Dependability, vol. 18 no.4, 2018 Original article
DOI: 10.21683/1729-2646-2018-18-4-28-35

What should mean dependability calculation of unique highly vital systems with regards to single-use mechanisms of spacecraft

Yuri P. Pokhabov, *Joint Stock Company NPO PM – Maloe konstruktorskoye buro, Zheleznogorsk, Krasnoyarsk Krai, Russia*

Yuri P. Pokhabov

Aim. *Calculations are an integral part of the development of any complex technical object. Normally, they are subdivided into the calculations to confirm product operability (kinematic, electrical, thermal, strength, hydraulic and pneumatic systems analysis, etc.) and calculations to confirm its dependability (calculation of reliability, longevity, maintainability, storability and other indicators). As it is understood and provided in statutory documents, dependability calculation involves procedures of identification of an object's dependability indicators using methods based on their calculation using reference information on the object's components dependability, on the dependability of analog objects, on the properties of the materials and other information available at the time of calculation. However, in the case of development of unique highly vital systems, obtaining statistical data for dependability calculation is impossible due to two conflicting conditions, i.e. the limited number of produced objects and the requirement of high accuracy of the input information. Nevertheless, in the author's opinion dependability calculations must be performed. The only question is how to calculate the dependability and what such calculation should mean.* **Methods.** *In the classic dependability theory, the conventional understanding of probability of no-failure is the frequency of failures in time, yet for unique highly vital systems the failure rate must tend to zero over the entire period of operation (preferably, there should be no failures at all). For this reason the concept of "failure" in the context of unique highly vital systems should probably be interpreted not as an event, i.e. any fact, which as a result of experience can occur or not occur, but as possible risk, i.e. an undesirable situation or circumstance that is characterized by the probability of occurrence and potentially negative consequences. Then, an event in the form of a real or potential failure in operation can be associated with a risk in the form of probability of failure with negative consequences, which in terms of the consequences is equally unacceptable with regard to unique highly vital systems. In this case dependability calculation can be reasonably substituted with risk assessment, a process that encompasses risk identification, risk analysis and comparative risk assessment. Thus, risk assessment enables the achievement of the target dependability directly by substantiating the stability of manifestation of a specific product's properties and not indirectly through undependability caused by failures of analog products.* **Results.** *The paper shows the procedure of risk assessment for unique highly vital systems. Using the example of a mechanical system with actuated parts represented by a spacecraft single-section pivoted rod the risk assessment procedures are shown. The feasibility of risk assessment with the use of design engineering analysis of dependability is demonstrated.* **Conclusions.** *It is shown that the absence of statistical data on the dependability of analogs of unique highly vital systems does not prevent dependability calculation in the form of risk assessment. Moreover, the results of such calculations can be a source and guidelines for adopting design and process engineering solutions in the development of products with target dependability indicators. However, legalizing the method of such calculations requires the modifications of the technical rules and regulations to allow for dependability calculation by other means than with the use of statistical data on the failures of analogs.*

Keywords: *unique highly vital system, calculation, dependability calculation, risk assessment, design engineering dependability analysis.*

For citation: *Pokhabov YuP. What should mean dependability calculation of unique highly vital systems with regards to single-use mechanisms of spacecraft. Dependability 2018;18(4): 28-35. DOI: 10.21683/1729-2646-2018-18-4-28-35*

Introduction

The development of any complex technical products is impossible without calculations, i.e. *establishment and calculation of required data* [1]. Calculations in the form of ***documents*** *that contain calculations of parameters and values, e.g. dimension chain calculation, strength calculation, etc.*, are part of the list of design documentation per GOST 2.102. The codes and forms of calculations for engineering products are defined in the OST 92-0290 industry standard. For instance, according to GOST 2.119 the calculations are in general subdivided into the calculations to confirm product operability (kinematic, electrical, thermal, strength, hydraulic and pneumatic systems analysis, etc.) and calculations to confirm its dependability (calculation of reliability, longevity, maintainability, storability and other indicators). In technical rules and regulations (GOST 27.301 and GOST 27.410) dependability calculations are understood as only *procedures of identification of an object's dependability indicators using methods based on their calculation using reference information on the object's components dependability, on the dependability of analog objects, on the properties of the materials and other information available at the time of calculation.* Importantly, the availability of dependability calculations based on reference data on the dependability of analogs involves legal and financial implications in the context of insurance of the risks of loss of objects [2]. However, in the case of development of unique highly vital systems, obtaining statistical data for dependability calculation is impossible due to two conflicting conditions, i.e. the limited number of produced objects and the requirement of high accuracy of the input information. Despite the opinion that there is no need for dependability calculations for failsafe systems and they should be substituted with ensuring compliance with qualitative criteria of dependability [3], in the author's opinion dependability calculations as part of UHVC development are not optional. The only question is how to calculate dependability and what such calculation should mean.

The relevance of UHVC dependability calculation can be observed using the example of operation of single-use mechanisms of spacecraft. The efficiency of spacecraft operation in orbit wholly depends on the successful deployment of the solar panels and space antennas (reflectors), whose cost accounts for a negligible part of the total cost of the spacecraft and its placing into orbit. Experimental confirmation of dependable deployment is impossible due to high reliability requirements (0.9995 and higher) and unique environmental conditions of the deployment in orbit that cannot be accurately replicated as part of ground-based experimental activities. At the same time, practically any error in the design and manufacture of the deployment mechanisms may cause a failure that can entail the loss of the spacecraft. Therefore in this case dependability is largely defined by the calculations.

Approaches to the dependability calculation

Since failures of UHVC cause losses far greater than the cost of their creation [4], the dependability is characterized by the reliability and is defined by the indicator of probability of no-failure (PNF), i.e., *the probability that within the specified operation time no failure of the object occurs* [5, 6]. In the classic dependability theory PNF is normally understood as the frequency of failures in time, yet for the UHVC the failure rate must in theory tend to zero over the entire period of operation (preferably, there should be no failures at all). For this reason the concept of "failure" in the context of UHVC should probably be interpreted not as an **event**, i.e. *any fact, which as a result of experience can occur or not occur* [7], but as possible **risk**, i.e. *an undesirable situation or circumstance that is characterized by the probability of occurrence and potentially negative consequences* [8]. For single-use mechanisms of spacecraft we should talk of the risk as the *effect of uncertainty on the goals*, where uncertainty is understood as *"the state of complete or partial absence of information required for the understanding of an event, its consequences and their probabilities"* [9]. Then, an **event** in the form of a real or potential failure in operation can be regarded as a **risk** (probability of failure with negative consequences), which in terms of the consequences for UHVC is equally unacceptable. In this case **dependability calculation** can with no damage to the meaning be substituted with **risk assessment**, a *process that encompasses risk identification, risk analysis and comparative risk assessment* [10]. Importantly, risks of failure have no aspect of frequency, yet the risk assessment allows predicting the development scenarios of undesired situations that may cause failures and using such estimates in the adoption of engineering solutions as part of the UHVC development process. Thus, risk assessment enables the achievement of the target dependability directly by substantiating the stability of manifestation of a specific product's properties [11] and not indirectly through undependability caused by failures of analogs [12].

The departure from the understanding of an "event" as a fact of *disturbance of an object's operability* [5, 6] in the context of dependability calculation gives sensitivity to the concept of "dependability" in terms of its terminological definition. In the author's opinion, the shift of the standard definition of the term "dependability" to the functional interpretation diverts from an understanding of dependability other than that adopted in the current mathematics of the dependability theory. The use of the concept of "function" in the terminological definition of dependability as the requirements *established in the regulatory, design, project, contract and* ***other documentation*** *for an object* [6] causes the abstraction of the physical processes occurring within products and consequently does not encourage risk analysis. For example, in the organizational and engineering documentation, the deployment of folding spacecraft in orbit is considered as a function that enables the spacecraft's preparation to operation within the specified service life, but at the physical level it is achieved through planned and consistent operation of a set of design components that enable the performance of such function. The functional definition of dependability actually makes "invisible" the operation of structural components that ultimately ensure dependable performance of the function of deployment of spacecraft's folding structures.

In the author's opinion, the definition of dependability as the *property of a system to maintain in time and within the set limits the values of all parameters* ***and/or indicators*** *that characterize the system's ability to perform the required functions in specified modes and conditions of operation, maintenance, storage and transportation* [13] provides a uniform understanding (self-consistency) of the parametric and functional definition of dependability [14] and enables dependability estimation both in terms of the classic dependability theory and in terms of analysis of the risks of failure. This becomes doable due to the fact that it is now possibility to consider dependability as a physical value with intrinsic simple and/or essential properties that can be expressed in parametric or non-parametric models through parameters and/or indicators [11].

The method of analysis of risks related to UHVC failures is based on the principles of physicality (causal connections) and physical necessity (consistency with the laws of nature) of the causes of failures. The task of the risk analysis while using the above principles becomes the analysis and synthesis of the simple properties that make the (essential) property of dependability, which becomes possible in the context of A.I. Uiomov's paradigm of the triunity of things, their properties and relations [15] and extended interpretation of the concept of "relation" as the mutual spatial arrangement, interrelation and interaction of things [11]. The connection between the parametric and non-parametric nature of properties' manifestation becomes evident if the term "operation" given in the now obsolete GOST 22487 standard is used, i.e. *"execution in the object (system) of a process (processes) according to the specified algorithm and (or) manifestation of specified properties by the object"*. In this case functions prescribed by the organizational and engineering documentation [6] at the physical level can be represented as the manifestation by an object of the specified properties in accordance with the specified algorithm of the performed process. This circumstance is extremely important in the context of technical systems, where during operation a number of properties can manifest themselves simultaneously of sequentially causing performance or non-performance of the functions specified in the organizational and engineering documentation.

This approach extends the capabilities of the classic dependability theory that is applied in strength calculations of dependability enabling additional evaluation of products' operation based on the mechanical, kinematic, energy, electrical and other parameters [16]. As at some hierarchical level physical properties are independent (e.g. the properties of strength and electrical conductivity), when examining any of the properties identified by the risk analysis it becomes possible to use either the deterministic or stochastic approach in the quantitative estimation of a specific dependability property under consideration.

Unlike classic dependability calculation, risk assessment enables the elimination of ambiguity in the product development process, i.e. taking into consideration the fact that the designer's idea must be reflected in the design documentation in a way that ensures that this idea is clear to the persons not involved in the design process and not familiar with the original ideas without additional explanations and comments and most importantly without the loss of meaning. Typically, ambiguity stems from the perception of the term "operable state" that is defined as the *state of an object in which it is able to perform the required functions* [6]. Taking into account the explanation of the understanding of the concept of function in the term "dependability" given in the national standard, it is not possible to qualify the operable state as sufficient for the performance of a product's intended function. The situation is somewhat clarified by the explanation of the term "operable state", according to which it can be defined as a *state of an object in which the values of all parameters that characterize the ability to perform the specified functions comply with the requirements of the documentation for such object* [6]. This certainly is a more specific definition of the operable state for a complex technical object, but it also has serious inaccuracies. First, for UHVC the requirement in the documentation must be necessary and sufficient, but the national standard does not clarify how to achieve that, which undoubtedly increases the role of the human factor in the development process (some people believe that the requirements are sufficient for achieving the object's operable state, some people don't). Second, the primary document for the products' manufacture is the design documentation and not *another documentation*, as the same standard puts it. In this sense the abandonment of the previous definition of the term "operable state" [5] that clearly specified design documentation in no way contributes to the reduction of the role of the human factor (due to less precise definitions).

Example and sequence of risk assessment

Let us examine an example of risk assessment in its standard form. In accordance with the definition of the term "risk assessment" [10], at the first stage the *risk identification* is performed, which consists in the identification of the source of risk and possible causes of failure. At this stage the product functionality is identified at the physical level in accordance with GOST 28806 in the form of *availability and specific properties of a set of functions capable of satisfying the specified or assumed needs.* The aim of this procedure is to provide the formal description of failures as hypothetical situations that prevent the performance of the functions under consideration. It is assumed that each potential failure is due to causes that directly engender them, that appear, exist and develop within the conditions of the environment as a set of external factors and operating modes in view of the worst possible combinations. Obviously, each type of failure can have several causes at once. The identified possible causes of failures as a whole are the foundation of a check list of risk identification. It must be understood that the risk identification procedures define the completeness of the identified object functionality and must be performed by qualified experts, as the results of such procedures fill-up the check list and ultimately serve as the criteria for the establishment of the obligatory and sufficient requirements in the design documentation.

At the next stage of risk assessment analysis is performed that generates the information background for the comparative risk assessment and adoption of decision regarding their sources. The procedures of risk analysis follow a specific algorithm in strict compliance with the general logic of actions according to the check list (in this case the identified causes of failure are the starting point for any subsequent actions related to risk analysis and assessment):

• properties of the critical components are identified, whose presence makes each cause of failures impossible,

• each property of critical components is defined quantitatively based on parameters (indicators),

• for each parameter (indicator) a range of allowed values is defined based on the requirements of the design specifications (the customer's idea of the product) and product build (the developer's idea of the product design),

• the value of each parameter within the allowed range is substantiated by calculations and experiments in terms of operability and dependability,

• dependability is evaluated by method of dependability structure diagram in order to confirm the fact that the selected values of the parameters (indicators) comply with the specification requirements,

• operability conditions are verified for parameter values compliance with the requirements of the norms, specifications and design documentation (for each parameter there must be a corresponding requirement for manufacture and/or operation, whose performance can be verified by means of maintenance inspection),

• risks are identified that are associated with failures as the result of absence of requirements in the detailed design and process engineering documentation "as is".

• probability is analyzed of failures associated with the underestimation of design and/or process engineering errors made during the development of the detailed documentation for adoption of the final decision on the compliance of the design and detailed documentation with the specified dependability requirements.

At the final stage of risk assessment the value of identified probability of failure is compared with the specified reliability requirements and, if necessary, actions are taken to reconsider the engineering solutions and/or establishment of additional requirements in the detailed documentation.

An example of risk assessment

As a specific example of risk assessment let us examine a mechanical system with actuated parts represented by a spacecraft single-section pivoted rod that for some time is fixed on the resting surface with a locking device, then the mechanical constraints in the lock are removed, the rod, by the action of actuators, is deployed to the specified angle, locks in the end position and starts operating as a panel with specified performance parameters [4]. The reliability of rod operation is ensured by sequential performance by its structural components of their assigned functions that consist in the manifestation of the strength of the rod under load in the locked position, prevention of spontaneous removal of mechanical constraints in the lock, transmission of electrical signal to the electric fuses of pyro cartridges upon command, pyro cartridge firing, removal of mechanical constraints in the lock, separation of the rod from the resting surface, rod rotation through the specified angle, locking and specified operation of the rod in the service position. The structural components of the rotating rod during deployment must sequentially perform all of the above functions in the assigned conditions and modes of operation. Failure to deploy the rod may be due to the failure of any of the functions or a combination of causes that may be defined not so much by the conditions and modes of operation as a combination of adverse factors.

As an example, let us examine the function of rod rotation through the specified angle with the deployment actuator. Failure of the above functions may be caused by the following conditions: non-activation or breakdown of the actuator (failure to activate), absence of required reserve of drive moment (deceleration), disappearance of radial clearance in the joint (joint locking), disappearance of axial clearance in the articulated joint (wedging), sudden appearance of obstacles in the rod's path (catching).

Obviously, each of the causes of failures can be countered by solutions and/or actions of the rod developer that provide its design with such critical component properties that would enable unconditional fulfillment of the assigned functions. For instance, to prevent or attenuate the consequences of:

• failure to activate the actuator it is required to ensure the limit probability of its faultless operation by means of redundancy of critical components,

• deceleration of the rod, creating a sufficient reserve of drive moment relative to the moment of resistance forces in its path by selecting the correct power performance of the actuator,

• joint locking. Choosing such radial clearances in the bearing as to ensure rotation freedom subject to possible changes in the thickness of the layer of solid lubricant and thermal deformation,

• wedging in the articulated joint, making provisions for thermal decoupling in the direction of the bearing's axis of rotation,

• catching of the rod, eliminating all possible obstacles in the rod's path caused by the gravity-free environment, kinematics of the motion or design of adjacent structures.

The quantitative estimation of the conditions of operability per each identified property of critical components involves choosing a parameter (indicator) that fully characterizes the property in question and the corresponding allowed range of deviation [16]. The range of allowed deviation of the parameters (indicators) will be defined by the requirements of the design specifications (external parameters) or by the internal design parameters (selected materials, layout and force diagrams, manufacturing processes, etc.) [17].

Let us cite the parameters (indicators) and their allowed ranges that correspond to the unconditional fulfillment of the function of rod rotation through the specified angle in the form of conditions that prevent or attenuate the consequences of the causes of failures for the following risks under consideration:

1) failure to activate the actuator

$$\mathrm{P}_d \geq P_{lim}, \tag{1}$$

where P_d is the probability of activation (operation) of actuator; P_{lim} is the probability of fault-free operation of actuator in accordance with the distribution of the assigned requirement of rod dependability indicator per structural components

2) deceleration of the rod

$$M_d > M_c, \tag{2}$$

where M_d is the drive moment developed by the rod deployment actuator; M_c is moment of resistance forces in the rod's path

3) joint locking

$$\Delta_r = д - 2д_n - д_{pr} > 0, \tag{3}$$

where Δ_r is the radial clearance in the joint; д is the minimum clearance in the connection between the internal and external members of the joint not including the layer of lubricant; $д_n$ is the maximum thickness of solid lubricant subject to its possible changes in the course of operation; $д_{pr}$ is the limiting value of thermal deformations in the radial clearance in case of volume expansion (compression) of the internal (external) member of the joint

4) wedging in the articulated joint

$$\Delta_{sh} > \Delta l, \tag{4}$$

where Δ_{sh} is the axial clearance in the articulated joint; Δl is the thermal deformation, capable of causing thrust force within the articulated joint

5) catching of the rod

$$Q_{st} \to 0, \tag{5}$$

where Q_{st} is the probability of the rod being caught.

The fulfillment of each of the conditions (1) to (5) in the course of operation under the given conditions and modes can be expressed in the form the probabilities that the values of the parameters (indicators) do not exceed the allowed limits over the observation interval t and will equal

$$P_1(t) = P(P_d \geq P_{lim}), \tag{6}$$

$$P_2(t) = P(M_d > M_s), \tag{7}$$

$$P_3(t) = P(\Delta_r > 0), \tag{8}$$

$$P_4(t) = P(\Delta_{sh} > \Delta l), \tag{9}$$

$$P_5(t) = 1 - Q_{st}. \tag{10}$$

The probabilities (6) to (10) can be identified by stochastic or deterministic methods. In the first case, the probabilities of parameters being within the allowed range are calculated using the methods of the dependability theory, e.g. method of individual dependability [18] (which ultimately does not rule out possible failures, but can provide the idea of their possible frequency). In the second case the fact of the parameters being within the specified allowed range is substantiated (necessary measures are taken to prevent failures) based on the provision of design reserves (redundancy, safety factor, drive moment reserve, parametric redundancy, power and temperature decouplings, procedures to ensure guaranteed results, e.g. by using minimax criteria).

Under the deterministic approach, in order to achieve the probabilities $P_i(t) \approx 1$, where $i = 1, 2, \ldots, 5$, in expression (1) the actuator must be redundant, e.g. for an electromechanical actuator a redundant motor power supply must be provided, while for a mechanical actuator structural redundancy must be in place; in expression (2) it is required to ensure drive moment reserves not less than 200 % for the worst combination of operating conditions and zero kinetic energy of the rod [19]; in expression (3) minimax criteria must be provided that are based on the restriction of the ranges of realization of random parameters for the worst conditions of their realization [20]; in expression (4), thermal decouplings must be in place [21]; in expression (5), procedures to ensure guaranteed results are to be provided, e.g. with the use of computer simulation [22].

In case of application of any method (stochastic or deterministic) of probabilities (6)-(10) calculation the dependable performance of the function of rod rotation through the specified angle is identified using formula

$$P(t)=\prod_{i=1}^{n} P_i(t), \qquad (11)$$

where n is the number of indicators that ensure unconditional fulfillment of the function of rod rotation through a specific angle; $P_i(t)$ is the probability of the i-th parameter (i = 1, 2, …, 5) not exceeding the allowed limits; t is the observation interval.

The calculated value (11) provides the theoretical dependability indicator that may differ from the real one if the design and/or process engineering documentation does not contain some manufacturing requirements or they are specified incorrectly for non-ambiguous fulfillment of conditions (1)-(5). The absence, ambiguity or incorrect performance of requirements of the technical documentation can be caused by events associated with failure to conduct the required calculations and tests, omissions on the part of designers in the preparation of drawings, limited time of delivery of design documentation, lack of coordination between designers and process engineers, etc.

In order to reduce the risks associated with the failures caused by insufficient scope or ambiguity of the requirements, the design and process engineering documentation must be analyzed for compliance of the scope of the parameters (indicators) that describe the performance of certain functions, e.g. (1)-(5), with the respective requirements.

Non-relevance of the parameters and requirements of the design and/or process engineering documentation, risks of non-fulfillment or undue fulfillment of requirements in the process of manufacture are regarded as events C_i, where index i corresponds to the i-th component of the system under consideration. The probability of each such event may be defined by formula:

$$P(C_i) = б_i \cdot P_i(t), \qquad (12)$$

where $б_i$ are adjusting factors that can be obtained by expert methods, e.g. using point-based estimation of failure severity:

$$б_i = 1 - Q_i,$$

where Q_i is the expected probability of failure of the i-th component in accordance with the scale of point-based estimation of failure severity per GOST 27.310.

In order to calculate the final probability of the performance of the function of rod rotation through the specified corner subject to the provisions of the design and process engineering documentation (12) the following formula is used

$$P(C)=\prod_{i=1}^{n} P_i(C_i). \qquad (13)$$

The above procedures of evaluation of the probability of performance of the function of rod rotation through the specified corner can be used as part of the analysis of each of the mentioned rod functions during deployment, while the probability of their performance and the general probability of no-failure of the rod are evaluated using formulas (11) and/or (13). The applicability of the above formulas is defined by the required accuracy of dependability evaluation [16]. For the purpose of estimation of reliability below three nines formula (11) may prove to be quite applicable, while if the required reliability is three nines and above formula (13) must be used.

Risk assessment with the use of design engineering analysis of dependability

The method and risk analysis and assessment subject to design and technical solutions (1)-(13) was named design engineering analysis of dependability (DEAD), whose general description is given in [23, 24]. The methodology can be described as a sequential performance of a set of specific methods:

• The functional analysis method is intended for the identification of the primary functions that enable the performance of products' intended function and identification of possible failures as the result of violation of operational conditions.

• Method of worst case analysis for the identification of the causes for possible failures including the worse combinations of factors of a product's technical condition, modes and conditions for its operation.

• The method of failure management for the identification of the properties of products' critical components, whose implementation makes the causes of failures impossible.

• Method of product design parametrization for quantification of the properties of critical components and definition of the ranges of allowed values, e.g. (1)-(5).

• Method of parameters substantiation for the evaluation of the probability of the operating parameters being within the allowed range, e.g. (6)-(10).

• Method of dependability evaluation using the method of dependability structure diagram (11) for decision-making regarding the compliance of the chosen design parameters with the assigned dependability requirements.

• Method of definition of necessary and sufficient requirements by means of continuous analysis of the design and process engineering documentation for identification of the degree of compliance of the operating parameters with the specified requirements.

• Method of identification of risks of failure due to non-specified requirements in the design and/or process engineering documentation (12) for identification and evaluation of possible failures as the result of compliance with the requirements of detailed documentation "as is".

• Method of dependability evaluation subject to the risks associated with the underestimation of design and/or process engineering errors (if identified), e.g. with the use of point-based estimation of failure severity (13) for adoption of final decisions regarding the compliance of the design with the specified dependability requirements.

Depending on the required accuracy of dependability estimation the obtained values of probabilities (11) or (13) are compared with the specified dependability requirements P_{pr} to ensure the fulfillment of condition

$$\forall P = [P(t) \vee P(C)] > P_{pr}. \quad (14)$$

In case of non-fulfillment of condition (14) DEAD procedures must be reiterated and new calculations must be performed with refined initial data.

It should be noted that the above approach to dependability calculation (11)-(14) was developed specifically for folding structures of spacecraft and has not yet been applied to other technical objects. Nevertheless, if we compare this approach with the procedure of dependability calculation of mechanical parts of aircraft rotary structures based on conventional approaches of the dependability theory [25, 26], the former allows significantly extending the capabilities of taking uncertainty factors into account. For example, out of five causes of failures considered in this paper, known sources only examine one, i.e. "rod deceleration" (2), which is completely explainable as such sources did not regard the design and process engineering solutions as uncertainty factors.

Conclusion

It is shown that the absence of statistical data on the dependability of UHVC analogs does not prevent dependability calculation in the form of risk assessment. Moreover, the results of such calculations can be a source and guidelines for adoption of design and process engineering solutions in the development of products with target dependability indicators. However, legalizing the method of such calculations requires the modifications of the technical rules and regulations to allow for dependability calculation by other means than with the use of statistical data on the failures of analogs.

References

[1]. Ushakov D. Dictionary of the Russian language in 4 volumes. Volume 3. Moscow: Terra; 1996 [in Russian].

[2]. Terminy kosmicheskogo strakhovaniya [Terms of space insurance], <http://www.space-ins.ru/index.php/kategoria8/8-terms.html> [in Russin].

[3]. Polovko AM, Gurov SV. Osnovy teorii nadiozhnosti [Introduction into the dependability theory]. Saint Petersburg: BHV-Peterburg; 2006 [in Russian].

[4]. Pokhabov YuP, Ushakov IA. O bezavariynosti funktsionirovaniya unikal'nykh vysokootvetstvennykh sistem [On the fail-safety of unique highly vital systems]. Metodi menedzhmenta kachestva 2014;11:50-56 [in Russian].

[5]. GOST 27.002-89. Industrial product dependability. General principles. Terms and definitions. Moscow: Izdatelstvo Standartov 1990 [in Russian].

[6]. GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform 2016 [in Russian].

[7]. Wentzel ES. Probability theory. Moscow: Nauka; 1969 [in Russian].

[8]. GOST R EN 9100-2011. Quality management systems of organizations of aviation, space and defence industries. Requirements. Moscow: Standartinform; 2012 [in Russian].

[9]. GOST R ISO 31000-2010. Risk management. Principles and guidelines. Moscow: Standartinform; 2012 [in Russian].

[10]. GOST R 51897-2011. Risk management. Terms and definition. Moscow: Standartinform; 2012 [in Russian].

[11]. Pokhabov YuP. About the philosophical aspect of reliability exemplified by unique mission critical systems. Dependability 2015;3:22-27.

[12]. Van-Jelen V. Fizicheskaya teoriya nadyozhnosti [Physical theory of dependability]. Simferopol: Krym; 1998 [in Russian].

[13]. Pokhabov YuP. On the definition of the term "dependability". Dependability, 2017;17(1):4-10.

[14]. Netes VA, Tarasyev YuI, Shper VL. How we should define what "dependability" is. Dependability 2014;4:15-26.

[15]. Uiomov AI. Veshchi, svoystva i otnosheniya [Things, properties and relations]. Moscow: USSR AS Publishing; 1963 [in Russian].

[16]. Pokhabov YuP. Teoriya i praktika obespecheniya nadyozhnosti mekhanicheskikh ustroystv odnorazovogo srabatyvaniya [Theory and practice of dependability of single-use mechanical devices]. Krasnoyarsk: SFU Publishing; 2018 [in Russian].

[17]. Chebotariov VE. Proektirovanie kosmicheskikh apparatov sistem informatsionnogo obespecheniya: v 2-kh kn. Kn. 2. Vnutrennee proektirovanie kosmicheskogo apparata [Design of information support spacecraft in 2 volumes. Volume 2. Internal design of spacecraft]. Krasnoyarsk: SibSAU Publishing; 2005 [in Russian].

[18]. Timashev SA, Pokhabov YuP. Problemy kompleksnogo analiza i otsenki individualnoy konstruktsionnoy nadyozhnosti kosmicheskikh apparatov (na primere povorotnykh konstruktsiy) [Problems of comprehensive analysis and assessment of individual design dependability of spacecraft (with the example of rotating structures)]. Ekaterinburg: AMB; 2018 [in Russian].

[19]. NASA Standard. Design and Development Requirements for Mechanisms; June 13, 2006. NASA-STD-5017.

[20]. Chebotariov VE, Kosenko VE. Osnovy proektirovania kosmicheskikh apparatov sistem informatsionnogo obespecheniya [Introduction to the design of information support spacecraft]. Krasnoyarsk: SibSAU Publishing; 2011 [in Russian].

[21]. Pokhabov YuP, Grinevich VV. Patent 2230945 Russian Federation. MPK F16B 1/00. Method of product fastening. No. 2002113143/11. Appl. 18.05.2002. Publ. 20.06.2004. Bull. No. 17 [in Russian].

[22]. Emelianov AA. Put ot analogovykh modeley k simulyatoru na tsifrovom kompyutere [From analogue models to digital computer simulator]. Prikladnaya informatika 2007;5:41-53 [in Russian].

[23]. Pokhabov Yu.P. Approach to ensuring of dependability of unique safety critical systems exemplified by large flexible structures. Dependability 2016;1:31-36.

[24]. Pokhabov YuP. Ensuring dependability of unique highly vital systems. Dependability 2017;17(3):17-23.

[25]. Kuznetsov AA. Nadyozhnost konstruktsii ballisticheskikh raket [Structural dependability of ballistic missiles]. Moscow: Mashinostroenie; 1978 [in Russian].

[26]. Kuznetsov AA, Zolotov AA, Komyagin VA et al. Nadyozhnost mekhanicheskikh chastey konstruktsii letatelnykh apparatov [Dependability of mechanical parts of aircraft design]. Moscow: Mashinostroenie; 1979 [in Russian].

About the author

Yuri P. Pokhabov, Candidate of Engineering, NPO PM – Maloe konstruktorskoye buro (OAO NPO PM MKB), Head of Center of Research and Development, Russia, Krasnoyarsk Krai, Zheleznogorsk, e-mail: pokhabov_yury@mail.ru

Received on: 16.04.2018