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

Original article
Dependability, vol. 19 no.2, 2019 DOI: 10.21683/1729-2646-2019-19-2-3-8

Method of dependability assessment of spacecraft in design and engineering studies

Vladimir Ya. Gecha, *A.G. IosifianResearch and Production Corporation Space Monitoring, Information, Control and Electromechanical Systems, Russian Federation, Moscow*
Ruslan N. Barbul, *A.G. IosifianResearch and Production Corporation Space Monitoring, Information, Control and Electromechanical Systems, Russian Federation, Moscow*
Nikolay I. Sidniaev, *Bauman Moscow State Technical University, Russian Federation, Moscow*
Yulia I. Butenko, *Bauman Moscow State Technical University, Russian Federation, Moscow*


Vladimir Ya. Gecha


Ruslan N. Barbul


Nikolay I. Sidniaev


Yulia I. Butenko

Abstract.*The paper examines the matters of operational dependability of space systems (SS), efficiency of complex systems, use of redundancy in spacecraft (SC) design. It presents methods of predicting the dependability of designed devices, design of devices with desired dependability and comparison of dependability of various SS. For that purpose, the authors set forth the fundamentals of the dependability theory for SS design, methods of collection and processing of data of equipment dependability based on the results of operation and special dependability tests. Methods, mathematical models are developed, the equipment architecture at the stage of design and manufacture is analyzed. The paper also cites the design ratios for various tested types of redundancy, lifetime extension of SC units based on the residual operating life estimation method. The existing methods of dependability analysis are classified and examined. The authors outline the problems of ambiguity of information of the input data in case of classical computing. The effect of nominal deviations of the external effects, irregularity of the failure rate, non-linear nature of the effect of external factors on the dependability are examined. The paper also takes a look at the way the external factors affect the dependability and the degree to which such factors are taken into consideration in the existing methods. It is noted that the qualitative, technical and organizational (design and software) requirements for dependability in the technical specifications for each stage of elements and SS development, shall be observed and confirmed at the respective stage of activities. The paper presents the methods of estimation of technical item operating life with the focus on those based on the physical premises of operating life depletion.Attention is drawn to the importance of the economic aspect in the research dedicated to SS lifetime extension.*

Keywords: *dependability, methods, operating life, design, spacecraft, operating life assessment.*

For citation: *GechaVYa, Barbul RN, Sidniaev NI, ButenkoYuI. Method of dependability assessment of spacecraft in design and engineering studies. Dependability 2019;2: 3-8. DOI: 10.21683/1729-2646-2019-19-2-3-8*

Introduction

The stages of design, starting from the development of the technical specifications for a system to the delivery of technical documentation for prototype production are of key significance within the overall problem of ensuring dependability of spacecraft (SC). An important activity that governs the relationships among all the parties involved in the SC development is the substantiation of the dependability program (DP) of a product as a whole, its components and element, as well as the development and approval of the procedure of dependability requirements confirmation at all stages of development [1-4]. For that purpose, DP models, standard DP and dependability confirmation models (procedures) are used. After the selection of all project, architectural, design and process engineering solutions before the final formalization of a project by the company's dependability service jointly with the developing units, the design outputs are evaluated in terms of dependability and the adopted solutions are adjusted [5-8].

SC is a complex multicomponent system that includes both hardware and software components [9-12]. Consequently, their operation involves real-time supervision of their characteristics and state analysis. Dependability is one of the primary characteristics of a technical system [3]. According to the Russian national standard, dependability us understood as the property of and item 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, repairs, storage and transportation [4]. Due to the complexity of SC structure (and, subsequently, complex nature of relations among the individual components), the process of obtaining the numerical values of dependability indicators becomes more complicated as well [5-8].

The methodological aspects and objectives of the problem

A number of methods and measures are used for prevention and detection of failures related to the design, manufacture and operation, as well as protection of system elements from their consequences. If preliminary studies of system efficiency determine the required quantity and level of guaranteed mission completion, the minimal required level of product dependability can be clearly determined by estimating and minimizing the total cost of development and application, i.e. program execution as a whole [6, 7].

Development of a limited use system (tens of items). In this case all components of the total cost must be taken into consideration: costs of system development, manufacture and operation of the whole fleet of products that ensures mission completion not less than N_{req} times (required number of products) with the guarantee not lower than γ_{req} [9-12]. Specifying system and components dependability requirements involves:

• making a list of dependability indicators,

• definition of dependability norms (specification of the required quantitative values of dependability indicators of system components),

• definition of confidence probability or mean square deviation norms, that must be observed while confirming the standard values of system dependability indicators by the time the state tests are complete,

• specification of managerial and technical requirements for dependability per system elements,

• definition of the procedure of confirmation of dependability requirements per design stages of system components.

In the general formulation, the dependability norms definition is as follows [8, 9,13].

Let SC consist of N elements integrated with a certain structure and performing certain functions. The following are known [9, 10, 14]: type of joint density of SC element failures (τ_i), $f_s\left\{\tau_i; i=\overline{1,N}\right\}$, required value (or a series of values) of the system dependability indicator P, functions of relations between dependability and considered factors $\phi_l\left\{P_i; i=\overline{1,N}, \Phi_\nu, \nu=\overline{1,S}\right\}$, $l=\overline{1,L}$; distribution function of faultless operation time of components $F_i = P_i\left\{f\left(\tau_i\right)\right\}$, $i=\overline{1,N}$; objective function (functional) $g = g\left\{P_i, i=\overline{1,N}\right\}$, where P_i is the pointwise value of the dependability estimate of the i-th element, Φ_ν is the considered ν-th factor, S is the number of factors under consideration, L is the number of functions of relations.

It is required to find such values of elements' dependability that optimize the objective function g [1, 9].

If it is required to design a SC with minimal cost or mass, the cost or mass $g = C, C = C\left\{P_i, i=\overline{1,N}\right\}$,or $g = M$ are chosen as the objective function, $M = M\left\{P_i, i=\overline{1,N}\right\}$.

The solution involves finding vector $P=\{P_1, P_2, \ldots, P_i, \ldots P_N\}$ that minimizes C or M, i.e. $C(\bar{P}) = \min C(\bar{P})$; $\bar{P} = \{P_1, P_2, \ldots, P_i, \ldots P_N\}$, or $M(\bar{P}) = \min M(\bar{P})$; $\bar{P} = \{P_1, P_2, \ldots, P_i, \ldots P_N\}$ if $\Phi(P) \geq \Phi_0$. If the task consists in maximizing function $\Phi(P)$ under the given cost (or mass) limitations, then $\Phi = \Phi\left\{P_i, i=\overline{1,N}\right\}$.Vector P is found that maximizes $\Phi(\bar{P})$, i.e. $\Phi(\bar{P}) = \max \Phi(P)$ if $C(\bar{P}) \leq C_0$ or $\Phi(\bar{P}) = \max \Phi(P)$ if $M(\bar{P}) \leq M_0$. Norm definition often takes into consideration not only system dependability requirements, but safety requirements as well. Then, the problem is solved using the safety function as function $\Phi(\bar{P})$, i.e. $B = \Phi(\bar{P})$,then condition $B = \Phi(\bar{P}) \geq P_B$. Is verified. If it is fulfilled, the problem is solved, if not, the solution continues starting from vector $P = \bar{P}_B$, i.e. vector that satisfies the solution at the first stage.

Methods of specific implementation

In the process of creation of space technology products that have no analogs and prototypes, instead of strict standard values of dependability indicators, algorithms and methods of specification and norm definition of quantitative dependability requirements are developed that take into consideration the characteristic aspects of application of a SC and its element [15,16], as well as the actual limitations.

Let us examine the application field of probabilistic dependability indicators as the basis for ensuring guarantees depending on the scope of SC application [4, 5, 7]. Let the objective of a one-off program of creation and application of a single-use satellite consist in satisfying the need for N_{req} of such products. The required satellite operation time is specified, probability of no-failure R is used as the product dependability indicator. The dependence between the level of product dependability and the cost as part of the dependability program is known to be $R = R_1R_2R_3$, where $R_1 = 1-(1-R_{10})\exp\left[-\alpha_1(C_1 - C_{10})\right]$ is the dependability component, that takes into consideration the effect of components failure subject to redundancy, $R_2 = 1-(1-R_{20})\exp\left[-\alpha_2(C_2 - C_{20})\right]$ is the dependability component that takes into consideration the quality level of manufacture and quality assurance, $R_3 = 1-(1-R_{30})\exp\left[-\alpha_3(N_{ed} - N_{ed0})\right]$ is the dependability component that takes into consideration the quality level of maturity, R_{10}, R_{20}, R_{30} are the initial (minimal) levels of components R_1, R_2, R_3 that correspond to the minimal expenditure C_{10}, C_{20}, $N_{от0}$ of resources C_1, C_2 and products N_{ed} spent on the experimental development, α_1, α_2, α_3 are the parameters that define the growth rate of components of indicator R as the costs increase.

Possible solutions and strategies take into consideration the fact that achieving the specified objective is possible both through increased expenses on higher level of dependability of each item and through extended scale of products manufacture [14].

As when N SC are manufactured, the number of SC N_s that successfully completed their mission is random, the practically achievable guarantee would be γ, where $\gamma = P\{N_s \geq N_{req}\}$. Each solution is defined by the vector of components R_1, R_2, R_3 or corresponding costs C_1, C_2, $N_{от}$, which unambiguously defines level R. For the specified γ and N_{req} subject to known R the number of manufactured SC $N_G = f(N_{req}, \beta, R)$ can be clearly identified that guarantees successful mission completion. The total costs of program implementation C_Σ can be identified using the dependence $C_\Sigma = (C_1 + C_2)(N_{ed} + N_G)$. The rationality (optimality) of the solution that involves the definition of the required level of dependability of the product and allocation of resources to dependability assurance measures consists in the minimization of the total cost of development and manufacture of the required number of SC [11, 15] that guarantees successful operation of $N_s \geq N_{req}$ products. As the outcome set we will use the sample space. Each sample event ω_i consists in the fact that the use of N SC resulted in exactly $N_s = i$ successes. From the point of view of achieving the set goal the whole outcome set W can be divided into two subsets W_1 and W_2 such that

$$\forall(i = 0,1,...,N)(w_i \in W_1) \leftrightarrow (i \geq N_{req});$$

$$\forall(i = 0,1,...,N)(w_i \in W_2) \leftrightarrow (i < N_{req}).$$

In this context the probability of event $w_i \leftrightarrow \{N_y = i\}$ under the known probability of no-failure of SC is identified according to formula [4]:

$$P\{w_i\} = C_N^i R^i (1-R)^{N-i}.$$

This formula defines the probability measure over the realm W.The event W_1 is the union of all ω_i under $i \geq N_{req}$, therefore its probability is defined as the sum of probabilities of such sample events.

$$P\{W_1\} = \sum_{i=N_{req}}^{N} C_N^i R^i (1-R)^{N-i}.$$

This probability ensures the level of practical guarantee of successful program performance. In order to ensure the required level of guarantee γ under known values of R and N_{req} we can increase N thus redefining the space W_1 until we obtain compliance with condition $P\{W_1\} \geq \gamma$ [2]. The value of N will be equal to the target value N_G. Thus, we will find the possible ways of constructing the functional correspondences $\phi : R \to N$.If the set R is taken as a space of strategies, out of which must be chosen the value R_{ed} that ensures the minimal total cost of program implementation $C_{\Sigma min}$, correspondence φ solves a part of the problem: for each R it defines N_G. The solution is complicated by the fact that dependability R can be ensured by various combinations of components R_1, R_2, R_3. Ineach particular case the problem of auxiliary optimization can be defined and solved. For instance, that may include finding vector R_1, R_2, that ensures $R' = R_1R_2$ under minimal cost $C = C_1 + C_2$. The procedure of extremum seeking is set forth in [2, 9] as part of a program that defines the dependence of unit costs $C_{un} = C_\Sigma / N_{req}$ and standardized unit costs $C_{un.s} = C_{un} / C_0$, where $C_0 = C_{10} + C_{20}$, from the required number N_{req} for specific sets of input data [11]. Additionally, calculations can help identify the cost component associated with the compensation of statistical instability of the result as compared to the mathematical expectation

$$\Delta C_\gamma = \frac{C}{C_\Sigma}\left(N_\Gamma - \frac{N_{req}}{R}\right),$$

as well as the cost component associated with assurance of dependability

$$\Delta C_R = 1 - \Delta C_\gamma - \frac{C_0}{C_\Sigma}(N_{req} + N_{ed0}).$$

The analysis of the last two formulas allows identifying the range of values of mass product manufacture with various capabilities of using probabilistic requirements as the basis of guaranteeing success [1, 4, 12]. For mass-production items ($N_{req} > 10^3$) the additional cost of ensuring guaranteed results that compensate for the statistical instability of random phenomena relative to average ones account for several percent of the total cost of program and an insignificant fraction of the total cost of the dependability program. For serial production items ($N_{req} > 10^2$) the costs associated with the instability compensation account for 10% of the total cost and about 20 % of the cost of the dependability

program. For low-volume items (N_{req} of tens) the costs associated with the instability compensation account for 25% of the total cost and up to 50 % of the DP cost. Finally, for unique items (N_{req} of several units) the costs associated with the compensation of statistical instability through larger scale manufacture can be several times higher than the initially planned cost of the program, which is obviously an unacceptable way of ensuring a guaranteed result. Analysis shows the applicability of stochastic determinism in ensuring guarantee. In the context of the above example, the dependence between the achieved level of product dependability and the expired costs is assumed to be defined by functional correspondence $\phi : C \to R$ with the following properties:

$$\forall\left(s_i, s_j \in S\right)\exists\left(w_i = \phi\left(s_i\right), w_j = \phi\left(s_j\right)\right):\left[w_i, R_w, w_j\right] \to \left[s_i R_s s_j\right],$$

which allows finding clearly the best strategy of cost allocation that ensures the maximum indicator R to the definition of the acceptable error of the extremum seeking procedure.

The only type of considered uncertainty consists in the uncertainty of functional correspondence, i.e. the random nature of the number of successes. The principle of guaranteed result allows eliminating this uncertainty through the introduction of the level of practical guarantee and construction of domain $f : R \times N \to N_G$.

The next step in accommodating the problem definition to the real-world problems consists in accounting for the uncertainty of correspondence $\phi : C \to R$ that, in a fairly general case, can be defined with a joint distribution of the constants that make the correspondence. Consistent application of the principle of guaranteed result is based on the construction of a confidence interval $\left[\underline{R}(C), 1\right]$ with the level of practical guarantee of assurance γ_{as}. The practical guarantee of successful program performance γ now depends on both the guarantee of assurance γ_{as} and the guarantee of successful application γ_{ap}: $\gamma = \gamma_{as}\gamma_{ap}$. Such definition of the problem would suggest an investigation into the expediency of the strategy of experimental confirmation of the achieved level of dependability[2].

Let us assume that for the purpose of confirming a certain level of dependability R_n it is planned to test n SC. The result of each test $\{n, m\}$, where m is the number of successful tests, are random and on the assumption of independence of outcomes have the probability

$$P\{n, m\} = \binom{n}{m} R_{as}^{n-m}\left(1 - R_{as}\right)^m,$$

where R_{dep} is the level of assured dependability. For each outcome $\{n, m\}$ a conditional density of the Bayesian estimate of the confirmed level of dependability R_n

$$\phi_{con}\left(R_n / n, m\right) = \frac{R_n^{n-m}\left(1 - R_n\right)^m \phi\left(R_n\right)}{\int_0^1 R_n^{n-m}\left(1 - R_n\right)^m \phi\left(R_n\right) dR_n}.$$

The weight-average conditional density of the estimate of the confirmed level of dependability will be:

$$\overline{\phi}_{con}\left(R_n\right) = (n+1)!\, n! \times R_{as}^{n-m}\left(1 - R_{as}\right)^m R_n^{n-m} \times \sum \frac{\left(1 - R_n\right)^m}{\left(m!\right)^2\left[(n-m)!\right]^2}.$$

Using this dependence, the functional correspondence can be obtained, $\phi : R_{as} \times n \times R_n \to \gamma_n$. In order to confirm the level R_n while testing n products with dependability R_{as}, a dependence of the following type should be used:

$$\gamma_n = (n+1)\sum_{m=0}^{n} R_{as}^{n-m}\left(1 - R_{as}\right)^m \left[\frac{n}{m!(n-m)!}\right]^2 \int_{R_n}^{1} z^{n-m}\left(1 - z\right)^m dz.$$

In case of high n (around 20 and more) and $m \geq 1$ the calculatedγ_n can be simplified using a normal approximation of the a posteriori density of distribution with dispersion $\sigma^2 = R_{as}\left(1 - R_{as}\right)/n$. Thus, for instance, the solution results of the problem of optimal values of R_{as}, n,γ_n, C, $N_G$for the level of guarantee γ = 0.9 for product application programs of various scope suggest insufficient efficiency of probabilistic indicators alone in planning unique product creation programs. At the same time, for programs with the scope of product application above a hundred, for ensuring the guarantee of 0.9 the optimal share of costs for dependability confirmation is 10%, 5% and 2% of the total cost for the scope of application 100, 500 and 2000 items respectively. The difference between the achieved and confirmed levels of guarantee goes down from 0.15 to 0.06.

Calculations show that confirmation of dependability is more efficient in cases of large scopes of application. In case of small scopes of application the priority funding should be directed towards ensuring dependability. The form of dependence $R_{as} = f(C)$ is defined based on the experience of the previous DP of similar products, which does not rule out the possibility of new unforeseen problems, types of failures, etc. In this context, it would be reasonable to develop efficient protection measures as part of DP that – by means of higher quality of SC application management – may enable the solution of the problem under a higher level of initial uncertainty.

Conclusions

The paper proposes a new approach to the analysis of operational dependability of multicomponent space systems (SS) that allows significantly improving and simplifying the analysis and supervision of dependability. One of the advantages of the developed method is that in situations when there is still not enough statistical information, expert judgement is the source of input data for dependability model setting, while subsequently operational data is used. Thus, a system's dependability model is maintained up to date throughout its life cycle stages.

The existing methods of dependability analysis are classified and examined. The authors acknowledge the problem of insufficiency of information for classical com-

puting, disregard of such factors as the effect of deviations of the operating mode or external effects, irregularity of the failure rate, non-linear nature of the effect of external factors on the dependability. The paper examines the way the external factors affect the dependability and the degree to which such factors are taken into consideration in the existing methods. The problem of dependability analysis is formulated. The qualitative, technical and organizational (design and software) requirements for dependability in the technical specifications for each stage of elements and SS development, shall be observed and confirmed at the respective stage of activities. The confirmation does not require a statistical experiment, which is their major advantage. The design rules for dependability currently under development in a number of branches of the aerospace industry, i.e. a system of quantitative and qualitative requirements and rules to be observed during the development of SC, significantly contribute to the reduction of costs of experimental research of SC and, in general, creation of highly dependable products at the stages of design and engineering development. Although it should be noted that the proposed method of estimation is examined only for the case of space technology products as part of SS, and it may be the starting point for the development of specific methods of evaluation of the economic efficiency of lifetime extension of specific types of space technology.

References

[1] Gnedenko B.V., BeliaevYu.K., Soloviev A.D. Matematicheskie metody v teorii nadezhnosti [Mathematical methods in the dependability theory]. Moscow: Nauka; 1965 [in Russian].

[2] Sidniaev N.I. Teoria planirovania eksperimenta i analiz statisticheskikh dannykh: uchebnoe posobie [Experimental design theory and statistical data analysis: study guide]. Moscow: IzdatelstvoYurayt; 2011 [in Russian].

[3] Morozov D.V., Chermoshentsev S.F. Method of improving the functional dependability of the control systems of an unmanned aerial vehicle in flight in case of failure in the onboard test instrumentation. Dependability 2019;1:….. DOI: 10.21683/1729-2646-2019-19-1…

[4] Sidniaev N.I., Sadykhov G.S., Savchenko V.P. Modeli i metody otsenki ostatochnogo resursa izdeliy radioelektroniki [Models and methods of estimation of the residual operating life of electronics]. Moscow: Bauman MSTU Publishing; 2015 [in Russain].

[5] Morris S.F. Use and application of MIL-HDBK-217. Solid Slate Technology 1990;33(6):65-69.

[6] Sidniaev N.I. Matematicheskoe modelirovanie otsenki nadezhnosti obiektov slozhnykh tekhnicheskikh sistem [Mathematic simulation of dependability estimation of complex technical systems]. Problemy mashinostroenia i nadezhnosti mashin 2003;4:24-31 [in Russian].

[7] Brennom, T.R. Should US MIL-HDBK-217 be 8888. IEEE Trans. Reliab. 1988;37(5):474-475.

[8] Sidniaev N.I. Obzor i issledovanie fiziki otkazov dlia otsenki pokazateley nadezhnosti radioelektronnykh priborov sovremennykh RLS [Overview and research of physics of failure for the estimation of the dependability indicators of today's radar electronics]. Physical Bases of Instrumentation 2017;2(23):4-52 [in Russian].

[9] Barlow R., Proschan F. Mathematical theory of reliability. Moscow: Sovetskoye radio; 1969.

[10] RD 50-690-89. Metodicheskie ukazania. Nadezhnost v tekhnike. Metody otsenki pokazateley nadezhnosti po eksperimentalnym dannym [Guidelines. Dependability of technology. Methods of estimation of dependability indicators based on experimental data]. Moscow: State committee of the USSR for products quality management and standards; 1990 [in Russian].

[11] Sidniaev N.I., Makridenko L.A., GechaV.Ya., Onufriev V.N. Faktory kosmicheskoy pogody, vliaiushchie na bortovye elementy nizkoorbitalnykh kosmicheskikh apparatov [Factors of space weather affecting the airborne devices of low-orbiting spacecraft]. In: Electromechanical matters. VNIIEM studies. Proceedings of the Fourth International Science and Technology Conference Topical Issues of the Design of Space-Based Earth Remote Sensing Systems. Moscow: VNIIEM Corporation; 2016. p. 90-100 [in Russian].

[12] PokhabovYu.P. What should mean dependability calculation of unique highly vital systems with regards to single-use mechanisms of spacecraft. Dependability 2018;18(4):28-35.

[13] Antonov S.G., Klimov S.M. Method for risk evaluation of functional instability of hardware and software systems under external information technology interference. Dependability 2017;17(1):32-39.

[14] Sidniaev N.I., GechaV.Ya., Barbul R.N. O sovremennykh podkhodakh razvitia teorii effektivnosti kosmicheskikh sistem [On the modern approaches of the space systems efficiency theory]. In: Sistemy upravlenia polnym zhiznennym tsiklom vysokotekhnologichnoy produktsii v mashinostroenii: novye istochniki rosta: Vserossiyskaia nauchno-prakticheskaia konferentsiia [Proceedings of the All-Russian Science and Practice Conference Complete Lifecycle Management Systems of High-Technology Engineering Products]. Moscow: Bauman MSTU Publishing; 2018. p. 69-75.

[15] Klimov S.M., Polikarpov S.V., Fedchenko A.V. Method of increasing fault tolerance of satellite communication networks under information technology interference. Dependability 2017;17(3):32-40.

[16] KolobovA.Yu., Dikoun E.V. Interval estimation of reliability of one-off spacecraft. Dependability 2017;17(4):23-26.

About the authors

Vladimir Ya. Gecha, Doctor of Engineering, Professor, Deputy Director General, A.G. IosifianResearch and Production Corporation Space Monitoring, Information, Control

and Electromechanical Systems, Russian Federation, Moscow, e-mail: vniiem@orc.ru, vniiem@vniiem.ru

Ruslan N. Barbul, Senior Researcher, Deputy Director General for Quality and Dependability, A.G. IosifianResearch and Production Corporation Space Monitoring, Information, Control and Electromechanical Systems, Russian Federation, Moscow, e-mail: vniiem@orc.ru, vniiem@vniiem.ru

Nikolay I. Sidniaev, Doctor of Engineering, Professor, Head of Department, Bauman Moscow State Technical University, Russian Federation, Moscow, e-mail: Sidn_ni@mail.ru

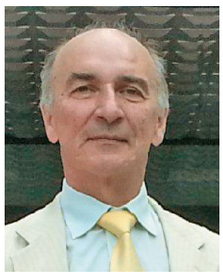
Yulia I. Butenko, Candidate of Engineering, Associate Professor, Bauman Moscow State Technical University, Russian Federation, Moscow, e-mail: iuliiabutenko2015@yandex.ru

Received on: 17.12.2018

Original article
Dependability, vol. 19 no.2, 2019 DOI: 10.21683/1729-2646-2019-19-2-9-17

Study of the beta-factor model application for common cause failure modeling

Alexander V. Antonov, *JSC RASU, Russian Federation, Moscow*
Valery A. Chepurko, *JSC RASU, Russian Federation, Moscow*
Alexey N. Cherniaev, *JSC RASU, Russian Federation, Moscow*



Alexander V. Antonov

Valery A. Chepurko

Alexey N. Cherniaev

Abstract. **Aim.** *Common cause failures (CCFs) are dependent failures of groups of certain elements that occur simultaneously or within a short period of time (i.e. almost simultaneously) due to a single common cause (e.g. a sudden change of climatic operating conditions, flooding of premises, etc.). A dependent failure is a multiple failure of several elements of a system, whose probability cannot be expressed as a simple product of the probabilities of unconditional failures of individual elements. CCA probabilities calculation uses a number of common models, i.e. the Greek letter model, alpha, beta factor and their variants. The beta-factor model is the most simple in terms of simulation of dependent failures and further dependability calculations. Other models, when used in simulation, involve combinatorial enumeration of dependent events in a group of n events that becomes labour-intensive if the number n is high. For the selected structure diagrams of dependability, the paper analyzes the calculation method of system failure probability with CCF taken into account for the beta-factor model. The* **Aim** *of the paper is to thoroughly analyze the beta-factor method for three structure diagrams of dependability, research the effects of the model parameters on the final result, find the limitations of beta-factor model applicability.* **Methods.** *The calculations were performed using numerical methods of solution of equations, analytical methods of function studies.* **Conclusions.** *The paper features an in-depth study of the method of undependability calculation for three structure diagrams that accounts for CCF and uses the beta-factor model. In the first example, for the selected structure diagram out of n parallel elements with identical dependability, it is analytically shown that accounting for CCF does not necessarily cause increased undependability. In the second example of primary junction of n elements with identical dependability, it is shown that accounting for CCF subject to parameter values causes both increased and decreased undependability. A number of beta factor model parameter values was identified that cause unacceptable values of system failure probability. These sets of values correspond to relatively high model parameter values and are hardly practically attainable as part of engineering of real systems with highly dependable components. In the third example, the conventional bridge diagram with two groups of CCFs is considered. The complex ambivalent effect of beta factor model parameters on the probability of failure is shown. As in the second example, limitations of the applicability of the beta-factor model are identified.*

Keywords: *common cause failure, total cause failure, independent failures, dependent failures, antithetic events, beta factor, undependability function.*

For citation: *Antonov AV, Chepurko VA, Cherniaev AN. Research of the beta-factor model of accounting for common cause failures. Dependability 2019;2: 9-17. DOI: 10.21683/1729-2646-2019-19-2-9-17*

Introduction

Today's dependability analysis of complex systems often includes taking into consideration possible common cause failures (CCFs). CCF is a failure of two or more structures, systems or components due to a single specific event or single specific cause [1]. A simultaneous failure of two or more structures, systems or components is caused by certain shortcomings associated with the design or manufacture, errors of operation or maintenance that manifest themselves as the result of natural effects, operational processes in a nuclear powerplant, human actions or internal events within the control and supervision system [2]. As an example, we can mention the blocking of a number of safety systems as the result of a wrong decision taken by the personnel of the Chernobyl NPP. The existing CCF classification includes failures caused by internal or external effects, failures caused by personnel's errors, general failures due to commonality of design or operating conditions.

There is a number of probabilistic methods of accounting for CCF, i.e. the alpha-factor model, Greek letter model, beta-factor model, etc. The beta-factor model is one of the simplest ones. It considers either single independent failures of a group's elements that have a common cause (CCF groups), of simultaneous failure of all elements of a CCF group. The other models consider the possible failure of random subgroups of a CCF group. In this case, depending on the specific model, in a certain manner, the vector is found of the parameters corresponding with the probability of CCF of a group of the specified size. As the beta-factor model involves the CCF of the whole group, it contains the single parameter β.

The aim of this paper is to investigate how accounting for CCF using the beta-factor model affects the probability of failure of various structure diagrams. Aside from finding the dependence between the probability of system failure and the model parameter β, in each case the probabilities of failure are analyzed to determine the possible limitations of the model.

CCF in parallel structures

Let us analyze the dependability of the parallel (backup) structure in terms of dependability subject to CCF. Let the system consist of n parallel equally dependable elements with the probability of failure q each. Obviously, not accounting for CCF, the system's probability of failure will be equal to q^n.

Let us assume that all n element can fail due to one common cause. In this case the following events will be possible: i_j, independent failure of the j-th element, C, dependent CCF of all elements.

According to the assumptions of the beta-factor model, a failure of any element of the group may occur due to an independent or common cause identical for all the elements, i.e. events i_j and C will be antithetic. The probabilities of such events will be proportional to q, i.e. the probability of total cause failure of an element.

$$P(C)=\beta q,\ P(i_j)=(1-\beta)q,\ j=1,\ldots n. \qquad (1)$$

Non-negative proportionality factor β depends on many factors, such as system structure, redundancy method, operating conditions, etc. Normally, this coefficient is quite low and technical systems contain highly dependable elements, i.e. the probability of failure q is also low. In this context, the use of the beta-factor model normally yields paradoxical or even impossible results. In case of relatively high values of β and q it is quite possible to attain them.

The logic function of operability subject to CCF will be as follows:

$$Y_s=\overline{(i_1\wedge i_2\wedge\ldots\wedge i_n)\vee C},$$

the probability of failure $Q(Y_s)$ will be defined by the formula:

$$Q(Y_s)=1-P(Y_s)=$$
$$=P(i_1\wedge i_2\wedge\ldots\wedge i_n)+P(C)=((1-\beta)q)^n+\beta q. \qquad (2)$$

Let us examine (2) in order to identify possible problems with the calculations.

Whereas $0\le(1-\beta)q\le 1$, then $((1-\beta)q)^n\le(1-\beta)q$. Therefore, the probability of failure (2) will not exceed one. I.e. the normalization requirement for the parallel structure will be fulfilled.

Let us verify the commonly held opinion that accounting for CCF in redundant structures causes increasing probability of failure of the system. For that purpose, let is identify the parameter values of the CCF model that enable a relative growth of dependability of a parallel structure system when accounting for CCF. Obviously, the following condition is to be fulfilled in order to enable a growth of dependability:

$$Q(Y_s)=((1-\beta)q)^n+\beta q<q^n.$$

After a simplification we obtain the following condition:

$$\left(\frac{\beta}{1-(1-\beta)^n}\right)^{\frac{1}{n-1}}=q_{\beta,n}<q. \qquad (3)$$

If (3) is fulfilled, the dependability of a parallel structure calculated subject to CCF will be higher than the dependability calculated otherwise. Figure 1 shows the dependence graphs of function $q_{\beta,n}$ of parameter β under various n.

Let us assume that parameter β>0. Then, if the total cause probability q is lower than boundary $q_{\beta,n}$, accounting for CCF will cause decreased dependability of a redundant system. This effect is what is normally expected as the natural reaction of the beta-factor model to accounting for CCF. If $q=q_{\beta,n}$, accounting for CCF will not affect the dependability of the

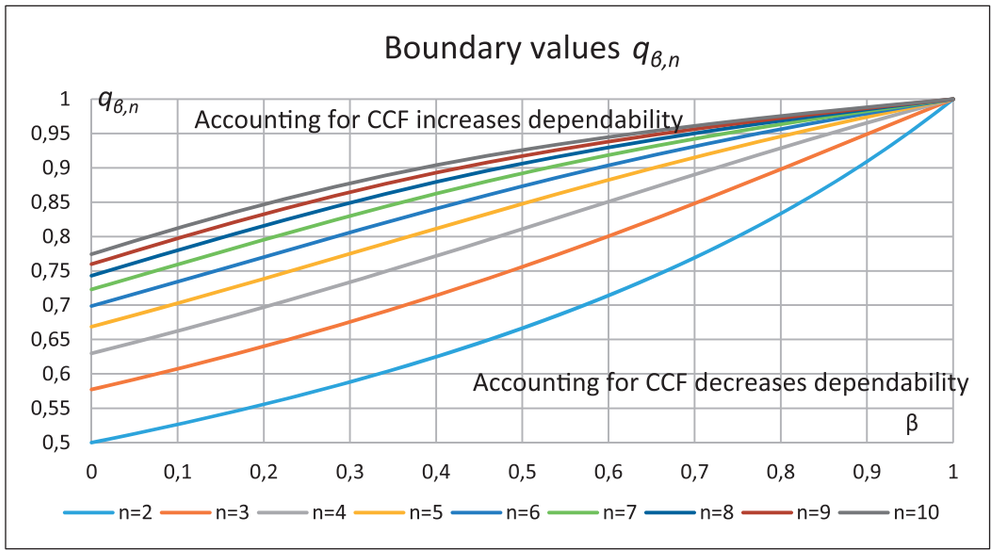


Figure 1. Boundary values of $q_{\beta,n}$

system. And finally, if $q>q_{\beta,n}$, accounting for CCF will, surprisingly, cause increased dependability of the system. Let us take, for example, β=1/4, q=3/4, n=2. The probabilities of failure accounting and not accounting for CCF will be equal to $\left((1-\beta)q\right)^n+\beta q=\frac{129}{256}$ and $q^n=\frac{9}{16}=\frac{144}{256}$ respectively.

In order to get this effect clarified, let us examine an extreme situation. Let us assume that q=1, i.e. the probability of total cause failure of one element equals 1. In this case the probability of failure not accounting for CCF will be equal to 1 as well. If $n\geq 2$ and $\beta\in(0,1)$, accounting for CCF will have the following result

$$(1-\beta)^n+\beta<1.$$

The probabilities of one independent failure and CCF of any element will be respectively equal to $(1–\beta)u\beta$. It turns out that the unitary probability of failure was decomposed by the beta-factor model into two components conditioned by the cause of failure. If the system consisted of one element, the probability would not decrease: $(1–\beta)+\beta=1$. In case of the redundant structure the probability of failure decreased due to the "rigidity" of the assumptions of the beta-factor model. The failure of j-th element is a disjunction of antithetic events $i_j\vee C$. System failure is a conjunction of $\Lambda_{j=1}^{n}\left(i_j\vee C\right)$. If an event of type $i_1\wedge i_2\wedge i_n\wedge C_{3,4,\ldots,n-1}$ (1-st, 2-nd and n-th elements failed due to an independent cause, the others failed due to the common cause) and all possible combinatorial enumerations of such events that are present in other models of accounting for CCF (alpha-factor model, Greek letters model, etc.) were possible, the probability would probably be higher. However, in the beta-factor model such events are impossible as, for instance, event $C_{3,4,\ldots,n-1}$ is impossible.

On the other hand, the change of behaviour of the dependability (or undependability) function under various parameter values can be explained quite simply by conducting a qualitative analysis of the undependability function, analyzing, among other things, the derivatives of q and β.

The derivative of function $Q(Y_s)$ of q will be defined by the formula:

$$\frac{\partial Q(Y_s)}{\partial q}=nq^{n-1}(1-\beta)^n+\beta>0 \text{ if } \beta\in(0,1),$$

i.e. growing undependability of the element causes growing undependability of a parallel system as a whole.

Now, let us take a derivative of another parameter

$$\frac{\partial Q(Y_s)}{\partial \beta}=-nq^n(1-\beta)^{n-1}+q. \qquad (4)$$

Let us analyze (4). The derivative is equal to 0 in the critical point

$$\beta_{\text{crit.}}=1-\frac{1}{q}\left(\frac{1}{n}\right)^{\frac{1}{n-1}}=1-\frac{1}{q}\exp\left(-\frac{\ln n}{n-1}\right). \qquad (5)$$

The critical point is attainable if $\beta_{crit.}\in(0,1)$.. Condition $\beta_{crit.}<1$ is fulfilled, while $\beta_{crit.}>0$ occurs when and only when

$$q>\exp\left(-\frac{\ln n}{n-1}\right).$$

Let us note that

$$\lim_{\beta\to 0+}q_{\beta,n}=\lim_{\beta\to 0+}\left(\frac{\beta}{1-(1-\beta)^n}\right)^{\frac{1}{n-1}}=\exp\left(-\frac{\ln n}{n-1}\right).$$

Thus, if $q\in\left(0,exp\left(-\frac{\ln n}{n-1}\right)\right]$ derivative (4) for any values of β will be positive, since $\left.\frac{\partial Q(Y_s)}{\partial\beta}\right|_{\beta=1}=q>0$ and the critical point is outside the interval [0,1]. Therefore, increasing β will cause, as expected, increasing undependability.

If $q \in \left(exp\left(-\frac{\ln n}{n-1} \right), 1 \right]$, there will be a point of extremum (5), and, as derivative (4) is positive for β=1, the critical point will be the minimum point. Then, $\left.\frac{\partial Q(Y_s)}{\partial \beta}\right|_{\beta=0} < 0$ and the undependability function will paradoxically decrease with respect to parameter β. That is the complete proof of the behaviour of the undependability function.

CCF in serial structures

In this section, let us analyze the dependability of the serial (primary) structure in terms of dependability subject to CCF. Let the system consist of n serial equally dependable elements with the probability of failure q each. Not accounting for CCF, the system's PNF will be equal to $P(Y_s) = (1-q)^n$.

The logic function of operability subject to CCF will be as follows:

$$Y_s = \overline{i_1 \vee i_2 \vee \ldots \vee i_n \vee C}.$$

PNF subject to CCF is

$$P(Y_s) = P(\bar{i}_1 \wedge \bar{i}_2 \wedge \ldots \wedge \bar{i}_n) - P(C) = (1-(1-\beta)q)^n - \beta q. \quad (5)$$

Similarly to the parallel structure, accounting for CCF may either reduce or increase the dependability of the primary junction. In order to identify the boundary values of $q_{\beta,n}$ it is obviously required to solve the following algebraic equation:

$$(1-(1-\beta)q)^n - \beta q = (1-q)^n. \quad (6)$$

Figure 2 shows dependence graphs of function $q_{\beta,n}$ of parameter β under various n. The solution of equation (6) was obtained by means of the numerical method of segment bisection.

If the probability for any reason q is lower than boundary $q_{\beta,n}$, accounting for CCF will cause increased dependability of a serial system. If $q=q_{\beta,n}$, accounting for CCF will not affect the dependability of the system. And finally, if $q>q_{\beta,n}$, accounting for CCF will cause decreased dependability of the system. Let us, as previously, take, for example, $\beta = \frac{1}{4}$, $q = \frac{3}{4}$, n = 2. The probabilities of failure accounting and not accounting for CCF will be equal to $1-(1-(1-\beta)q)^n + \beta q = \frac{255}{256}$ and $1-(1-q)^n = \frac{15}{16} = \frac{240}{256}$ respectively.

As above, let us try to explain the change of the behaviour of the dependability (or undependability) function under various parameter values by conducting a qualitative analysis addressing, among other things, the derivatives of q and β.

The derivative of function $Q(Y_s)$ of q will be defined by the formula:

$$\frac{\partial Q(Y_s)}{\partial q} = n(1-\beta)(1-(1-\beta)q)^{n-1} + \beta > 0 \text{ if } \beta \in (0,1).$$

Growing undependability of the element causes growing undependability of a parallel system as a whole.

Derivative per another parameter

$$\frac{\partial Q(Y_s)}{\partial \beta} = -nq(1-(1-\beta)q)^{n-1} + q. \quad (7)$$

Let us analyze (7). The derivative is equal to 0 in the critical point

$$\beta_{crit.} = 1 - \frac{1}{q}\left(1 - \left(\frac{1}{n}\right)^{\frac{1}{n-1}}\right) = 1 - \frac{1}{q}\left(1 - \exp\left(-\frac{\ln n}{n-1}\right)\right). \quad (8)$$

The critical point is attainable if $\beta_{crit.} \in (0,1)$. Condition $\beta_{crit.} < 1$ is obviously fulfilled, while $\beta_{crit.} > 0$ occurs when and only when

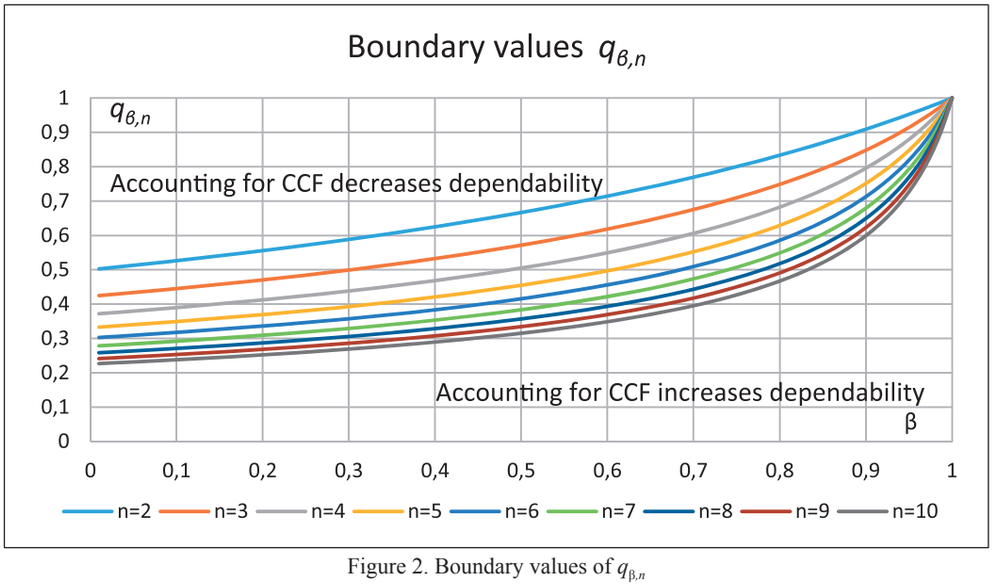


Figure 2. Boundary values of $q_{\beta,n}$

$$q > 1 - \exp\left(-\frac{\ln n}{n-1}\right).$$

Thus, if $q \in \left[0,1-\exp\left(-\frac{\ln n}{n-1}\right)\right]$, derivative (7) for any values of β will be negative, as $\left.\frac{\partial Q(Y_s)}{\partial \beta}\right|_{\beta=1} = q - nq < 0$ if $n \geq 2$ and the critical point is outside the interval [0,1]. Therefore, increasing β will cause, as expected, decreasing undependability.

If $q > \exp\left(-\frac{\ln n}{n-1}\right)$, there will be a point of extremum (8), and, as derivative (7) is negative for β=1, the critical point will be the maximum point. Then, $\left.\frac{\partial Q(Y_s)}{\partial \beta}\right|_{\beta=0} > 0$ and the undependability function will increase with respect to parameter β.

Unlike in the parallel structure, in the serial structure for each β there are limit values of the probability of failure due to any cause for each element, exceeding which may bring about unacceptable values of probability of system failure. In order to identify such values, the following equation must be solved:

$$\left(1-(1-\beta)q\right)^n - \beta q = 0. \quad (9)$$

An unacceptably high value of probability of failure is directly associated with the assumptions of the beta-factor model. In terms of logic algebra, out of the occurrence of event C follows that no independent cause failures took place, i.e. $C \Rightarrow \bar{i}_1 \vee \bar{i}_2 \vee \ldots \vee \bar{i}_n$. In this case

$$P\left(\bar{i}_1 \wedge \bar{i}_2 \wedge \ldots \wedge \bar{i}_n\right) \geq P(C), \text{ i.e.}$$

$$\left(1-(1-\beta)q\right)^n \geq \beta q.$$

Thus, for instance, if $n = 2,3,4,5,10,50,100$ the range of acceptable values of probability q will be the area beneath the curve in figure 3.

Let us, as previously, take, for example, β=0,1, q=0,9, n=2. The probabilities of failure accounting and not accounting for CCF will be equal to $1-\left(1-(1-\beta)q\right)^n + \beta q = 1,0539$ and $1-(1-q)^n$=0,99 respectively.

CCF in bridge diagram

Let us research the effect of beta factor model parameters in a bridge diagram. The structure of a bridge diagram is shown in figure 4. Let us assume that there are two different common causes of failure of several bridge elements at once:

– common cause *a* that may cause simultaneous failure of elements 1 and 2,

– common cause *b* that causes simultaneous failure of elements 3 and 4.

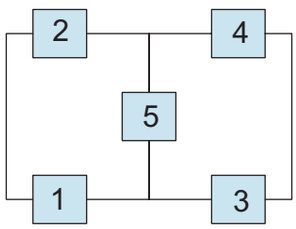


Figure 4. Bridge diagram

Thus, elements 1 and 2 form the first CCF group, while elements 3 and 4 form the second one. Evidently, those two groups do not contain identical elements, although, in general, one element can simultaneously be part of several CCF groups. Such situation is to be considered in the next paper.

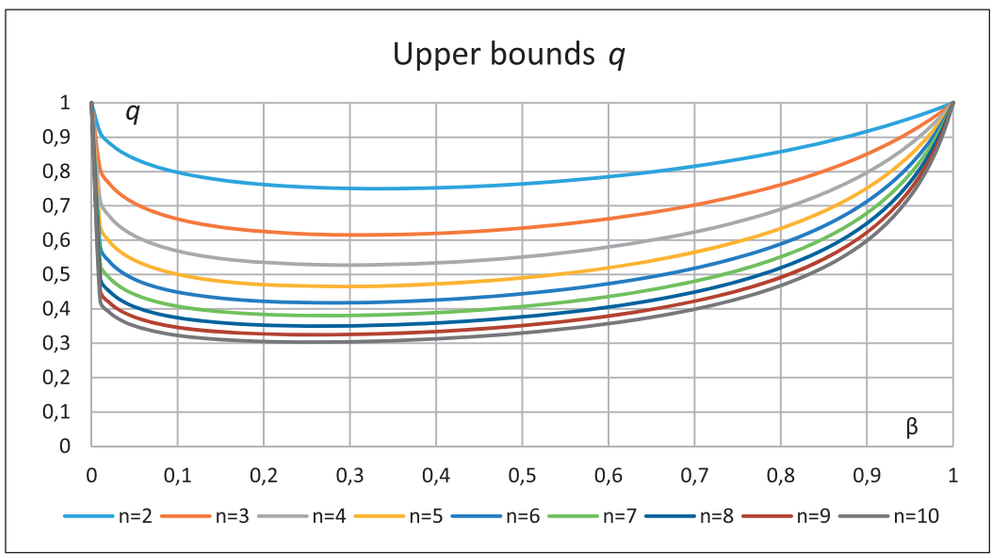


Figure 3. Acceptable values of q

Let β_a and β_b be parameters of the beta-factor model in the respective groups. In this case the following events are possible: i_1 is independent failure of the 1-st element, i_2 is independent failure of the 2-nd element, C_a is dependent CCF of the 1-st element and 2-nd element (group *a*), figure 5. Similarly, the events from the second CCF group can be shown in this same sample space: i_3 is independent failure of the 3-rd element, i_4 is independent failure of the 4-th element, C_b is dependent CCF of the 3-rd element and 4-th element (group *b*).

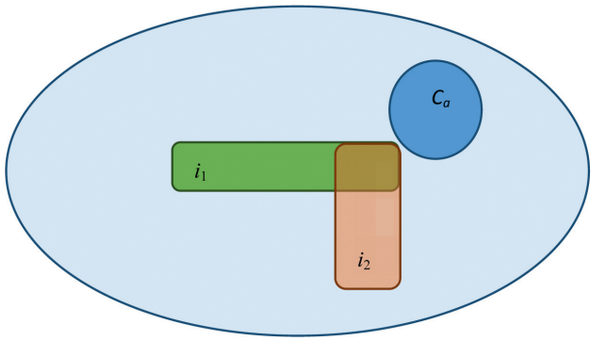


Figure 5. Events in case of CCF

Figure 5 shows possible mutual location of the events in a group. Importantly, antithetic (mutually exclusive) pairs of events will be the following: i_1 and C_a, i_2 and C_a, i_3 and C_b, i_4 and C_b. Let us indicate the event x_k, the *k*-th element is operable, $k = 1, \ldots, 5$. Then,

$$\overline{x_1} = i_1 \vee C_a, \overline{x_2} = i_2 \vee C_a, \overline{x_3} = i_3 \vee C_b, \overline{x_4} = i_4 \vee C_b.$$

The logic function of inoperability will be as follows

$$\overline{Y_s} = \left[x_5 A\right] \vee \left[\overline{x}_{5\,51} B\right], \tag{10}$$

where $A = (\overline{x}_1 \overline{x}_2) \vee (\overline{x}_3 \overline{x}_4)$ and $B = (\overline{x}_2 \vee \overline{x}_4)(\overline{x}_1 \vee \overline{x}_3)$.

Let all the elements be equally dependable and the probabilities of their total cause failures be equal to q. In this case the undependability of the bridge regardless of CCF will be equal to:

$$Q(Y_s) = q^3(2-q)^2 + q^2(1-q)(2-q^2) = \\ = 2q^5 - 5q^4 + 2q^3 + 2q^2. \tag{11}$$

Let us substitute the events A and B involved in (1) and containing $\overline{x}_1, \overline{x}_2, \overline{x}_3$ and $\overline{x}_4$ with independent and CCF events:

$$A = (\overline{x}_1 \overline{x}_2) \vee (\overline{x}_3 \overline{x}_4) = (i_1 i_2 \vee C_a) \vee (i_3 i_4 \vee C_b).$$

$$B = (\overline{x}_2 \vee \overline{x}_4)(\overline{x}_1 \vee \overline{x}_3) = (i_1 \vee i_3)(i_2 \vee i_4) \vee C_a \vee C_b.$$

Let us identify the probabilities of such events:

$$P(A) = f(\beta_a, q) + f(\beta_b, q) - f(\beta_a, q) f(\beta_b, q), \tag{12}$$

where $f(\beta, q) = (1-\beta)^2 q^2 + \beta q$.

In order to calculate the probability of event *B*, let us use the addition theorem that, in the case of antithetic events of a CCF group will result in the following:

$$P(B) = P\left((i_1 \vee i_3)(i_2 \vee i_4)\right) + P(C_a) + P(C_b) - \\ - P(i_1 i_2 C_b) - P(i_3 i_4 C_a) - P(C_a C_b) = g^2(\beta_a, \beta_b, q) + \\ + \beta_a q + \beta_b q - (1-\beta_a)^2 \beta_b q^3 - (1-\beta_b)^2 \beta_a q^3 - \beta_a \beta_b q^2,$$

where $g(\beta_a, \beta_b, q) = (1-\beta_a)q + (1-\beta_b)q - (1-\beta_a)(1-\beta_b)q^2$.

Upon the substitution of the obtained results and simplification, we will obtain the bridge's undependability subject to CCF:

$$Q(Y_s) = c_5 q^5 + c_4 q^4 + c_3 q^3 + c_2 q^2 + c_1 q, \tag{13}$$

where the polynomial coefficients are defined by the following formulas:

$$c_5 = 2(1-\beta_a)^2 (1-\beta_b)^2,$$

$$c_4 = (1-\beta_a)(1-\beta_b)(-5 + 3\beta_a + 3\beta_b - \beta_a \beta_b),$$

$$c_3 = 2 - 3\beta_a - 3\beta_b + \beta_a \beta_b (6 - \beta_a - \beta_b),$$

$$c_2 = (1-\beta_a)^2 + (1-\beta_b)^2 - \beta_a \beta_b,$$

$$c_1 = \beta_a + \beta_b.$$

As the result of the conducted research of function (13) the following dependences were identified.

If $q \leq 0{,}5$ undependability $Q(Y_s)$ classically monotonically increases per each parameter β_a, β_b (figure 6). I.e. when calculating a bridge with highly dependable elements no unexpected effects were identified.

If $q \in (0{,}5, \approx 0{,}85)$ the undependability function has a global minimum. In the vicinity of point (0,0) the undependability decreases if each parameter increases (figure 7). When the minimum point has been reached, further increase of CCF parameters causes growing undependability. If $\beta_a = \beta_b = 1$ maximum undependability is reached. Thus, in case of average undependability of the bridge's component elements accounting for CCF may cause a reduction of undependability of the system as a whole. The value 0.85 was obtained visually, accurate estimation requires an analytical study of (13).

If $q \in (\approx 0{,}85, \approx 0{,}91)$ the undependability function has a complex dependence: four local boundary minimums and one maximum (figure 8). In the vicinity of point (0,0) the undependability decreases if each parameter increases. When the minimum point has been reached, further increase of CCF parameters causes growing undependability. Further behaviour depends on the specific parameter values. If $\beta_a = \beta_b = 1$ maximum undependability is reached. In case of high undependability of the bridge's component elements accounting for CCF may cause a reduction (in

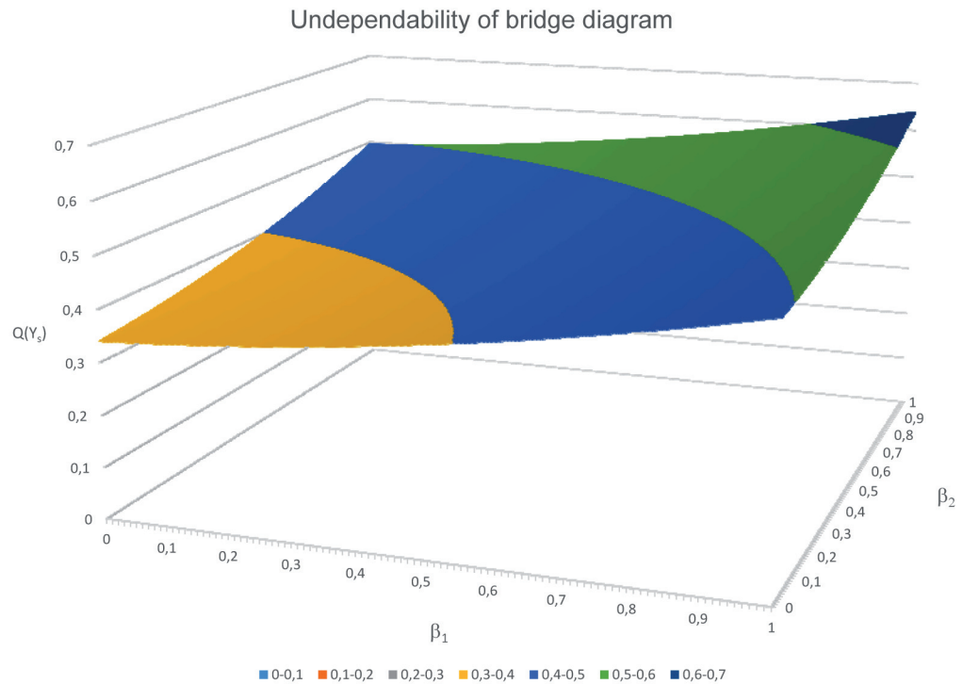


Figure 6. Bridge undependability function (q=0,3)

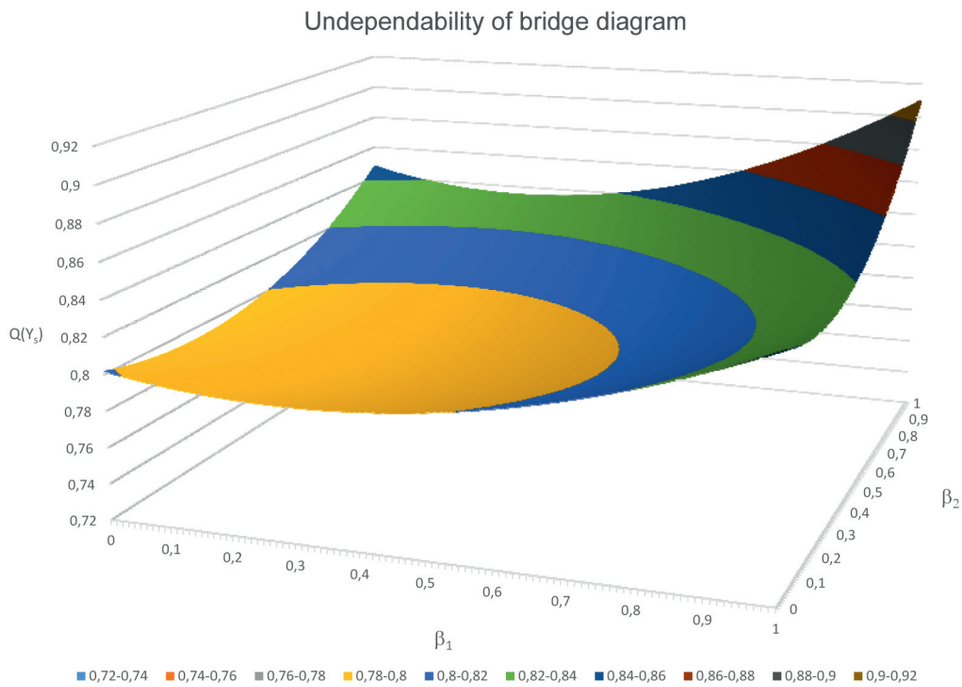


Figure 7. Bridge undependability function (q=0,7)

case of low β_a, β_b) or an increase of undependability of the system as a whole.

If $q \in (\approx 0{,}91{,}1)$ the undependability function has, as previously, a complex dependence: four local boundary minimums and one maximum (figure 9). In the vicinity of point (0,0) the undependability decreases if each parameter increases. When the minimum point has been reached, further increase of CCF parameters causes growing undependability. Further behaviour depends on the specific parameter values. If $\beta_a=\beta_b=1$, maximum undependability is reached. It must be noted that there is a range of unacceptable values of parameters β_a, β_b, under which the systems' undependability assumes a value higher than one. Thus, a serial structure does not necessarily have unacceptable beta-factor model parameter values.

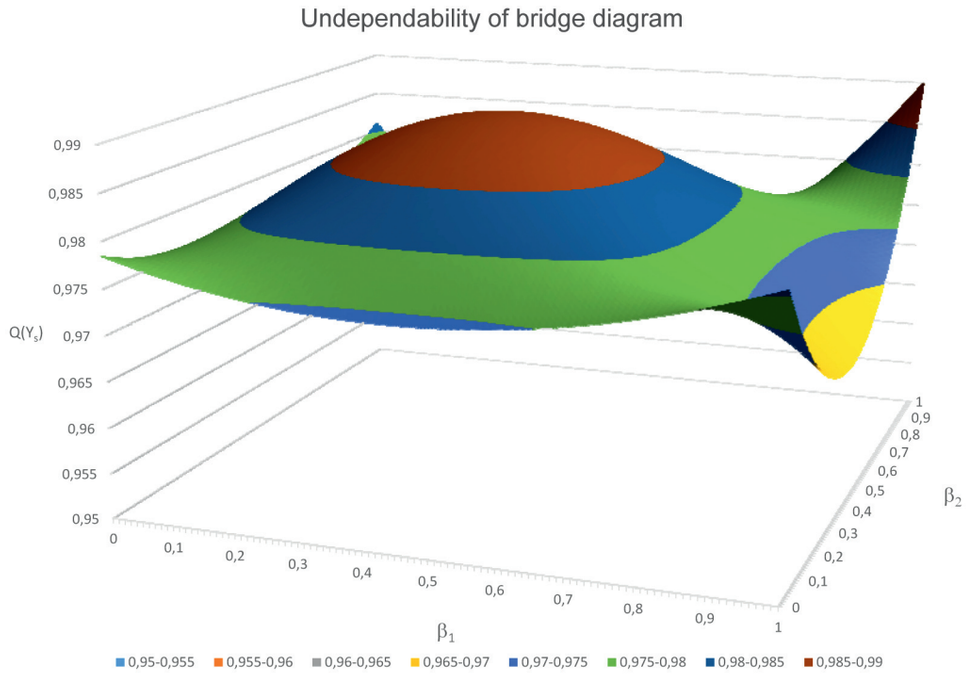


Figure 8. Bridge undependability function (q=0,9)

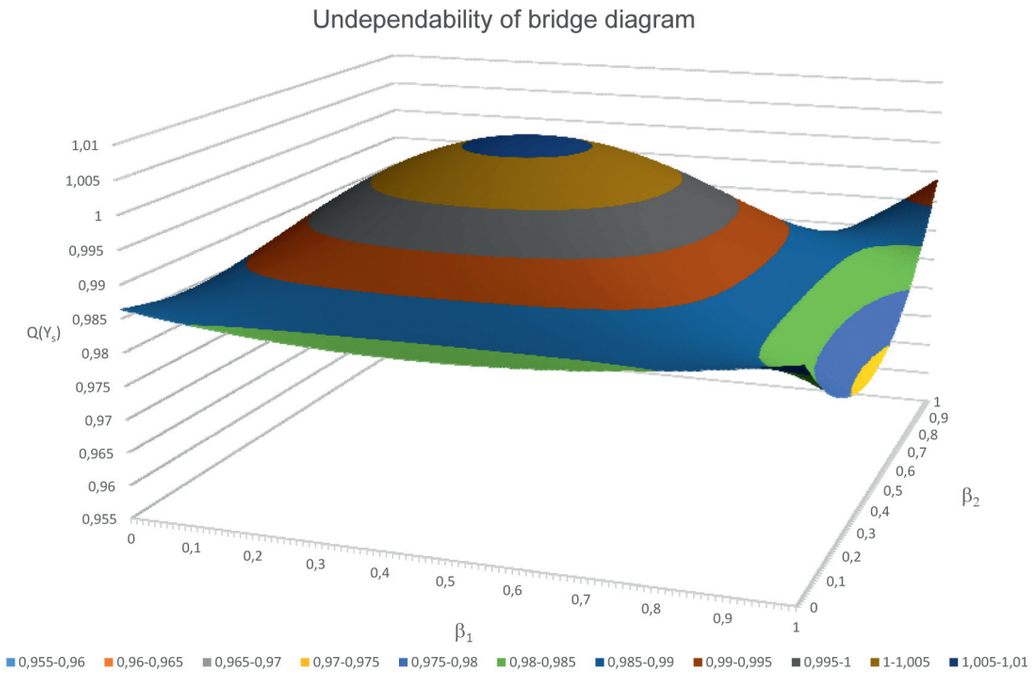


Figure 9. Bridge undependability function (q=0,92)

Conclusion

The paper conducts a mathematical research of the beta-factor model of accounting for CCF. The research covered three dependability diagrams: parallel, serial and bridge. The two latter diagrams reveal the problem of unacceptable beta factor model parameter values in case of high undependability of component elements. For all three dependability diagrams it is shown that increasing beta factor model parameters do not necessarily cause the growth of undependability.

References

[1] GOST R IEC 61226-2011. Nuclear power plants. Instrumentation and control systems important for safety. Classification of instrumentation and control functions. Moscow: Standartinform; 2011 [in Russian].

[2] GOST R IEC 62340-2011. Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure. Moscow: Standartinform; 2012 [in Russian].

[3] Antonov A.V., Galivets E.Yu., Chepurko V.A., Cherniaev A.N. Fault tree analysis in the R programming environment. Dependability 2018;18(1):4-13. DOI: 10.21683/1729-2646-2018-18-1-4-13.

[4] Antonov A.V., Galivets E.Yu., Chepurko V.A., Cherniaev A.N. Fault tree analysis in the R programming environment. Accounting for common cause failures. Dependability 2018; 18(3):3-9. DOI: 10.21683/1729-2646-2018-18-3-3-9.

[5] Pereguda A.I., Pereguda A.A., Timashev D.A. The mathematical model of computer networks' reliability. Dependability 2013;(4):31-43. DOI: 10.21683/1729-2646-2013-0-4-18-43.

[6] Alpeev A.S. Dependability of control systems software and safety of nuclear power plants. Dependability 2015;(4):78-80. DOI: 10.21683/1729-2646-2015-0-4-75-80.

[7] Mosleh A., Rasmuson D.M., Marshall F.M. Procedures Guidelines in Modeling Common Cause Failures in Probabilistic Risk Assessment. NUREG/CR-5485. University of Maryland; 1998.

[8] O'Connor A.N. A General Cause Based Methodology for Analysis of Dependent Failures in System Risk and Reliability Assessments. University of Maryland; 2013, <http://hdl.handle.net/1903/14285> [accessed 09.04.2019].

[9] Smith C.L., Wood S.T., Galyean W.J., Schroeder J.A., Sattison M.B. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8: Technical Reference. NUREG/CR-7039 INL/EXT-09-17009; Vol. 2. Washington, D.C.: U.S. Nuclear Regulatory Commission; 2011.

[10] O'Connor A.N. A general cause based methodology for analysis of dependent failures in system risk and reliability assessments; 2013.

[11] O'Connor A.N. A general cause based methodology for analysis of dependent failures in system risk and reliability assessments; 2013.

About the authors

Alexander V. Antonov, Doctor of Engineering, Professor, Chief Expert of the International Training Center, Rosatom Technical Academy, Russian Federation, Moscow, e-mail: AVAntonov@rosatomtech.ru

Valery A. Chepurko, Candidate of Physics and Mathematics, Associate Professor, Chief Specialist of Division for Justifying Calculations of Design Solutions, JSC RASU, Russian Federation, Moscow, e-mail: VAChepurko@rasu.ru

Alexey N. Cherniaev, Candidate of Engineering, Deputy Technical Director, Director of Design Department, JSC RASU, Russian Federation, Moscow, e-mail: AlNCherny-aev@rasu.ru

Received on: 06.02.2019

Original article
Dependability, vol. 19 no.2, 2019 *DOI: 10.21683/1729-2646-2019-19-2-18-21*

Estimation of the gamma-percentile life for the binomial test plan

Viktor S. Mikhailov, *D.I. Mendeleev Central Research and Design Institute of Chemistry and Mechanics, Russian Federation, Moscow*

Viktor S. Mikhailov

Abstract. *In today's industry of highly dependable, unique, complex products, it is a commonplace situation when it is required to obtain an estimate of gamma-percentile storing life (GPSL) or gamma-percentile time to failure (GPTF) (hereinafter referred to as GPL, meaning GPSL or GPTF respectively) based on tests that did not produce any failures. Normally, a test plan is classified as binomial tests or tests with limited time and recovery. GPTF is understood as the operation time during which no failure occurs with the probability expressed as percentage. Similarly, GPSL is understood as the total schedule time of product storage during and after which the product is able to perform the required function with the probability expressed as percentage. The* **Aim** *of this paper is to find such estimate of GPL that would be simple and more efficient as compared to the conventional one and not significantly inferior to the efficient estimate, if such exists, in terms of proximity to the GPL estimate in case a binomial test plan is used.* **Methods of research.** *The research of efficient estimates is based on the integrative approach that uses the construction of the choice rule (criterion) of efficient estimate specified on the vertical sum of biases of estimates selected out of a certain set based on the function of the distribution law parameter.* **Conclusions.** *The obtained estimate of GPL is simple and more efficient as compared to the conventional one and not significantly inferior to the efficient estimate, if such exists, in terms of proximity to the GPL estimate in case a binomial test plan is used. The obtained estimate of GPL has significant advantages, i.e. the estimate is efficient within a sufficiently wide range of estimates, it allows obtaining a value based on the results of tests that did not produce any failures. The obtained estimate of GPL is recommended for failure-free tests conducted using a binomial plan.*

Keywords: *gamma-percentile storing life, gamma-percentile time to failure, exponential distribution, test plan, point estimation.*

For citation: *Mikhailov VS. Estimation of the gamma-percentile life for the binomial test plan. Dependability 2019; 2: 18-21. DOI: 10.21683/1729-2646-2019-19-2-18-21*

Introduction

In today's industry of highly dependable, unique, complex products, it is a commonplace situation when it is required to obtain an estimate of gamma-percentile storing life (GPSL) or gamma-percentile time to failure (GPTF) (hereinafter referred to as GPL, meaning GPSL or GPTF respectively) based on tests that did not produce any failures. Normally, a test plan is classified as type NNτ or NRτ, where N is the number same-type test objects; τ is the operation time (identical for each product); N (R) is the characteristic of the plan that indicates that the product's operability after each failure within the testing time is not recovered (recovered) [1]. GPTF is understood as the operation time during which no failure occurs with the probability γ expressed as percentage [2]. Similarly, GPSL is understood as the total schedule time of product storage during and after which the product is able to perform the required function with the probability γ expressed as percentage [2]. If the time to failure complies with the exponential distribution law with parameter T_0 (mean time to failure, hereinafter referred to as MTF), the expected values of GPL (hereinafter referred to as t_γ) is calculated according to formula:

$$t_\gamma = -T_0 \ln(\gamma). \quad (1)$$

Problem definition

Let us consider the case of tests according to a binomial plan.

For a binomial plan, a sufficient statistic is (r) of observed failures and total operation time $S(R,N,\tau,t_i)$ [1, 4, 5], $R = r$ is the random number of failures, t_i is the moments of failures, i=1,2,…,R, then for a binomial test plan the random value R (hereinafter referred to as r.v.) has a binomial distribution $p_N(k)$ [3, formula (1.4.55)] with parameters N and p, $0<p<1$, i.e. r.v. R equal to the number of successful tests in a series of N independent tests, takes on whole-number values 0, 1, 2, …, N with probabilities:

$$p_N(k) = C_N^k p^k (1-p)^{N-k}. \quad (2)$$

Distribution function $F_R(r,N,p)$ of binomial r.v. R will be written as

$$F_R(r,N,p) = \sum_{k=0}^{r} p_N(k). \quad (3)$$

In order to estimate the GPL ($\hat{t}_\gamma$) it would be quite natural to use the conventional mean time to failure estimate constructed for an exponential distribution as the estimate of parameter T_0 [1, 5]:

$$T_{02} = \frac{S(R,N,\tau,t_i)}{r}, \text{ if } r > 0.$$

However, thus obtained estimate $\hat{t}_{\gamma 2} = -T_{02}\ln(\gamma)$ has significant disadvantages, i.e.:

- the estimate is biased [1],
- the estimate is not efficient [1],
- the estimate does not allow obtaining value t_γ based on the results of tests that did not produce any failures.

In order to solve the above problem, it suffices to find an unbiased efficient estimate ($\hat{t}_{\gamma ef}$), if such exists in the class of consistent biased estimates. (The class of consistent estimates that includes all estimates generated by the method of substitution, inclusive of the maximum likelihood method, contains estimates with any bias, including those with a fixed one, in the form of function of parameter or constant [3]). In some cases, the generated unbiased efficient estimates are quite lengthy and have a complex calculation algorithm [4]. They are also not always sufficiently efficient in the class of all biased estimates and not always have a considerable advantage over simple yet biased estimates in terms of proximity to the estimated value [6].

The Aim of the paper

The aim of this paper is to find such estimate of GPL (hereinafter referred to as $\hat{t}_{\gamma 1}$) that would be simple and more efficient as compared to the conventional one and not significantly inferior to the efficient estimate $\hat{t}_{\gamma ef}$, if such exists, in terms of proximity to t_γ in case a binomial test plan is used.

Methods of research and results

Let us consider the class of estimates that can be presented as $\hat{t}_\gamma = -\hat{T}_0 \ln(\gamma)$, where $\hat{T}_0$ is the estimate of MTF for a binomial test plan.

In order to find the efficient estimate we will use integral characteristics [6]. Similarly to [6], let us construct a functional (hereinafter referred to as $A(\hat{t}_\gamma)$) based on the total squared deviation of the expected estimate $\hat{t}_\gamma$ from t_γ for all possible values t_i, T_0, γ, N and τ:

$$A\left(\hat{t}_\gamma(R,N,\tau,t_i)\right) = \\ = \frac{1}{3}\sum_{\tau_j=1E+3}^{\tau_j=1E+5}\frac{1}{10}\sum_{N=1}^{10}\int_0^\infty \left(\frac{1}{T_0}\right)^2 \left\{ \begin{matrix} E\hat{t}_\gamma(R,N,\tau_j,t_i) - \\ -(-T_0\ln(\gamma)) \end{matrix} \right\}^2 \partial T_0, \quad (4)$$

where $E\hat{t}_\gamma$ is the mathematical expectation of the estimate. According to (3), the mathematical expectation $E\hat{t}_\gamma(R,N,\tau,t_i)$ will be as follows:

$$E\hat{t}_\gamma(R,N,\tau,t_i) = \sum_{k=0}^{N} p_N(k)\hat{t}_\gamma(k,N,\tau,t_i) = \\ = \sum_{k=0}^{N} p_N(k) * (-\hat{T}_0\ln(\gamma)).$$

An efficient estimate of GPL t_γ must have the minimal value of functional of $A(\hat{t}_\gamma)$.

Let us take –ln(γ) outside the integral sign, then the formula will become as follows:

$$A(\hat{t}_\gamma) = \ln^2(\gamma) V(\hat{T}_0), \quad (5)$$

where

$$V\left(\hat{T}_0(R,N,\tau)\right)=$$
$$=\frac{1}{3}\sum_{\tau_j=1E+3}^{\tau_j=1E+5}\frac{1}{10}\sum_{N=1}^{10}\int_0^{\infty}\left(\frac{1}{T_0}\right)^2\{E\hat{T}_0(R,N,\tau_j)-T_0\}^2\partial T_0.$$

In accordance with [6] the functional $V(\hat{T}_0)$ (along with the functional $A(\hat{t}_\gamma)$) in formula (5) assumes the minimal value, if the estimate of parameter T_0 is substituted with its efficient estimate based on a sufficiently wide class of biased estimates. In this case, the implicit efficient estimate $\hat{T}_4$ from [6] should be used in the binomial test plan as the parameter of T_0 (MTF):

$$\hat{T}_4=\frac{\tau}{-\ln(1-\hat{p}(R,N))}, \quad (6)$$

where the probability of failure estimate $\hat{p}$ is obtained by solving the equation (see formula (3)):

$$F_R\left(r,N,\hat{p}\right)=\sum_{k=0}^{r}\mathrm{p}_N\left(k,\hat{p}\right)=0,5.$$

Then, the efficient estimate of GPL $\hat{t}_{\gamma 1}$ based on a sufficiently wide range of estimates [6] will be as follows (see formula (1)):

$$\hat{t}_{\gamma 1}=-\hat{T}_4\ln\left(\gamma\right) \quad (7)$$

For failure-free tests the estimate $\hat{t}_{\gamma 1}$ can be used for the NRT as well. Thus obtained estimate of GPL t_γ has significant advantages, i.e.:

- the estimate is efficient within a sufficiently wide range of estimates [6],
- the estimate allows obtaining value t_γ based on the results of tests that did not produce any failures and conducted using test plans of types NNT or NRT.

Examples

Example 1. As the dependability indicator of a product the gamma-percentile time to failure t_γ (γ=0,9) is used, that must not be lower than 1500 h. Based on the results of 10000-hour-long failure-free tests of one product it is required to estimate t_γ and verify the product's compliance with the dependability requirements.

Out of formulas (6) and (7) follows that the estimate of the GPTF value will be

$$\hat{t}_{\gamma 1}=-\hat{T}_4\ln\left(\gamma\right)=-\ln(0,9)*\frac{\tau}{-\ln\left(1-\hat{p}\left(R=0,N=1\right)\right)}=$$
$$=0,1053*\frac{10000}{-\ln(1-0,5)}=1519\text{ h}.$$

Based on the estimates of t_γ it can be concluded that the product complies with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 1519 h, which is in line with the product dependability requirements.

For comparison, let us mention the conventional solution of example 1.

Normally, for tests that did not produce any failures, parameter T_0 (instead of point estimation) is estimated per the lower confidence contour (hereinafter referred to as LCC) of MTF with the confidence probability of $\gamma = 0.9$. Then, in accordance with [5] the result will be:

$$T_{01н}=\frac{2t_\Sigma}{x^2(1-\propto;2r+1)}=\frac{2*1*10000}{2,71}=7380\text{ h},$$

where $x^2(1-\propto;2r+1)$ is the quantile of the x^2 distribution with a $2r$+1 degree of freedom (for the NRT test plan), ($\alpha = 1 - \gamma = 1 - 0.9 = 0.1$) is the level of significance per GOST R 50779.26-2007.

$$\hat{t}_{\gamma 1}=-T_{01н}\ln\left(\gamma\right)=0,1053*7380=777\text{ h}.$$

Based on the conventional estimates of t_γ it can be concluded that the product does not comply with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 777 h, which is not in line with the product dependability requirements.

The comparison of the conventional $\hat{t}_{\gamma 1}=777$ ($\gamma=90\%$) and proposed $\hat{t}_{\gamma 1}=1519(\gamma=90\%)$ estimates of gamma-percentile time to failure t_γ shows that for tests that did not produce any failures the conventional estimation using lower confidence estimates significantly underestimates the gamma-percentile time to failure t_γ in comparison with the proposed estimation $\hat{t}_{\gamma 1}$.

Example 2. In the conditions of example 1, based on the results of tests of ten products, one failure occurred at the end of the tests. It is required to estimate t_γ and verify the products' compliance with the dependability requirements.

Out of formulas (6) and (7) follows that the estimate of the GPTF value will be

$$\hat{t}_{\gamma 1}=\hat{T}_4\ln\left(\gamma\right)=-\ln(0,9)*\frac{\tau}{-\ln\left(1-\hat{p}\left(R=1,N=10\right)\right)}=$$
$$=0,1053*\frac{10000}{-\ln(1-0,16226)}=5947\text{ h}.$$

Based on the estimates of t_γ it can be concluded that the product complies with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 5947 h, which is in line with the product dependability requirements.

For comparison, let us mention the conventional solution of example 2.

Normally, parameter T_0 is estimated in accordance with [5] using the following formula:

$$T_{01}=\frac{t_\Sigma}{R+1}=\frac{10*10000}{2}=50000\text{ h}.$$

Then,

$$\hat{t}_{\gamma 1} = -T_{01}\ln(\gamma) = 0{,}1053 * 50000 = 5265 \text{ h}.$$

Based on the conventional estimates of t_γ it can be concluded that the product complies with the requirements for the gamma-percentile time to failure. The time within which not more than 10 % of products will fail will be 5265 h, which is in line with the product dependability requirements.

The estimate of MTF T_{01} is less efficient than estimate $\hat{T}_4$ [6]. Therefore, the estimate of gamma-percentile time to failure $\hat{t}_{\gamma 1}$ is more efficient than the conventional estimate of the gamma-percentile time to failure $\hat{t}_{\gamma 1}$. Then, the comparison of the conventional $\overline{t}_{\gamma 1} = 5265$ ($\gamma = 90\%$) and proposed $\hat{t}_{\gamma 1} = 5947(\gamma = 90\%)$ estimates of gamma-percentile time to failure t_γ shows that the conventional estimation $\hat{t}_{\gamma 1}$, as expected, significantly underestimates the gamma-percentile time to failure t_γ in comparison with the proposed estimation $\hat{t}_{\gamma 1}$.

Example 3. As the dependability indicator of a product the gamma-percentile storing life t_γ (γ=0,9) is used, that must not be lower than one year. Based on the results of 10-year-long storage of one product it is required to estimate t_γ and verify the product's compliance with the dependability requirements.

Out of formulas (6) and (7) follows that the estimate of the GPSL value will be

$$\hat{t}_{\gamma 1} = \hat{T}_4\ln(\gamma) = -\ln(0{,}9) * \frac{\tau}{-\ln\left(1-\hat{p}\left(R=0, N=1\right)\right)} =$$

$$= 0{,}1053 * \frac{10}{\ln(1-0{,}5)} = 1{,}519 \text{ years}.$$

Based on the estimates of t_γ it can be concluded that the product complies with the requirements for the gamma-percentile storing life. The calendar time within which not more than 10 % of products will fail will be 1.519 years, which is in line with the product dependability requirements.

Conclusions

The obtained estimate of GPL $\hat{t}_{\gamma 1}$ is simple and more efficient as compared to the conventional one and not significantly inferior to estimate $\hat{t}_{\gamma ef}$, if such exists, in terms of proximity to t_γ in case a binomial test plan is used.

The obtained estimate of GPL $\hat{t}_{\gamma 1}$ has significant advantages, i.e.:

- the estimate is efficient within a sufficiently wide range of estimates [6],
- the estimate allows obtaining value t_γ based on the results of tests that did not produce any failures.

The obtained estimate of GPL $\hat{t}_{\gamma 1}$ is recommended for failure-free tests conducted using a binomial plan.

References

[1] Barzilovich EYu, Beliaev YuK, Kashtanov VA et al., Gnedenko BV, editor. Voprosy matematicheskoj teorii nadezhnosti [Matters of mathematical dependability theory]. Moscow: Radio i sviaz; 1983 [in Russian].

[2] GOST 27.002-2015. Industrial product dependability. Terms and definitions. Moscow: Standartinform; 2016 [in Russian].

[3] Shulenin VP. Matematicheskaya statistika. Chast 1. Parametricheskaya statistika: ouchebnik [Mathematical statistics. Part 1. Parametric statistics: a textbook]. Tomsk: Izdatelstvo NTL; 2012 [in Russian].

[4] Voinov VG, Nikulin MS. Nesmeshchennye otsenki i ikh primenenie [Unbiased estimates and their application]. Moscow: Nauka; 1989 [in Russian].

[5] GOST R 50779.26-2007. Statistical methods. Point estimates, confidence intervals, prediction intervals and tolerance intervals for exponential distribution. Moscow: Standartinform; 2008 [in Russian].

[6] Mikhailov VS. Implicit estimates for the *N*Bτ test plan. Reliability and quality of complex systems 2018;1(21):64-71 [in Russian].

[7] Mikhailov VS. Efficient estimation of mean time to failure. Dependability 2016;4:40-42.

[8] Ishkov AS, Zuev VD. Evaluation methodology of C-percentile time to failure of electronic components in information-measuring systems by short-term test results. Dependability 2015;2:86-89.

[9] Shvetsova-Shilovskaya TN, Gromova TV, Sokolov FP, Ratushenko VG. Computational and experimental method for estimating reliability indicators of technological complex based on the results of its testing using prior information on reliability derived from testing of its components. Dependability 2013;2:87-92.

[10] Chumakov IA, Chepurko VA, Antonov AV. Estimations of residual lifetime of alternating process. Common approach to estimations of residual lifetime. Dependability 2013;2:65-79.

About the author

Viktor S. Mikhailov, Lead Engineer, D.I. Mendeleev Central Research and Design Institute of Chemistry and Mechanics, Russian Federation, Moscow, e-mail: Mvs1956@list.ru

Received on: 25.11.2018

Original article
Dependability, vol. 19 no.2, 2019 *DOI: 10.21683/1729-2646-2019-19-2-22-27*

Neural network integration of classical statistical tests for processing small samples of biometrics data

Alexander I. Ivanov, *Penza Research and Design Electrical Engineering Institute, Russian Federation, Penza*
Evgeny N. Kuprianov, *Penza State University, Russian Federation, Penza*
Sergey V. Tureev, *Research and Design Institute for Communications and Control Systems***,** *Russian Federation, Moscow*


Alexander I. Ivanov


Evgeny N. Kuprianov


Sergey V. Tureev

Abstract. *The* **Aim** *of this paper is to increase the power of statistical tests through their joint application to reduce the requirement for the size of the test sample.* **Methods.** *It is proposed to combine classical statistical tests, i.e. chi square, Cram r-von Mises and Shapiro-Wilk by means of using equivalent artificial neurons. Each neuron compares the input statistics with a precomputed threshold and has two output states. That allows obtaining three bits of binary output code of a network of three artificial neurons.* **Results.** *It is shown that each of such criteria on small samples of biometric data produces high values of errors of the first and second kind in the process of normality hypothesis testing. Neural network integration of three tests under consideration enables a significant reduction of the probabilities of errors of the first and second kind. The paper sets forth the results of neural network integration of pairs, as well as triples of statistical tests under consideration.* **Conclusions.** *Expected probabilities of errors of the first and second kind are predicted for neural network integrations of 10 and 30 classical statistical tests for small samples that contain 21 tests. An important element of the prediction process is the symmetrization of the problem, when the probabilities of errors of the first and second kind are made identical and averaged out. Coefficient modules of pair correlation of output states are averaged out as well by means of artificial neuron adders. Only in this case the connection between the number of integrated tests and the expected probabilities of errors of the first and second kind becomes linear in logarithmic coordinates.*

Keywords: *statistical tests: chi square, Cram r-von Mises, Shapiro-Wilk; artificial neural networks, small samples, normal law of data distribution hypothesis testing.*

For citation: *Ivanov AI, Kuprianov EN, Tureev SV. Neural network integration of classical statistical tests for processing small samples of biometrics data. Dependability 2019;2: 22-27. DOI: 10.21683/1729-2646-2019-19-2-22-27*

The problem of control of the data distribution law of small samples

The problems of ensuring the reliability of unique critical systems [1, 2] are multifaceted and can be solved only through a set of organizational and technical measures. These problems are especially prominent in neural network biometrics. Each of us has a unique biometric image that is to be transformed into a cryptographic key or long access password generated through random symbols. The uniqueness of the transformation is enabled by means of neural network learning, while the learning sample has a close to normal multidimensional data distribution law. The problem is that learning samples are small. In particular, the standard learning algorithm [3] is able to solve the task on samples of 20 examples, if this sample is obtained correctly and has no outliers (gross errors).

In cases of large biometrics data samples (200 tests and more) it is not difficult to test the hypothesis of normal distribution. The chi square criterion or any other statistical criterion can be used [4]. One of the problems of biometrics [5] is that its users do not wish to provide to an automatic neural network learning machine [3] 200 and more instances of their biometric image. Users feel satisfied having submitted a learning sample consisting of 10 to 20 examples of their unique biometric image, for example, a handwritten password or voice password. Users perceive negatively the requirements to present more than 20 examples.

The situation is similar in botany, biology, and medicine. A plan breeder or a biologist is not able to quickly get a sample of 200 animals (plant specimens) with necessary rare characteristics. A sufficient sample for correct statistical estimation can be obtained after a long period of time by selecting and consolidating the desired rare characteristics over several generations.

There is a similar situation in medicine. Large samples are required to test statistical hypotheses. The subject matter of statistical processing of small samples is very popular, but the well-known recommendations [6, 7] do not significantly improve the situation. As a rule, improvements are achieved through the application of several statistical criteria [8].

An attempt could be made to enhance the known statistical criteria [9], but this does not result in major improvements. As a rule, new statistical criteria or variants of earlier criteria individually provide poor results.

The main idea of this paper is the neural network integration of standard statistical criteria [4, 10, 11]. The progress achieved by the Russian neural network biometrics is very significant. Regulators of the Russian information security market have developed the GOST R 52633.xx Russian national series of standards that regulate a number of tough requirements for neural network biometrics. In this paper we will actually attempt to apply the well-developed mathematical techniques of neural network biometrics to new subject areas. At the same time, we will try to show that the very tough requirements of the Russian information security regulators for the probability of error of the first and second kind can be fulfilled in other subject areas through the implementation of the primary recommendations of the GOST R 52633.xx series of neural network biometrics standards.

Synthesis and adjustment of the chi square neuron with 5 inputs

When testing the normality hypothesis in practice, the Pearson's chi square test is most often used. For a small sample with 21 tests, the formula for calculating the chi square criterion value is the following:

$$\chi^2 = 21 \cdot \sum_{i=1}^{5} \frac{\left(\frac{n_i}{21} - \Delta\tilde{P}_i\right)^2}{\Delta\tilde{P}_i}, \qquad (1),$$

where n_i is the number of tests in the i-th histogram interval; $\Delta\tilde{P}_i$ is the expected probability of tests being within the i-th histogram interval under the normal data distribution law of the checked sample.

Let us note that in accordance with the national standard recommendations [10], the average number of tests within each of the histogram intervals is to be close to 5. That is the reason why in formula (1) summation over 5 histogram intervals for a small sample of 21 tests is used.

When developing the formula in 1990, Pearson had no access to computer technologies. For this reason, he was forced to look for asymptotic relations for infinitely large samples. Today the situation has changed. Any student is able to write a program that can produce millions of samples of 21 tests. Figure 1 shows the probability density distribution of the chi square criterion values for samples with a normal and uniform value distribution law.

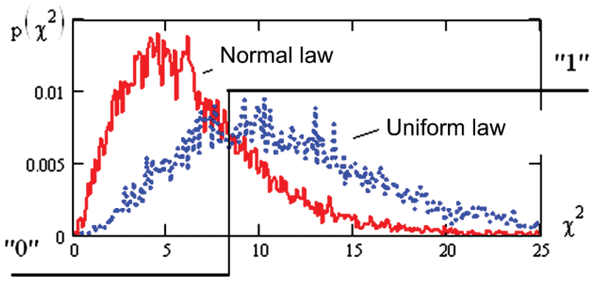


Figure 1. Distribution of chi square criterion values for samples with a normal and uniform value distribution law

Let us note that artificial neurons are configured in such a way as to effectively divide input data into two classes: normal and uniform [12]. Figure 1 shows that the threshold element of the chi square neuron divides the continuum of output elements into two areas: 0 is normal data and 1 is uniform data. The output quantifier of a chi square neuron is configured based on the condition of equally probable error values of the first and second kind of $P_1 = P_2 = P_{EE} = 0.292$.

Let us sort the data of the checked sample according to their values to obtain five input parameters of chi square neuron:

$$x = \text{sort}(x). \tag{2}$$

At the same time, it is required to calculate the width of the histogram intervals:

$$\Delta x = \frac{x_{20} - x_0}{5}. \tag{3}$$

Furthermore, the position of the interval ends is calculated:

$$X_i = x_0 + \Delta x \cdot i \quad \text{when} \quad i = 0, 1, ..., 5. \tag{4}$$

Only after that, it is possible to calculate the number of hits for each of the histogram intervals and form a vector of input parameters $\{n_1, n_2, \ldots, n_5\}$ for the neuron (1). The final result is quantized:

$$\begin{cases} z(\chi^2) \leftarrow \text{"0"} \ \text{ if } \ \chi^2 \le 7.72; \\ z(\chi^2) \leftarrow \text{"1"} \ \text{ if } \ \chi^2 > 7.72. \end{cases} \tag{5}$$

As the result, we have a complete formal description of the chi square neuron implementation for a sample of 21 tests.

Synthesis and configuration of Shapiro-Wilk neuron with 10 inputs

Obviously, the Shapiro-Wilk criterion can be applied to the same sample of 21 tests [4, 11]. This criterion is calculated as following:

$$\upsilon^2 = \frac{1}{\left(\sigma(x)\right)^2} \cdot \left\{ \sum_{i=0}^{9} a_i \cdot \left(x_{20-i} - x_i\right) \right\}^2, \tag{6}$$

where x_i is the ordered values of the sample being checked, $\sigma(x)$ is the standard deviation, a_i is the table values of the Shapiro-Wilk coefficients.

Figure 2 shows the distribution of the values of this criterion for the uniform and normal laws.

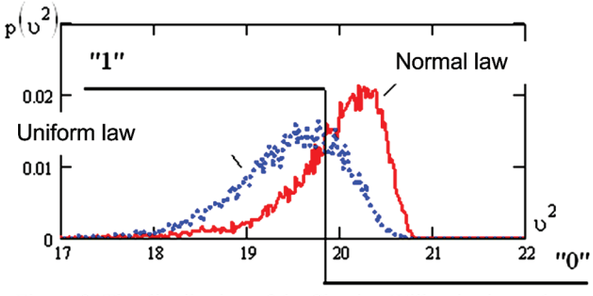


Figure 2. The distribution of the Shapiro-Wilk criterion values for the samples with 21 tests with uniform and normal distribution laws

If the functions of (6) are considered as some kind of artificial neuron, then its outputs will be 10 differences of data of the sample being checked, and the output quantifier will be described as follows:

$$\begin{cases} z(\upsilon^2) \leftarrow \text{"0"} \ \text{ if } \ \upsilon^2 \ge 19.8; \\ z(\upsilon^2) \leftarrow \text{"1"} \ \text{ if } \ \upsilon^2 < 19.8. \end{cases} \tag{7}$$

Such configuration of the threshold of the quantifier provides the errors probability of the first and second kind of $P_1 = P_2 = P_{EE} = 0.303$.

Synthesis and configuration of a Cram r-von Mises neuron with 20 inputs

If we compare the chi square neuron (1) and the Shapiro-Wilk neuron (6), we can see the growth of their input dimension (the number of inputs of their adders). The Cramér-von Mises neuron has an even higher input dimension:

$$\omega^2 = \sum_{i=0}^{19} \left(\frac{i+1}{21} - \tilde{P}(x_i) \right)^2 \cdot \frac{x_{i+1} - x_i}{x_{20} - x_0}. \tag{8}$$

Figure 3 shows the distribution of values at the output of the Cramér-von Mises neuron adder.

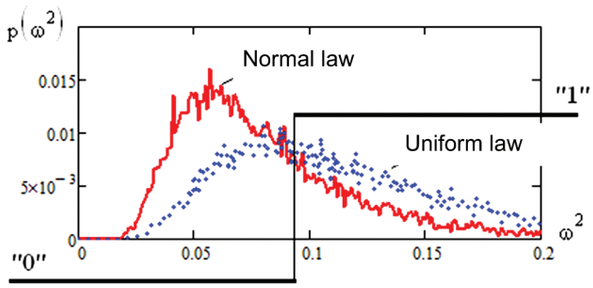


Figure 3. Distribution of values of the Cramér-von Mises criterion for samples with 21 tests with the uniform and normal distribution laws

The configured output quantifier of the neuron adder is described as follows:

$$\begin{cases} z(\omega^2) \leftarrow \text{"0"} \ \text{ if } \ \omega^2 \le 0.087; \\ z(\omega^2) \leftarrow \text{"1"} \ \text{ if } \ \omega^2 > 0.087. \end{cases} \tag{9}$$

Such threshold configuration for quantifier operation provides the same values of errors probability of the first and second kind of $P_1 = P_2 = P_{EE} = 0.342$.

Joint application of three statistical criteria

The statistical criteria described above are linearly independent (they have modules of correlation coefficients less than 1):

$$\begin{cases} \text{corr}(\chi^2, \upsilon^2) \approx +0,559; \\ \text{corr}(\chi^2, \omega^2) \approx -0,708; \\ \text{corr}(\omega^2, \upsilon^2) \approx -0,667. \end{cases} \tag{10}$$

The absence of a complete linear dependence (10) of the output states of the three criteria allows combining them for joint application. In this case, the output code of the three neurons "000" will correspond to a triple confirmation of the hypothesis of the data normality of the checked sample. The inverted state of this code "111" will correspond to the triple confirmation of the hypothesis of the uniform law of distribution of small sample data.

Let us consider one of two hypotheses for the majority of states of "0" or "1" in the output code of the three neurons code by analogy with practical application of neural network converters, which is biometrics and code. In this case, each of the four code states "normal distribution" will correspond to its own probability of errors. Table 1 shows these data.

Table 1. Error probability for the code states "normal distribution"

Code	"000"	"001"	"010"	"100"
P_1	0.0404	0.0423	0.0441	0.0621

Then, if we consider the codes from Table 1 as some complex characteristic of "data normality" it can lead to errors arising with the probability from 0.0404 to 0.0621. There is about a 7-fold decrease in probability of taking wrong decisions, when using three statistical criteria in comparison with their application one by one.

Effect of increasing accuracy of estimates with the growing size of the group of neural network integration of statistical criteria

Dozens of statistical criteria have so far been developed and applied [4, 10, 11]. Supposedly, an equivalent artificial neuron can be developed for each of them. Moreover, previously unknown statistical criteria are under development [13–17]. The first progress in this area will allow adding dozens of completely new statistical criteria to the existing ones. That means that in a few years it will be possible to develop a series of hundreds of different statistical criteria and their neural analogs.

The question arises: up to what level is it possible to reduce the probability of errors by means of neural network integration of a collection composed of 100 and more statistical criteria? This question can be answered based on the accumulated technological experience in processing of neural network biometrics data.

The neural network symmetrization technology can be used for prediction [18, 19]. To implement it, let us average the error probability of the three previously examined neurons (0.292+0.303+0.342)/3 = 0.312. Then, let us average the modules of correlation coefficients between the output states of the three neurons (10): $E(|\text{corr}(.)|) = 0.645$. We proceed from the fact that all of the 100 integrated criteria have symmetric matrices of correlation coefficients with the elements' values outside its diagonal of 0.645.

Another simplification is the normalization of the output states of neuron adders that contradicts the data presented in Figures 1, 2, 3, but at the moment only for this simplification there is a positive experience of using symmetrization.

Figure 4 shows the block diagram of the numerical experiment. Initial data for the numerical experiment are obtained from 100 software generators of pseudorandom numbers with normal distribution.

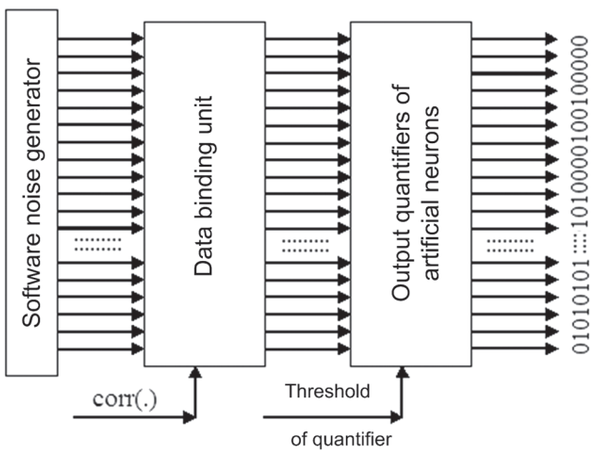


Figure 4. Block diagram for modelling completely symmetrical artificial neural networks

As 100 software generators provide independent data, such data needs to be interconnected and correlated equally. Figure 4 shows that this function is performed by the second left block that multiplies the vector of independent random numbers and by a symmetric connecting matrix:

$$\begin{bmatrix} 1 & a & \vdots & a \\ a & 1 & \vdots & a \\ \vdots & \vdots & \vdots & \vdots \\ a & a & \vdots & 1 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{100} \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{100} \end{bmatrix}. \quad (11)$$

Due to the symmetry that connects the transfer matrix (11), the output data is correlated equally. To obtain a given value of coefficients of equal correlation $\text{corr}(y_i y_{i+1}) = 0.645$, it suffices to find the value of one control parameter a.

Let us note that the procedure of relations and data symmetrization cannot provide exact correspondences of predictions and real data. If we set the quantization threshold of the neuron emulation block in such a way that the error probability is 0.312, then the output triple will have a total error of 0.138. This result is about 3 times worse than the actual data in Table 1.

Let us reduce the equal probability of errors of each neuron from 0.312 to 0.141 to match the results with the observed data. In this case the probability of errors of joint operation of three neurons will be 0.0404.

The transition from normal data to data with the equal correlation is profitable as for this special case in logarithmic coordinates the error probabilities and number of neurons are connected by a linear dependence as shown in Figure 5.

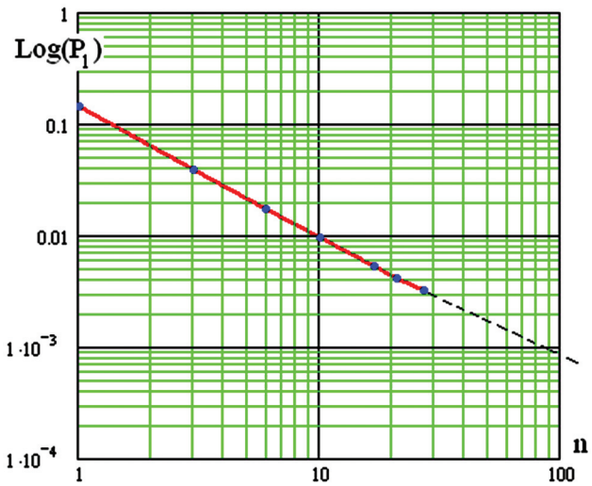


Figure 5. The line of decreasing probability of errors of the first kind due to application of several statistical criteria with correlation coefficients of 0.645

The line was constructed in 7 groups, composed of 1, 3, 6, 10, 16, 21, 27 neurons. When conducting an experiment, a sample of 10 000 000 tests was used; the computation time for a conventional computer is about 9 minutes. It should be noted that using this computer it is difficult to conduct a numerical experiment for a group of 100 neurons, as such experiment would take several months. It is possible to reduce the time by means of extrapolation (dashed line in Figure 5).

As the result, the predicted value of the error probability for a neural network generalization of 10 criteria should be $P_1 = 0.01$, and when summarizing 100 criteria the probability of errors should go down to 0.0009. Such a significant reduction of errors probability is a greater incentive for the synthesis of new statistical criteria [13-17].

Conclusion

Pearson, who created the chi square criterion in 1900, essentially launched a revolution in statistical processing. The path of development discovered by Pearson proved to be very fruitful and over 119 years his followers have created dozens of different statistical criteria.

Neural networks have been a focus of scientific research since the middle of the 20-th century, but only at the beginning of the 21-st century this technology was implemented into the industry and standardized [3].

The key statement of this paper is that it is possible to combine two seemingly different branches of mathematics. Their integration only requires the neural network biometric data processing technologies that are standardized in Russia and are applied to 3 or more standard statistical criteria. In the case of the considered triple of statistical criteria, this approach reduces the probability of errors more than 7 times. In this case, thesis on expediency of expansion of nomenclature of the existing statistical criteria becomes obvious. The larger is the size of the group of statistical criteria generalized by neurons the better is the final result.

In this context, the approach to the synthesis of new statistical criteria is fundamentally changing. After Pearson, mathematicians were trying to find a new, more powerful criterion. A great number of analyzed criteria proved to have low power, and therefore were not published. With neural network integration of a set of statistical criteria, the power of each of them becomes secondary. The correlation relationships between the added criterion and the group of other criteria are also very important. In our case, two integrated criteria have almost the same power, but in this group there is a special Shapiro-Wilk criterion that has low correlation with the primary chi square and Cramér-von Mises criteria.

Thus, the possible diversity of statistical criteria is to be researched again, taking into account not only their relative power, but also the values of their correlation coefficients in groups with other relevant statistical criteria. New statistical criteria with relatively low power of hypothesis separation were previously rejected and not published, but now the situation has changed. It is more important to understand how the new criterion complements the already studied statistical criteria. Probably, it will be necessary to create a table of the level of affinity (correlation) of already known and promising statistical criteria in the nearest future. Linearly independent (weakly correlated) statistical criteria have to be grouped, and neural network integrations are to be created for them.

References

[1] Pokhabov Yu.P. Problems of dependability and possible solutions in the context of unique highly vital systems design. Dependability 2019;19(1):10-17.

[2] Pokhabov Yu.P. Ensuring dependability of unique highly vital systems. Dependability 2017;17(3):17-23,

[3] GOST R 52633.5-2011. Information protection. Information protection technology. The neural net biometry-code converter automatic training. Moscow: Standartinform; 2012 [in Russian].

[4] Kobzar A.I. Prikladnaia matematicheskaia statistika: dlia inzhenerov i nauchnykh rabotnikov [Applied mathematical statistics: for engineers and researchers]. Moscow: FIZMATLIT; 2006 [in Russian].

[5] Iazov Yu.K., editor, Volchikhin V.I., Ivanov A.I., Funtikov V.A., Nazarov I.G. Neyrosetevaia zashchita personalnykh biometricheskikh dannykh [Neural network protection of biometric data]. Moscow: Radiotekhnika; 2012 [in Russian].

[6] Sukhoruchenkov B.I. Analiz maloy vyborki. Prikladnye statisticheskie metody [Small sample analysis. Applied statistical methods]. Moscow: Vuzovskaya kniga; 2010 [in Russian].

[7] Doerffel K. Statistics in analytical chemistry. Moscow: Mir; 1994.

[8] Dayev Zh.A., Nurushev E.T. Application of statistical criteria for improving the efficiency of risk assessment methods. Dependability 2018;2:42-45.

[9] Akhmetov B.B., Ivanov A.I. Estimation of quality of a small sampling biometric data using a more efficient form of the chi-square test. Dependability 2016;16(2):43-48.

[10] R 50.1.037-2002. Rekomendatsii po standartizatsii. Prikladnaia statistika. Pravila proverki soglasia opytnogo raspredelenia s teoreticheskim. Chast I. Kriterii tipa $\chi 2$ [Standardization recommendations. Applied statistics. Rules for compliance verification of experimental distribution with the theoretical one. Part I. Chi-square-type criteria]. Moscow: Gosstandart of Russia; 2001 [in Russian].

[11] R 50.1.037-2002. Prikladnaia statistika. Pravila proverki soglasia opytnogo raspredelenia s teoreticheskim. Chast II. Neparametricheskie kriterii [Applied statistics. Rules for compliance verification of experimental distribution with the theoretical one. Part II. Non-parametric tests]. Moscow: Gosstandart of Russia; 2002 [in Russian].

[12] Haykin S. Neural Networks: A Comprehensive Foundation. Moscow: Viliams; 2006.

[13] Serikova N.I., Ivanov A.I., Serikova Yu.I. Otsenka pravdopodobia gipotezy o normalnom raspredelenii po kriteriu Dzhini dlia chisla stepeney svobody, kratnogo chislu opytov [Likelihood estimation of the hypothesis of normal Gini distribution for the number of degrees of freedom multiple of the number of experiments]. Voprosy radioelektroniki 2015;1(1):85-94 [in Russian].

[14] Perfilov K.A. Kriteriy srednego geometricheskogo, ispolzuemyy dlia proverki dostovernosti statisticheskikh gipotez raspredelenia biometricheskikh dannykh [Criterion of geometric mean used for validity verification of the statistical hypotheses of biometric data distribution]. Proceedings of the science and technology conference of the Penza information technology security cluster. Penza; 2014. Vol. 9. p. 92-93, <http://www.pniei.penza.ru/RV-conf/T9/S92> [in Russian].

[15] Ivanov A.I., Perfilov K.A. Otsenka sootnoshenia moshchnostey semeystva statisticheskikh kriteriev "srednego geometricheskogo" na malykh vyborkakh biometricheskikh dannykh [Assessment of the relations of the strengths of the "geometric mean" family of statistical tests on small samples of biometric data]. XI All-Russian Science and Practice Conference Modern security technologies and comprehensive facility security assets. Penza-Zarechny; 2016. p. 223-229 [in Russian].

[16] Ivanov A.I., Perfilov K.A., Malygina E.A. Multivariate statistical analysis of the quality of biometric data on extremely small samples using the criteria of the geometric mean tests calculated for the analyzed probability functions. Measuring. Monitoring. Management. Control 2016;2(16):64-72 [in Russian].

[17] Ivanov A.I., Perfilov K.A., Malygina E.A. Evaluation of the quality of small samples of biometric data using a differential variant statistical test of the geometric mean. Vestnik SibGAU 2016;4(17):864-871 [in Russian].

[18] Malygin A.Yu., Volchikhin V.I., Ivanov A.I., Funtikov V.A. Bystrye algoritmy testirovania neyrosetevykh mekhanizmov biometriko-kriptograficheskoy zashchity informatsii [Fast algorithms for testing of neural network mechanisms of biometric and cryptographic protection of information]. Penza, Penza State University Publishing 2006 [in Russian].

[19] Akhmetov B.S., Volchikhin V.I., Ivanov A.I., Malygin A.Yu. Algoritmy testirovania biometriko-neyrosetevykh mekhanizmov zashchity informatsii [Algorithms for testing biometric and neural network mechanisms of information protection]. Almaty: Satpayev KazNTU; 2013 [in Russian].

About the authors

Alexander I. Ivanov, Doctor of Engineering, Associate Professor, Lead Researcher of Laboratory of Biometric and Neural Network Technologies, Penza Research and Design Electrical Engineering Institute, Russian Federation, Penza, e-mail: ivan@pniei.penza.ru

Evgeny N. Kuprianov, post-graduate student, Department of Information Security Technology, Penza State University, Russian Federation, Penza, e-mail: ibst@pnzgu.ru

Sergey V. Tureev, Head of Research and Technology Center, Research and Design Institute for Communications and Control Systems, Russian Federation, Moscow, e-mail: niissu@niissu.ru

Received on: 22.01.2019

Original article
Dependability, vol. 19 no.2, 2019 DOI: 10.21683/1729-2646-2019-19-2-28-32

Model of efficiency assessment of diagnostic tools of onboard equipment

Efim N. Rozenberg, *JSC NIIAS, Russian Federation, Moscow*
Alexander S. Korovin, *JSC NIIAS, Russian Federation, Moscow*
Natalia G. Penkova, *JSC NIIAS, Russian Federation, Moscow*

Efim N. Rozenberg

Alexander S. Korovin

Natalia G. Penkova

Abstract. *The* **Aim** *of this paper is to show that the development, deployment of new diagnostic tools and improvement of the existing diagnostic tools in onboard equipment enables better operational characteristics and reduced probability of transition of intelligent railway systems into a forbidden state.* **Method.** *In the context of intelligent railway systems, the construction of the analytical model of probability evaluation is of principal interest due to the feasibility of demonstrating the factors that are taken into consideration by such a model. Forbidden events that cause inoperability of intelligent railway systems are random; they can be represented as a random process. A random process of system development, transition from an allowed state into a forbidden state, system state changes in time can be described with a semi-Markovian process. When assessing the probability of system transition into a forbidden state, the question arises as to the selection of a method of calculation. The paper shows the feasibility of representation and solution of a semi-Markovian model with the help of a coupled graph model [3, 5] that has a high level of visualization and is a well-formalized method of identification of the probability of a system's transition into a forbidden state. The set of system states and their connections are represented with a directed state graph with defined topological concepts [3]. In order to identify the effect of the introduction of new diagnostic tools and improvement of the existing diagnostic tools in onboard equipment on the probability of transition of intelligent railway systems into a forbidden state, the authors use the theorem of identification of the probability of system's transition from the initial unhazardous state into a hazardous state and set forth the formula to calculate this probability.* **Results.** *The graph method implemented in this paper shows that the use of additional diagnostic tools reduces more than twice the probability of a system's transition into a forbidden state, i.e. a state when the failure will not be detected by the inbuilt or additional diagnostic tools.*

Keywords: *onboard train protection systems, display unit, functional dependability, graph model*

For citation: *Rozenberg EN, Korovin AS, Penkova NG. Model of efficiency assessment of diagnostic tools of onboard equipment. Dependability 2019;2: 28-32. DOI: 10.21683/1729-2646-2019-19-2-28-32*

Introduction

Simulation is widely used in the railway industry for planning of forbidden state handling. In case of intelligent systems, mathematic simulation is advantageous. Methods of mathematic simulation are subdivided into two groups: analytical and simulation modeling. Due to certain shortcomings of simulation modeling [1], in the context of intelligent railway systems, the construction of the analytical model of probability evaluation is of principal interest due to the feasibility of demonstration of the factors that are taken into consideration by such model. Forbidden events that cause inoperability of intelligent railway systems are random; they can be represented as a random process. A random process of system development, transition from an allowed state into a forbidden state, system state changes in time can be described with a semi-Markovian process. In general, the construction and solution of semi-Markovian models comes down to building a system of homogenous differential equations. This procedure always involves mathematical difficulties. For this reason the paper shows the feasibility of representation and solution of semi-Markovian models with a coupled graph model [3, 5]. Such models are highly visual, allow formalizing the wanted system states, as well as paths of transition from allowed into hazardous states, does not require the use of complex mathematics in the preparation of measures of forbidden event handling.

Problem definition

Currently, the Russian railway industry employs the following intelligent onboard systems: KLUB-U (standardized integrated onboard train protection system), BLOK (vital integrated onboard system) and BLOK-M (scalable vital integrated onboard system). The KLUB-U, BLOK and BLOK-M systems have their own display units equipped with man-machine interfaces. A display unit is a hardware and software system. This system is to ensure information display to the driver, assistant driver, operator in case of driverless operation, service personnel in case of locomotive driving and pre-trip diagnostics.

The display of information on the permitted speed, target speed, actual speed, track profile, distance, stopping point ahead, train schedule, train ahead, stop aspect enables safe locomotive driving in terms of observation of speed limits in normal operation and prediction of safe mode of locomotive driving.

In the process of operation, system operability may be disrupted due to a random hardware failure, manifestation of a systematic failure in its software, driver's error while interacting with the system, input data error. Any disruption of system operability is regarded as its failure. This causes the display of incorrect information and wrong decisions by the driver in terms of safety of locomotive driving.

That is why great attention is paid to the development and application of diagnostic tools that allow minimizing the probability of the display unit transitioning into a forbidden state that causes disruption of display unit operability. A forbidden state, in this case, is understood as a hidden (not detected by diagnostic tools) failure.

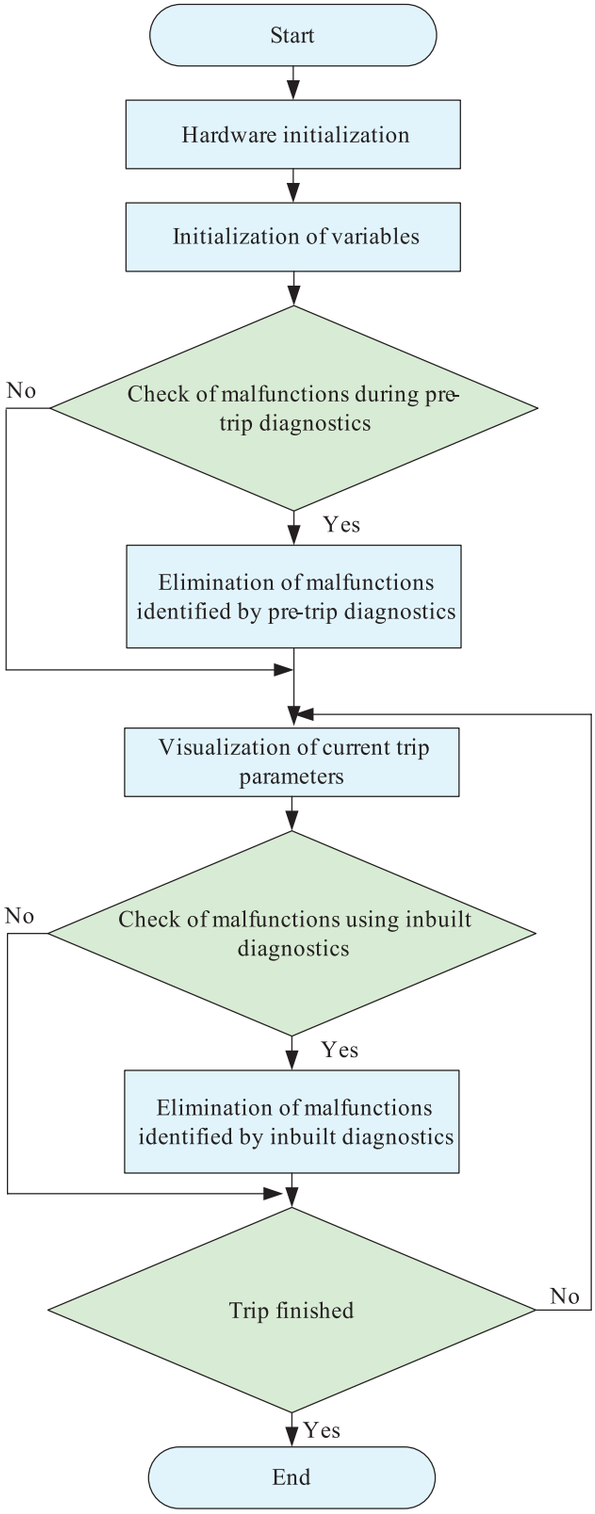


Figure 1. Flow diagram of the operation algorithm of a display unit with inbuilt diagnostic tools and pre-trip diagnostics

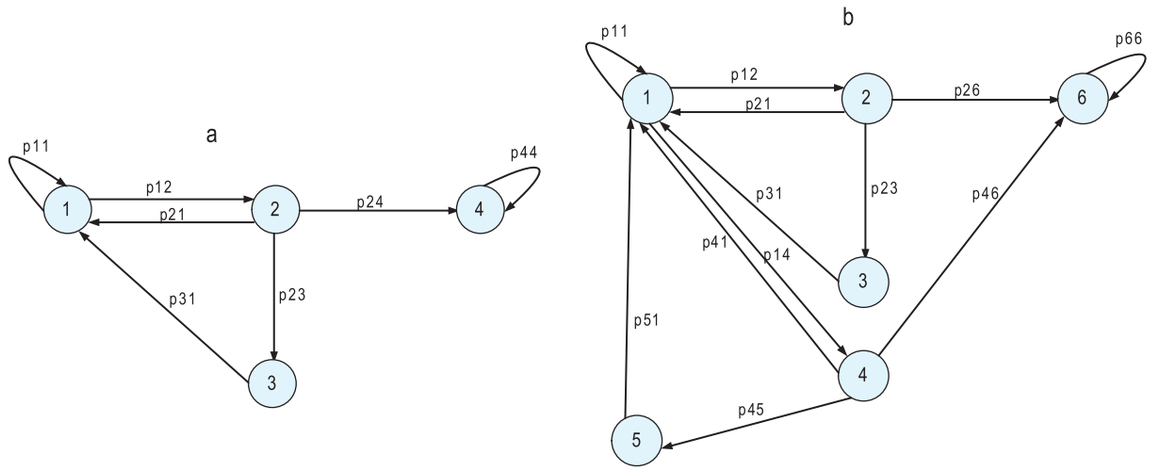


Figure 2. State graph: a) with inbuilt diagnostic tools, b) with inbuilt diagnostic tools and added pre-trip diagnostics of the display unit by the driver or service personnel.

The display unit has inbuilt diagnostic tools that verify the operability of the display unit with a level of diagnostic coverage that is sufficient to ensure safety.

Inbuilt diagnostic tools are able to detect a number of irregularities in the display unit operation. In order to extend the list of detectable errors, it is proposed to introduce additional pre-trip diagnostics by the driver or service personnel to be conducted before each trip. Among other things, that will allow preventing locomotives with faulty safety devices to be cleared for operation.

The aim of this paper is to show the efficiency of diagnostic tools in man-machine interaction in the context of onboard systems. It is also to demonstrate that the development, deployment of new diagnostic tools and improvement of the existing diagnostic tools enables better operational characteristics of the display unit and reduced probability of its transition into a forbidden state.

Models description

Let us represent the operation algorithm of a display unit with inbuilt diagnostic tools and pre-trip diagnostics in the form of a flow diagram (figure 1).

Let us construct the graph of the operation algorithm of the display unit shown in Figure 1.

Events of irregularities of display unit operation are random in their nature. Let us represent the considered operation algorithms of the display unit with a directed state graph *G(S, H)*, where *S* is the finite set of system states; *H* is the finite set of edges between nodes *i, j* (states s_i, s_j). The states of display unit operation can be described as follows: if the display unit is in state s_i, then with probability p_{ij} it can transition into state s_j.

Figure 2a shows a state graph in which only the inbuilt diagnostic tools are used for detection of display unit failure. Figure 2b shows a state graph in which the detection of system failures involves not only the inbuilt display unit diagnostic tools, but additional pre-trip diagnostics of the display unit by the driver or service personnel. In order to attain the goal of this paper, let us consider the graph in Figure 2b. The graph has the following states:

State *S*1, display of the current operational situation by the display unit software;

State *S*2, testing for failures by inbuilt diagnostic tools (software check for CAN errors, software check for controller freeze by watchdog timer switching, software check of display unit being present in the configuration);

State *S*3, elimination by the display unit of failures detected by the inbuilt diagnostic tools (software reboot of CAN interface, hardware controller reboot by means of watchdog timer, hardware reboot of display unit software);

State *S*4, testing for failures by means of pre-trip diagnostics of display unit (correctness of command processing, correctness of operational situation display, correctness of installed version of software, correctness of parameter values of constant characteristics);

State *S*5, elimination by the driver or service personnel of failures detected by means of pre-trip diagnostics (immediate elimination of detected errors, display unit software update input of correct parameter values of constant characteristics);

State *S*6, i.e. display unit being in a state with a hidden failure.

S is the complete set of states, $S = \{S1, S2, S3, S4, S5, S6\}$;

S_p is the subset of non-forbidden states, $S_p = \{S1, S2, S3, S4, S5\}$;

$\overline{S}_p$ is the subset of forbidden states, $\overline{S}_p = \{S6\}$.

Provided that the display unit's inbuilt and pre-trip diagnostic tools are operable, the existence of failure in the display unit is identified and the system is put into failure elimination mode.

It is assumed that in case of failure detection the system is restored. In case of non-detection of failure by the inbuilt and pre-trip diagnostic tools of the display unit due to their failure or insufficient efficiency the system is put into hidden failure mode (forbidden state).

States *S*1 and *S*2 are allowed and belong to the set "normal operation of display unit during intended operation". The values of transition probability *p*11 and *p*12 were selected based on the ratio of the part of the program that implements the function of current operational situation display and function of failure detection by inbuilt diagnostic tools. A trip lasts 10 hours (i.e. every 10 hours the state a pre-trip diagnostics is to be initiated).

The value *p*21 is selected based on the actual dependability of the display unit in the course of its operation. Statistically, a failure of the display unit is a low-probability event (70 failures were registered in 2018 throughout the railway network based on operational data, the total number of systems being 11740). The fact that a failure has not been registered in the course of operation does not mean that the unit is operational the whole time. It may have been in a forbidden state of hidden failure for some period of time. The values of probabilities of transitions *p*23 and *p*26 were distributed based on the efficiency of the internal diagnostic tools implemented in the unit. The failure detectivity by the inbuilt diagnostic tools implemented in the display unit are at 0.5 in accordance with GOST R 61508-7-2012.

Table 2 shows the values of probabilities of one-step transitions from the *i*-th state to state *j* (p_{ij}).

Table 1. Transition probabilities matrix

		State						
		1	2	3	4	5	6	∑
State	1	0,72	0,18	0	0.1	0	0	1
	2	0,85	0	0,075	0	0	0,075	1
	3	1	0	0	0	0	0	1
	4	0.7	0	0	0	0,15	0,15	1
	5	1	0	0	0	0	0	1
	6	0	0	0	0	0	1	1

The problem consists in the identification of the effect of introduction of pre-trip diagnostics on the probability of display unit transitioning into a forbidden state during intended operation, when only in-built diagnostic tools are used.

In order to solve this problem, let us use theorem that states that the probability of system transition from the specific *i*-th initial non-hazardous state into any hazardous state *f* is defined by formula [5]

$$b_{if} = \frac{\sum_{f \in \bar{S}p} \sum_k l_k^{if} \Delta G_k^f}{\Delta G_{\bar{S}p}},$$

where l_k^{if} is the *k*-th path leading from a non-hazardous state of graph *i* into a hazardous state *f*;

ΔG_k^f is the weight of graph resolution without the *f*-th node and graph nodes situated on the *k*-th path;

$\Delta G_{\bar{S}p}$ is the weight of graph resolution without the nodes of the hazardous state set.

Let us set forth the following topological concepts used in mathematical simulation [3]:

- *path* is a chain of series-connected unidirectional edges with the beginning in the state *i* and the end in the state *j*, the path weight being

$$l_k^{ij} = \prod_{i,r,j \in S} p_{ir} p_{rj},$$

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

p_{rj} is the probability of one-step transition from state *r* into state *j*;

- *closed circuit* is a chain of series-connected unidirectional edges, in which the output of the final node in the circuit is connected to the initial node of the circuit. The weight of the *j*-th circuit is identified by the formula:

$$C_j = \prod_{i,j \in S} p_{ij} p_{ji};$$

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

- *graph resolution* is a part of a graph that does not contain defined nodes and connected edges; the weight of resolution ΔG^i is calculated subject to the exclusion of node *i* and connected edges out of the graph; the weight of resolution $\Delta G_{\bar{S}p}$ is calculated subject to the additional exclusion of nodes of set $\bar{S}_p$ and connected edges out of the graph; the weight of resolution ΔG_k^f is calculated subject to the exclusion of node *f* out of the graph, as well as the nodes situated in the *k*-th path from the initial node to *f* and connected edges;

- the *weight of resolution* is found using Mason's formula:

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

In order to evaluate the efficiency of introducing pre-trip diagnostics, let us calculate the conditional probability of transition from the initial state "1" into the forbidden state "6", provided that the inbuilt diagnostic tools (internal diagnostics) are disabled (paths *S*1→*S*2→*S*6 and *S*1→*S*2→*S*3).

In accordance with the theorem for evaluation of the probability of system transition from the initial allowed state into a forbidden state, the conditional probability of transition from *S*1 to *S*6 is defined with the formula:

$$b_{16/\bar{S}_{126}} = \frac{\sum_{f \in \bar{S}p} \sum_k l_k^{16} \Delta G_k^6}{\Delta G_{\bar{S}p}}.$$

As it can be seen in the graph in Figure 2b, the number *k* of transition paths from *S*1 to *S*6 - provided that display unit failure detection relies only on pre-trip diagnostics of the display unit by the driver or service personnel - equals 1.

Identification of path weights: l_1^{16} = *S*1→*S*4→*S*6 = *p*14·*p*46.

Identification of circuit weights:

*C*1: *S*1→*S*1, circuit weight is *p*11;

*C*2: *S*1→*S*2→*S*1, circuit weight is *p*12·*p*21;

*C*3: *S*1→*S*2→*S*3→*S*1, circuit weight is *p*12·*p*23·*p*31;

$C4$: $S1 \rightarrow S4 \rightarrow S1$, circuit weight is $p14 \cdot p41$;

$C5$: $S1 \rightarrow S4 \rightarrow S5 \rightarrow S1$, circuit weight is $p14 \cdot p45 \cdot p51$;

$C6$: $S6 \rightarrow S6$, circuit weight is $p66$.

For the considered case, the weight of graph resolution without the nodes of the forbidden state set equals: $\Delta G_{\bar{S}p} = 1 - (C1+C2+C3+C4+C5)$.

The weight of resolution accounting for the exclusion of node "6" out of the graph, as well as the nodes situated in the k-th path from node "1" to node "6" and connected edges equals to: $\Delta G_1^6 = 1$.

By substituting data from Table 1 we obtain the conditional probability of transition from state $S1$ to state $S6$:

$$b_{16/\bar{S}_{126}} = \frac{\sum_{f \in \bar{S}p} \sum_k l_k^{16} \Delta G_k^6}{\Delta G_{\bar{S}p}} =$$

$$= \frac{p14 * p46 * \Delta G_1^6}{1 - C1 - C2 - C3 - C4 - C5} = 0,53.$$

As the considered models describe a complete group of events, the probability of hitting the only forbidden state is in both cases 1. Thus, based on the calculated value of conditional probability $b_{16/\bar{S}_{126}}$, we conclude that adding pre-trip diagnostics of the display unit by the driver or service personnel allows reducing the probability of the display unit transitioning into a forbidden state during the trip more than twice (from 1 to 0.47).

Conclusion

This paper shows the efficiency of adding pre-trip diagnostics of the display unit by the driver or service personnel to the inbuilt tools for diagnosing failures in the display unit. Thus, the probability of a system's transition into a forbidden state, i.e. a state when the failure will not be detected by the inbuilt or additional diagnostic tools, will be reduced more than twice.

Acknowledgement

The authors express their gratitude to Prof. Igor B. Shubinsky, Doctor of Engineering, for his assistance, valuable advice and observations that contributed to this paper.

References

[1] Ivnitsky V.A. Modelirovaniye informatsionnykh sistem zheleznodorozhnogo transporta. Uchebnoye posobiye [Simulation of information systems of the railway industry. Study guide]. Moscow: MIIT; 2011 [in Russian].

[2] Shubinsky I.B. Funktsionalnaya nadezhnost informatsionnykh sistem: Metody analiza [Functional dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012 [in Russian].

[3] Shubinsky I.B. Nadiozhnie otkazoustoychivie informatsionnie sistemy. Metody sinteza [Dependable failsafe information systems. Synthesis methods]. Moscow: Dependability Journal; 2016 [in Russian].

[4] Shubinsky I.B. O poniatii funktsionalnoy nadezhnosti [On the concept of functional dependability]. Dependability 2012;4:74-84 [in Russian].

[5] Shubinsky I.B. Methods of software functional dependability assurance. Dependability 2014;4:95-101.

[6] Shubinsky I.B., Zamyshlyaev A.M., Pronevich O.B. Graph method for evaluation of process safety in railway facilities. Dependability 2017;17(1):40-45.

[7] Pronevich O.B., Shved V.E. Algorithm of calculation and forecasting of functional safety indicators of railway power supply systems. Dependability 2018;18(3):46-55.

[8] Rozenberg E.N., Penkova N.G., Korovin A.S. Functional dependability of the display unit software of the BLOK system. Dependability. 2017;17(2):36-40.

[9] Shukhina E.E., Astrakhan V.I. Bezopasny lokomotivny obiedinenny kompleks BLOK [BLOK vital integrated onboard system]. Moscow; 2013 [in Russian].

[10] Zorin V.I., Astrakhan V.I. Unifitsirovannoe kompleksnoe lokomotivnoe ustroystvo bezopasnosti (KLUB-U) [Standardized integrated onboard train protection system (KLUB-U)]. Moscow: Training and Methodology Centre for Railway Transport; 2008 [In Russian].

[11] GOST R IEC 61508–7–2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 7. Techniques and measures. Moscow: Standartinform; 2014 [in Russian].

About the authors

Efim N. Rozenberg, Professor, Doctor of Engineering, First Deputy Director General, JSC NIIAS Russia, Moscow, e-mail: info@vniias.ru

Alexander S. Korovin, Chief Specialist of Computer-Based Devices Development Sector, JSC NIIAS, Russia, Moscow, e-mail: A.Korovin@vniias.ru

Natalia G. Penkova, Deputy Head of Safety and Algorithmic Support, JSC NIIAS, Russia, Moscow, e-mail: N.Penkova@vniias.ru

Received on 08.04.2019

Original article
Dependability, vol. 19 no.2, 2019 DOI: 10.21683/1729-2646-2019-19-2-33-41

Indicator-based approach to safety management of railway infrastructure facilities

Leonid A. Baranov, *Russian University of Transport (MIIT), Russian Federation, Moscow*
Vladimir V. Kulba, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences (ICS RAS), Russian Federation, Moscow*
Alexey B. Shelkov, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences (ICS RAS), Russian Federation, Moscow*
Dmitry S. Somov, *Sberbank, Russian Federation, Moscow*


Leonid A. Baranov


Vladimir V. Kulba


Alexey B. Shelkov


Dmitry S. Somov

Abstract. *The Aim of this paper is to develop the methods of analysis and simulation of the processes of occurrence and development of emergencies at complex railway infrastructure facilities. It cites analysis data on the threats, causes and consequences of sudden emergencies at complex railway infrastructure facilities. For the purpose of ensuring reliable operation of technical objects, as well as timely identification of faults, it is proposed to use the indicator-based approach that allows diagnosing and formally analyzing the processes of occurrence and propagation of malfunctions across the elements of complex technical systems. For the purpose of simulating the processes of propagation of the disturbances (hazards of emergencies) that occur as the result of malfunctions, it is proposed to use the theoretic graph approach that involves model and visual representation of the structure of a technical system under consideration in the form of a directed graph that shows the correlations between its elements. Each node and edge of a graph is assigned certain parameters or functionals that reflect the processes of correlated operation of the elements of the simulated system. The propagation of disturbances within a system is simulated with pulse processes initiated in one or several nodes. The paper refers to the developed formalized models of disturbance propagation in a technical system based on the construction of structural components and correlation matrices. The authors introduce the concept of critical element of a technical system that helps identify the event of its failure. Two basic criteria of technical system failure, i.e. the exclusive (a system is considered to have failed if the disturbance has reached any of the critical elements) and absolute criterion (failure occurs if the disturbance has reached the specified subset of critical elements) are defined. The paper provides an analytical example that illustrates the capabilities of the proposed model of disturbance propagation within the structure of a technical system. For the purpose more efficient diagnostics of the hazard of emergencies in railway infrastructure facilities the paper proposes a model of application of structurally integrated indicators that consists in the integration of indicators within the structure of a technical system that would immediately deliver the required and sufficient information in case of emergency. The main task would be to identify a set of indicators with the primary purpose of reducing the information-related stress and concentration of dispatchers' or operators' attention on the processes within a technical system that are most relevant in terms of accident-free and safe operation. Basic criteria are identified for the generation of the set of indicators within a complex technical system: maximum of reliability of the disturbance consequences estimate, maximum of accuracy of emergency causes identification, minimum of emergency identification time, minimum of nonrecurrent and current costs. A modified graph model of disturbance propagation in a complex technical system is provided that is the prerequisite for solving the multicriterion problems of optimal location of indicators within the structure of a technical system in terms of completeness, accuracy and timeliness of detection of failures of various types. Automation of the processes of generation of indicator sets using models of disturbance propagation in technical systems will allow using the proposed methods as part of further development of the URRAN methodology in terms of improvement of the decision support in railway infrastructure facilities management.*

Keywords: *control, railway transportation, infrastructure facility, technical system, emergency, sensors, indicators, simulation.*

For citation: *Baranov LA, Kulba VV, Shelkov AB, Somov DS. Indicator-based approach to safety management of railway infrastructure facilities. Dependability 2019;2: 33-41. DOI: 10.21683/1729-2646-2019-19-2-33-41*

Introduction

Being a crucial part of the Russian transportation industry railways play an essential role in the process of the country's socio-economic development, since this type of transport has practically no alternative in terms of the volume and structure of freight and passenger traffic. The leading role of railway transportation is also determined by the country's specific characteristics, including significant transport distances, remoteness of primary main mining facilities and sources of raw materials from the points of processing and consumption, as well as seaports, insufficient infrastructure development of other types of transport in Siberia and the Far East, which are of strategic importance for the national development. The condition, safety and quality of rail transportation define not only the prospects for further social and economic development, but also the nation's ability to effectively perform such essential functions as protecting its sovereignty and security, providing citizens with transportation and creating conditions for more even economic development of individual regions, etc.

The URRAN integrated system for management of resources, risks and dependability of railway infrastructure facilities at lifecycle stages is being developed and widely implemented by specialized organizations and divisions of the Russian Railways since 2010 [1]. Essentially, the system implements a comprehensive process of dependability, resources and functional safety management in railway transportation and is essentially an extended RAMS (reliability, availability, maintainability and safety) and LCC (life cycle cost) methodology.

The primary strategic railway safety objectives are [2]:

1. Improving the efficiency of the main activity, utilization of infrastructure, technical reliability and fixed assets availability,
2. Ensuring the quality of products, services and processes,
3. Ensuring transportation safety.

The system of railway facilities and processes is a massive geographically distributed multi-purpose infrastructure that includes JSC Russian Railways facilities (track and structures, signalling, communication, electrification and power facilities; locomotive, car and passenger facilities) that are different in purpose and solve different process-specific tasks. At the same time, the complexity of the technical systems included in the above facilities continuously increases, which inevitably leads to an increase in the number and variety of risks associated with the production, adjustment, maintenance, operation and upgrading of these systems [3].

Ensuring safety and dependability becomes especially important with the use of "driverless" vehicles. According to the International Association of Public Transport, there are 5 Grades of Automation of trains (from GOA0 to GOA4). When GOA4 level is implemented, there is no operational personnel onboard rolling stock. Under these conditions, centralized automatic train control systems for subways should contain subsystems that ensure the completeness, accuracy and timeliness of detection of failures of various types and preventive decision making [4].

Today, the technological development goes hand in hand with the increase in the number of elements involved in technical systems (dimensional complexity), the increase in the diversity of interaction structures of these elements (structural complexity) and the increase in the diversity of the forms and methods of this interaction (functional complexity). This significantly complicates the task of ensuring the reliable operation of complex technical systems (CTS) that are part of the railway infrastructure facilities, since, depending on their structural and functional features, the manifestation of the risks and the nature of failures and faults propagation in the considered systems may differ [5]. In this case, the realization of risks may take the form of the possibility of malfunctioning or failure of a separate node and the entire system. The aim of this paper is to develop the methods of analysis and simulation of the processes of occurrence and development of emergencies at complex railway infrastructure facilities from indicator-based approach point of view.

1. Simulation of disturbance propagation in the technical system

The extensive experience of operating CTS of various types and purposes shows that the occurrence of failures and faults of various nature, as well as incidents and emergencies they lead to (hereinafter referred to as sudden emergencies, or SE) is usually preceded by the stage of accumulation of defects in the equipment or deviations in a particular process [6]. The duration of this stage can vary significantly (from minutes to days). At the same time, at first the defects or deviations themselves do not pose an immediate threat of SE occurrence. In practice the processes of accumulation of such deviations are usually associated either with the unobservability of the CTS elements and subsystems due to the lack of effective monitoring and diagnostic tools, or, even more often, with the fact that personnel are accustomed to such deviations, since they do not always lead to accidents. At the next stage a sudden so-called initiating event occurs, which leads to an avalanche-like development of unfavorable processes and the occurrence of SE, the consequences of which are significantly aggravated by the lack of organizational and technical countermeasures, as well as lack of time and resources for their effective implementation. It is obvious that the SE, occurring at the third stage as a result of the rapid development of events, for the most part would be impossible without the accumulation of deviations and errors in the first stage.

Thus, one of the main tasks of ensuring the smooth operation of CTS is the timely identification of malfunctions,

other disorders in the technical system, pre-emergency (emergency) situations and the transfer of information on their occurrence to the visualization, dispatching and situational management systems at various levels (to decision makers (DM), dispatchers, operators, etc.). The sources of information on possible abnormal deviations (malfunctions) in CTS or their subsystems (nodes) operation are sensors, elements of the system that can register various parameters of the system state, environment, parameters of the CTS operation, etc.

The resulting risk of malfunction, failure, accident, SE or other disruption of the normal CTS operation, registered by the sensor, is called a threat. In this case, the occurrence of a certain threat presumably leads to the processes of disturbance propagation along the structural elements of CTS accordance with their interaction scheme. Since, in accordance with the definition above, threats can be of different nature (type, nature of occurrence and manifestation, etc.), the CTS elements can interact with each other in various ways during the disturbance propagation process. As a result, schemes of interaction between elements will be different for each type of threat. Hence, the disturbances will also propagate through the elements of the CTS along different paths.

Technical systems of high structural, dimensional and functional complexity usually include a large number of sensors, which makes it significantly more difficult to monitor their readings, diagnose abnormal situations, and most importantly, make timely accurate control decisions in the event of reading deviation from the norm and especially the threat of SE occurrence. Thus, problem of choosing the structure of the dispatching or situational management information system arises. It should allow reducing the operator's stress in order to increase the emergency response rate without a significant loss of awareness about safety critical processes [5, 7-8].

For the purpose of simulating the processes of propagation of the disturbances that occur as the result of malfunctions, the theoretic graph approach will be used. The representation of the structure of a technical system in the form of a graph is widely used for visualization and modeling of the correlations between system elements. At the same time, the structure of the system can be rigidly fixed or undergo certain regular changes (which is typical of dynamic systems) depending on the process or phenomenon being simulated.

In this approach the structure of a system and the interactions between its elements are represented in the form of a directed graph. Each node and edge of a graph is assigned certain parameters and functionals that reflect the processes of operation of the simulated system elements. The initial pulse (disturbance) applied to one or several nodes is propagated through the whole graph changing the parameters of the nodes. In the general case, the magnitude of the pulse itself can change as well in accordance with the functionals assigned to the edges of the graph. The simulation uses discrete time with a fixed step Δt. This approach to simulation of dynamic systems has now found application in a number of areas [9].

Let us assume that $A = \{a_1, a_2, ..., a_n\}$ is a set of elements in a model, where n is their number. At any point in time any element can take on a value of 0 or 1. One stands for an active state (the disturbance has reached the element), zero stands for inactive state. The state of element a_i at the point of time t will be designated as $a_i(t)$, and the row-vector of states of model elements ($a_1(t)$, $a_2(t)$, ..., $a_n(t)$) will be designated as $\overline{A}(t)$. The set of sensors constitute a subset of model elements $A \supseteq D = \{d_1, d_2, ..., d_{n_D}\}$, where n_D is the number of sensors.

Adjacency matrix M shall mean $n \times n$ binary matrix, indexed along both axes by the set of model elements. Positions $(i, j), i, j \in \overline{1,n}$ of the adjacency matrix contain 1 if and only if the relation R_1 between model elements a_i and a_j is such that when element a_i is active at the moment t_1, the element a_j will also be active at the moment $t_2 = t_1 + \Delta t$. In other words, relation R_1 specifies the paths of disturbance propagation through the system. By relation R_1 we shall mean an adjacency relation or reachability of depth of 1 relation. The adjacency relation between model elements a_i and a_j will be designated as $a_i R_1 a_j$ and the absence of such relation will be designated as $a_i \overline{R_1} a_j$. If there is no adjacency relation R_1 between elements a_i and a_j, there is a 0 in the position (i, j) of the adjacency matrix M. Let us suppose that the adjacency relation has reflexive property, i.e. $\forall a \in A \quad aR_1a$. Within the model, this means that once activated, the element remains activated during the entire simulation time. For each specified type of threat, its own adjacency relationship can be defined, R_1^1, R_1^2, R_1^3 and so on. Accordingly, each type of threat has its own adjacency matrix. The adjacency matrix M corresponds to the digraph of the cause-effect relationships of the model elements $G(A, R_1)$, the nodes of which are the set of model elements, and the edge (a_i, a_j) corresponds to one in the matrix position (i, j). This graph will be called the relationship digraph.

The activation of the model elements is described by the Boolean equation $\overline{A}(t_{i+1}) = \overline{A}(t_i) \times M$. In other words, all elements of the model connected by edges with already active elements are activated at further steps. In this case, once activated elements remain activated during the entire simulation, since the diagonal elements of the adjacency matrix are equal to 1.

Among the set of model elements the subset of sensors $D = \{d_1, d_2, ..., d_{n_D}\}$ is selected. The sensors register the specified parameters of the CTS and indicate the occurrence of a threat. The disturbance caused by this threat spreads from the sensors to other elements of the system along the edges of the correlation graph $G(A, R_1)$. The set of model elements, the correlation matrix and the subset of sensors are determined together with the system designer according to the results of the system operation scheme analysis at the development stage. The subset of critical elements $K = \{k_1, k_2, ..., k_{n_K}\}$ that determine the criterion for system failure is also selected among the elements of the model. Different sets of criti-

cal elements can be considered for each type of threat (edge coloring).

Simulation starts at the moment of activation of the first sensor t_0 and continues either until the moment of stabilization (termination of change in the state of the model elements), or until the system fails in accordance with the selected system failure criterion.

The time of system failure will be designated as t_S. The criterion for system failure is determined by critical elements. Depending on the features of the system or node under consideration, as well as other features of the problem being solved, different criteria for evaluating the system failure can be selected. There are two basic criteria among them.

Exceptional criterion for system failure. The system is considered failed if the disturbance has reached any of the critical elements: $t_S = \min(t : \exists k \in K : k(t) = 1)$.

Absolute criterion for system failure. The system is considered failed if the disturbance has reached a given subset $K^* \subseteq K$ of (in the degenerate case of all) critical elements: $t_s = \min(t : \forall k \in K^* : k(t) = 1)$.

Other criteria can also be considered, for example, those related to the number, mutual arrangement and other parameters of the critical element set to which the disturbance has reached.

To illustrate the possibilities of the proposed model of disturbance propagation in the structure of a CTS, let us consider a simplified example. Let us suppose that the structure of the system include 12 elements, n=12, A={a_1, a_2, ..., a_{12}}. Elements a_1 and a_2 are sensors, $d_1 = a_1$, $d_2 = a_2$, D={d_1, d_2}= {a_1, a_2}, n_D=2. Elements a_{11} and a_{12} are critical elements, $k_1 = a_{11}$, $k_2 = a_{12}$, K={k_1, k_2}= {a_{11}, a_{12}}, n_K=2. The adjacency matrix M is defined as:

$$M = \begin{array}{|cccccccccccc|}\hline 1&0&1&0&0&0&0&0&0&0&0&0\\ 0&1&0&1&1&0&0&0&0&0&0&0\\ 0&0&1&1&0&0&0&1&0&0&0&0\\ 0&0&0&1&0&1&0&0&0&0&0&0\\ 0&0&0&0&1&0&1&0&0&0&0&0\\ 0&0&1&0&0&1&1&0&0&0&0&0\\ 0&0&0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&0&0&1&1&0&0&0\\ 0&0&0&0&0&0&0&0&1&0&1&0\\ 0&0&0&0&0&0&0&0&1&1&0&1\\ 0&0&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&0&0&1\\ \hline\end{array}.$$

The relation R_1, defined by the matrix M forms the relation digraph $G(A, R_1)$ shown in Figure 1, where the sensors are designated by a circle ●, and the critical elements are indicated by a square ■. Let us suppose that there is only one type of threat, hence, only one set of critical elements, one adjacency relationship and one relationship graph are defined.

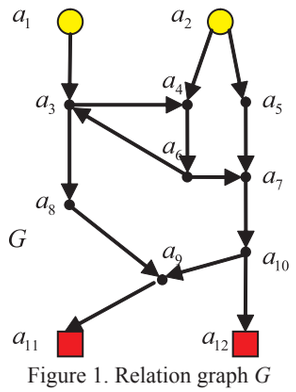


Figure 1. Relation graph G

Let us suppose that at time $t = t_0$ the sensor d_1=a_1 registers a threat $a_1(t_0)$=1, $a_{i,j\neq1}(t_0)$=0, $\overline{A}(t_0) = \underbrace{(1,0,0,...,0)}_{12}$. Then, the states of the model elements at the time point $t = t_1 = t_0 + \Delta t$ are calculated as follows:

$$\overline{A}(t_1) = \overline{A}(t_0) \times M = \underbrace{(1,0,1,0,0,...,0)}_{12}.$$

Figure 2 shows the process of disturbance propagation along the edges of the relation graph G from active elements (marked by an additional circle) to inactive ones, as well as the states of the corresponding model elements at different points in time. The disturbance spreads along the edges of the graph from the active elements to the inactive ones, covering one edge at a step. The state of the elements at a specific time point is determined by a Boolean formula $\overline{A}(t_i) = \overline{A}(t_0) \times M^i$.

The elements status lines for different points in time are as follows:

$$\overline{A}(t_0) = (1,0,0,0,0,0,0,0,0,0,0,0);$$

$$\overline{A}(t_1) = (1,0,1,0,0,0,0,0,0,0,0,0);$$

$$\overline{A}(t_2) = (1,0,1,1,0,0,0,1,0,0,0,0);$$

$$\overline{A}(t_3) = (1,0,1,1,0,1,0,1,1,0,0,0);$$

$$\overline{A}(t_4) = (1,0,1,1,0,1,1,1,1,0,1,0);$$

$$\overline{A}(t_5) = (1,0,1,1,0,1,1,1,1,1,1,0);$$

$$\overline{A}(t_6) = (1,0,1,1,0,1,1,1,1,1,1,1).$$

As the above example shows, at the time point t=t_4 the first critical element is activated. If the system uses an exceptional criterion for system failure, then at the time point t_4 the system would fail. With absolute criteria, the system fails at the time point t=t_6.

2. Models of using the indicator-based approach

For the purpose of more efficient diagnostics of emergency hazard, a model of application of structurally integrated indicators in railway infrastructure facilities will be considered. The indicator-based approach means that, in addition to the sensors, indicators are integrated within the structure of a technical system immediately delivering the required and sufficient information to the corresponding visualization, dispatching or situational management systems in case of emergency in order to inform the DM (dispatchers, operators, etc.) if increased attention to the situation or direct intervention are required.

The main task is to identify a set of indicators (the concept of "indicator dashboard" generally accepted in organizational management [10] can be used here) with the primary purpose of reducing the information-related stress and concentration of dispatchers' or operators' attention on the processes within a technical system that are most relevant in terms of accident-free and safe operation.

The values of the parameters reflected by the selected indicators should reliably demonstrate the deviations from the normal operation of the system. Thus, within the framework of control, dispatching or situational management, the approach under consideration is to first and foremost provide the decision makers with the necessary and sufficient information on the status of the CTS in visual form, as well as ensure the possibility of operational (including scenario) analysis of alternative ways of emergency situation developing on a specific time horizon. Ultimately, it should improve the efficiency of management decisions on transport safety.

In order to achieve these objectives, the location of the indicators in the CTS structure should allow for informing the DS on the occurrence and development of a potentially dangerous situation at the earliest possible stage. At the same time, it should be noted that at the early stages of a situation's development, the possible (most probable, pessimistic, optimistic, etc.) scenario for an abnormal situation is not always clear. As a result, the set of consequences may be too broad, which does not allow reliably predicting the consequences and making the right decision. In this case, real-time and detailed monitoring of the potentially pre-emergency state of the CTS is required in order to collect additional information to analyze it and decide on the appropriate response.

Naturally, an equally important criterion for choosing a specific placement of indicators is the cost of such placement. Depending on the specific task, it is necessary to take into account not only the number of indicators, but also their weight, volume, physical distance between indicators, sensors, etc. When selecting a set of indicators one should obviously strive to reduce their total number,

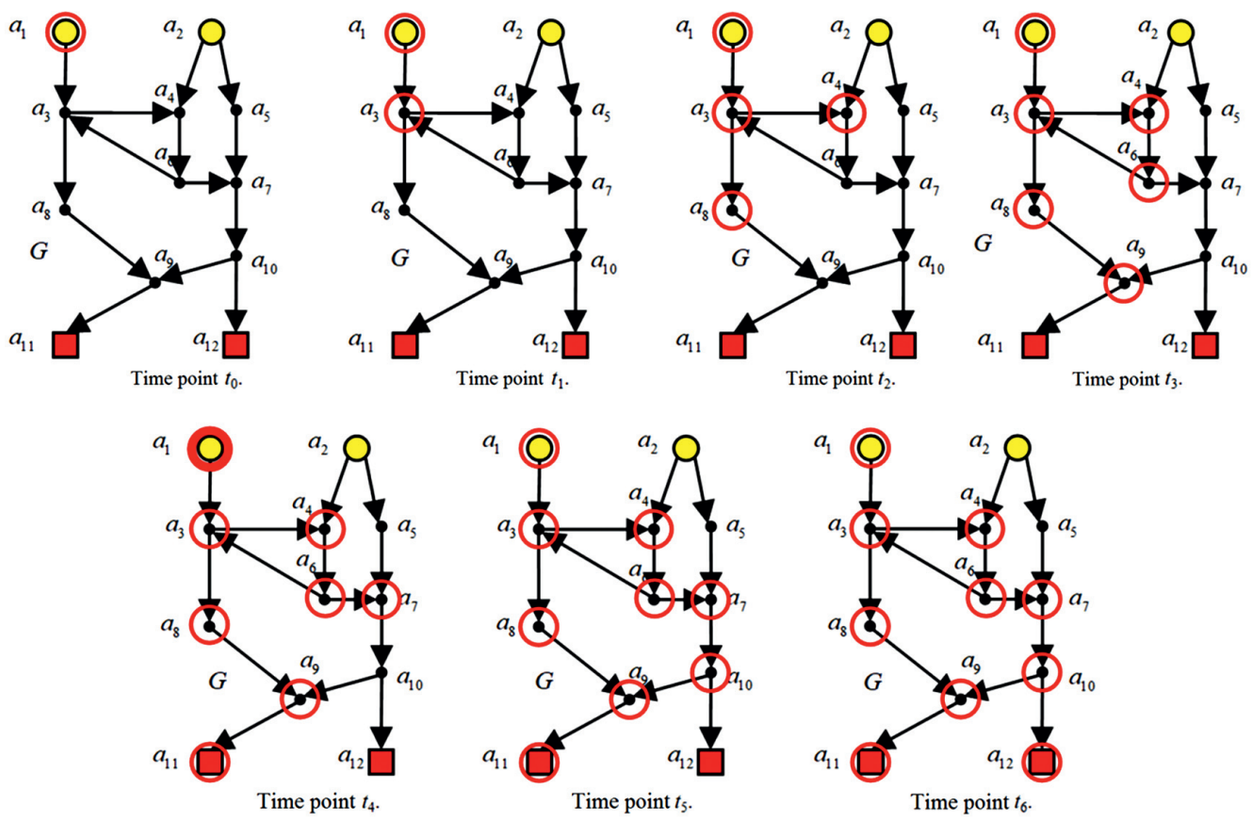


Figure 2. The process of disturbance propagation in the system

while ensuring the minimum possible reduction in the accuracy and information content of the data they send to the visualization, dispatching or situational management systems.

At the substantive level, the following main criteria for choosing the set of indicators in a complex technical system can be distinguished.

Reliability of consequence evaluation. The selection of the indicator set should allow for making judgment on the nature of the situation development and possible consequences with maximum accuracy based on their readings.

Accuracy of cause identification. Indicators should allow not only for timely detection and consequences assessment of abnormal situations, but also for identification of their causes. For example, indicators should show with which CTS node (element) the spread of the negative impact started, whether the cause of the deviations was external or internal, etc.

Abnormal situation detection time. Indicators' selection and localization in the structure of the CTS should allow for detecting deviation from normal operating at the earliest possible stages of their development in order to maximize the amount of time available for a decision made by system operator.

Cost. Indicators' selection and localization in the structure of the CTS should minimize one-time and current costs.

The proposed criteria are contradictory in a way. For example, in order to determine the cause of an abnormal situation as precisely as possible, strictly speaking, one should place indicators in all elements of the system, but this will increase the cost, the information-related stress on the decision maker, the time required for abnormal situation detection, etc.

To solve the problem of composing a set of indicators, the above graph model of disturbance propagation in the CTS is modified. The concept of edge passing time is introduced expressed as a positive number associated with the edge of the relation graph and meaning the time, during which the disturbance passes from the model element at the beginning of the edge to the element at the end of the edge. To register the edge passing times, the matrix of temporal relations Mt, which is a square matrix $n \times n$, indexed along both axes by the model elements. Positions (i, j), $i, j, \in 1, n$ of the temporal relations matrix contain edge passing time (a_i, a_j), if such edge exists, and infinity sign ∞, if such edge does not exist.

Temporal distances matrix N shall mean a $n \times n$ square matrix indexed along both axes by the set of model elements. Position (i, j), $i, j, \in 1, n$ of this matrix contains temporal distance between graph nodes a_i and a_j. The temporal distance matrix is the result of applying the Floyd-Warshall algorithm for finding the shortest distances between the nodes to the matrix of temporal relations [11].

An optimization problem of placing indicators in a technical system is formulated using a series of definitions introduced below. A subset of indicators will be denoted by $I=\{i_1, i_2, ..., i_{n_I}\}$. The set of time t precedence of element a shall mean a set of model elements $Bef_t(a)$, from which the element a can be reached in a time not exceeding time t. The set of time t precedence of element a shall mean a set of model elements $Bef_t(a)$, from which the element a can be reached in a time not exceeding time t. The set of time t afteraction of element a shall mean a set of model elements $Aft_t(a)$, which can be reached from the element a in a time not exceeding time t.

Indicator coverage of time t precedence shall mean a set of time t precedence sets for all indicators:

$$I_t^{Bef} = \left\{ Bef_t(i_1), Bef_t(i_2), \ldots, Bef_t\left(i_{n_t}\right)\right\}.$$

Indicator set of coverage of time t precedence shall mean the union of the set of model elements included in the indicator coverage of time t precedence, or, what is the same, the union of time t precedence sets for all indicators:

$$\overline{I_t^{Bef}} = \bigcup_{j=n_t} Bef_t\left(i_j\right).$$

Similarly, indicator coverage of time t afteraction shall mean a set of time t afteraction sets for all indicators:

$$I_t^{Aft} = \left\{ Aft_t(i_1), Aft_t(i_2), \ldots, Aft_t\left(i_{n_t}\right)\right\}.$$

Indicator set of coverage of time t afteraction shall mean the union of the set of model elements included in the indicator coverage of time t afteraction, or, what is the same, the union of time t afteraction sets for all indicators:

$$\overline{I_t^{Aft}} = \bigcup_{j=n_t} Aft_t\left(i_j\right).$$

Overall set of coverage precedence shall mean the union of sets of time given for each indicator precedence for all indicators:

$$I_T^{Bef} = \left\{ Bef_{t_1}(i_1), Bef_{t_2}(i_2), \ldots, Bef_{t_{n_T}}\left(i_{n_t}\right)\right\},$$

where $T=\{t_1, t_2, ..., t_{n_T}\}$ is a set of times of precedence sets. Similarly, the concept of overall indicator precedence coverage

$$I_T^{Aft} = \left\{ Aft_{t_1}(i_1), Aft_{t_2}(i_2), \ldots, Aft_{t_{n_T}}\left(i_{n_t}\right)\right\}.$$

Diameter of the overall coverage shall mean the maximum value of all times of a set.

$$T : D\left(I_T^{Bef} \right) = D\left(I_T^{Aft} \right) = \max_{j \le n_I} \left(t_j \right).$$

Similar to the time coverage, the concept of the indicator set of the overall indicator coverage of precedence and afteraction is introduced:

$$\overline{I_t^{Bef}} = \bigcup_{j \le n_I} Bef_t \left(i_j \right), \overline{I_t^{Aft}} = \bigcup_{j \le n_I} Aft_t \left(i_j \right).$$

Let us suppose that the solutions to the indicator localization problem is a subset of model elements $I \subseteq A$. With the introduction of some restrictions on the set of solutions the set of feasible solutions is obtained.

The number of indicators should be limited. This restriction derives from the requirement to reduce the information-related stress on the operator. Mathematically this restriction can be expressed as $\left| I \right| = n_I \le N_I$, where N_I is some constant given in a specific task.

The set of indicators shall cover all possible threats known at the current stage of system development. In other words, in terms of the model in question, there should not be a situation in which the disturbance caused by the sensor reaches a critical element before it reaches the indicator. The mathematical interpretation of this restriction can be written as $\forall d \in D : Alf\left(d \right) \cap K \ne \varnothing \, \exists i \in I : i \in Aft_S \left(d \right)$

Thus, the region of feasible solutions must satisfy the afteraction requirements:

$$I \subseteq A,$$

$$\left| I \right| = n_I \le N_I,$$

$$\forall d \in D : Alf\left(d \right) \cap K \ne \varnothing \, \exists i \in I : i \in Aft_S \left(d \right).$$

Optimization criteria for finding the optimal solution among the feasible solutions are formulated.

1. *Criterion of maximizing the allowable time for decision making*. From the system's operational safety and failure prevention point of view the earliest possible threat detection is required. This criterion implies maximizing the time from the moment of activation of the critical element to the critical event. In terms and designations of the model it is written as follows:

$$\min_{d \in D, k \in K} \left(\max_{i \in I \cap Alf(d)} \left(dis^t \left(d, k \right) - dis^t \left(d, i \right) \right) \right) \to \max_I.$$

2. *Completeness of coverage*. For each set of indicators, coverage by precedence and afteraction sets is defined.

In order to judge of the possible causes and consequences of the current situation most accurately, the selected indicators must allow for the precedence and afteraction sets to covers as much of the model elements as possible. Mathematically, it can be expressed as:

$$\left| \overline{I^{Alt}} \right| \to \max_I; \left| \overline{I^{Bef}} \right| \to \max_I.$$

3. *Accuracy of coverage.* In the previous criterion coverage is used without consideration of time. However, to accurately identify the developing situation, the indicators should be "close" to the propagating through the system disturbance in time. For that purpose, the minimal diameter of precedence or afteraction coverage (the set of which covers the whole set of precedence I^{Bef} or afteraction I^{Alt}) must be minimal:

$$\min_{T : I_T^{Alt} = \overline{I^{Alt}}} \left(D\left(I_T^{Alt} \right) \right) \to \min_I;$$

$$\min_{T : I_T^{Bef} = \overline{I^{Bef}}} \left(D\left(I_T^{Bef} \right) \right) \to \min_I.$$

Let us formulate the task of optimizing the placement of indicators.

Let us suppose that the given model of disturbance propagation through a technical system is: the set of model elements is $A=\{a_1, a_2, ..., a_n\}$, the subset of sensors is $D=\{d_1, d_2, ..., d_{n_D}\}$, the subset of critical elements is $K=\{k_1, k_2, ..., k_{n_K}\}$. The model elements are interconnected in relations graph G, edge passing times are given in the matrix of temporal relations M.

It is required to find such subset of elements (a set of indicators) $I=\{i_1, i_2, ..., i_{n_I}\}$ that would comply with the following conditions:

$$\left| I \right| = n_I \le N_I,$$

$$\forall d \in D : Alf\left(d \right) \cap K \ne \varnothing \, \exists i \in I : i \in Aft_S \left(d \right).$$

$$\min_{d \in D, k \in K} \left(\max_{i \in I \cap Alf(d)} \left(dis^t \left(d, k \right) - dis^t \left(d, i \right) \right) \right) \to \max_I,$$

$$\left| \overline{I^{Alt}} \right| \to \max_I; \left| \overline{I^{Bef}} \right| \to \max_I,$$

$$\min_{T : I_T^{Alt} = \overline{I^{Alt}}} \left(D\left(I_T^{Alt} \right) \right) \to \min_I;$$

$$\min_{T : I_T^{Bef} = \overline{I^{Bef}}} \left(D\left(I_T^{Bef} \right) \right) \to \min_I.$$

Due to the orientation to the systems of high dimensional, structural and functional complexity and in light of opposing nature of the criteria formulated above, the precise algorithms for solving the problem in question will have too high computational complexity. Thus this problem is proposed to be solved using a combination of various approximate algorithms that create solutions according to individual criteria, or modify some existing indicator placement created based on other performance criteria [5, 12]. The practical application of this problem algorithms should be carried out using interactive procedures to collaborate with experts or specialists in a given subject area. Such approach can significantly improve the quality of the solution results (variants of indicator placement) in terms of achieving the set goals.

Conclusion

The main aim of the proposed indicator-based approach is to increase the dependability of CTS in operation and to prevent SE through the early diagnostics of the hazard of emergencies in technical systems. The indicator-based approach offers means to reduce the information-related stress and to concentrate dispatchers' or operators' attention on the processes that are most relevant in terms of safety. The approach also allows locating the sources of emergency situations with the required accuracy.

The proposed models of the disturbance propagation in the CTS are the basis for the formulation and development of formalized methods for timely detection of abnormal situations during the CTS operation and preventing SE. The developed indicator-based approach includes a set of models and technologies for analyzing the processes of hazard effect and disturbances propagation in complex technical systems, as well as methods for solving multi-criteria problems of optimal placement of indicators in the structure of the CTS based on criteria of completeness, accuracy and timeliness of detecting failures of various types.

References

[1] Gapanovich V.A. Development and implementation of the URRAN technology on railway transport. Dependability 2013;4:11-17.

[2] Gapanovich V.A., Shubinsky I.B., Rozenberg E.N., Zamyshlyaev A.M. System of adaptive management of railway transport infrastructure technical maintenance (URRAN project). Dependability 2015;2:14-22.

[3] Kulba V.V., Kosyachenko S.A., Shelkov A.B. Methodology of research of railway transport safety problems. Large-Scale Systems Control 2012;38:5-19 [in Russian].

[4] Baranov L.A. Automatic control of metro trains. World of Transport and Transportation. 2018;16(3):156-165 [in Russian].

[5] Kulba V.V., Kononov D.A., Kosyachenko S.A., Kochkarov AA, Somov DS. Ispolzovanie scenarnogo i indikatornogo podhodov dlya upravleniya zhivuchestyu, stojkostyu i bezopasnostyu slozhnyh tekhnicheskih sistem [Use of scenario and indicator-based approaches to controling the survivability, durability and safety of complex technical systems]. Moscow: ICS RAS;2011 [in Russian].

[6] Bykov A.A. O problemah tekhnogennogo riska i bezopasnosti tekhnosfery [On the problems of technology-related risk and safety of the technosphere]. Issues of risk analysis 2012:9(3):4-7 [in Russian].

[7] Shults V.L., Kulba V.V., Shelkov A.B., Chernov I.V., Somov D.S. Upravlenie tekhnogennoy bezopasnostyu na osnove scenarnogo i indikatornogo podhodov. Nauchnoe izdanie [Technogenic safety management using scenario and indicator approaches. A scientific publication]. Moscow: ICS RAS; 2013 [in Russian].

[8] Shults V.L., Kulba V.V., Shelkov A.B., Chernov I.V. Metodologiya upravleniya tekhnogennoy bezopasnostyu obiektov infrastruktury zheleznodorozhnogo transporta na osnove indikatornogo podhoda [Method of technogenic safety management of railway infrastructure facilities using indicator approach]. Trends and management 2013;3:4-23 [in Russian].

[9] Shults V.L., Kulba V.V., editors. Modeli i metody analiza i sinteza scenariev razvitiya socialno-ekonomicheskih sistem [Models and methods of analysis and synthesis of development scenarios of socio-economic systems]. Moscow: Nauka; 2012 [in Russian].

[10] Eckerson W. Performance Dashboards: Measuring, Monitoring, and Managing your Business. Moscow: Alpina Business Books; 2007.

[11] Cormen T., Leiserson C., Rivest R., Stein C. Introduction to Algorithms. Third edition. Moscow: Izdatelstvo Viliams; 2013.

[12] Kulba V.V., Somov D.S., Kochkarov A.A. The use of structure-integrated indicators in complex technical systems monitoring. Izvestiya SFedU. Engineering sciences 2011;3(116):52-65 [in Russian].

About the authors

Leonid A. Baranov, Doctor of Engineering, Professor, Head of Department, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: baranov.miit@gmail.com

Vladimir V. Kulba, Doctor of Engineering, Professor, Head of Laboratory, V.A. Trapeznikov Institute of

Control Sciences of the Russian Academy of Sciences, Russian Federation, Moscow, e-mail: kulba@ipu.ru

Alexey B. Shelkov, Candidate of Engineering, Lead Researcher, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Russian Federation, Moscow, e-mail: abshelkov@gmail.com

Dmitry S. Somov, Chief Analyst, Sberbank, Russian Federation, Moscow, e-mail: somov.dmitry@gmail.com

Received on: 27.02.2019

Original article
Dependability, vol. 19 no.2, 2019 DOI: 10.21683/1729-2646-2019-19-2-42-47

On the matter of the terminology of aeronautical structures survivability

Vadim V. Efimov, *Moscow State Technical University of Civil Aviation, Russian Federation, Moscow*

Vadim V. Efimov

Abstract. Aim. *The paper examines the existing definitions of survivability and damage tolerance (operational survivability) of aeronautical structures. An attempt is made to unambiguously define the survivability of aeronautical structures that can subsequently be extended to an aircraft as a whole and other complex technical items. The primary goal of this paper is to clearly distinguish between dependability and survivability. In order to ensure efficient operation and flight safety, an aircraft must possess airworthiness, a comprehensive characteristic of an aircraft that is defined by the implemented design principles and solutions and that allows performing safe flights under expected conditions and under the established methods of operation. The expected operating conditions are described in the Aviation Regulations – Airworthiness Requirements. Despite the fact that compliance with the Airworthiness Requirements ensures a sufficiently high level of flight safety, the most vital structural components are designed in such a way as to remain operable even under extreme conditions beyond the expected operating conditions. But dependability cannot be responsible for operability outside the expected operating conditions. Conclusion suggests itself that under extreme conditions beyond the expected operating conditions operability is to be ensured by another property, i.e. survivability.* **Methods.** *This research was conducted using the logical and probabilistic approaches. The author examined literary sources primarily dedicated to the matters of dependability and survivability of aeronautical structures, as well as other complex technical items. In order to ensure an optimal understanding of the differences and correlation between the concepts of dependability and survivability, the probabilistic approach was used.* **Results.** *Upon the analysis of literary sources, survivability was defined as the property of an item to retain in time the capability to perform the required functions under extreme conditions beyond the expected operating conditions under the specified methods of maintenance, storage and transportation. Additionally, the paper proposes the definition of damage tolerance (operational survivability) as the property of an item to retain in time the capability to perform the required functions under extreme conditions beyond the expected operating conditions depending on the methods of maintenance, storage and transportation. The probabilistic approach to the delimitation of the concepts of dependability and survivability of aeronautical structures was examined using the known indicator of operating efficiency of a transport aircraft that is represented as the mathematical expectation of the efficiency indicator. An aircraft may be either in the expected operating conditions or in extreme conditions beyond the expected operating conditions. No third option exists. Then, the sum of the probabilities of an aircraft encountering such conditions must be equal to one. The probability of no-failure can be calculated by means of the probability of the contrary event, i.e. the probability of failure that can be represented as the product of the probability of an aircraft encountering certain operating conditions and the probability of failure in such conditions. For the case of extreme conditions beyond the expected conditions the well-known concepts of perishability and vulnerability with the author's improvements can be used.* **Conclusions.** *A definition of survivability was obtained that is clearly different from the concepts of dependability and fail-safety. Additionally, the concept of damage tolerance (operational survivability) was proposed that was introduced similarly to the previously introduced concept of operational dependability.*

Keyword: *survivability, damage tolerance (operational survivability), dependability, failure, reliability, fail-safety, aeronautical structure, aircraft.*

For citation: *Efimov VV. On the matter of the terminology of aeronautical structures survivability. Dependability 2019;2: 42-47. DOI: 10.21683/1729-2646-2019-19-2-42-47*

Introduction

Any aircraft is characterized by a wide range of properties and parameter, including operating properties, i.e. the set of aircraft properties that manifest themselves in the course of operation. They include dependability, survivability, safety and maintainability. Whereas the terms dependability, safety and maintainability are covered in sufficient detail and with sufficient consistency in specialized literature, and some terms are even part of corresponding standards, the term "survivability" does not have an unambiguous and generally accepted definition. That is true not only in case of the aircraft survivability terminology, but that of other items as well [1–5].

In this paper, an attempt is made to unambiguously define the survivability of aeronautical structures that can subsequently be extended to an aircraft as a whole and other complex technical items. The primary goal of this paper is to clearly distinguish between the concepts of dependability and survivability.

Primary concepts and definitions of the theory of survivability of aeronautical structures

In order to ensure efficient operation and flight safety, an aircraft must possess airworthiness that is defined by its design and is maintained in operation. *Airworthiness* is a comprehensive characteristic of an aircraft defined by the implemented design principles and solutions that allows performing safe flights under expected conditions and under the established methods of operation [6]. Airworthiness Requirements of transport aircraft [7] define *expected operating conditions* as the conditions that are known from practice or whose occurrence can be reasonably predicted within the useful life of an aircraft subject to its purpose. Such conditions include state parameters and external factors that affect an aircraft, operational factors that affect flight safety.

The expected operating conditions do not include the following:

– extreme conditions that can be reliably avoided by introducing operating restrictions and rules,

– extreme conditions that occur so rarely, that observing the Airworthiness Requirements in such conditions would result in a higher level of airworthiness than required and practical.

Airworthiness depends on the *dependability* of the aircraft, including the dependability of its structure that, in turn, is defined by its strength.

At the stage of design, an aircraft's airworthiness in terms of strength is ensured by correct choice of design solutions, strength, stiffness and fatigue calculations and testing.

In the course of aircraft operation, fatigue and corrosion damage, destruction of non-metallic materials, exposure to extreme operating conditions beyond the expected conditions may cause the loss of airworthiness in terms of structural strength. In this context, aircraft operation requires maintaining its airworthiness by means of appropriate measures as part of service and repair operations.

Despite the fact that compliance with the Airworthiness Requirements ensures a sufficiently high level of flight safety, the most vital structural components are designed in such a way as to remain operable even under extreme conditions beyond the expected operating conditions. But dependability cannot be responsible for operability outside the expected operating conditions, as in accordance with GOST 27.002-2015 Dependability in technics. Terms and definitions [8] dependability is a property of an item to retain in time the ability to perform the required functions in *specified modes and conditions of application*, maintenance, storage and transportation, while in accordance with the terminology of the Airworthiness Requirements, the specified modes and conditions of application are to be understood as the *expected operating conditions*. Conclusion suggests itself that under extreme conditions beyond the expected operating conditions operability is to be ensured by another property, i.e. *survivability*. But does any of the existing definitions of survivability fit this purpose? Let us examine the existing terminology of survivability of aeronautical structures and aircraft as a whole.

Currently, terminology of survivability is not represented in any Russian national standard. In the previous version of the above standard (GOST 27.002-89, [9]) the dependability terminology was covered in an annex, in which survivability was defined, but it was done so in three different ways, which did not contribute to a clear understanding of the term. Let us take a look at those definitions. Survivability is understood as:

1) property of an item that consists in its ability to resist the development of critical failures from defects and damage under the adopted system of service and repair,

or

2) property of an item to retain limited operability when exposed to effects not provided for by the operating conditions,

or

3) property of an item to retain limited operability in the presence of defects or damage of a certain type, as well as in case of failure of some components. An example would be the retaining of the carrying capacity by structural components affected by fatigue cracks whose size does not exceed the specified values.

That is a classification of sorts of the existing definitions of survivability. In the literature dedicated to the survivability of aeronautical structures all of the three above definitions are used to various extents, but the third one is the most common. Let us give examples of the survivability definitions of this type:

– survivability is the property of a structure to retain strength when damaged (including fatigue damage) [10],

– survivability is the property of a structure to perform its functions despite the sustained damage of various nature [11].

In accordance with these definitions, in case of any damage the operability of a structure will depend on its survivability. But a structure may sustain damage under expected operating conditions. That may be the case of partial failures caused, among other things, by design flaws, poor quality of structural components manufacture. Examples include fatigue failure of elements due to miscalculations of fatigue endurance or defects caused at the stage of manufacture of parts that prove to be stress raisers.

If a structure has redundant elements, i.e. its design complies with the principle of safe destruction, the remaining structural components will ensure design load accommodation and the structure as a whole will remain operable. But then the concept of survivability overlaps with the concept of reliability that is a component of dependability. In accordance with [8], *reliability* is a property of an item to continuously retain the ability to perform the required functions during a certain period of time or operation time in specified modes and conditions of application, i.e. under the expected operating conditions in terms of the Airworthiness Requirements. As it is known, component redundancy is one of the simplest ways of improving reliability. If one or even several parallel elements (in case of multiple redundancy) fail, the remaining elements will ensure the operability of the item or its system. Then, what is the difference between the above definitions of survivability and reliability? It is obvious that the difference can only be in the operating conditions, under which a defect or partial failure occurred. If it happened under the expected operating conditions, the operability must be ensured by the dependability (reliability), if it happened under extreme operating conditions beyond the expected conditions, the operability must be ensured by the survivability. But the above definitions of survivability say nothing about that.

Some papers use the term "damage tolerance (operational survivability)" along or instead of "survivability". The understanding of this term varies too. Let us examine the following definitions:

– damage tolerance (operational survivability) is a property that ensures normal performance of the specified functions by all systems of an aircraft in flight in case of failures or damage to individual assemblies, elements, units [12],

– damage tolerance (operational survivability) of aeronautical structures is a property of structures of an aircraft to ensure safe operation in terms of strength in case of partial or complete destruction of load-carrying elements due to fatigue, corrosion, accidental damage in operation, or damage caused in the process of manufacture and repairs [13].

In terms of their meanings, those definitions are no different from the above definitions of survivability, while the word "operational" is apparently used to indicate that in this case combat survivability is not implied – the latter being the kind of survivability associated with the effects of munitions – and only survivability in "normal" operation is covered.

But in some works [10, 11] the concept of "damage tolerance (operational survivability)" implies something different:

damage tolerance (operational survivability) is a generalized term that characterizes the properties of a structure and ways of ensuring its safety in terms of strength and includes the allowability of damage and safety of destruction (damage). *Allowability of damage* is a property of a structure and way of ensuring its safety in terms of strength by specifying the time of the first and subsequent inspections of the structure in operation in order to detect possible damage and repairs or replacement of the damaged element before the onset of such state, when degraded strength is unacceptable. *Safety of destruction (damage)* is a property of a structure and way of ensuring its safety in terms of strength by designing a structure in which, after possible significant damage or destruction of one of the main load-carrying elements, the residual strength, despite the structure being unrepaired, will not go below the allowed level over an interval of time, within which the damage (destruction) will be undoubtedly identified.

This definition is quite cumbersome and complex, but essentially it comes down to survivability being the property that ensures safety through the capability to resists the development of critical failures out of defects. This understanding of damage tolerance (operational survivability) can be attributed to the first type of definitions in the above classification of definitions of survivability. But in this case, it overlaps with the standardized definition of *fail-safety,* the property of an aircraft as a whole and/or its functional systems that characterizes the capability to ensure safe completion of the flight in the expected operating conditions in case of possible failures onboard [14].

Given the above, the second type of definitions of survivability appears to be the most logical and consistent. In [15], a definition is set forth that is the closest to the second type: survivability is the property of an airplane to retain its operability when affected by projectiles and off-design loads, as well as subject to the existence of accumulated damage.

If we remove "as well as subject to the existence of accumulated damage" from this definition, it can be deemed quite acceptable.

Thus, similarly to the above definition of dependability, survivability can be defined as follows:

survivability is the property of an item to retain in time the capability to perform the required functions under extreme conditions beyond the expected operating conditions under the specified methods of maintenance, storage and transportation.

Thus, any item or aircraft may be, among other things, either in the expected operating conditions, or in extreme operating conditions beyond the expected operating conditions. No third option exists. Under expected operating

conditions the operability of an item is the responsibility of dependability, while under extreme operating conditions it is the responsibility of survivability.

The concept of "damage tolerance (operational survivability)" has the right to exist as well. If we examine the definition of dependability and the above recommended definition of survivability, in both cases the specified methods of maintenance, storage and transportation are covered. But real operating conditions are characterized by a significant variety and instability due to the varied environmental conditions, level of training of the flight and maintenance personnel, physical infrastructure, organization of service and repair, etc. Thus, the methods and conditions of maintenance, storage and transportation of an item may differ from the specified ones. Due to that [16] introduced the concept of *operational dependability* that can be formulated as follows: the property of an item to retain in time the capability to perform the required functions under the expected operating conditions depending on the methods and conditions of maintenance, storage and transportation. Similarly to this definition the definition of *damage tolerance (operational survivability)* can be formulated as the property of an item to retain in time the capability to perform the required functions under extreme conditions beyond the expected operating conditions depending on the methods of maintenance, storage and transportation.

Thus, dependability and survivability are interrelated, yet clearly delimitated concepts each of which has its own area of responsibility.

In order to better understand this delimitation, let us examine the difference and correlation between the dependability and survivability using the probabilistic approach.

Probabilistic approach to the delimitation of the concepts of dependability and survivability of aeronautical structures

In order to ensure a better understanding of the differences and correlation between the concepts of dependability and survivability, let us use the approach described in [15].

Let use examine the indicator of operating efficiency of a transport aircraft that can be represented in the form of mathematical expectation:

$$W = W_0 P_{dep} P_{sur},$$

where W_0 is the initial efficiency indicator that is defined by the aircraft's functional properties (most importantly its performance), under conditions of its absolute dependability and survivability. That may be, for instance, the indicator of productive capacity [17] $W_0 = m_{pl} L/m_0$, where m_{pl} is the maximum mass of payload, L is the flight distance with the maximum mass of payload, m_0 is the maximum takeoff mass of the aircraft,

P_{dep} is the dependability indicator (probability of retained operability under the expected operating conditions),

P_{sur} is the survivability indicator (probability of retained operability under extreme conditions beyond the expected operating conditions).

The dependability indicator can be represented as the product of probabilities:

$$P_{dep} = P_a P_f P_{ff},$$

where P_a is the availability coefficient,

P_f is the probability of flight execution under conditions of the aircraft being operable,

P_{ff} is the probability of no-failure during the flight under the expected operating conditions.

Let us examine these probabilities.

In order to perform the flight mission, an aircraft must be initially in the up state which depends on its availability. Quantitatively, that is evaluated with the corresponding probability P_a named availability coefficient.

In order to perform the flight mission, an aircraft, being in the up state, must conduct the flight. That depends on many factors, including managerial ones, but if we only talk about the aircraft properties, that depends, for instance, on the capabilities of the flight and navigation equipment (capability to ensure flights in nighttime, in poor weather conditions). The capability to conduct a flight under conditions of the aircraft being operable is defined by the corresponding conditional probability P_f.

However, during a flight, *special situations* may arise as the result of the effect of adverse factors or their combinations that cause reduced flight safety [7], including accidents and crashes that prevent the flight mission performance. Adverse factors include failures, extreme operating conditions, crew errors and maintenance errors.

In this classification of adverse factors, failures are normally understood as disruptions of operability that occur under expected operating conditions. They may include failures caused by design flaws, poor quality of structural components and aircraft equipment manufacture. The possibility of such failures is estimated by the corresponding probability Q_{fl}, while the probability of no-failure under the expected operating conditions is identified according to formula:

$$P_{ff} = 1 - Q_{exp} Q_{fl}, \quad (1)$$

where Q_{exp} is the probability of an aircraft encountering expected operating conditions.

As an aircraft, as stated above, may be either in the expected operating conditions, or in extreme conditions beyond the expected operating conditions while no third option exists, the sum of the probabilities of an aircraft encountering such conditions must be equal to one:

$$Q_{exp} + Q_{ext} = 1,$$

whereQ_{ext} is the probability of an aircraft encountering extreme operating conditions.

Fortunately, $Q_{exp} >> Q_{ext}$, while $Q_{exp} \cong 1$, so in formula (1) it is usually omitted.

But failures may also be caused by an aircraft encountering extreme conditions beyond the expected operating conditions. In other words, failures may be caused by anomalous external effects (for instance, single gusts with the speed higher that the value specified in the Airworthiness Requirements, which can cause the destruction of structural components or appearance of permanent deformations, excessive continued air turbulence, whose parameters are also specified in the Airworthiness Requirements, which may cause premature depletion of operating life and, as consequence, fatigue failure of a structural component, effects of munition), crew error (for instance, hard touchdown or excess of maximum allowed value of maneuver load factor, which may cause the destruction of structural components or occurrence of permanent deformations) or maintenance error (for instance, damage to structural components as the result of careless performance of service and repair operations and, as consequence, premature fatigue failure). In this case mission performance relies on the survivability.

In accordance with [15], aircraft survivability is defined by the perishability and vulnerability. Let us make improvements to the definitions of these concepts in accordance with the above considerations. Then, *perishability* is the property of an aircraft that characterizes the possibility of it encountering extreme conditions beyond the expected operating conditions (the indicator of perishability is the probability of an aircraft encountering extreme operating conditions, Q_{ext}). *Vulnerability* is the property of an aircraft that characterizes the possibility of disruption of its operability as the result of effects beyond the expected operating conditions (the indicator of vulnerability is the probability of loss of aircraft operability under condition of effects beyond the expected operating conditions, Q_{vul}). Given the above, similarly to formula (1), the expression for the survivability indicator, i.e. probability of retained operability under extreme conditions, is as follows:

$$P_{sur} = 1 - Q_{ext}Q_{vul}.$$

Conclusion

In this paper, an attempt was made to unambiguously define the survivability of aeronautical structures. The obtained definition can be extended to an aircraft as a whole, as well as other complex technical objects.

There is no point in singling out the concept of combat survivability, since the effect of munitions is covered by the concept of the effects of adverse factors.

The advantage of the obtained definition of survivability consists in its clear difference from the standardized terms for dependability and fail-safety.

Additionally, the concept of damage tolerance (operational survivability) was proposed that was introduced similarly to the concept of operational dependability.

In the author's opinion there is a long-standing need to stipulate the concept of survivability in an appropriate national standard or at least issue an annex to GOST 27.002-2015 similar to an annex to the previously effective GOST 27.002-89, but taking into account the proposals made in this paper.

References

[1] Cherkesov GN, Nedosekin AO, Vinogradov VV. Functional survivability analysis of structurally complex technical systems. Dependability 2018;18(2):17-24. DOI:10.21683/1729-2646-2018-18-2-17-24.

[2] Cherkesov GN, Nedosekin AO. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy. Dependability 2016;16(2):3-15. DOI:10.21683/1729-2646-2016-16-2-3-15.

[3] Zarubsky VG. Organization features of functional diagnosis of a control computer with improved survivability. Dependability 2016;16(3):35-38. DOI:10.21683/1729-2646-2016-16-3-35-38.

[4] Yurkevich EV, Kriukova LN, Saltykov SA. Aspects of information support in ensuring the survivability of spacecraft under electrophysical effects. Dependability 2016;16(4):30-35. DOI:10.21683/1729-2646-2016-16-4-30-35.

[5] Klimov SM, Polikarpov SV, Fedchenko AV. Method of increasing fault tolerance of satellite communication networks under information technology interference. Dependability 2017:17(3):32-40. DOI:10.21683/1729-2646-2017-17-3-32-40.

[6] Smirnov NN, Chiniuchin YuM, Tarasov SP. Sokhranenie letnoy godnosti vozdushnykh sudov [Maintaining the airworthiness of aircraft]. Moscow: MGTU GA; 2005 [in Russian].

[7] Aviatsionnye pravila. Chast 25. Normy letnoy godnosti samoletov transportnoy kategorii: utv. Postanovleniem 23-ey sessii Soveta po aviatsii i ispolzovaniiu vozdushnogo prostranstva 5 sentiabria 2003 goda [Aviation rules. Part 25. Airworthiness Requirements for transport category airplanes: approved by Order of the 23-rd session of the Council for aviation and airspace management of September 5, 2003]. Moscow: Aviaizdat; 2004 [in Russian].

[8] GOST 27.002-2015. Industrial product dependability. Terms and definitions. Moscow: Standartinform; 2016 [in Russian].

[9] GOST 27.002-89. Industrial product dependability. General concepts. Terms and definitions. Moscow: Izdatelstvo standartov; 1990 [in Russian].

[10] Arepiev AN, Gromov MS, Shapkin VS. Voprosy ekspluatatsionnoy zhivuchesti aviakonstruktsiy [Matters of damage tolerance of aerostructures]. Moscow: Vozdushny transport; 2002 [in Russian].

[11] Butushin SV, Nikonov VV, Feygenbaum YuM, Shapkin VS. Obespechenie letnoy godnosti vozdushnykh sudov grazhdanskoy aviatsii po usloviam prochnosti [Insuring

the airworthiness of civilian aircraft in terms of strength]. Moscow: MGTU GA; 2013 [in Russian].

[12] Smirnov NN. Osnovy teorii tekhnicheskoy ekspluatatsii letatelnykh apparatov: Chast 2 [Fundamentals of aircraft maintenance: Part 2]. Moscow: MGTUGA; 2003 [in Russian].

[13] Svishchev GP, editor. Aviatsia: entsiklopedia [Aviation: encyclopedia]. Moscow: Bolshaia Rossiyskaia entsiklopedia; 1994 [in Russian].

[14] GOST R 56079-2014. Aircraft items. Flight safety, reliability, testability and maintainability. Indices nomenclature. Moscow: Standartinform; 2014 [in Russian].

[15] Antseliovich LL. Nadezhnost, bezopasnost i zhivuchest samoleta [Dependability, safety and survivability of an airplane]. Moscow: Mashinostroenie; 1985 [in Russian].

[16] Gerasimova ED, Smirnov NN, Poliakova IF. Ekspluatatsionnaia nadezhnost i rezhimy tekhnicheskogo obsluzhivania LA i AD [Operational dependability and maintenance conditions of aircraft and aircraft engines]. Moscow: MGTUGA; 2002 [in Russian].

[17] Sheynin VM, Kozlovsky VI. Vesovoe proektirovanie i effektivnost passazhirskikh samoletov. T. 2. Raschet tsentrovki i momentov inertsii samoleta. Vesovoy analiz [Weight design and efficiency of passenger airplanes. Vol. 2. Balance and moments of inertia calculation of an airplane. Weight analysis]. Moscow: Mashinostroenie; 1977 [in Russian].

About the author

Vadim V. Efimov, Doctor of Engineering, Associate Professor, Professor, Moscow State Technical University of Civil Aviation, Russian Federation, Moscow, e-mail: efimowww@yandex.ru

Received on: 19.11.2018

Original article
Dependability, vol. 19 no.2, 2019 DOI: 10.21683/1729-2646-2019-19-2-48-53

Economic assessment of the accidental risk of natural emergencies for train traffic

Vladimir G. Popov, *Russian University of Transport (MIIT), Russian Federation, Moscow*
Filipp I. Sukhov, *Russian University of Transport (MIIT), Russian Federation, Moscow*
Yulia K. Bolandova, *Russian University of Transport (MIIT), Russian Federation, Moscow*


Vladimir G. Popov


Filipp I. Sukhov


Yulia K. Bolandova

Abstract. Aim. *The paper is dedicated to the evaluation of the risk of transportation accidents caused by natural emergencies affecting train traffic on a specific line. The ever-growing anthropogenic burden on the environment inevitably causes climate change that, in turn, gives rise to higher numbers of extreme weather events. The latter usually cause industrial accidents and disasters. The assessment of the factors of climate-related risk that quantitatively characterize their effect on the railway infrastructure is the starting point of calamity risk management and adaptation of human activities to the ever-changing climate.* **Methods.** *The authors propose a method of risk assessment that takes into consideration the effect of various natural emergencies that affect rolling stock in motion. The method is based on elements of the probability theory and mathematical statistics. The developed method enables the assessment of the risk of a transportation accident caused by natural emergencies specific to not only a line, but a route on a railway network.* **Results.** *For the Nevinnomysskaya – Tuapse line that includes 6 sections of the North Caucasus Railway, one of which was damaged due to abundant precipitations on October 24 and 25, 2018, the risk of transportation accident caused by the effects of three types of natural emergencies on the sociotechnical system of this line has been calculated:*
– flood,
– hurricane with wind strength of over 22 mps,
– heavy rain.
The parameters of such emergencies are characterized by the following factors:
– frequency as compared to other types of emergencies,
– average annual number of natural emergencies,
– characteristic spatial scale of the natural emergency,
– characteristic duration of the natural emergency.
The conditional probabilities of the effects on the railway sociotechnical system of an event that has characteristic spatial scale and duration and has caused a transportation accident involving a train were estimated based on the assumption that a train flow in space follows the normal Erlang distribution of the k-th kind. The risk of transportation accident involving up and down trains travelling along the i-th line of the j-th railway caused by a hazardous effect of a natural emergency of the m-th type is identified subject to the jointness of events. Using the discounting method, an equation was obtained for estimating the mathematical expectation of economic damage by traffic safety disturbances, which allowed estimating the economic component of the risk. **Conclusions.** *As the result, a method is proposed for estimation of the risk of transportation accidents caused by natural emergencies, an example is provided of such risk estimation, including the economic component, for the Nevinnomysskaya – Tuapse line.*

Keywords: *accidental risk, accidents, emergencies, railway transportation, natural emergencies, railway freight transportation, traffic safety disturbances.*

For citation: *Popov VG, Sukhov FI, Bolandova YuK Economic assessment of the accidental risk of natural emergencies to train traffic. Dependability 2019;2: 48-53. DOI: 10.21683/1729-2646-2019-19-2-48-53*

Today's world statistics show growing damage caused by hazardous weather and climate events around the globe. The diagram (Figure 1) shows that 90% worst economic losses are caused not by geophysical phenomena, such as volcano eruptions, tsunamis and earthquakes, but meteorological, climate and hydrological events, i.e. floods, strong winds, heavy rains, hail, droughts [1].

Importantly, hazardous climate events can initiate industrial emergencies. Significant social and economic losses were caused by mudflows that accompanied a deep depression with showers between August 6 and 9, 2002 around Novorossiysk on the Black Sea coast of Russia. According to operational messages of the EMERCOM of Russia, on August 6 powerful mud-and-stone flows with the total volume over 15 ths. m^3 destroyed 300 meters of railway track between Sochi and Tuapse, as well as the nearby motorway. 47 passenger trains were blocked. According to preliminary estimations, direct economic damage amounted to USD 71 mln. [2].

As the result of abundant precipitations on October 24 and 25, 2018 (275-330 mm) in three municipalities of the Krasnodar Krai, harm was inflicted on two road bridges and one railway bridge, sections of the Tuapse – Maykop and Dzhubga – Sochi motorways, roadbed in the Tuapse – Krivenkovskaya and Tuapse – Adler railway lines. 36 passenger trains were cancelled and 39 were delayed.

Fault-free and safe operation of railway transportation largely depends on the climate conditions. The assessment of the factors of climate-related risk that quantitatively characterize their effect on the railway infrastructure is the starting point of calamity risk management and adaptation of human activities to the ever-changing climate.

Risk assessment consists in its quantitative measurement [3]. Quantitative estimation of risk requires the analysis of the probabilities of occurrence of hazards and consequences of such hazards' realization.

The main purpose of risk management in railway transportation consists in achieving and maintaining the acceptable level of risk while ensuring the functional safety of infrastructure facilities and rolling stock [4]. As of late, special emphasis is placed on the matters of dependability of rolling stock and development of systems and methods of risk estimation and management aimed at ensuring the safety of transportation processes [5-8]. However, the latest research into this matter examines the system of railway infrastructure operation separately from the environment. The authors propose a method of transportation accident risk assessment that takes into consideration the effect of various natural emergencies.

A transportation accident is understood as train wrecks, train accidents, as well as derailments and collisions of rolling stock that do not cause train wrecks and accidents in accordance with the classification of the Decree of the Ministry of Transportation of the Russian Federation no. 344 of December 18, 2014 [10].

Let us introduce the following notations for the purpose of characterizing natural emergencies:

C_j,i,m, an event that is a natural emergency of the m-th type that occurred in the Russian geographical region where the i-th line of the j-th railway is situated,

D_j,i,m, an event that characterizes the effect of a natural emergency of the m-th type (event C_j,i,m) on the sociotechnical railway system on the i-th line of the j-th railway and causes a transportation accident,

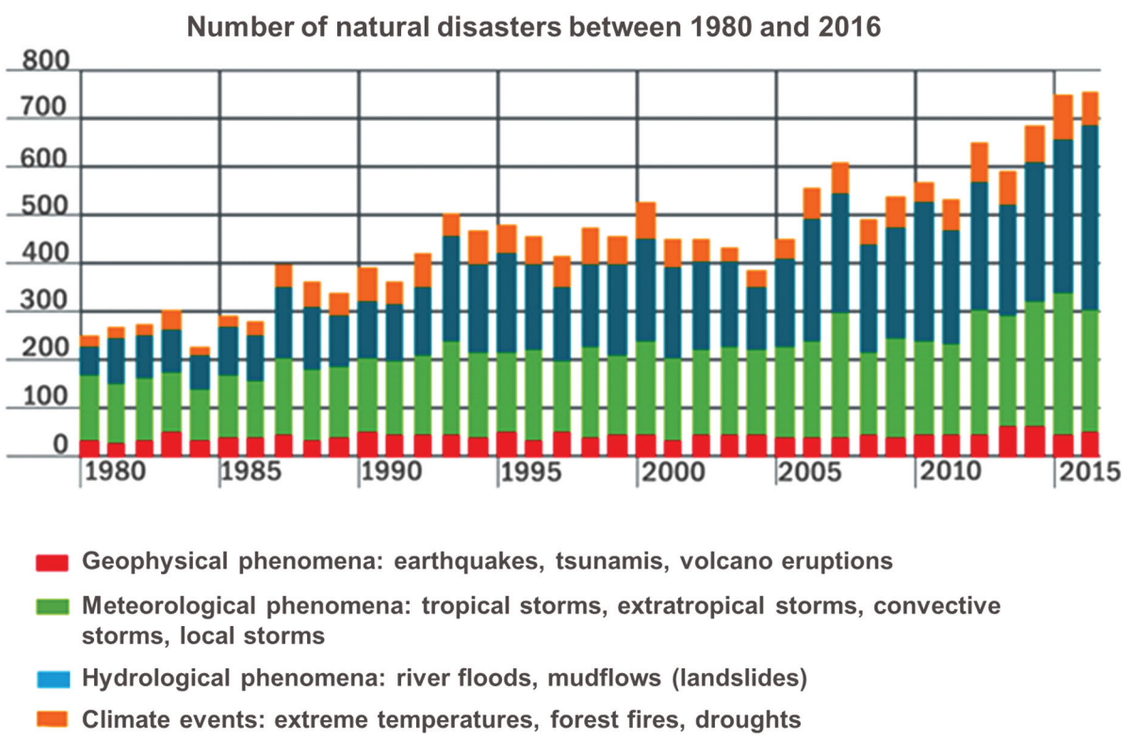


Figure 1. Number of natural disasters between 1980 and 2016

$B_j,i,m = D_j,i,m$ Ч C_j,i,m, a transportation accident [10] caused by the effect of a natural emergency of the m-th type on the sociotechnical railway system on the i-th line of the j-th railway,

N_j,i,m, the average yearly number of natural emergencies of the m-th type that occur in the Russian geographical region where the i-th line of the j-th railway (m = 1, 2, ..., M) is situated, 1/year,

L_j,i,m, the characteristic spatial scale of a natural emergencies of the m-th type that occurs in the Russian geographical region where the i-th line of the j-th railway (m = 1, 2, ..., M) is situated, km,

T_j,i,m, the characteristic duration of a natural emergency of the m-th type that occurs in the Russian geographical region where the i-th line of the j-th railway (m = 1, 2, ..., M) is situated, h,

We will estimate the probability of a transportation accident affecting an up train on the i-th line of the j-th railway caused by a natural emergency of the m-th type using the following formulas:

$$R''(B_{j,i,m}) = R''(D_{j,i,m} \times C_{j,i,m}) = \\ = P''(C_{j,i,m}) \cdot P''(D_{j,i,m} \left| C_{j,i,m}\right.), \quad (1)$$

where $P''(D_{j,i,m}\left|C_{j,i,m}\right.) = P''(L_{j,i,m}\left|C_{j,i,m}\right.) \cdot P''(T_{j,i,m}\left|C_{j,i,m}\right.)$.

$P''(C_{j,i,m})$ is the probability of occurrence in the specific geographical region of a natural emergency of the m-th type with the characteristic spatial scale L_j,i,m within the average time of presence of an up train on the i-th line with the length of $L_{j,i}$ [9],

$$P''(C_{j,i,m}) = 1 - \exp\left(-\frac{N_{j,i,m} \cdot t''_{j,i}}{365 \cdot 24}\right), \quad (2)$$

where $t''_{j,i} = L_{j,i} / V''_{j,i}$, $V''_{j,i}$ is the up service speed on the i-th line of the j-th railway,

$P''(L_{j,i,m}\left|C_{j,i,m}\right.)$ is the conditional probability of the effect on the sociotechnical railway system of event C_j,i,m with characteristic spatial scale L_j,i,m causing a transportation accident involving an up train on the i-th line of the j-th railway [9]

$$P''(L_{j,i,m}\left|C_{j,i,m}\right.) = 1 - \exp(-k_x \lambda''_x L_{j,i,m}) \sum_{k=0}^{k_x-1} \frac{(k_x \lambda''_x L_{j,i,m})^k}{k!}; \\ \lambda''_x = 1 \Big/ \Delta \bar{X}''_{j,i}, \quad (3)$$

where k_x is the kind of the standard Erlang distribution,

$\Delta \bar{X}''_{j,i} = V''_{j,i} \times \Delta \bar{T}''_{j,i}$ is the average spacing of up trains on the i-th line of the j-th railway, km,

$\Delta \bar{T}''_{j,i}$ is the average headway between up trains on the i-th line of the j-th railway, h,

$P''(T_{j,i,m}\left|C_{j,i,m}\right.)$ is the conditional probability of the effect on the sociotechnical railway system of event C_j,i,m with characteristic duration T_j,i,m that caused a transportation accident involving an up train on the i-th line of the j-th railway [9]

$$P''(T_{j,i,m}\left|C_{j,i,m}\right.) = 1 - \exp(-k_t \lambda''_t T_{j,i,m}) \sum_{k=0}^{k_t-1} \frac{(k_t \lambda''_t T_{j,i,m})^k}{k!}; \\ \lambda''_t = 1 \Big/ \Delta \bar{T}''_{j,i}, \quad (4)$$

where k_t is the kind of the standard Erlang distribution,

In formula (1) written to estimate the probability of a transportation accident involving a down train on the i-th line of the j-th railway $R'(B_{j,i,m})$, the corresponding values $P'(C_{j,i,m})$, $P'(L_{j,i,m}\left|C_{j,i,m}\right.)$, $P'(T_{j,i,m}\left|C_{j,i,m}\right.)$ are identified according to formulas similar to those for up trains subject to appropriate data.

Then, the probability $R(B_{j,i,m})$ of a transportation accident affecting up and down trains on the i-th line of the j-th railway caused by a hazardous effect of a natural emergency of the m-th type can be identified using the following formula (accounting for the jointness of events):

$$R(B_{j,i,m}) = R''(B_{j,i,m}) + R'(B_{j,i,m}) - R''(B_{j,i,m}) \times R'(B_{j,i,m}). \quad (5)$$

Out of formulas (1), (5), we can obtain the following estimates of the probability of a transportation accident affecting a moving train.

I. We will estimate the probability of a transportation accident affecting a train on the i-th line of the j-th railway caused by all possible natural emergencies of M types (m = 1, 2, 3, …, M) using the following formula:

for an up train

$$R''(B^M{}_{j,i}) = \sum_{m=1}^{M} \phi_m \cdot R''(B_{j,i,m}), \quad (6)$$

for a down train

$$R'(B^M{}_{j,i}) = \sum_{m=1}^{M} \phi_m \cdot R'(B_{j,i,m}), \quad (7)$$

for up and down trains

$$R(B^M_{j,i}) = R''(B^M_{j,i}) + R'(B^M_{j,i}) - R''(B^M_{j,i}) \cdot R'(B^M_{j,i}), \quad (8)$$

where ц$_m$ is the frequency of emergencies of the m-th type out of all the other types of emergencies, $\sum_{m=1}^{M} \phi_m = 1$,

$B^M{}_{j,i}$ is a transportation accident, an event that followed the effect of all possible M types of natural emergencies on the sociotechnical railway system on the i-th line of the j-th railway.

II. We will estimate the probability of a transportation accident affecting a train on I (i =1, 2, 3, …, I) lines of the j-th railway caused by a natural emergency of the m-th type using the following formulas:

for an up train

$$R''(B^I_{j,m}) = 1 - \prod_{i=1}^{I} [1 - R''(B_{j,i,m})], \quad (9)$$

for a down train

$$R'(B^I_{j,m}) = 1 - \prod_{i=1}^{I}[1 - R'(B_{j,i,m})], \quad (10)$$

for up and down trains

$$R(B^I_{j,m}) = 1 - \prod_{i=1}^{I}[1 - R(B_{j,i,m})], \quad (11)$$

where $B^I_{j,i}$ is a transportation accident, an event that followed the effect of a natural emergency of the *m*-th type on the sociotechnical railway system on *I* (*i* =1, 2, 3, …, *I*) lines of the *j*-th railway.

III. We will estimate the probability of a transportation accident affecting a train moving along *I* (*i* = 1, 2, 3, …, *I*) lines of the *j*-th railway caused by all possible natural emergencies using the following formulas:

for an up train:

$$R''(B^{I,M}_j) = 1 - \prod_{i-1}^{I}[1 - R''(B^M_{j,i})], \quad (12)$$

for a down train:

$$R'(B^{I,M}_j) = 1 - \prod_{i-1}^{I}[1 - R'(B^M_{j,i})], \quad (13)$$

for up and down trains:

$$R(B^{I,M}_j) = 1 - \prod_{i-1}^{I}[1 - R(B^M_{j,i})], \quad (14)$$

where $B^{I,M}_j$ is an event that followed the effect of all possible *M* types of natural emergencies of the sociotechnical railway system on *I* (*i* =1, 2, 3, …, *I*) lines of the *j*-th railway.

IV. We will estimate the probability of a transportation accident affecting a train on *I* (*i* = 1, 2, 3, …, *I*) lines of *J* (*j* = 1, 2, 3, …, *J*) railways caused by all possible natural emergencies using the following formulas:

for an up train

$$R''(B^{J,I,M}) = 1 - \prod_{j-1}^{J}[1 - R''(B^{I,M}_j)], \quad (15)$$

for a down train

$$R'(B^{J,I,M}) = 1 - \prod_{j-1}^{J}[1 - R'(B^{I,M}_j)], \quad (16)$$

for up and down trains

$$R(B^{J,I,M}) = 1 - \prod_{j-1}^{J}[1 - R(B^{I,M}_j)], \quad (17)$$

where $B^{J,IM}$ is a transportation accident, an event that followed the effect of all possible *M* types of natural emergencies on the sociotechnical railway system on *I* (*i* =1, 2, 3, …, *I*) lines of *J* (*j* = 1, 2, 3, …, *J*) railways.

If in formulas (9) to (14) for *I* we take all the lines of the *j*-th railway, we can obtain the corresponding estimates of accidental risk for the *j*-th railway as a whole (*j* = 1, 2, 3, …, *J*). If in formulas (15) to (17) we take *I* (*i* = 1, 2, 3, …, *I*) lines of *J* (*j* = 1, 2, 3, …, *J*) railways, we can obtain the corresponding estimates of accidental risks for various routes.

For the economic assessment of the consequences of transportation accidents let us use the information set forth in [11–16]. According to [10], transportation accidents, i.e. traffic safety disturbances (TSD) are subdivided into train wrecks, B_1, train accidents, B_2, transportation accidents (derailment or collision without consequences in the form of train wreck or train accident), B_3.

Using the discounting method [11] and statistical data of [12, 13], we can write the estimation equation of the mathematical expectation of economic damage caused by TSD as B_n ($B_n = B_1, B_2, B_3$):

$$Y(B_n) = Y_0(B_n)(1 + r)^p, \quad (18)$$

where $Y_0(B_1) = 2 \cdot 10^6$ rubles, $Y_0(B_2) = 0.5 \cdot 10^6$ rubles, $Y_0(B_3) = 7 \cdot 10^3$ rubles are the average values of economic damage caused by one event of types B_1, B_2, B_3 in 2000 rubles,

$p = Y - 2000$ is the conventional year,

Y is the calendar year of risk analysis,

r is the rate of discounting (*r* = 0.1–0.12).

The practical impossibility of predictive estimation of the economic damage caused by TSD of type B_n associated with the effect of natural emergencies on sociotechnical railway systems and causing transportation accidents involving moving trains forces us to resort to using conservative assumptions and a posteriori statistical data on the TSD that affect trains. Given the above, the equation can be written as follows:

$$Y(B) = \sum_{n=1}^{3} \alpha_n \cdot Y(B_n), \quad (19)$$

where α_n is the relative rates of TSD of type B_n ($n = 1, 2, 3$) that according to [14, 16] can be estimated as $\alpha_1 = 0.01$, $\alpha_2 = 0.1$, $\alpha_3 = 0.89$.

Then, the economic estimate of the risk of transportation accident affecting a train on the *i*-th line of the *j*-th railway caused by a natural emergency of the *m*-th type can be obtained using the following formulas:

$$\begin{aligned} &\text{up } R''_E(B_{j,i,m}) = R''(B_{j,i,m}) \cdot Y(B), \\ &\text{down } R'_E(B_{j,i,m}) = R'(B_{j,i,m}) \cdot Y(B), \\ &\text{up and down } R_E(B_{j,i,m}) = R(B_{j,i,m}) \cdot Y(B). \end{aligned} \quad (20)$$

The economic estimate of risks for cases $B^I_{j,m}$; $B^{I,M}_j$; $B^{I,J,M}$ (for *I* lines in one railway or *J* railways) can be obtained similarly by multiplying the corresponding probability of a transportation accident (formulas (6) – (17)) by the size of damage *Y*(*B*).

Let us estimate the probability of transportation accident $R(B^M_{j,i})$ involving trains on the Nevinnomysskaya – Tuapse line of 6 sections (*i* = 1, 2, 3, …, 6) of the North Caucasus Railway caused by the effect of three types of natural emergencies below on the sociotechnical system:

– flood (*m* = 1), frequency as compared to other types of emergencies $ц_1 = 0.06$, average annual number $N_1 = 1$, characteristic spatial scale $L_1 = 15$ km, characteristic duration $T_1 = 1$ h,

Table 1. Calculation data of transportation accident probability

i	Name of line	Length of line, km	Amount of traffic, trains per day	Flood (m = 1; φ_1 = 0.06; N_1 = 1; L_1 = 15; T_1 = 1)	Hurricane with wind strength not less than 22 mps (m = 2; φ_2 = 0.11; N_2 = 2; L_2 = 300; T_2 = 120)	Heavy rain (m = 3; φ_3 = 0.83; N_3 = 15; L_3 = 1; T_3 = 3)	Probability $R(B^M_{j,i})$
				Probability $R(B_{j.i.m})$	Probability $R(B_{j.i.m})$	Probability $R(B_{j.i.m})$	
1	Nevinnomysskaya – Armavir Rostovsky	77	46	$1.506 \cdot 10^{-4}$	$9.058 \cdot 10^{-4}$	$1.028 \cdot 10^{-9}$	$1.087 \cdot 10^{-4}$
2	Armavir Rostovsky – Kurgannaya	40.5	40	$5.165 \cdot 10^{-5}$	$4.765 \cdot 10^{-4}$	$2.122 \cdot 10^{-10}$	$5.552 \cdot 10^{-5}$
3	Kurgannaya – Belorechenskaya	63.8	41	$8.830 \cdot 10^{-5}$	$7.506 \cdot 10^{-4}$	$3.944 \cdot 10^{-10}$	$8.786 \cdot 10^{-5}$
4	Belorechenskaya – Komsomolskaya	19.8	42	$2.961 \cdot 10^{-5}$	$2.33 \cdot 10^{-4}$	$1.44 \cdot 10^{-10}$	$2.741 \cdot 10^{-5}$
5	Komsomolskaya – Krivenkovskaya	87.6	42	$1.31 \cdot 10^{-4}$	$1.03 \cdot 10^{-3}$	$6.361 \cdot 10^{-10}$	$1.212 \cdot 10^{-4}$
6	Krivenkovskaya – Tuapse	18.2	77	$8.89 \cdot 10^{-5}$	$2.142 \cdot 10^{-4}$	$7.187 \cdot 10^{-9}$	$2.89 \cdot 10^{-5}$

– hurricane with wind strength over 22 mps (m = 2), frequency as compared to other types of emergencies $ц_2$ = 0.11, average annual number of natural emergencies N_2 = 2, characteristic spatial scale L_2 = 300 km, characteristic duration T_2 = 120 h,

– heavy rain (m = 3), frequency as compared to other types of emergencies $ц_3$ = 0.83, average annual number of natural emergencies N_3 = 15, characteristic spatial scale L_3 = 1 km, characteristic duration T_3 = 3 h.

The calculation data is given in Table 1.

Using formula (14), let us estimate the probabilities of a transportation accident involving trains on 6 (i = 1, 2, 3, …, 6) lines of the North Caucasus Railway (j = 1) caused by three hazardous states (M = 3) of environmental objects: $R(B^{6.3}_1) = 4.295 \cdot 10^{-4}$. The mathematical expectation of the economic damage of TSD calculated as of 2019 will amount to $Y(B)$ = 429474.42 rub (formula (19)).

Then, the estimate of the economic risk of a transportation accident involving a train traveling on 6 (i = 1, 2, 3, …, 6) lines of the North Caucasus Railway (j = 1) will be (similarly to formula (20)):

$$R_E(B_j^{I,M}) = R(B_j^{I,M}) \cdot Y(B) = R(B_1^{6,3}) \cdot Y(B) =$$
$$= 24,295 \cdot 10^{-4} \cdot 429474,42 \cong 184,45 \text{ rub.}$$

If, for instance, we consider the case of transportation of 1 t of hazardous freight on this route that amount to approximately 6000 rub, the obtained economic estimate can be considered as the amount of coverage for the purpose of risk management (risk treatment) by means of transfer.

References

[1] Katsov V.M., editor. Doklad o klimaticheskikh riskakh na territorii Rossiyskoy Federatsii [Report on the climate-related risks in the Russian Federation]. Saint Petersburg; 2017 [in Russian].

[2] Ragozin A.L., editor. Otsenka i upravlenie prirodnymi riskami: tematicheskiy tom [Assessment and management of natural risks: a subject-matter publication]. Moscow: Izdatelskaya firma KRUK; 2003 [in Russian].

[3] Akimov V.A., Lesnykh V.V., Radaev N.N. Osnovy analiza i upravleniya riskom v prirodnoy i tekhnogennoy sferakh [Basics of the natural and man-made risk analysis and management]. Moscow: Delovoy ekspress; 2004 [In Russian].

[4] GOST 33433-2015. Functional safety. Risk management on railway transport. Moscow: Standartinform; 2016 [in Russian].

[5] Volodarsky V.A., Orlenko A.I. On the dependability of reconditioned rolling stock. Dependability. 2015;1(52):29-31.

[6] Zamyshliaev A.M., Ignatov A.N., Kibzun A.I., Novozhilov E.O. Functional dependency between the number of wagons derailed due to wagon or track defects and the traffic factors. Dependability 2018;18(1):53-60.

[7] Dayev Zh.A., Nurushev E.T. Application of statistical criteria for improving the efficiency of risk assessment methods. Dependability 2018;18(2):42-45.

[8] Aksenov V.A., Raenok D.L., Zavyalov A.M. Improving the system of risk management to ensure the safety of production processes. Dependability 2013;(3):112-120.

[9] Popov V.G., Sukhov F.I., Bolandova Yu.K. Accidental risk assessment of train movement consequently the impact of natural emergencies in the environment. Science and Technology in Transport 2018;4:115-120 [in Russian].

[10] Decree of the Ministry of Transportation of the Russian Federation no. 344 of December 18, 2014 On the approval of the regulations on the classification, procedure of investigation and registration of transportation accidents and other events caused by violations of rules of traffic safety and operation of railway transport (Registered by the Ministry of Justice of the Russian Federation on 26.02.2015, no. 36209).

[11] Legasov V.A., Demin V.F., Shevelev Ya.V. Diskontirovanie i kompromiss mezhdu pokoleniyami [Discounting and compromise between generations]. Issues of Risk Analysis 2005;2(2):141-146 [in Russian].

[12] Kraskovsky A.E. Ekonomicheskie mekhanizmy upravleniya bezopasnostyu dvizheniya [Economic mechanisms of traffic safety management]. Zheleznodorozhny transport 2002;5:29-33 [in Russian].

[13] Popov V.G., Sukhov F.I. Indeks prognoz and indeks otklik [Prediction index and response index]. World of Transport and Transportation 2007;5(3):130-133 [in Russian].

[14] Popov V.G., Petrov S.V. Metod otsenki urovnya bezopasnosti dvizheniya i avariynogo riska pri perevozke gruzov po zheleznym dorogam [Method of assessment of traffic safety and accidental risk associated with carriage of goods by rail]. Transport: science, equipment, management 2008;7:1-5 [in Russian].

[15] Popov V.G., Petrov S.V. Metod otsenki avariynogo riska pri perevozke nefti i nefteproduktov po zheleznym dorogam [Method of assessment of accidental risk associated with the rail transportation of oil and petroleum products]. Life safety 2010;11:39-43 [in Russian].

[16] Popov V.G., Sukhov F.I., Petrov S.V. Accident risk assessment. World of Transport and Transportation 2012;6;150-155 [in Russian].

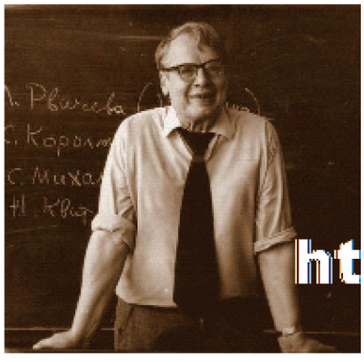
About the authors

Vladimir G. Popov, Doctor of Engineering, Professor, Head of Department of Chemistry and Ecological Engineering, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: vpopov_miit@mail.ru

Filipp I. Sukhov, Candidate of Engineering, Senior Lecturer, Department of Chemistry and Ecological Engineering, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: philipp.sukhov@mail.ru

Yulia K. Bolandova, post-graduate student, teaching assistant, Department of Chemistry and Ecological Engineering, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: jbolandova@gmail.com

Received on: 17.12.2018



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: 109029, Moscow, Str. Nizhegorodskaya, 27, Building 1, office 209, 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: evgenya.patrikeeva@yandex.ru

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