardous, pre-hazardous and non-hazardous events.

A tool for evaluating the industrial safety risk by means of a graph model of safety analysis was developed. The theorem was proven for identifying the probability of system transition from initial non-hazardous or pre-hazardous state into desired hazardous state that allows finding the analytical or numerical value of the probability of hazardous state of a railway facility. A practical application was shown.

References

1. Elektronny slovar terminov MChS [EMERCOM electronic vocabulary of terms]. Available from: http://www.mchs.gov.ru/dop/terms/item/88773.

2. GOST 33433-2015. Functional safety. Risk management in railway transportation. Russian.

3. Shubinsky IB. Nadiozhnie otkazoustoychivie informatsionnie systemi. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016. Russian.

4. Shubinsky IB. Topologicheskij metod i algoritm opredeleniya statsionarnykh pokazatelej nadezhnosti tekhnicheskikh sistem [Topological method and algorithm of identification of steady-state dependability indicators of technical systems]. Nadiozhnost i kontrol kachestva [Dependability and quality control]. 1984; 5: 3. Russian.

5. Novozhilov EO. Printsipy postroeniya matritsy riskov [Principles of risk matrix construction]. Dependability. 2015; 3 (54): pp. 73-86. Russian.

About the authors

Igor B. Shubinsky, Doctor of Engineering, Professor, Director, ZAO IBTrans, 109029, Russia, of. 310, bld.15, 32 Nizhegorodskaya Str. Moscow, phone: +7 (495) 786 68 57, e-mail: igor-shubinsky@yandex.ru

Alexey M. Zamyshlyaev, Doctor of Engineering, Deputy Director General, JSC NIIAS, 109029, Russia, of. 209, bld.1, 27 Nizhegorodskaya Str. Moscow, phone: +7 (495) 967 77 02, e-mail: A.Zamyshlyaev@vniias.ru

Olga B. Pronevich, Head of Unit, JSC NIIAS, 109029, Russia, of. 209, bld.1, 27 Nizhegorodskaya Str. Moscow, phone: +7 (495) 967 77 05, ext. 516, e-mail: O.Pronevich@vniias.ru

Received on: 28.12.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-46-52

Evaluation of safety and reliability parameters of supervision and control systems

Oleg L. Makoveev, *Radioavionica, Saint Petersburg, Russia, e-mail: makoveev38@mail.ru*
Sergey Yu. Kostyunin, *Radioavionica, Saint Petersburg, Russia, e-mail: kostyunin.sergey@gmail.com*

Oleg L. Makoveev

Sergey Yu. Kostyunin

Abstract. The aim *of this article is the analytical evaluation of dependability and reliability indicators of vital facility supervision and control systems. Such indicators include: probability of no-failure, collective failure rate, wrong-side and right-side failure rate, average service life. The article considers systems with different redundancy rates (2-oo-2, 2-oo-3, 2-oo-2-by-2) ensuring recovery of failed equipment (channels) without interruption of operation. The paper covers such safety and reliability mechanisms as interchannel data comparison, mutual channel blocking and protection against negative failure development by mutual channel blocking.* **Methods.** *For the purpose of achieving the set goal, the article suggests a mathematical functional model based on absorbing homogenous Markovian continuous-time chains. The states of this chain reflect the number of good channels of the system, while state transition rates are identified based on the equipment failure rates of each channel and repair rates (subject to the mechanisms of interchannel data comparison and failed channel blocking). The absence of protection can be caused by such events as non-detection of failure by supervision facilities, disability of blocking mechanisms, protection tripping delay. In such case the failure of a channel (channels) causes the failure of the whole system and forces the Markovian chain into the absorbing state. The probabilities of transition into the absorbing state are divided into the probabilities of transition into state of right-side failure and state of wrong-side failure. As a failure occurrence in a situation of absent guaranteed protection against its possible negative consequences in a system that continues operating may cause undue inputs to the system's executive mechanisms and on the assumption of the worst case scenario we deem such failure to be a wrong-side one. The used methods allow finding the probabilities of each state of the chain by solving a system of Kolmogorov-Chapman differential equations. Based on the given probabilities, the collective failure rate and average service life are identified along with the right-side and wrong-side failure rates. In order to ensure the usability of the presented methods, the authors provide approximate formulas of failure rates and approximation errors.* **Results.** *A mathematical model of operation of a multichannel microprocessor system has been developed. Formulas for calculation of system state probabilities, average service life, wrong-side and right-side failure rates have been obtained that allow evaluating the safety and fault tolerance of various systems with hot standby and in-operation operability recovery capabilities. The given formulas for calculation of system state probabilities allow increasing the number of safety and reliability indicators, if needed. The article presents the feasibility of simplified calculation of failure rates.* **Conclusions.** *The formulas given in the article can be used for evaluation of reliability, safety and longevity indicators of microprocessor-based supervision and control circuits of vital facilities (ship-borne technical facilities, trackside equipment in railway stations and open lines, fixed power facilities, etc.). In the development process they allow finding the rational system organization by means of comparative evaluation of performance of structures with various degrees of redundancy. In the context of system adaptation for application in various facilities as well as its modernization the formulas in question enable analytical calculation of the above indicators.*

Keywords: *functional safety, reliability, supervision, diagnostics, wrong-side failure, right-side failure, failure rate.*

For citation: *Makoveev O.L., Kostyunin S.Yu. Evaluation of safety and reliability parameters of supervision and control systems. Dependability, 2017, vol. 17, no. 1, pp. 46-52. (in Russian) DOI: 10.21683/1729-2640-2017-17-1-46-52*

Vital facility supervision and control systems are expected to meet reliability and safety requirements [1]. High levels of reliability and safety are ensured by multichannel architectures of computer-based systems, supervision and diagnostics.

It is suggested to use the following indicators for quantitative evaluation of such systems [2, 3, 4]:

– in terms of reliability: probability of no-failure and failure rate (collective failure rate);

– in terms of longevity: average service life;

– in terms of safety: wrong-side and right-side failure rates.

The standard for functional safety of equipment [4] sets forth a formula that serves as the foundation for deduction of wrong-side and right-side failure rates.

$$\Lambda = \Lambda_S + \Lambda_D, \quad (1)$$

where Λ is the collective failure rate;

Λ_S is the right-side failure rate;

Λ_D is the wrong-side failure rate.

The same formula shows the connection between dependability and safety.

In order to highlight the importance of protection of the considered systems against the negative consequences of failures of railway automation equipment, safe failures are conventionally called right-side failures.

There is a number of Russian and foreign computer-based systems, whose safety and reliability [4, 5] are based on hardware and software redundancy and automatic engineering supervision and diagnostics. Under identical safety and reliability requirements, the structure of such systems significantly depends on the operation conditions. Thus, in systems whose operation conditions do not allow replacement of failed equipment in operation, the required safety and reliability characteristics are achieved through significant redundancy of hardware and software facilities [5].

A noticeably smaller redundancy in hardware and software facilities is required for systems of which the operation conditions do allow replacement of failed equipment in operation. In this case the most common solutions are the 3-channel "2-oo-3" and 4-channel "2-by-2-oo-2" hot standby with recovery, as well as combinations of the above (different levels of redundancy for different devices of the system). It should be noted that in a number of cases 2-channel "2-oo-2" devices are used, in which each channel is secure.

In such systems, on-line inspection and testing allow localizing malfunctions with subsequent replacement of failed modules or redundant channels without interruption of operation ("smooth" replacement). On-line inspections are based on interchannel comparisons and checks per a limited number of parameters over the system's operation cycle. Diagnostic tests are performed routinely in the background in order to eliminate failure accumulation. Checks are performed on all hardware ever used regardless of the current facility management program.

The distinctive feature of such systems is the continuation of normal operation after one failure and transition to limit state after the second failure. Two types of limit state exist that correspond to the two types of failure consequences [2], namely:

– state upon wrong-side failure, that causes the emergence of hazard to human life and/or significant material and/or moral damage;

– state upon safe failure that does not cause hazardous situations.

In case of failures in order to eliminate the possibility of hazardous situations as best possible, based on the results of supervision and diagnostics, the system is automatically transferred into state of safe failure, i.e. the system is protected against potential negative consequences of a wrong-side failure.

Among system components responsible for providing protection against possible negative consequences of wrong-side failures are system state supervision and diagnostics facilities, as well as failed component and whole product operation blocking mechanism. Designing secure and reliable systems with all types of redundancy involves maximal possible elimination of wrong-side failures, while maintaining a required level of operability. For that purpose, it is required to ensure high reliability of supervision and diagnostics with a dependable and fast-operating blocking mechanism.

In order to ensure product recovery in operation, malfunction reporting is specific to replacement modules, while replacement of failed equipment is performed with the power on.

As a failure in a situation of absent protection against its possible negative consequences in a system that continues operating may cause undue inputs to the system's executive mechanisms and on the assumption of the worst case scenario, we deem such failure to be a wrong-side one (WSF).

The absence of protection may be due to such unrelated events as non-detection of failure by the supervision facilities, failure of the blocking mechanism or the time between failures being longer than the protection operation time. Therefore, the probability of non-availability of protection (q_1,q_2) can be identified as follows:

in case of first failure:

$$q_1 = q_{1C} + q_{1b}, \tag{2}$$

where: q_{1C} is the probability of control facilities did not detect the system failure,

q_{1b} is the probability of blocking mechanism failure.

in case of second failure:

$$q_2 = (1 - q_{2\tau})\,(q_{2C} + q_{2b}) + q_{2\tau}, \tag{3}$$

where: q_{2C} is the probability of control facilities did not detect the system failure,

q_{2b} is the probability of blocking mechanism failure;

$q_{2\tau}$ is the probability of the time between failures being shorter than the protection operation delay (we assume that the protection mechanisms are guaranteed to operate within time τ).

For the purpose of malfunction detection, over each operation cycle the on-line inspection checks primary procedures data (data input, calculations, supervision, data output, diagnostics, etc.).

The list of such procedures is specific and permanent to each system.

In 3 and 4-channel systems on-line inspection is based on interchannel comparison, and in those double checking is possible up to the second failure. In 2-channel systems, blocking per first failure is also based on interchannel comparison. Additionally, the integrity of data batches received and transmitted by users (external systems) is verified by beans of redundant coding. The reliability of supervision under double verification is quite high. It declines if interchannel comparison is performed by means of convolutions and signatures [6, 7].

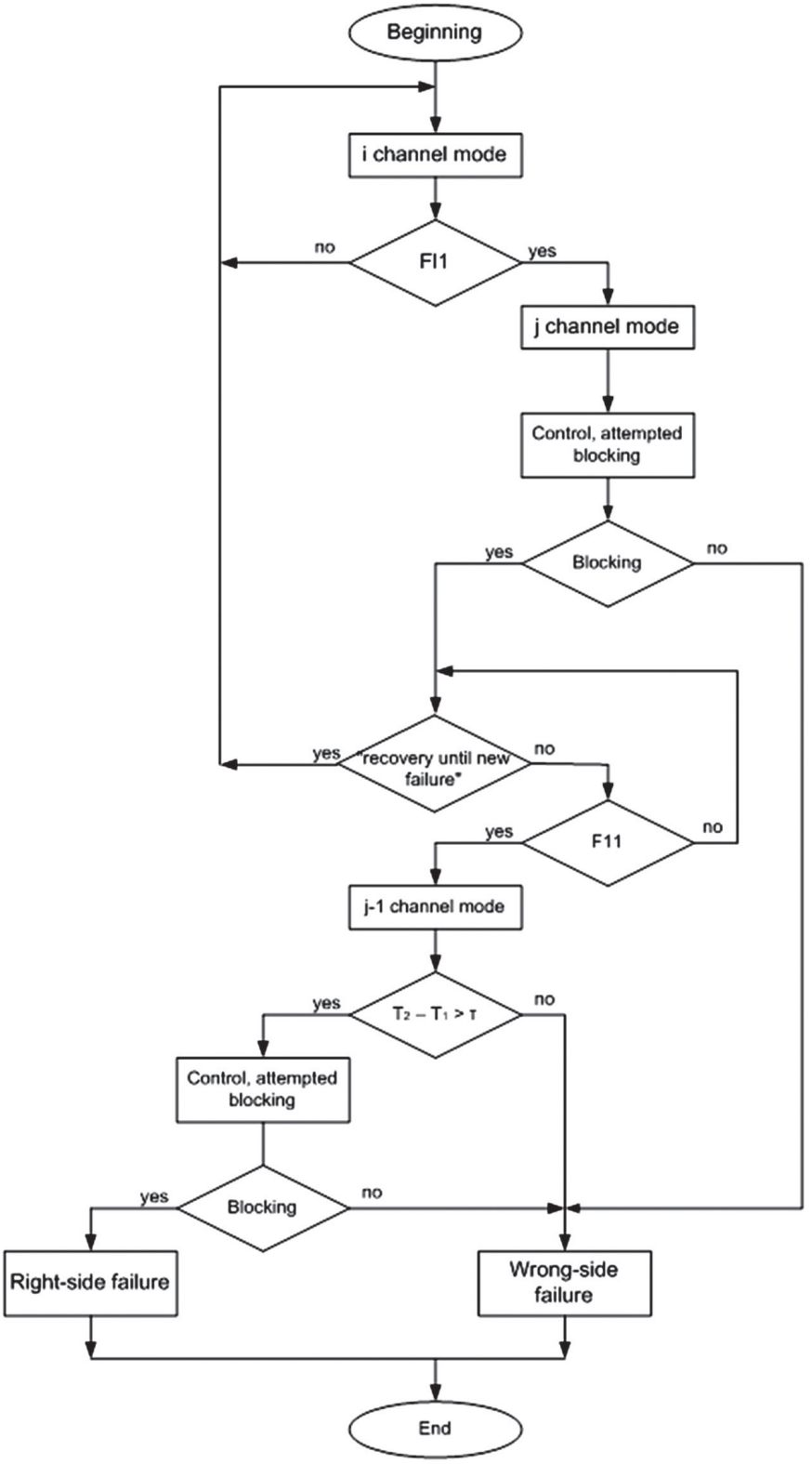


Figure 1. Block diagram of system state change

After the second failure, in 3 and 4-channel systems a single check is done. For this case, the most typical supervision reliability limitations are due to failures with identical consequences in different channels (non-detectable by interchannel comparison). Most probably, identical failure consequences may take place in case of practically simultaneous occurrence (within one operation cycle) of same-type failures of elements with identical reference designations in two channels.

In 2-channel systems, after blocking per first failure operation may continue if safety facilities are available for each channel [8] or through external checking. That is a serious limiting factor of such systems' application.

Given the above, let us consider the operation of a system in case of failures.

At the initial start the system is in fully operational state. After the first failure (event F1) the system passes into state in which malfunction detection is performed. In case of malfunction detection and protection operation (with the probability $1 - q_1$), as well as in the absence of the second failure during recovery, the failed channel is excluded from operation without loss of function. After failure recovery the system passes onto the initial state.

If protection is not available (with the probability q_1), the first failure is considered a wrong-side one.

If within time before recovery of a failed channel the second failure occurs (event F2), the system passes into state of complete failure under the following circumstances:

1) the second failure occurred sometime after the protection operation for the consequences of the first failure, and during that time the protection was implemented (with the probability $1 - q_2$). However, due to depleted reserves (number of good channels) recovery causes the loss of function. In other words, the event F1 was followed by the event "protection of device with loss of function", i.e. the so-called right-side failure (RSF);

2) the second failure occurred in absence of protection (with the probability q_2), but the operation continues, which allows considering such failure a wrong-side one.

Figure 1 shows a diagram of system state change with failures and recoveries based on the results of condition supervision.

In Figure 1, some states are referred to by the number of good channels at a specific moment in time according to Table 1, where:

– initial state is «i channel mode» (all channels operational);

– state after the first failure (event F1) is «j channel mode»;

– state after the second failure (event F2) is «(j-1) channel mode»;

Each type of the considered systems (type of redundancy) is characterized by two parameters, i.e. *i* and *j*, that are different type to type, which allows using *"ij"* as a designation of belonging to a specific type.

Transition from state to state occurs in the following cases:

– in case of recovery of a failed channel, return into the initial state;

– if $T_2 - T_1 > \tau$ (time between failures is longer than the protection operation delay), transition to control and, in case of detected malfunction, blocking of the failed channel;

– in case of failures (F1 and F2) and operation and failure to operate of protection, transitions in (j-1) channel mode into states of "right-side failure" and "wrong-side failure".

For the purpose of evaluation of secure fail-safe supervision and control systems, let us consider a Markovian process with a discrete set of states and continuous time represented as a graph of model transition from state to state.

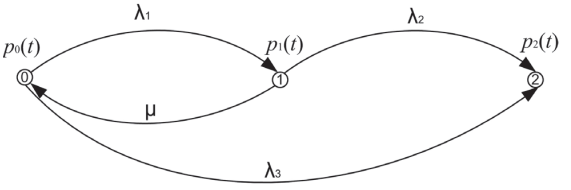


Figure 2. Transition graph

The states of the model reflect the changes related to product failures and recoveries, while the transitions are defined by the failure and recovery rates.

The model has the following features:

the failure flow of individual redundant channels is most simple with the rate of i λ or j λ.

Here, the *i* and *j* are presented as multipliers of λ, while in Table 1 they were designations of belonging to a specific type of system, in which there is no contradiction.

2) the recovery flow is adopted as the simplest, of which the rate $\mu = 1/T_r$, where T_r is the time of recovery;

3) the probabilities of states are as follows:

– $p_0(t)$ is the probability of initial state (after initial start or recovery, when all *i* channels are good);

– $p_1(t)$ is the probability of state, at which one channel has failed with the rate of $i\lambda$ (following an event F1), while *j* channels are good;

Table 1

***i* channel system (*i, j*)**	**Number of good channels**		
	in initial state, *i*	**after first failure, *j***	**after second failure, *j*-1 (right-side or wrong-side failure)**
2 channel system – (2,1)	2	1	0
3 channel system – (3,2)	3	2	1
4 channel system – (4,2)	4	2	1

– $p_2(t)$ is the probability of absorbing state, at which a second channel has failed with the rate of $j\lambda$ (following an event F2) and the whole device enters the state of right-side failure (operation is impossible) or the state of wrong-side failure, when operation continues with a malfunction.

F0, F1 and F2 represent exhaustive events, therefore:

$$p_0(t) + p_1(t) + p_2(t) = 1. \quad (4)$$

Based on the transition graph, with known λ and μ a system of differential equations (Kolmogorov equations) is constructed:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = -(\lambda_1 + \lambda_3)\, p_0(t) + \mu\, p_1(t) \\ \dfrac{dp_1(t)}{dt} = -(\mu + \lambda_2)\, p_1(t) + \lambda_1\, p_0(t) \\ \dfrac{dp_2(t)}{dt} = \lambda_3\, p_0(t) + \lambda_2\, p_1(t) \end{cases} \quad (5)$$

Solving the system allows finding the probabilities of model states, rates of right-side and wrong-side failures, as well as mean time to failure.

The following formulas are used:

$\Lambda(t) = f(t)/(1 - F(t))$ is the system's overall failure rate, where: $f(t)$ is time to failure density function;

$F(t)$ is the distribution function.

Due to the fact that beside the overall failure rate of the system we need to find the wrong-side and right-side failure rates subject to the type of the system let us introduce the following notations:

Λ(t) is the collective failure rate of the system;

$\Lambda(t)_{WSF}$ is the wrong-side failure rate;

$\Lambda(t)_{RSF}$ is the right-side failure rate.

Under the introduced notations:

$$\Lambda(t) = \frac{\dfrac{dp_2(t)}{dt}}{1 - p_2(t)}, \quad (6)$$

2) the rates of transition from state to state in case of failures depend on parameters i and j, as well as availability or non-availability of protection:

$$\lambda_1 = i(1 - q_1)\lambda,\ \lambda_2 = j(1 - q_2)\lambda + j\, q_2\, \lambda = j\lambda,\ \lambda_3 = i\, q_1\, \lambda;$$

for the systems under consideration the time to failure is as follows

$$T_{cp} = \int_0^\infty t\, p_2'(t)dt \approx \frac{\mu}{ij\lambda^2}. \quad (7)$$

4) an event "time between failures is shorter than the protection operation delay" is equivalent to the event "occurrence of second failure over the time period not exceeding τ". The probability of the second event is identified as follows:

$$q_{2\tau} = 1 - e^{-\lambda_2 \tau} \approx j\lambda\tau. \quad (8)$$

The formulas for identifying the probabilities of duration of various system states deduced by solving the differential equations, as well as other parameters are given in Table 2.

Table 2

Parameters	Formulas
$P_0(t)$	$\dfrac{1}{k_1 - k_2}\left[(\mu + j\lambda + k_1)e^{k_1 t} - (\mu + j\lambda + k_2)e^{k_2 t}\right]$
$P_1(t)$	$\dfrac{\lambda_1}{k_1 - k_2}\left(e^{k_1 t} - e^{k_2 t}\right)$
$P_2(t)$	$\dfrac{1}{k_1 - k_2}\left[(iq_1\lambda + k_2)e^{k_1 t} - (iq_1\lambda + k_1)e^{k_2 t}\right] + 1$
T_{cp}	$\dfrac{1}{k_1 k_2 (k_1 - k_2)}\left[(k_2 - k_1)\lambda_3 + k_2 k_1 - k_1 k_1\right] \approx \dfrac{\mu}{ij\lambda^2}$

Here k_1 and k_2 are the roots of the characteristic equation for the differential equations system (5):

$$k_1 = \frac{-(\mu + (i+j)\lambda) + \sqrt{(\mu + (i+j)\lambda)^2 - 4(ij\lambda^2 + iq_1\lambda\mu)}}{2} \approx$$
$$\approx -\lambda\left(\frac{ij\lambda}{\mu} + iq_1\right). \quad (9)$$

$$k_2 = \frac{-(\mu + (i+j)\lambda) - \sqrt{(\mu + (i+j)\lambda)^2 - 4(ij\lambda^2 + iq_1\lambda\mu)}}{2} \approx -\mu. \quad (10)$$

The absolute approximation error of k_1 and k_2 are found using the formula:

$$\Delta = \frac{i\lambda(j\lambda + q_1\mu)}{\mu^2}. \quad (11)$$

In accordance with (6) the collective failure rate equals to:

$$\Lambda(t) = \frac{k_1(iq_1\lambda + k_2) - k_2(iq_1\lambda + k_1)e^{(k_2 - k_1)t}}{(iq_1\lambda + k_1)e^{(k_2 - k_1)t} - (iq_1\lambda + k_2)}. \quad (12)$$

As $|k_2| >> |k_1|$ and $|k_2| >> iq_1\lambda$, we obtain

$$\Lambda(t) \approx (\lambda_3 + k_1)e^{(k_2 - k_1)t} - k_1. \quad (13)$$

If Λ(t) is found as the specified service life T_S, where, for instance, $T_S \approx 10^5$ hours, then

$$\Lambda(t) \approx \frac{ij\lambda^2}{\mu} + iq_1\lambda. \quad (14)$$

Let us find the wrong-side and right-side failure rates.

Under the notations used in this article, formula (1) is as follows:

$$\Lambda(t) = \Lambda(t)_{RSFI} + \Lambda(t)_{WSFI}. \quad (15)$$

Consequently:

$$\Lambda(t) = \Lambda(t)p(t)_{RSFI} + \Lambda(t)p(t)_{WSFI}. \quad (16)$$

$$p(t)_{RSFI} + p(t)_{WSFI} = 1, \quad (17)$$

where $p(t)_{RSF}$, $p(t)_{WSF}$ are the probabilities of right-side and wrong-side failures.

In order to identify $p(t)_{RSF}$ and $p(t)_{WSF}$,we should deduce the formula for probability of absorbing state $p_2(t)$. That is done by integrating $\frac{dp_2(t)}{dt} = \lambda_3 p_0(t) + \lambda_2 p_1(t)$ (from differential equation system (5). Here, $\lambda_3 = iq_1\lambda$ is the rate of transition from the initial state to the absorbing state in absence of protection (with the probability q_1), i.e. transition to the wrong-side failure, $\lambda_2 = j(1-q_2)\lambda + jq_2\lambda$ is the rate of transition from the state after the first failure to the absorbing state in presence of protection (with the probability $1 - q_2$) and in the absence of protection (with the probability q_2), i.e. transition to right-side and wrong-side failure respectively.

Thus, the probabilities of transition to wrong-side failure and right-side failure are divisible, i.e.:

$$p_2(t) = p_{2,WS}(t) + p_{2,RS}(t), \quad (18)$$

therefore,

$$p(t)_{RSFI} = \frac{p_{2,RS}(t)}{p_2(t)}, p(t)_{WSFI} = \frac{p_{2,WS}(t)}{p_2(t)}. \quad (19)$$

If $p_2(t)$ is written as

$$p_2(t) = \frac{\lambda_3}{k_1 - k_2}\left[\frac{1}{k_1}\left(\mu + \lambda_2 + k_1\right)e^{k_1 t} - \frac{1}{k_2}\left(\mu + \lambda_2 + k_2\right)e^{k_2 t}\right] + \frac{\lambda_3\left(\mu + \lambda_2\right)}{k_1 k_2} + \frac{\lambda_1\lambda_2}{k_1 - k_2}\left(\frac{1}{k_1}e^{k_1 t} - \frac{1}{k_2}e^{k_2 t}\right) + \frac{\lambda_1\lambda_2}{k_1 k_2},$$

then after substitution of values of transition rate we deduce the divided formula

$$p_2(t) = \frac{iq_1\lambda}{k_1 - k_2}\left[\frac{1}{k_1}\left(\mu + j\lambda + k_1\right)e^{k_1 t} - \frac{1}{k_2}\left(\mu + j\lambda + k_2\right)e^{k_2 t}\right] + \frac{i\left(1-q_1\right)\lambda jq_2\lambda}{k_1 - k_2}\left(\frac{1}{k_1}e^{k_1 t} - \frac{1}{k_2}e^{k_2 t}\right) + \frac{i\lambda\left(\mu q_1 + jq_1\lambda + jq_2\lambda - jq_1q_2\lambda\right)}{k_1 k_2} + \frac{i\left(1-q_1\right)\lambda j\left(1-q_2\right)\lambda}{k_1 k_2\left(k_1 - k_2\right)}\left(k_2 e^{k_1 t} - k_1 e^{k_2 t} + k_1 - k_2\right),$$

where

$$p_{2,WS}(t) = \frac{iq_1\lambda}{k_1 - k_2}\left[\frac{1}{k_1}\left(\mu + j\lambda + k_1\right)e^{k_1 t} - \frac{1}{k_2}\left(\mu + j\lambda + k_2\right)e^{k_2 t}\right] + \frac{i\left(1-q_1\right)\lambda jq_2\lambda}{k_1 - k_2}\left(\frac{1}{k_1}e^{k_1 t} - \frac{1}{k_2}e^{k_2 t}\right) + \frac{i\lambda\left(\mu q_1 + jq_1\lambda + jq_2\lambda - jq_1q_2\lambda\right)}{k_1 k_2}, \quad (20)$$

$$p_{2,RS}(t) = \frac{i\left(1-q_1\right)\lambda j\left(1-q_2\right)\lambda}{k_1 k_2\left(k_1 - k_2\right)}\left(k_2 e^{k_1 t} - k_1 e^{k_2 t} + k_1 - k_2\right). \quad (21)$$

In order to simplify formulas for $p(t)_{RSF}$ and $p(t)_{WSF}$ by using approximate values k_1 and k_2 (9), (10) and that $\mu >> \lambda$, we deduce:

$$p(t)_{RSFI} = \frac{p_{2,RS}(t)}{p_2(t)} \approx \left(1-q_1\right)\left(1-q_2\right), \quad (22)$$

$$p(t)_{WSFI} = \frac{p_{2,RS}(t)}{p_2(t)} \approx 1 - \left(1-q_1\right)\left(1-q_2\right). \quad (23)$$

Given the value $\Lambda(t)$ (15) we have:

$$\Lambda(t)_{RSFI} \approx \lambda\left(\frac{ij\lambda}{\mu} + iq_1\right)\left(1-q_1\right)\left(1-q_2\right), \quad (24)$$

$$\Lambda(t)_{WSFI} \approx \lambda\left(\frac{ij\lambda}{\mu} + iq_1\right)\left[1 - \left(1-q_1\right)\left(1-q_2\right)\right]. \quad (25)$$

Conclusion

The article presents formulas that allow evaluating the safety and fault tolerance of various systems with the hot standby capability. Those systems operate normally up to two failures in different channels and provide for condition-monitored recovery without interruption of operation.

Advanced supervision and diagnostics enable condition-based operation of the presented systems.

References

1. Gapanovich VA, Rozenberg EN, Shubinsky IB. Nekotorye polozheniya otkazobezopasnosti i kiberzashhishhennosti sistem upravleniya [Some concepts of fail-safety and cyber protection of control systems]. Dependability. 2014; 2: 88 – 100. Russian

2. GOST R 27. 002-89. Industrial product dependability. General concepts. Terms and definitions. Russian.

3. GOST R 51901.5-2005 (IEC 60300-3-1:2003). Guide for application of analysis techniques for dependability. Russian.

4. GOST R IEC 62061-2013. Safety of machinery. Functional safety of safety-related electrical, electronic, programmable electronic control systems. Russian.

5. Theeg G, Vlasenko S, editors. Sistemi avtomatiki i telemekhaniki na zheleznykh dorogakh mira [Railway Signalling & Interlocking. International Compendium]. Moscow: Inteks; 2010. ISBN 978-5-89277-098-9. Russian.

6. Avakian AA. Sozdanie sverkhnadyozhnykh ehlektronnykh sistem dlya aehrokoosmicheskoj tekhniki [Development of fail-safe electronic systems for aerospace structures]. Kontrol. Diagnostika [Testing. Diagnostics]. 2013; 2: 67 – 75. Russian

7. Novik GH. O dostovernosti signaturnogo analiza [On the integrity of signature analysis]. Avtomat. i telemekh. [Automation and remote control]. 1982; 5: 157 – 159. Russian.

8. Goldshtein VB, Mironov SV. Khesh-funktsii dlya sokrashheniya diagnosticheskoj informatsii [Hash functions for reduction of diagnostics information]. Izvestia Saratovskogo universiteta. Novaia seria. Seria Matematika. Mekhanika. Informatika. [Journal of the University of Saratov. New series. Mathematics. Mechanics. Information technologies Series]. 2007; 2 (7). Russian.

9. Iyudu KA. Nadiozhnost, kontrol i diagnostika vychislitelnykh mashin i sistem [Dependability, supervision and diagnostics of computer systems]. Moscow: Vyshaya shkola; 1989. Russian.

About the authors

Oleg L. Makoveev, Candidate of Engineering, Science Adviser, Radioavionica. Troitskiy pr., 4, building B, Saint-Petersburg, Russia 190005, e-mail: makoveev38@mail.ru

Sergey Yu. Kostyunin, Candidate of Physics and Mathematics, Head of Unit, Radioavionica. Troitskiy pr., 4, building B, Saint-Petersburg, Russia 190005, e-mail: kostyunin.sergey@gmail.com

Received on 29.09.2016

Original article
DOI: 10.21683/1729-2640-2017-17-1-53-58
Dependability, vol. 17 no.1 2017 УДК 519.876.5:37.012.4:004.6

Parametric method of observation results processing with regard to missed data

Dmitri A. Nikilayev, *Obninsk Institute for Nuclear Power Engineering, Obninsk, Russia. e-mail: dafanday@gmail.com*

Dmitri A. Nikilayev

Abstract. *The matters of ensuring dependable and safe operation of NPP facilities is of significant relevance. That is due to the fact that the proportion of equipment at the end of assigned service life in the nuclear power industry is very high, thus dependability analysis of NPP elements and systems is required. In the process of dependability characteristics analysis a number of problems occur, i.e. evaluation of residual life of equipment, justification of life extension decisions. Also, it is required to provide spare parts for elements and systems, select maintenance strategies, etc. That increases the value of activities aimed at analyzing the dependability of nuclear power facilities and, subsequently, the requirement to develop the methods of analysis of statistical information on the operation of NPP elements, subsystems and systems for the purpose of identifying their performance parameters. At nuclear power plants, activities are organized to collect information on the operation of various facilities, i.e. failures and defects of system components, maintenance procedures, operating modes, storage conditions, etc. The information provided by the NPPs has a number of distinctive features. That is due to the following factors: presence of censorship of failure data, absence of sufficient service hours within the given observation interval and the limited volume of available data. All those factors cause an uncertainty in the resulting evaluations and, subsequently, lower that optimal accuracy on dependability characteristics calculation. In the process of evaluating the dependability of facilities in operation a certain part of facilities and systems often does not fail over the period of observation. In such situations statistical analysis of dependability is required that is based on the so-called right censored samples of which the distinctive feature consists in the fact that the inspected product does not fail within the period of observation. In some cases the operation times of specific facilities are unknown. For instance, at the initial stage of facility operation information on its performance was not collected, and the decision to collect data was taken later. In this case the required method must take into consideration the missing information that was not collected at the initial stage. The limited volume of information is due to the fact that the nuclear energy facilities fall into the category of highly dependable equipment. Failures are rare events. Therefore in order to increase the reliability of dependability indicators estimation all the available information must be used. Thus, taking into account all the available information enables more accurate results that can be used to calculate NPP facility service life. The purpose of this article is to show the application of the method of repeated sample and examine its efficiency. The main focus is on missed data that are to be recovered. The authors provide the results of evaluation of the exponential distribution law parameter subject to right censored and missed data. The suggested method of repeated sample is compared with the bootstrap method and mean substitution method. For evaluation of exponential distribution law parameter the authors suggest using the maximum likelihood method. Statistical characteristics calculation is provided. All the calculations and results are based on test cases.*

Keywords: *single substitution method, repeated sample method, bootstrap method, maximum likelihood method, censored data, missed data, data recovery.*

For citation: *Nikolayev D.A. Parametric method of observation results processing with regard to missed data. Dependability, 2017, vol. 17, no. 1, pp. 53-58. (in Russian) DOI: 10.21683/1729-2640-2017-17-1-53-58*

Introduction

The matters of ensuring dependable and safe operation of NPP facilities is of significant relevance. That is due to the fact that the proportion of equipment at the end of assigned service life in the nuclear power industry is very high, thus dependability analysis of NPP elements and systems is required. For that purpose the article looks into the state of the art of statistical analysis of information that includes time to failure, time to censoring and missed data. Taking into account all the available information enables more accurate results.

Thus, the goal is to develop the parametric approach to recovering operation time distribution density based on times to failure, times to censoring and missed data, which would allow identifying a facility's behavior pattern. Consequently, it is required to evaluate the parameter of recovered distribution density and identify the statistical indicators of dependability.

Data description

It should be noted that the object of this research is recoverable facilities of which the operability is to be restored in

case of failure. Before proceeding to the solution of the set goal let us define the types of data to be processed. The first and primary type of data is the time to failure.

In practical situations, particularly during inspections of operating facilities the information submitted to processing is extremely limited. In such cases the need arises to perform statistical analysis of dependability based on the particular samples of which the distinctive feature consists in the absence of information on operating times of the inspected facility. This type of information includes censored data. Censoring is an event that causes the interruption of product observation before the onset of the system event or the onset of the event at an unknown moment of time within a certain interval. We are focusing on cases when this interval may not be limited from the right, i.e. the sample is right censored [1, 2, 5]. The next type of data is the missed data.

Missed data are commonplace in analytical tasks and can significantly affect the conclusions that can be made based on such data.

Possible situations of application of observed information are given in Figure 1.

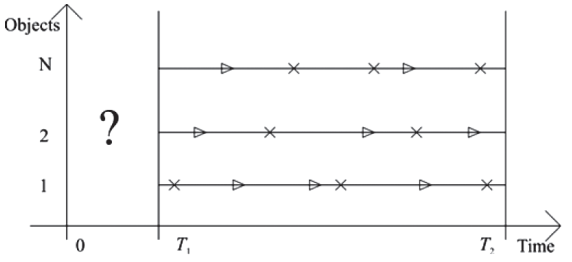


Figure 1. Event chart for data flow

This chart shows what happens to objects over the course of their operation. Data is shown as a continuous flow for a specific object, where × denotes a failure, while □ denotes right censoring. The chart also shows the interval $[0,T_1]$ in which data is not collected, i.e. within this interval observation is not conducted. Within the interval $[T_1,T_2]$ observations were conducted and information on each of the objects was registered. Therefore, the goal is to recover data for the first interval in order to be able to evaluate the parameter of the times-to-failure distribution law within the interval $[0,T_2]$.

Development of the method for missed data management using the repeated sample method

In solving the task of statistical evaluation of dependability indicators of elements and systems of special importance is the matter of collection and presentation of input information on the behavior of analyzed objects. The accuracy and integrity of input information conditions the accuracy of evaluation of the distribution density parameters and the results of dependability characteristics calculation.

As noted above, during statistical analysis operation it is often the case that within certain time intervals information of object behavior is missing. That causes the situation of missed data (Figure 1) which significantly complicates mathematical processing due to the presence of bias in primary statistical characteristics, e.g. mathematical expectation or variance.

Problem definition. Let N objects be under observation (figure 1). For each object, there is a set of data for a certain period of time. Over the time of object operation within the interval from 0 to T_1 information on its behavior was not recorded. Between moments T_1 and T_2 information was collected. Based on the results of observations within the interval $[T_1,T_2]$ for each object time to failure and times to censoring are recorded. The goal is to recover data for the interval $[0,T_1]$ that may constitute either failures or censored data and to evaluate the parameter of the times-to-failure distribution within the interval $[0,T_2]$.

It is suggested to solve the problem of missed data recovery by means of the repeated sample method.

The method consists in the following:

Based on the results of observation for the interval $[T_1,T_2]$ the distribution law parameter is calculated individually for times to failure and time to censoring using the maximum likelihood method.

The number n of operation times is evaluated for the interval $[0,T_1]$ for each type of operation time: $n = mT_1/(T_2-T_1)$, where m is the number of operation times for the interval $[T_1,T_2]$ in case of uniform data flow.

N operation times are modeled according to specified distribution law F(t) (Figure 2) for each type of operation times. I.e. on the probability axis we model the uniformly distributed random number γ_i. Let us perform bijective mapping onto time axis t.

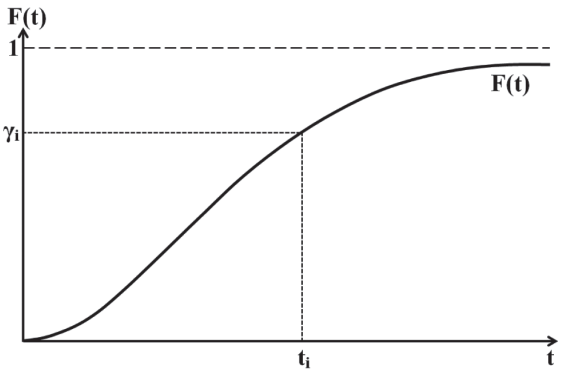


Figure 2. Method for recovery of missed data based on distribution function

Samples obtained within the intervals $[0,T_1]$ and $[T_1,T_2]$ are integrated.

Distribution law parameter of θ_i operation times is evaluated for the interval $[0,T_2]$, as well as mean square deviation σ_i is calculated using the maximum likelihood method.

Then, the distribution law parameter evaluation is calculated individually for times to failure and time to censoring for the interval $[0,T_2]$.

The evaluations obtained at step 6 are used for repeated modeling of operating times at the interval $[0,T_1]$. Steps 3 to 7 are repeated k times. The number of iterations k is defined by the researcher.

Upon completion of step 7 the average distribution law parameter is calculated:

$$\hat{\theta} = \frac{1}{k}\sum_{i=1}^{k}\theta_i \quad (1)$$

as well as the mean square deviation:

$$\hat{\sigma} = \frac{1}{k}\sum_{i=1}^{k}\sigma_i. \quad (2)$$

The obtained values $\hat{\theta}$ and $\hat{\sigma}$ are the result of application of the repeated sample method.

Test case

Step 1: As input information we use the information obtained as the result of modeling of random value in accordance with the exponential distribution law. The total number of data within the interval $[0,T_2]$ is 1000 operation times, out of which 581 are times to failure, 419 are censored data. The number is defined randomly. For data modeling, an exponential distribution was used with the following parameters: $\lambda_t = 0{,}003$ and $\lambda_c = 0{,}002$ for times to failure and times to censoring respectively. Out of the resulting set, data for each experiment (10%, 20%, …, 50%) was removed artificially. Figure 1 outlines the obtained set of data.

Step 2: Using the developed method we obtain the mean estimator of the exponential distribution law parameter $\hat{\lambda}$ and the average mean square deviation $\hat{\sigma}$. Dependability characteristics were calculated based on the method of maximum likelihood. The results are given in Table 1.

Table 1 shows not only the results of operation of the repeated sample method, but also the results obtained using such methods as mean substitution (single substitution) [3], [4] and bootstrapping [9].

The mean substitution method involves replacing missed data with the arithmetic average of sample calculated for the interval $[T_1,T_2]$ instead of each missed value within the interval $[0,T_1]$. Dependability characteristics are calculated using the method of maximum likelihood.

Bootstrapping is a practical computer-based method for researching probability distribution statistics based on repeated sampling by means of the Monte Carlo method based on the available samples. I.e. data for the interval $[T_1,T_2]$ is taken, out of which at each step of n consecutive iterations evenly distributed over the interval [1, n], a random element is retrieved that is then returned in the initial sample (i.e. can be retrieved again). Where n is the number of operation times within the interval $[0,T_1]$. The obtained elements make the data set for the interval $[0,T_1]$. Then, the sample for the interval $[0,T_2]$ is evaluated by means of the maximum likelihood method. The number of iterations for generation of a new sample is defined by the researcher. In our case the research included 1000 iterations. The mean estimator of the exponential distribution law parameter and the average mean square deviation are found using formulas (1) and (2).

The results of both method are given in Table 1.

Table 1. The results of application of the repeated sample method

Percentage of gaps	Gap-fill algorithm	Evaluation of the distribution law parameter for recovered sample, * 10^{-3}	Mean square deviation, * 10^{-3}
10%	Without recovery	2,908	0,110
	With arithmetic average	2,959	0,107
	Bootstrap value	2,909	0,104
	Repeated sample method	2,911	0,105
20%	Without recovery	2,874	0,116
	With arithmetic average	2,917	0,105
	Bootstrap value	2,877	0,103
	Repeated sample method	2,877	0,103
30%	Without recovery	2,877	0,125
	With arithmetic average	2,923	0,106
	Bootstrap value	2,881	0,104
	Repeated sample method	2,878	0,103
40%	Without recovery	2,894	0,136
	With arithmetic average	2,946	0,106
	Bootstrap value	2,895	0,104
	Repeated sample method	2,897	0,104
50%	Without recovery	2,963	0,151
	With arithmetic average	3,015	0,109
	Bootstrap value	2,966	0,106
	Repeated sample method	2,968	0,106

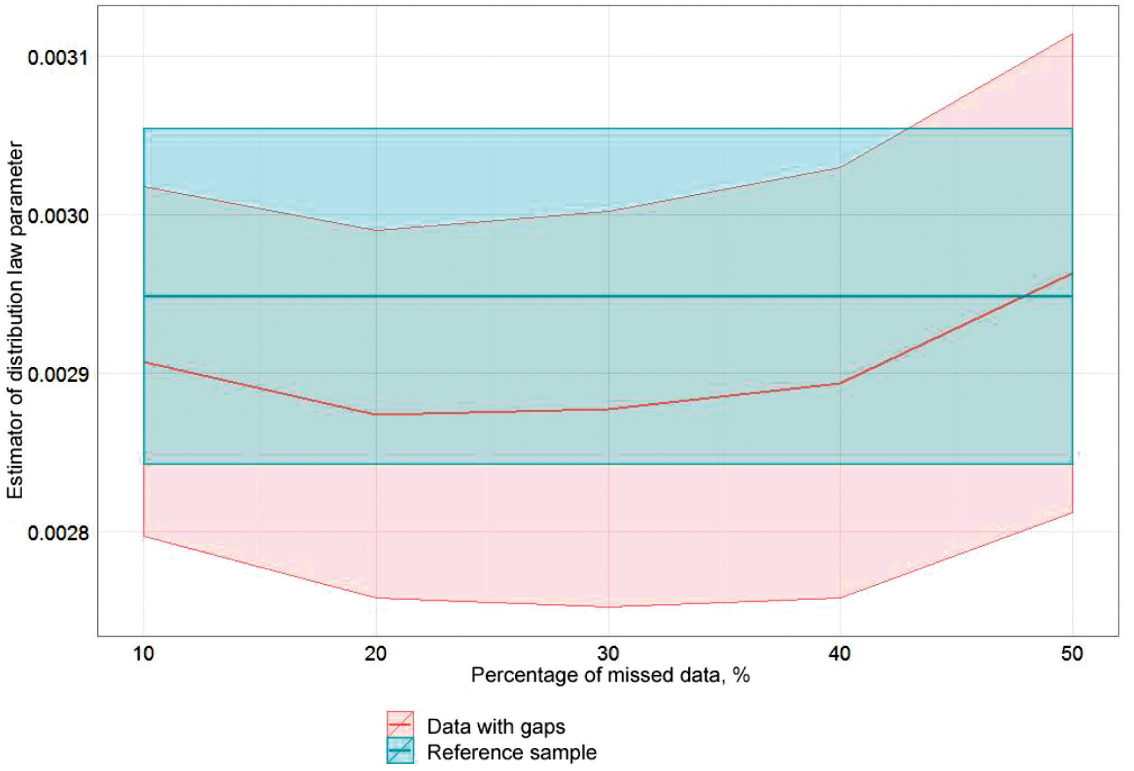


Figure 3. Estimator comparison of reference data and data with gaps

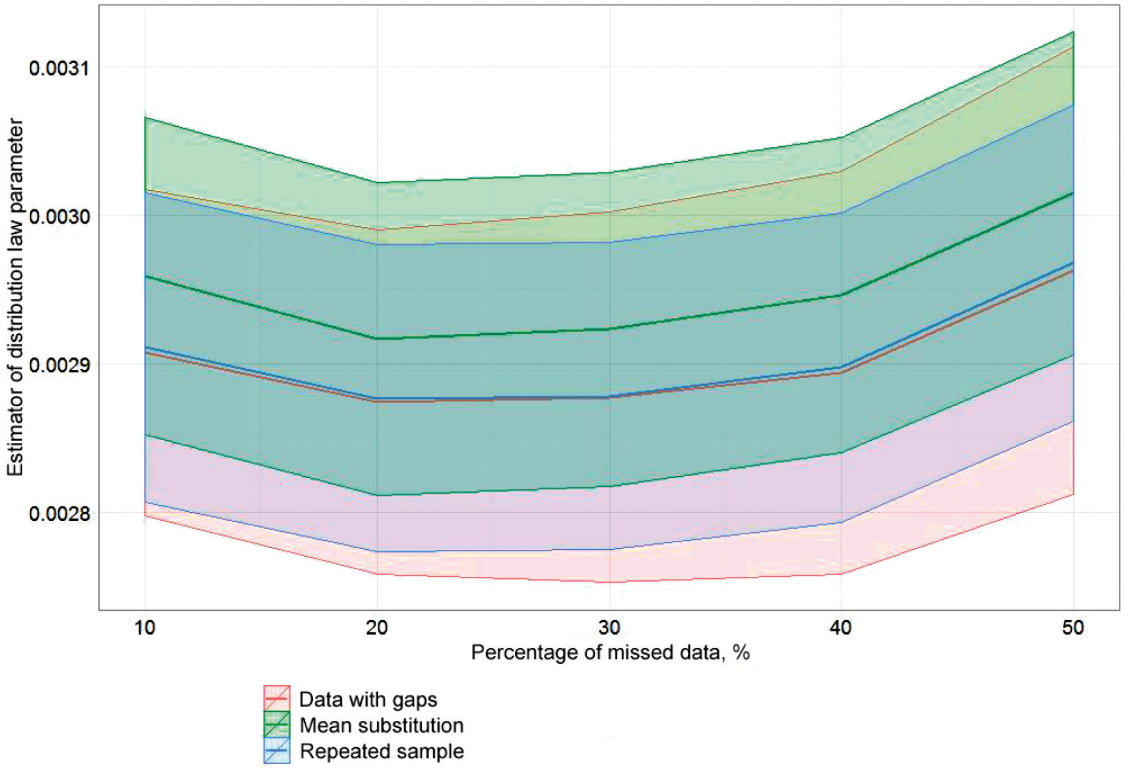


Figure 4. Comparison of estimators obtained by means of the repeated sample method and mean substitution

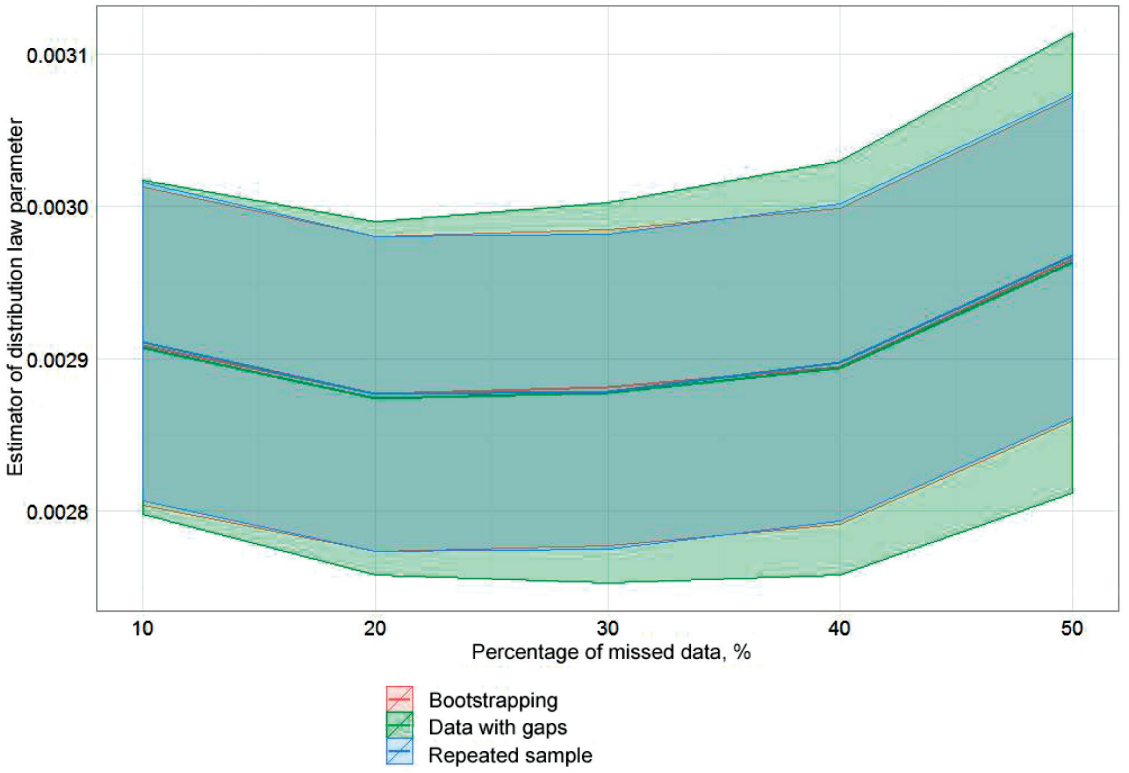


Figure 5. Comparison of estimators obtained by means of the repeated sample method and bootstrapping

In order to simplify the result comparison let us show our data in the following figures (3, 4, 5) and make conclusions for each.

Figure 3 shows the estimator of the distribution law parameter for the reference sample and the estimator for the data flow with gaps (10% ч 50%). As it can be seen in Figure 3 and Table 1, the higher the percentage of missed data the higher the mean square deviation. Therefore, it is required to recover missed data in order to reduce the deviation.

Let us analyze the resulting information in Figure 4. First, let us compare the distribution law parameter estimators. As it can be seen, the estimator obtained by means of the repeated sample method and the estimator of data with gaps match. This suggests that missed data recovery does not affect the estimator. The estimator obtained based on the mean substitution method has a bias. That is a natural consequence of the gaps being substituted with the means, i.e. the values in the middle of the sample. Therefore, the mean square deviation is biased. Let us consider the deviation for the repeated sample method. By using this method in gap recovery we managed to reduce the mean square deviation.

The results obtained by means of the repeated sample method match the results obtained by mans of bootstrapping (Figure 5). From here, two conclusions can be drawn. First, the proposed repeated sample method is not less accurate than the bootstrapping. Second, both methods fall within the class of sample modeling methods. The only difference is that the proposed method is a parametric one, while bootstrapping is a nonparametric one.

Conclusion

The activities described above have yielded the following main results and conclusions.

Various types of data were described. The parametric method for recovering missed data subject to censored information was developed and tested with a test case. Comparison with other methods was made (mean substitution and bootstrapping) and shown the efficiency of the proposed method.

Procedures were developed for recovery of information and evaluation of the exponential distribution law parameter: repeated sample value, mean substitution method, maximum likelihood method. The performed calculations allowed concluding that the proposed repeated sample method is as accurate as bootstrapping. It is also of note that the repeated sample is a parametric method, while bootstrapping is a nonparametric one.

The accuracy of distribution density recovery was researched. The results show that data recovery reduces uncertainty in the calculated indicators (parameters of the exponential distribution law) thereby indicating the requirement to take account of the missed data.

A comparison was made of the results of evaluation of information that was recovered using various methods: re-

peated sample, bootstrapping and mean substitution. It was shown that the mean substitution method causes a bias in the parameter of distribution law. At the same time, repeated sample and bootstrapping produced unbiased results.

References

1. Antonov AV. Sistemny analiz [System analysis]. Moscow: Vyshaya shkola; 2004. Russian.

2. Antonov AV, Nikulin MS. Statisticheskie modeli v teorii nadiozhnosti: Ouchebnoie posobie [Statistical models in the dependability theory: A study guide]. Moscow: Abris; 2012. Russian.

3. Zangiyeva IK. Reshenie problem nepolnykh dannykh massovykh oprosov [Solving the problem of incomplete data of mass survey]. Rossiyskaya sotsiologia zavtrashnego dnia [Russian social science tomorrow]. 2008: 84 – 95. Russian.

4. Zloba E, Iatskiv I. Statisticheskie metody vosstanovleniya propushhennykh dannykh [Statistical methods for recovery of missed data]. Computer Modeling & New Technologies. 2004; 6: 55 – 56. Russian.

5. Cox DR, Oakes D. Analiz dannykh tipa vremeni zhizni [Analysis of survival data]. Moscow: Financy i statistika; 1988. Russian.

6. Little RA, Rubin DB. Statisticheski analiz dannykh s propuskami [Statistical analysis with missed data]. Moscow: Financy i statistika; 1991. Russian.

7. Efron B. Netraditsionnie metody mnogomernogo statisticheskogo analiza [Unconventional methods of multivariate statistical analysis]. Moscow: Financy i statistika; 1988. Russian.

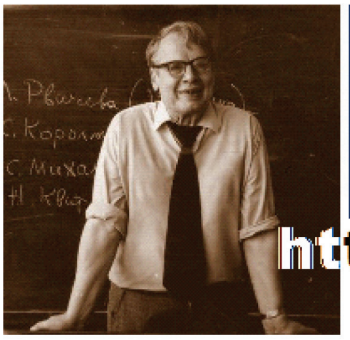
8. Bischl B, Mersmann O, Trautmann H. Resampling methods in model validation. Algorithm Engineering Report. 2010 Aug; 9: 14 – 31.

9. Meeker WQ, Escobar A. Statistical Methods for Reliability Data. New York: John Wiley & Sons, Inc.; 1998.

About the author

Dmitri A. Nikilayev, postgraduate, Obninsk Institute for Nuclear Power Engineering, 1 Studgorodok, 249040 Obninsk, Kaluga Oblast, Russia, e-mail: dafanday@gmail.com

Received on 01.06.2016



Gnedenko e-Forum

International Group on Reliability

http://Gnedenko-Forum.org/

Dear colleagues!

In 2005 the informal Association of Experts in Reliability, Applied Probability and Statistics (I.G.O.R.) was established with its own Internet website GNEDENKO FORUM. The site has been named after the outstanding mathematician Boris Vladimirovich Gnedenko (1912-1995). The Forum's purpose is an improvement of personal and professional contacts between experts in the mathematical statistics, probability theory and their important branches, such as reliability theory and quality control, the theory of mass service, storekeeping theory, etc.

Since January 2006, the Forum has published a quarterly international electronic magazine

"Reliability: Theory and Applications".

The magazine is registered with the Library of Congress in the USA (ISSN 1932-2321). All rights reserved for authors so that articles can be freely published in any other publications or presented at conferences.

Join Gnedenko Forum!

Welcome!

More than 500 experts from 44 countries worldwide have already joined us!

To join the Forum, send a photo and a short CV to the following address:

Alexander Bochkov, PhD

a.bochkov@gmail.com

Membership is free.

REQUIREMENTS OF EDITION ON EXECUTION OF PAPERS IN JOURNALS OF PUBLISHING GROUP OF IDT PUBLISHERS

A letter from the organisation where the author (s) works or from the author (s) personally with the paper offered for publication should be sent to the de facto editorial office address: 107078, Moscow, 5 Orlikov lane, Office 755, LLC "JOURNAL DEPENDABILITY" or e-mail: E.Patrikeeva@gismps.ru (in scanned form). The letter should be attached to a paper text containing the summary and keywords, information on authors, bibliographic list, and one complete set of figures. All listed items are to be presented in an electronic form (on CD or via the e-mail address provided above).

Attention! Titles of papers, names of authors, summary and keywords must be presented, in Russian and English languages, according to the requirements of the Higher Attestation Commission. The information on each author should contain the following standard data:

- Surname, name, patronymic;
- Scientific degree, academic status, honorary title;
- Membership of relevant public unions, etc.;
- Place of employment, position;
- The list and numbers of Journals of IDT Publishers in which papers of the author have been previously published;
- Contact information.

Texts should be presented in Word 97-2003 format in a 12-point typeface; the text should not be formatted. Paragraphs should be arranged by pressing the "return" key. The text of the paper should be double-spaced on pages of A4; on the left there should be a margin of 2 cm; pages should be numbered, the «first line indent» is obligatory.

All alphabetical designations represented in figures should be explained in the body text or in a legend. Inconsistencies between designations in figures and in the text are inadmissible. Numbering should only be applied to those formulas and equations that are referred to in the text.

Simple formulas appearing directly in the text (for example, m^2, n^2t, $c = 1 + DDF - A_2$), and the Greek letters and symbols, for example, β, © may be typed using the Symbol font. When it is not possible to type directly in the text editor, use the "Microsoft Equation" formula editor (available with the complete installation of Microsoft Office) or the "Mathtype" formula-editing program. Representation of formulae in the text in the form of images is not admissible. Photos and figures for papers should be provided in individual files with extension TIF, EPS or JPG with a resolution of not less than 300 dpi. The list of literature referred to in the paper (bibliography) is presented according to order of citation and provided at the end of paper. References to the literature in the text are marked by serial numerals in square brackets.

To authors that are published in journals of "IDT Publishers".

In addition to the journal, information on each author will be presented at the techizdat.ru site in the «Authors» section on the individual web page.

Authors of papers for publication have the opportunity to send an electronic photo and additional material to appear on this individualised Internet-business card. At their own discretion, authors can present more details about themselves, interesting examples and stories of solutions to technical problems, about contemporary problems according to subjects of corresponding journal, etc. This material should not exceed 1000 characters including spaces.

SUBSCRIPTION TO THE JOURNAL «DEPENDABILITY»

It is possible to subscribe to the journal:

- Through the agency «Rospechat»
  – for the first half of the year: an index 81733;

- Under the catalogue "Press of Russia" of the agency «Books-services»:
  – for half a year: an index 11804;

- Through the editorial office:
  – for any time-frame
  tel.: 8-916-105-81-31; e-mail: E.Patrikeeva@gismps.ru

Igor B. Shubinsky

FUNCTIONAL DEPENDABILITY OF INFORMATION SYSTEMS

2012

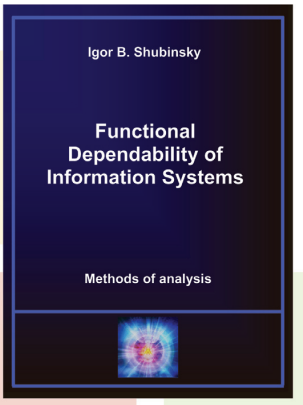
For the first time, this book presents the theory of functional dependability of information systems as a component of the general dependability theory. The book comprises basic concepts and definitions, major threats for the functional dependability of information systems, system parameters, methods for estimating the functional dependability of digital devices, and methods and models of estimating software functional dependability. A separated chapter considers the functional reliability of critical information systems, including the concept of a critical system, features of faults, estimation of functional reliability of operators, estimation of hazardous failures and risks, the requirements of functional dependability and the software architecture of critical information systems. A checklist of the most complex and significant subjects is provided at the end of each chapter.

The book is primarily intended for experts who are engaged in practical development, manufacture, operation and updating of information technologies and information systems. It is intended for researchers in the field of software-hardware of information systems, academic staff, post-graduate students and students specializing in the field of information technologies as well as those working in the field of automated control systems.

Publication can be purchased through the editorial board of Journal Dependability Ltd.
by phone 8 (495) 967-77-05, ext.186; 8-916-105-81-31 (Patrikeeva Evgenia)
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

НАДЁЖНОСТЬ
DEPENDABILITY SCIENTIFIC AND TECHNICAL JOURNAL
ISSN 1729-2646

REPRESENTS



Publication can be purchased through the editorial board of Journal Dependability Ltd.

8 (495) 967-77-05, ext.186; 8-916-105-81-31 (Patrikeeva Evgenia)

E.Patrikeeva@gismps.ru, www.dependability.pro

Journal Dependability Ltd.
109029, Moscow,
Nizhegorodskaya str., 27, bldg. 1, office 209
Tel. / Fax: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

Igor B. Shubinsky

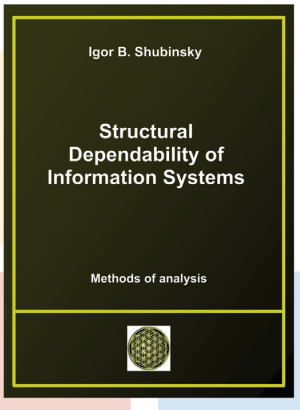
STRUCTURAL DEPENDABILITY OF INFORMATION SYSTEMS
Methods of analysis

Editor: Patrikeeva Evgenia
Make-up: Kurtish Boris S.
Proofreading: Komarova Catherine E.

Copy deadline 12.07.2012. Format of the edition 70x100/16.
Offset printing. Offset paper. Conv. Sheet l. 24,05.
Circulation of 700 copies. Order number 1452.

НАДЁЖНОСТЬ
DEPENDABILITY SCIENTIFIC AND TECHNICAL JOURNAL
ISSN 1729-2646

REPRESENTS



Publication can be purchased through the editorial board of Journal Dependability Ltd.

8 (495) 967-77-05, ext.186; 8-916-105-81-31 (Patrikeeva Evgenia)

E.Patrikeeva@gismps.ru, www.dependability.pro

Journal Dependability Ltd.
109029, Moscow,
Nizhegorodskaya str., 27, bldg. 1, office 209
Tel. / Fax: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

Igor B. Shubinsky

STRUCTURAL DEPENDABILITY OF INFORMATION SYSTEMS
Methods of analysis

Editor: Patrikeeva Evgenia
Make-up: Kurtish Boris S.
Proofreading: Komarova Catherine E.

Copy deadline 12.07.2012. Format of the edition 70x100/16.
Offset printing. Offset paper. Conv. Sheet l. 24,05.
Circulation of 700 copies. Order number 1452.

Igor B. Shubinsky

STRUCTURAL DEPENDABILITY OF INFORMATION SYSTEMS

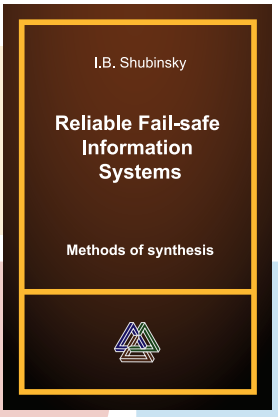
2012

The book presents the basic concepts and parameters of the structural dependability of information systems. It discusses general and specific differences in dependability indices used in domestic and international standards, along with recent developments in approaches to dependability modeling. Markov reliability models together with graph semi-Markov methods for calculating reliability are described in detail and illustrated by numerous examples. Considerable attention is paid to the engineering methods of calculation and the approximate prediction of structural dependability and error estimation of information systems as well as to the statistical assessment of dependability parameters. At the end of each chapter there are checklists of the most complex and significant subjects of the chapter.

The book is intended primarily for professionals involved in practical work on the development, production, operation and modification of information systems. It is designed for scientists in the field of structural dependability of various discrete systems, academic staff and graduates (students) specializing in information systems as well as in the field of automated control systems.

Publication can be purchased through the editorial board of Journal Dependability Ltd.
by phone 8 (495) 967-77-05, ext.186; 8-916-105-81-31 (Patrikeeva Evgenia)
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

НАДЁЖНОСТЬ
DEPENDABILITY SCIENTIFIC-TECHNICAL JOURNAL
ISSN 1729-2646
REPRESENTS



Publication can be purchased through the editorial board of Journal Dependability Ltd.

+7 (495) 967-77-05, ext.186
+7-916-105-81-31
(Patrikeeva Evgenia)

E.Patrikeeva@gismps.ru,
www.dependability.pro

Igor B. Shubinsky

RELIABLE FAIL-SAFE
INFORMATION SYSTEMS
Methods of synthesis

Journal Dependability Ltd,
109029, Moscow,
Nizhegorodskaya str.27, bldg.1, office 209
Tel./fax: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

Copy deadline 12.02.2016. format of the edition 70x100/16.
Offset printing. Offset paper. Conv. Sheet. P. 17,55.
Circulation of 700 copies. Order number 1452.

I.B.Shubinsky

Reliable Fail–safe Information Systems

2016

The book describes conceptual provisions to ensure structural and functional reliability of information systems at all stages of a life-cycle. It represents different types of redundancy taking into account limited efficiency of the failure detection system. Under these conditions a broad-based assessment of their efficiency is performed, with determination of capabilities of structural redundancy with an endless number of standby facilities. Ways to ensure functional reliability of software are represented, including the recommendations for the development of software programs requirement specification, with the description of the process of a reliable program architecture development and well proven rules and recommendations used for design and implementation of software, as well as for integration with system hardware.

The book also presents theoretical and practical provisions of adaptive fault tolerance (active protection) of information systems, including the methods and disciplines of active protection, as well as the ways of implementation. A method of synthesis of active protection and the results of research of information system reliability with various disciplines of active protection are offered. There are also certain assessments of the efficiency of active protection in relation to the traditional methods of structural redundancy.

You can find the description of the principles to ensure functional safety of information systems, with a substantiation of the possibility to restart independent channels in two-channel safe systems. The rules of determination of the allowed time for a guaranteed detection of single and double hazardous failures are developed, including the method of synthesis of a combined two-level information system developed with higher functional safety requirements.

To prove the conformance of reliability with functional safety the method of accelerated field testing of the information system has been developed. The book contains the description of this method, including the example of its practical implementation. You will also find the information about the procedures of certification tests based on the requirements of information safety and software certification conformance.

A checklist of the most complex and significant subjects is provided at the end of each chapter. The book is primarily intended for experts who are engaged in practical development, manufacture, operation and updating of information. It is intended for researchers in the field of structural reliability of different discrete systems, academic staff, post-graduate students and students specializing in the field of information systems and as well as those working in the field of automated control systems.

Publication can be purchased through the editorial board of Journal Dependability Ltd.
By phone +7 (495) 967-77-05, ext. 186; +7-916-105-81-31 (Patrikeeva Evgenia)
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

SUBSCRIBER APPLICATION FOR DEPENDABILITY JOURNAL

Please subscribe us for 20___
from No. _____ to No._____ number of copies _____

Company name	
Name, job title of company head	
Phone/fax, e-mail of company head	
Mail address (address, postcode, country)	
Legal address (address, postcode, country)	
VAT	
Account	
Bank	
Account number	
S.W.I.F.T.	
Contact person: Name, job title	
Phone/fax, e-mail	

Publisher details: Dependability Journal Ltd.
Address of the editorial office: office 209, bldg 1, 27 Nizhegorodskaya Str., Moscow 109029, Russia Phone/fax: 007 (495) 967-77-02, e-mail: E.Patrikeeva@gismps.ru
VAT 7709868505 Account 890-0055-006
Account No. 40702810100430000017
Account No. 30101810100000000787

Address of delivery:

To whom:_____

Where:_____

_____

To subscribe for Dependability journal, please fill in the application form and send it by fax or email.
In case of any questions related to subscription, please contact us.
Cost of year subscription is 4180 rubles, including 18 per cent VAT.
The journal is published four times a year.

THE JOURNAL IS PUBLISHED WITH PARTICIPATION AND SUPPORT

OF JOINT-STOCK COMPANY RESEARCH & DESIGN INSTITUTE
FOR INFORMATION TECHNOLOGY, SIGNALLING AND TELECOMMUNICATIONS
ON RAILWAY TRANSPORT (JSC NIIAS)

JSC NIIAS is RZD's leading company in the field of development of train control and safety systems, traffic management systems, GIS support technology, railway fleet and infrastructure monitoring systems

Mission:

transportation

- ❑ efficiency,
- ❑ safety,
- ❑ reliability

Key areas of activity

- Intellectual control and management systems
- Transportation management systems and transport service technology
- Signalling and remote control systems
- Automated transportation management centers
- Railway transport information systems
- Geoinformation systems and satellite technology
- Transport safety systems
- Infrastructure management systems
- Power consumption and energy management systems
- Testing, certification and expert assessment
- Information security
- Regulatory support

www.vniias.ru