Original article
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. $C(\overline{P})=\min C(\overline{P})$; $\overline{P}=\left\{P_1, P_2, \ldots, P_i, \ldots P_N\right\}$, or $M(\overline{P})=\min M(\overline{P})$; $\overline{P}=\left\{P_1, P_2, \ldots, P_i, \ldots P_N\right\}$ 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 $\Phi(\overline{P})$, i.e. $\Phi(\overline{P})=\max \Phi(P)$ if $C(\overline{P}) \leq C_0$ or $\Phi(\overline{P})=\max \Phi(P)$ if $M(\overline{P}) \leq M_0$. 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 $\Phi(\overline{P})$, i.e. $B=\Phi(\overline{P})$,then condition $B=\Phi(\overline{P}) \geq P_B$. Is verified. If it is fulfilled, the problem is solved, if not, the solution continues starting from vector $P=\overline{P}_B$, 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 $R_1 = 1-\left(1-R_{10}\right)\exp\left[-\alpha_1\left(C_1-C_{10}\right)\right]$ is the dependability component, that takes into consideration the effect of components failure subject to redundancy, $R_2 = 1-\left(1-R_{20}\right)\exp\left[-\alpha_2\left(C_2-C_{20}\right)\right]$ is the dependability component that takes into consideration the quality level of manufacture and quality assurance, $R_3 = 1-\left(1-R_{30}\right)\exp\left[-\alpha_3\left(N_{ed}-N_{ed0}\right)\right]$ 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}, $N_{\text{от}0}$ 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 $\gamma = P\left\{N_{\text{s}} \geq N_{req}\right\}$. Each solution is defined by the vector of components R_1, R_2, R_3 or corresponding costs C_1, C_2, $N_{\text{от}}$, which unambiguously defines level R. For the specified γ and N_{req} subject to known R the number of manufactured SC $N_{\text{G}} = f\left(N_{req}, \beta, R\right)$ can be clearly identified that guarantees successful mission completion. The total costs of program implementationC_Σ can be identified using the dependence $C_\Sigma = \left(C_1+C_2\right)\left(N_{ed}+N_G\right)$. 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 $N_{\text{s}} \geq N_{\text{req}}$ 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 $N_{\text{s}} = i$ 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

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

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

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

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

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

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

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 $P\left\{W_1\right\} \geq \gamma$ [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 $\phi : R \rightarrow N$.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 $C_{\Sigma\,\text{min}}$, 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

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

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 ($N_{\text{req}} > 10^3$) 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 ($N_{\text{req}} > 10^2$) 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}: $\gamma = \gamma_{\text{as}}\gamma_{\text{ap}}$. 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:

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

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:

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

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, $N_{\text{G}}$for the level of guarantee $\gamma = 0.9$ 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 $R_{\text{as}} = f(C)$ 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 computing, 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