Dependability, vol. 20 no. 4, 2020 Original article
https://doi.org/10.21683/1729-2646-2020-20-4-13-20

Dependability from a designer’s standpoint

Yuri P. Pokhabov, *Joint Stock Company NPO PM – Maloe Konstruktorskoye Buro (AO NPO PM MKB), Russian Federation, Krasnoyarsk Krai, Zheleznogorsk*
pokhabov_yury@mail.ru

Yuri P. Pokhabov

Abstract. *The* **Aim** *of the paper is to let the reader look at dependability through the eyes of a designer who is to develop an entity with specified dependability requirements. The result of such work is not yet dependability as a property, but the ability proper to a structure, without which the required dependability cannot manifest itself. Designing highly dependable entities requires the use of formalized practices with specific operating procedures, that, on the one hand, do not contradict the provisions of the dependability theory, while, on the other hand, are to be useful, clear and easy-to-understand by any designer in order to ensure the required dependability.* **Methods.** *The paper examines the primary approaches that allow a designer, without violating the existing notions and terminology of dependability, solving problems of technical object dependability in the course of design and development based on engineering disciplines and design methods intended to ensure the dependability of products, starting with the very early life cycle stages. If such approaches to dependability research are employed, preventing failures only requires the application of the principles of physicality (causal connections) and physical necessity (consistency with the laws of nature) of the causes of failures.* **Results.** *The paper sets forth simple mathematical models that helped create a generalized parametric model of complex technical systems operation. Based on the cited models, it can be concluded that dependability calculation in terms of the known dependability indicators of components and elements can be replaced with dependability estimation in terms of the probability of performance by the components and elements of the required functions. This conclusion not only does not contradict the provisions of the dependability theory, but makes dependability an effective tool helping the designer ensure the specified dependability. The generalized parametric model of operation is solved using the method of design and process dependability analysis developed for the purpose of analyzing and assessing design solutions as part of high-dependability item design.* **Conclusion***. The concepts, approaches, models and methods suggested in the paper allow the designer to take dependability as operability expanded in time. Such dependability is always specific and takes into consideration all the distinctive features of an entity. In this case, the process of design and assurance of dependability becomes an integral part of the entity creation activities regardless of uniqueness, series production, availability of dependability indicators of components and elements. But most importantly, such approach to dependability, on the one hand, does not contradict the foundations of the modern dependability theory, and, on the other hand, relieves the designer of the impression that dependability is something foreign, not associated with the real design.*

Keywords: *dependability theory, highly dependable system design, dependability calculation, unique highly vital system, design engineering analysis of dependability (DEAD).*

For citation: *Pokhabov Yu.P. Dependability from a designer’s standpoint. Dependability 2020;4: 13-20. https://doi.org/10.21683/1729-2646-2020-20-4-13-20*

Received on: *20.07.2020* / **Revised on:** *31.08.2020* / **For printing:** *18.12.2020.*

Introduction. Dependability requirements are to be set forth in the design specifications as it is required, for instance, in GOST 15.016–2016. Quantitative estimation of dependability is conventionally done based on the indicators defined through statistical testing (operation) of products or their components (elements) ([1], Annex (informative). Notes to the terms given in the standard). However, before such statistical testing is possible, at the stage of release of working design documentation, it is required to substantiate the ability of the employed engineering solutions to ensure the specified dependability requirements (normally, that involves dependability calculations according to GOST 27.301–95). As dependability is often understood as reliability, we should consider what exactly a designer is to do in order to ensure dependability if it (for simplicity) is defined through the probability of no failure[1].

In order to fulfil the design specification requirements in terms of specified probability of no failure, the designer, according to today's vision of dependability, is to develop the structure of the product (as a set of elements and relations between them) with known data on the dependability of its components and elements in the specified modes and conditions of operation. On the outside, it might look like putting Lego bricks together, creating a structure with a specified dependability out of components and elements with known dependability data. Whereby, if such data is not available, then, according to the modern dependability theory, they must be obtained through experimental means [2-4]. In practice, that is the design process of electronics with specified dependability that are based on electronic components with known dependability indicators [5]. Electronic components are mass-produced and they normally are sufficiently compact in order to enable in-laboratory production of statistical dependability information in specified application modes under extreme temperatures, temperature cycling, vacuum, radiation, corrosive environments, etc.

In the case of complex technical systems (entities) consisting of diverse components with different principles of operation: body parts, mechanisms, electromechanical devices, electronic assemblies, pyrotechnical devices, etc., Lego-like dependability development may become difficult. The collection of statistical data on the dependability of full-sized components of large-format entities (primarily, large deployable structures, complex mechanical and electromechanical devices, distributed structures made of composite materials, etc.) in unique operating conditions different from the normal environment of the Earth (deep underwater, in presence of high radiation, in outer space, etc.), will most probably be impossible for technical and economic reasons [6]. Certainly, there are available data on the dependability of similar items operating in slightly different modes and conditions, e.g. for spacecraft structures that are to be deployed in the orbit only once, as well as statistical data on land-based activations (if the project budget allows conducting the required number of uniform independent tests in order to confirm the specified dependability). However, it is not clear what to think of the reliability of dependability calculations (given that the land-based test conditions are different from the conditions of normal operation in space). It is even worse, if the product is one-of-a-kind (let alone unique), and there is no available dependability data on similar items, e.g. when it comes to landing vehicles of interplanetary spacecraft intended for traveling to a planet with a Venus-type atmosphere.

The situation might be more complicated, when reliability is defined by at least three nines after the decimal point (rounded to a smaller number of nines to improve the confidence). Formally, that does not rule out the possibility of failures, however in each particular case loss of functionality is not acceptable, as it can cause immeasurably more damage than the cost of development and manufacture of the failed product. A typical example is the deployment of structures of unmanned spacecraft in a near-Earth orbit. The failure of any of the deployment mechanisms may cause the loss of the satellite. For instance, due to the non-deployment of the solar panels in 2006, the 190-millon dollar Sinosat-2 communication satellite was lost, followed in 2019 by the 250-million dollar Chinasat-18. Besides direct damage due to the loss of spacecraft, such incidents bring costs associated with repeated manufacture of a replacement satellite and loss in goodwill. Additionally, in peacetime, the loss of a telecommunication satellite can cause faults in the global communication system with many risks of loss due to disrupted mobile communication, while in wartime it may cause a critical deterioration of (and even loss of) state security.

If it is impossible to follow the rules of the statistical dependability theory, the designer has to solve the problem of ensuring the specified dependability through non-formalized heuristic methods, that either do not imply dependability estimation, or allow dependability calculation with no regard for the design specificity of the respective entities. In any case, they do not answer the question of how exactly to achieve the dependability, under which failures due to certain causes are not allowable [7]. Then, all that remains is to hope for luck or use such design method that even without reliable statistical dependability data may prove to be useful, clear and easy-to-understand for any designer aiming to ensure the required dependability.

Why making and calculating dependability are two different things. Any calculation of performance parameters aims to substantiate the designer's decisions on the choice of materials, intermediate products, heat treatment, coatings, dimensions, tolerances, etc. Such calculations are based on the principle of redundancy for

[1] According to GOST R 50779.10-2000, probability is defined with a real number between 0 and 1 that is to reflect the relative frequency in a set of observations, or the level of confidence that a certain event will occur.

the purpose of eliminating (or reducing) the uncertainty factors between the "required" entity structure and the "randomness" of the environmental factors. The degree of such redundancy defines the allowable relation between the specified dependability and the possible undependability [8]. A good example is the strength calculation. The redundancy of structural strength of the selected structural materials and specified dimensions of structures that bear the external loads defines the required safety factor and thus conditions the choice of design solutions (the materials, dimensions, mass, action principles, manufacturing processes and other structural features). Any designer who knows that his/her structure has an insufficient safety factor (e.g. 0.9) has the required knowledge of the strength of materials that allow, through the use of design methods, bringing the strength to the required level. With dependability, the situation is completely different. No designer, knowing that the operational reliability of his/her structure is, e.g. 0.998, is able to substantiate its increase to, for instance, 0.999. Moreover, based on the external features, it is practically impossible to distinguish same-purpose entities with the reliability of, let us assume, 0.9 and 0.(9) (i.e. zero and nine in period). At the same time, an expert opinion regarding the strength can be provided by any qualified engineer even without calculations (at least in terms of "strong – flimsy").

Such uncertainty with dependability is explained by the fact that its purpose is to provide an integral characteristic of literally all properties of an entity able to affect its reliable operation, whose list alone is difficult to identify. If we take, for instance, strength, it characterizes the ability of the structural material to resist destruction under the stress caused by external forces and simultaneously is a property that constitutes dependability. Whereby, along with other component properties of dependability, when evaluating dependability, strength is to be considered in terms of retention over time (formally, dependability is a property that characterizes the manifestation of properties over time). As complex technical systems are endowed with a sum of multidisciplinary properties (material, dimensional, temporal, thermal, electrical, mechanical, etc.), each of which is examined using various engineering disciplines, there are two possible approaches to the research of dependability:

- identifying and taking into consideration in the course of dependability evaluation each of the component properties of an entity;
- not individualize each of the properties of an entity, but characterize its operation with certain generalized indicators.

In the Russian school of dependability (at least since 1989, at most since 1983), out of such approaches followed the unity and opposition of the two definitions of the term "dependability", i.e. the functional and the parametric [9], whose priority in the terminological dependability standard GOST 27.002 changes over time.

In practice, both approaches to dependability with not limitation are employed in strength calculation using the "load – strength (resistance)" failure model. In this case it is deemed that the probability of no failure (generalized strength indicator) is the same as the probability that within the given time interval the value of the stress parameter will not once exceed the value assumed by the strength parameter (specific parameters affecting strength) ([1], Annex (informative). Notes to the terms given in the standard). Whereby the degree of excess strength corresponding to the specified probability of no failure, in practice, is normally standardized through specified reliability coefficients and margins of safety [10]. However, such failure model is only valid for those cases when dependability is defined only by the strength or mainly strength, if the required dependability is not too high.

If dependability, besides strength, is equally affected by another factor, e.g. excess driving torque in case of moving mechanical assemblies, dependability, subject to both factors, is defined using the method of dummy items [11]. Nevertheless, that approach has its limitations as well. It is applicable for design dependability when substantiating fundamental design solutions as regards the selection of design parameters of structures. In the present case, it is the structural strength and power sufficiency of the opening drives installed in the structure, provided that it has required strength [12]. In the course of development of working design documentation, besides ensuring the strength and power sufficiency of drives, it is always required to carefully design all the aspects of the structure in view of the manufacturing capabilities, therefore it is required to additionally consider a large number of design and manufacturing factors that have an effect on dependability [12]. Statistical methods of dependability calculations in this case are not applicable, as they do not allow identifying sufficient factors for characterizing dependability subject to specific design features of an entity and substantiating them quantitatively in order to verify the required dependability indicators.

The primary contradiction between designing and researching dependability consists in the fact that, according to the modern dependability theory, the dependability indicators of an entity characterize the consequences as the result of the design activities with no consideration for the underlying causes, while a designer has to "design" (take into consideration all) the causes in order to obtain the required consequence, i.e. the specified dependability [13]. In other words, a designer must evaluate and prevent practically all possible causes of failure, while a researcher (estimator) of dependability only needs to represent dependability with a probabilistic indicator that provides an integral characteristic of all properties of an entity enabling the performance of the required functions (without elaborating on the causes of non-performance of each individual function). In practice, a dependability expert looks at the results of a designer's work from the point of view of the accidental nature of events and processes, whose causes not necessarily can (or must) be known, while for a designer any structure obeys the causality principle: each decision and action causes potential events able to entail failures. Thus, a designer always examines an entity as a deterministic set of causal relationships, while a dependability estimator sees it as a certain technical item with no regard for the genesis, whose behaviour is postulated in the form of statistical hypotheses. This difference between the perspectives of a designer and estimator of dependability is so, that in the aerospace industry there is a common saying that goes: "*dependability is calculated by those who don't know how to make it"* and *"nines don't fly"*, which once again confirm the absence of correlation between the results of design activities on a specific entity and dependability calculation based on statistical data regarding similar items.

The terminological aspect of the designers' perspective of dependability. In order to substantiate the relevance and viability of the designer vision of dependability, let us address the dependability terminology. Without engaging into a terminological dispute [9], let us accept the definition of the term "dependability" in accordance with GOST 27.002: *"Dependability is the property of an object to maintain in time the ability to perform the required functions in the specified modes and conditions of operation, maintenance, storage and transportation."* As it can be clearly observed, the term "dependability" is based on term elements, whose meanings in the above standard are defined only for one term, i.e. "(*technical*) *item"*. The other term elements that are significant for an unambiguous understanding by a designer of the meaning of dependability are not defined in the dependability terminology standard. Most importantly, those are the "*property"*, "*ability"* and "(*required*) *function*". Probably, the standard's developers thus intentionally provided anyone interested (based on the specificity) with the opportunity to decide upon the meaning of the concepts that make up the primary term of dependability. Let us use this right, taking into consideration a designer's vision of the matters of dependability.

The term "*property"* was many times defined in Russian standards GOST R 8.614, GOST R ISO 22745-2, GOST R 54136 and GOST R 15531-31, but, in the context of fail-safe entities (that operate without failures), the author prefers the concise and aphoristic concept of property set forth in [14] as the *relation of things*. Terminologically, that concept is defined as follows: *"Property is a philosophical category that expresses such aspect of an object that conditions its difference or similarity with other objects and is manifested in its relation to them"* [15].

The term "*ability*" is defined in the Russian standards GOST 33707 and GOST R ISO 15531-1, but, again, in the context of fail-safe entities (for lack of a better option) the author deems it to be appropriate to use the dictionary definition [16]: *"Ability is a quality, property, state that enables the performance of certain actions, work"*.

The situation with the definition of "(*required*) *function" per* GOST 27.002 is more complicated. First, it is not very clear what is the difference between the "(*required*) *function"* and the concepts used in other dependability standards, i.e. "(*specified*) *function"* per DSTU 2860 and "(*target*) *function"* from the Space Systems and Stations group of standards. Given that the "(*required*) *function"* and "(*specified*) *function"* are indiscriminately used in GOST 27.002, those are probably equivalent. Second, taking into consideration the homonymic and synonymic specificity of the concept of "*function*", let us address the definitions of that terms' synonymic chain that best match the characteristic of technical items (assuming that such function can indiscriminately indicate required, specified or target):

- *description (normally, verbal) of the service purpose of an entity, i.e. what the entity (component) is to do when used* [GOST R 53394, article 3.2.4];
- *implementation of output effect by the item*[1];
- *execution within the item of a process corresponding to its purpose, manifestation of a specified condition or property of the item according to the requirements of the regulatory technical and/or design (project) documentation* [DSTU 2860, article 3.1.8];
- *external manifestation of the properties of a certain item in the given relational system* [17].

Given that the required function is a function that was initially conceived by man (designer) and is to be executed in the course of an item's operation in order to achieve its service purpose, let us agree – when talking about fail-safe items – to understand the ***required function*** as the *external manifestation of the expected properties of the item in specified modes and conditions of operation (when the item performs the specified output effect) that have been identified and correspond to the provisions of the design documentation*.

Let us note that the above concepts of "*property*", "*ability*", and "(*required*) *function*" clearly show an orderly evolution of the states of matter that changes in time in the form of ***properties*** as certain relations between objects within a material system, ***ability*** as the state that enables the manifestation of certain properties and ***required functions*** as the realization by the object of the specified abilities. Thus, the required function is the result of the manifestation of an object's inherent properties that, in turn, are the realized ability (potential capability) of an object to manifest such required functions. The above hierarchy of concepts allows, from the very beginning, conceiving (designing and developing) the ability of an object to perform the required functions, describing (analyzing and calculating) the ability quantitatively as a property and realizing (manufacturing and using the item) this property in the form of the required function. If the non-performance of any of the required functions is considered as failure, then early prevention of possible failures becomes just a result of the methodological approach to the design (adoption of design solutions, their

[1] The definition of the term is in accordance with the upcoming Russian standard "Space systems and complexes. Analysis of the types, consequences and criticality of failures of entities and processes. Availability analysis. General requirements".

substantiation, execution and supervision). Consequently, all problems of technical object dependability as part of design and development can be solved on the basis of the engineering disciplines and design methods of product dependability starting from the early stages of the life cycle. In this case, preventing failures only requires the application of the principles of physicality (causal connections) and physical necessity (consistency with the laws of nature) of their causes.

Models required by the designer in order to understand dependability. Let us use the principles of construction of simple mathematical models that enable the creation of functional models of complex technical systems [18]:

- the simpler the model, the lower is the probability of improper conclusions;
- the model must be simple, but not simpler than possible;
- anything can be neglected; we only need to make sure we know how it will affect the decision;
- the model must be crude: small corrections are not to radically modify its behaviour;
- the model and calculation must not be more accurate than the input data;
- while analyzing the results of model study, what matters is not only the specific numerical results, but the understanding why and how everything happens and how it depends on the parameters.

In practice, in order to achieve the design objectives, a designer uses two models that reflect his/her idea of the actual object and its operating environment:

- an information model of temporal factors and external effects on the item through the interfaces in the form of operating modes and conditions as per the design specifications;
- a digital model that corresponds with the stationary probabilistic model of the item in the form of design documentation that he/she is ultimately developing.

The information model of temporal factors and external effects defines the allowable set and range of values of the factors of the environment, in which a structure is to resist possible failures. The distinctive feature of this model is that it normally remains unchanged throughout development iterations. If failures in operation are due to the fact that some model parameters do not correspond to reality, that has nothing to do with dependability (the latter, according to its definition, is the property that manifests itself only in predefined modes and conditions of operation). For instance, the first descent vehicles of the Venera automatic interplanetary stations were designed for pressures of up to 20 ATM and were simply crushed in the planets' atmosphere without achieving the specified goals, as the actual pressure on the surface of Venus, as it turned out later, was about 90 ATM (probably, at 20 ATM the descent vehicles were sufficiently dependable; the problem is that the design objectives were defined incorrectly). A designer initially regards any external effects as deterministic regardless of the reasons they were designated as such (this difference in the standpoints of the designer, dependability specialist and final user is a potential source of conflicts).

The stationary probabilistic model of an object is an abstract description of actual or hypothetical (not yet manufactured) entities that can be obtained as the result of repeated manufacture under condition of strict observance of all requirements of the design documentation. This model is subject to iterative improvement (modification) up to the moment the entity is put into operation, therefore, the probabilistic model of an item at each iteration step of modification of documentation is considered to be stationary "as is". Tolerances of structure parameters within each iteration step are unchanged (stationary), but the values of such parameters may change randomly (stochastically) within the set tolerances in each actual or hypothetical implementation, and, subsequently, can be realized and expanded in time. Thus, the number of hypothetical reproductions of same-type entities τ (manufactured using the same documentation, same equipment, same specialists), whereas they are able to ensure reliability is a random value that, in its meaning, cannot be anything else but the failure-free time of entity t expressed in the number of actual reproductions. The above property of the stationary probabilistic model of an item corresponds to the condition of dependability $R(t)=P(\tau>t)$ at each iteration step of modification of the technical documentation "as is". Among the examples of practical application of stationary probabilistic models are the dimension chain calculations per GOST 16320 using the probabilistic method based on a model, according to which closing dimensions are allowed to overrun the tolerance limits with substantiated economic risk, and using the maximum-minimum method based on a model, according to which closing dimensions are not allowed to overrun the tolerance limits in order to ensure complete interchangeability.

An item's operation subject to a temporal factor model and external effects can be represented as two mathematical models that describe the performance of the required functions in the specified modes and conditions of operation:

- the stochastic, whereas the stationary probabilistic model of the item is regarded as the information model in the form of a black box that implements the output effects depending on the specified modes and conditions of operation (based on mathematical processing of the statistical information on the behaviour of the actual item or its physical model with no regard for the laws of nature) (similar to the dimension chain calculation by the probabilistic method);
- the physical (or, most probably, quasi-physical, as no actual item exists yet), when a stationary probabilistic model of the item in the specified modes and conditions of operation is represented as a system of corresponding mathematical equations that reflect the sum of the knowledge, notions and hypotheses associated with the realization of output effects based on the physical laws of nature (equivalent of dimension calculation by the maximum-minimum method).

The above mathematical functional models correspond to the dependability models that are based on the functional and parametric definition of dependability [9]:

- functional, whereas the required functions are characterized by the probability measures of failures (statistical, logical, Bayesian, subjective);
- parametric, whereas the required functions are represented as a set of parameters that characterize the ability to perform them and the allowed range of variation of such parameters (the parameters are measurable or calculated physical values).

If required, the parameters and probabilistic functional indicators of the item can be reduced to a consistent dimensionless form (if the parameters can be represented as the probability of value variation within the allowed range similarly to the explanation given in GOST 27.002 [1]). That allows considering the functional dependability model as a special case of the single parametric model of dependability that simultaneously takes into consideration the physical and statistical (mathematical) nature of things based on the physical (quasiphysical) and stochastic models [19, 20].

The above models allow regarding an entity as a set of properties of structural components and elements that are to become manifest in the course of required operation. Such properties may be conceived in drawings separately from the entity as abilities and implemented in its physical form provided that required functions are fulfilled at the stage of manufacture and operation. The abilities and properties can be described indiscriminately by both parameters, and probability measures depending on the adopted dependability models (functional or parametric). The dependability of the required functions is defined using a dependability structure diagram after reducing the quasi-physical functional model to the dimensionless form consistent with the probabilistic model. As the result, the known model of dependability calculation of unique and small-batch entities based on known dependability indicators of components and elements [1] is replaced – with no loss of meaning – with a dependability calculation model based on the probabilities of performance by the components and elements of the required functions. In this case the designer is able to choose the dependability calculation model based on the objective knowledge of the nature (mathematical or physical) of the entities' operation, while the probability of performance by the entity of any of its functions can be conceived, implemented and supervised by the designer at any life cycle stage.

Generalized parametric model of product operation. If an entity is regarded as a structure that, in the course of operation, is able to resist the environmental effects [7], it can be represented with a set of output parameters (or probability measures), whose values are defined and limited by the modes and conditions of such exposure under the specified operation time. Thus, any entity can be reduced to a parametric representation in the form of:

- a set of output parameters that characterize the required functions for the performance of the service purpose,
- the allowed values of output parameter variation defined by the modes and conditions of application;
- the operation time, during which the values of the output parameters will not exceed the allowed limits.

The sum of an entity's output parameters (or probability measures) that characterize the presence and specific set of abilities to perform the required functions is its ***functionality*** that can be expressed as

$$X = \{X_1, X_2, \dots, X_i\}, \qquad (1)$$

where X is the set of output parameters X_i that define the performance of the required functions.

Output parameters can be any parameters of an entity that can be associated with the environmental effects based on the "more-less" criteria, e.g. for instance:

- strength as a generalized characteristic of the geometrical dimensions of the cross-sections of structural units and mechanical properties of structural materials resisting environmental loads (the load-carrying ability of the structure is to exceed the actual loads);
- the drive moment as the characteristic of the power sufficiency of the mechanism actuator for the purpose of overcoming the obstructing stress (drive moment is to be higher than the moment of the resisting forces);
- gaps in kinematic pairs as the parameters that resist the possible temporal variation of the dimensions of the mating parts, e.g. due to thermal deformations (the allowances within the couplings are to be positive);
- other parameters that characterize an entity in terms of resistance to the specified environmental loads and effects (that can be calculated and measured).

In the course of operation of a structure, the output parameters X_i can change their values with time within the allowable ranges defined by the modes and conditions of application. The values of output parameters (or probability measures), under which an entity is able to perform the required functions, characterizes its ***operability*** (up state):

$$D_x = \{X_i(t) | \alpha_i \leq X_i(t) \leq \beta_i\}, \qquad (2)$$

where D_x is the range of acceptable values of variation of output parameters $X_i(t)$; α_i and β_i are the lower and upper limits of the variation range of output parameters.

Identifying operability (2) involves all necessary calculations of entity parameters based on the physical models of natural phenomena and man-made processes with regard to the limitations imposed by the modes and conditions of operation.

The probability of output parameter (or probability measure) values of a structure being within the allowable area over time is characterized by the ***dependability***, the property of retaining in time the ability to perform the required functions in the specified modes and conditions of operation:

$$R = P\{X_i(t) \in D_x, 0 < t < t_k\}, \qquad (3)$$

where R is the dependability of the item as the probability P of the values of output parameters $X_i(t)$ being within the allowable range D_x within the time to failure t_k.

Identifying the probabilities (3) by estimating if parameter values are within the allowable limits within the time to failure can be done with the use of two interchangeable methods [1, 19, 20]:

- deterministic (by designing reserves per each of the parameters in such a way as to, with a certain degree of confidence, guarantee the presence of the values of the considered parameters within the allowable limits);
- stochastic (e.g. by estimating the design individual dependability, which essentially consists in calculating the probabilities of parameters being within the allowable limits based on the individual characteristics of the materials, loading/exposure processes and entity manufacture processes).

The set of formulas (1) – (3) is a generalized parametric model of an entity's operation [20], in which the criteria of the required functions (output parameters and allowable value variation limits) are interrelated, mutually conditioned and serve the aim of achieving the specified operability and dependability of the item in the process of completion of the service purpose.

As the presented model is based on the functional approach [21], such model allows disregarding the specifics of the design of entities and can be used for describing the operation of technical systems of various purposes, e.g. structures, single or multiple operation mechanisms, electromechanical devices, electronic assemblies, load-bearing and precision-built structures, etc. Researching the generalized parametric model of operation allows the designer to get rid of the cognitive distortion of the meaning of dependability, as it associates the feasibility of all calculations required for the selection of structural parameters with the consideration of compliance with the criteria of required functions to ensure the specified operability and dependability. The dependability in this case acts as operability expanded in time (3).

The above models can be solved using design engineering analysis of dependability (DEAD) described in detail in [19, 20] that, without getting into specifics, can be broadly reduced to the performance of three analysis procedures:

- initialization in the form of parametrization (transformation of the entity into a set of parameters or probability measures and allowable ranges of variation), that is done for establishing conditions (1) – (2);
- calculation of theoretical dependability based on design parameters according to (3);
- providing the evidence that the analysis (estimation) corresponds to the reality (requirements of the design and process engineering documentation, conditions of production, quality assurance measures) [19].

Thus, DEAD is in reality a roadmap for the design and development of entities with required dependability that allows – based on parametric modeling – selecting the structural parameters that ensure unconditional performance of the required functions that at the stage of manufacture must be executed and confirmed.

Conclusion. Applying the above concepts, approaches, models and methods, dependability – in the eyes of a designer – becomes operability expanded in time. Such dependability is always specific and takes into consideration all the distinctive features of an entity.

The process of design and assurance of dependability is becoming an integral part of entity creation activities regardless of their uniqueness, series production, presence or absence of dependability indicators of components and elements. But most importantly, such approach to dependability, on the one hand, does not contradict the foundations of the modern dependability theory, and, on the other hand, relieves the designer of the impression that dependability is something foreign, not associated with the real design.

References

1. GOST 27.002-89. Industrial product dependability. General principles. Terms and definitions. Moscow: Izdatelstvo Standartov; 1990. (in Russ.)

2. Riabinin I.A. [Academy member A.I. Berg and the problems of dependability, survivability and safety]. In: [Academy member Aksel Ivanovich Berg (On the occasion of centenary of the birth)]. Moscow: State Polytechnic Museum; 1993. (in Russ.)

3. Riabinin I.A. [Foundations of the theory and dependability calculation of naval power systems]. Leningrad: Sudostroenie; 1971. (in Russ.)

4. Bolotin V.V. [Application of probability theory and dependability theory methods in structural analysis]. Moscow: Stroyizdat; 1971. (in Russ.)

5. [Dependability of electronic products: a handbook]. Moscow: 22-nd Central Research, Design and Test Institute of the Ministry of Defense of Russia Publishing; 2006. (in Russ.)

6. Polovko A.M., Gurov S.V. [Introduction into the dependability theory]. Saint Petersburg: BHV-Peterburg; 2006. (in Russ.)

7. Plahotnikova E.V., Safonov A.S., Ushakov M.V. The design of products with requirements of reliability parameters. Izvestiya TulGU: Teknicheskie nauki. 2015;7(1):134-139. (in Russ.)

8. Venikov G.V. [Dependability and design]. Moscow: Znanie; 1971. (in Russ.)

9. Netes V.A., Tarasyev Yu.I., Shper V.L. How we should define what "dependability" is. Dependability. 2014;4:15-26.

10. Dhillon B.S., Singh C. Engineering reliability. NJ: John Wiley & Sons; 1981.

11. Kuznetsov A.A. [Structural dependability of ballistic missiles]. Moscow: Mashinostroenie; 1978. (in Russ.)

12. Pokhabov Yu.P. [Theory and practice of dependability of single-use mechanical devices]. Krasnoyarsk: SFU Publishing; 2018. (in Russ.)

13. Hubka V. Theory of technical systems. Moscow: Mir; 1987.

14. Uiomov A.I. [Things, properties and relations]. Moscow: USSR AS Publishing; 1963. (in Russ.)

15. Prokhorov A.M., editor. Great Soviet Encyclopedia in 30 volumes. Moscow: Sovetskaya entsyklopedia; 1970-1978. (in Russ.)

16. Ushakov D., editor. Dictionary of the Russian language in 4 volumes. Moscow: Terra; 1996. (in Russ.)

17. New dictionary of foreign words and expressions. Moscow: Sovremenny literator; 2005. (in Russ.)

18. Neymark Yu.I. [Mathematical models in natural science and technology]. Nizhny Novgorod: Lobachevsky University of Nizhny Novgorod Publishing; 2004. (in Russ.)

19. Pokhabov Yu.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.

20. Pokhabov Yu.P. Design for reliability highly responsible systems on the example of a moving rod. J. Sib. Fed. Univ. Eng. technol. 2019;12(7):861-883. (in Russ.)

21. Shcherbakov V.A., Prikhodko E.A. [Foundations of financial cost-effectiveness analysis]. Novosibirsk: NSTU; 2003. (in Russ.)

About the author

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

The author's contribution

The paper examines the mathematical models of dependability that can be solved using the method of design and process dependability analysis developed by the author for the purpose of analyzing and assessing design solutions as part of high-dependability item design. The paper builds upon the author's ideas set forth in the paper *Dependability in digital technology* (see. Dependability Journal no. 2, 2020).

Conflict of interests

The author declares the absence of a conflict of interests.