Original article
DOI: 10.21683/1729-2646-2019-19-1-10-17

Problems of dependability and possible solutions in the context of unique highly vital systems design

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


Yuri P. Pokhabov

Aim. *The paper examines the problems caused by the conventional interpretation of dependability that prevent the practical use of dependability analysis (assessment) as a tool for engineers involved in the creation of unique highly vital systems and substantiates proposals for their resolution.* **Methods.** *The paper analyzes the problem of quantitative estimation of the dependability of unique highly vital systems without the use of probability statistical models. The view of dependability as a physical property of a product (as a result of changes in its internal state) allows – at the physical level – ensuring lasting capability to fulfil the required functions and quantitatively estimating the criteria of the required functions' performance, that can be defined by, for instance, specifying a set of parameters for each function that characterize the capability to perform, as well as the permissible limits of such parameters' variation. Such approach causes the requirement to take the origin of dependability into consideration and examine the causes of unlikely failures that are to be identified by means of additional analysis in parallel with calculations and experiments performed to support dependability. The solution to the problems of fuzzy terminology allows revealing the interrelation between the quality and the dependability, thus enabling – using the single information basis of design and process engineering solutions – the analysis, synthesis and assessment of the dependability of unique highly vital systems based on performance parameters without the use of probabilistic statistical models.* **Results.** *The solution of the above dependability-related problems allows ensuring dependability based on the physicality (causal connections) and physical necessity (consistency with the laws of nature) of the causes of failures. The dependability of unique highly vital systems must be ensured from the very early lifecycle stages based on consecutive execution of certain design, process engineering and manufacturing procedures, as well as application of engineering and design analysis of dependability, which also allows solving problems indirectly related to dependability, e.g. improving the quality and reducing the cost of the manufactured products.* **Conclusions.** *The paper shows that the application of design engineering methods for the dependability analysis (assessment) allows – within the framework of existing views, yet with certain corrections – solving dependability-related problems without the use of the mathematics of the classic dependability theory. High dependability can be achieved by the same ways as undependability comes about, i.e. through design and process engineering solutions. The analysis, substantiation of engineering solutions and specification of necessary and sufficient requirements for the manufacturing process allows achieving the target dependability by engineering means through higher quality of design and process engineering. If we regard dependability as a multiparametric property, parametric models of products can be developed that enable the evaluation of the temporal stability of parameter values using methods of individual design dependability and/or design engineering analysis of dependability. The principles of unity of the design concept and its implementation in manufacture enables the development of products and assessment of their dependability based on a single foundation, i.e. the design and process engineering solutions directly associated with the capabilities of a specific manufacturing facility.*

Keywords: *unique highly vital system, individual design dependability, design engineering analysis of dependability, ensuring dependability.*

For citation: *Pokhabov YuP. Problems of dependability and possible solutions in the context of unique highly vital systems design. Dependability 2019;1: 10-17. DOI: 10.21683/1729-2646-2019-19-1-10-17*

Introduction

There are two approaches to ensuring dependability of non-repairable products depending on the end goal of their use:

• some products are intended for failure-free operation during an indefinitely long period or for dependable performance of one-time operations/functions (their failure is undesirable or unacceptable);

• other products are intended to operate for a strictly defined time (warranty period), after which their operation *should be terminated* due to irreversible changes in the design or its parameters.

The first approach is used when creating highly vital unique products that are non-repairable or difficult to replace with new ones without serious financial and time costs, or the failure of which leads to a catastrophic breach of safety. Unmanned space vehicles or industrial nuclear facilities are examples of such products. The second approach is used when manufacturing single use (non-repairable) consumer goods (cars, household appliances, computers, gadgets, etc.) by programming their breakdowns (failures) immediately after the end of the warranty period in order to encourage sales. Some examples of programmable breakdowns are:

• an ordinary incandescent electric lamp should have an average warranty period of 1 000 hours, and today it is no secret that this is the result of a 1924 cartel agreement, when the largest manufacturers of electric lamps agreed for the first time to artificially limit the life of the incandescent lamps (they basically started manufacturing light bulbs of a degraded quality);

• at the same time, it is known that an experimental light bulb by Shelby Electric has been shining almost continuously since 1901 (more than 1.000.000 hours) at a fire station in Livermore, California, although its rated power of 60 W has since dropped to 4 W.

In the former case, when failures are unacceptable or undesirable, in order to ensure the required dependability, the products are made with structural reserve of working capacity. In the latter case, when failures are expected and allowed, a certain probability of maintaining the stability of the performance parameters by the end of the warranty period is ensured. In both cases, the dependability of products is characterized by failure-free operation, but it has a different physical meaning. In the former case, failures are not planned or implied, and in the latter case, they are not excluded, but rather planned, however they are allowed with a frequency of occurrence not exceeding a predetermined value.

For products that are considered only at the ultimate limiting state, these approaches differ in terms of choice of safety factors and safety margins that allow achieving the required dependability by varying them (programming breakdown or, on the contrary, making it unlikely). Strength calculations in the first approach are carried out by deterministic methods based on the mechanics of deformable solids, while in the second approach it is carried out by probabilistic statistical methods based on the probability theory and mathematical statistics.

If a product is in two or more limiting states, dependability calculations in second approach are carried out in probabilistic statistical setting using phantom elements method [1]. The modern dependability theory does not provide the answer to calculating dependability in the first approach, when a product can simultaneously be in several limiting states and at the same time should have dependability close to one, even though solving such problems in some cases is of critical practical importance, for example, for unique highly vital systems [2-8].

The paper examines the problems caused by the conventional view of the dependability that prevents the practical use of dependability analysis (assessment) as a tool for engineers involved in the creation of unique highly vital systems/products and substantiates proposals for their resolution.

Problem 1: How to calculate dependability without failure statistics? First of all, it should be noted that it is fundamentally impossible to create dependable products without studying certain characteristics and properties of materials, as well as units and components. Of course, it would be useful to have at least some failure statistics, if it is possible to obtain any. However, the question is whether it is necessary to conduct statistical tests before failure (without building probabilistic statistical models) in order to create products with specified dependability indicators.

Terminological definition apart, in regard to its semantic meaning dependability is something that will not let you down, something you can rely on for a long time. Fail-free operation speaks for itself, it is a manifestation of operation without accidents. There is no conceptual difference between dependability and fail-free operation with regard to non-repairable products: in both cases there should be *continuous operation without failures within a given time interval.* Now let us consider the terminological definition of GOST 27.002–2015, according to which dependability is the "ability of an object to fulfil the required functions in time…". With this definition of the term "dependability", a question (and even a problem) obviously arises, i.e. how to calculate *continuous fulfilment of the functions within a given time interval* (without failure), which (meaning functions) also need to be defined. For lack of anything better, the solution of a purely physical problem, i.e. the quantitative estimation of the property *to continuously fulfil specified functions over time,* was transformed through inversion into the solution of a mathematical problem, i.e. counting the events that reflect facts of not being able to fulfil the functions (failures). With this approach, it is not hard to register failures as events (without getting into the specifics of functional performance criteria or their number). Moreover, failures can be statistically analyzed, and the probability of their occurrence can be calculated

for any given time interval based on the statistical data acquired. Thus, instead of studying dependability as a physical property (as a result of changes in the internal state of an object), which ensures *continuous fulfilment of the functions within a given time interval,* dependability assessment has been reduced to studying *undependability,* a model in which failures are a priori possible (predefined). Eventually, studying actual causes of failures was reduced to studying their effects, i.e. failures as the results of events the causes of which are not always known. This approach is clear and convenient for mathematicians, but has neither sense nor value for engineers, since it is not clear how to use dependability calculations for making and analyzing real technical solutions.

As a result, a rather common notion appeared: dependability can only be quantitatively estimated by probabilistic statistical analysis of the failures of technology in operation, based on "reference data on the dependability of components and elements of an object, data on the dependability of similar objects ..." (GOST 27.002–2015). Meanwhile, the definition of the term "dependability" does not set any limitations on this matter. For example, according to the GOST there is no reason why dependability cannot be defined qualitatively (alternatively), if there is a way to ensure the "*ability to fulfil functions over time*" on the physical level and quantitatively estimate criteria of the required functions, which "*can be defined, for example, by setting for each function a set of parameters, characterizing the ability to perform it, and permissible limits for changing of these parameters' values*". After all, quantitative estimation of dependability is required when comparing different products with each other or a particular product with established development goals to evaluate their efficiency. However, this is not always necessary, for example, in the case of a unique production equipment, that cannot be compared to anything (the point here being to ensure the specified performance parameters during the service life). But without quality assurance of dependability (combined with specifying and justifying performance indicator values), it is impossible at the physical level to create a dependable product. At the same time, it is not always possible to accurately quantify dependability (logical and mathematical relations and dependences between quality assurance of dependability and its quantitative measure remain unknown without information on failure statistics). Meanwhile, the probabilistic statistical approach to dependability is firmly rooted in the GOST series Dependability in technics in the following forms: a restrictive list of products, to which statistical approaches can be applied, list of dependability indicators, standardized methods for determining (monitoring) dependability and dependability calculation methods etc. At the same time, it is quite obvious that any given quantitative requirement for dependability will be automatically met if the "*ability to fulfil functions over time…*" is provided on the physical level so that *the parameters characterizing the ability to perform them would certainly lie within the permissible limits of such parameters' variation* (as required by the GOST). Thus, the problem of calculating dependability as *continuous operation within a given time interval* centers around establishing the parameters of the structure's operation and justifying their values lying within permissible limits, not only (and not so much) around obtaining and processing statistical data on the products' behavior during operation.

Problem 2: Should the genesis of dependability be taken into account? The predominance of the probabilistic statistical approach in quantifying dependability resulted in a situation when, willingly or otherwise, "a blind eye is turned on" the genesis of dependability. Since the physical nature of any particular product's creation becomes somewhat unimportant, what is "important" is how its possible failures correspond to the chosen mathematical model. As a result, the focus of attention shifts from making and implementing specific engineering solutions to a model of products' behavior in operation (when it, unfortunately, becomes almost impossible to alter a poor decisions).

To fully realize how deeply the probabilistic statistical interpretation of dependability (or rather, undependability) is rooted in the regulatory documentation, let us take a look at GOST R 56526–2015, where an example of calculation of the dependability indicators of a single (small-batch) production unmanned space vehicle (USV) is preceded by the following hypothesis: "***It is assumed that*** *at the initial moment of time (the moment of the beginning of operating time calculation), the USV is in the up state...*". It is a rather strange situation: a highly vital product is made in only one copy, but instead of making sure that the product is 100% operational, it is **assumed** to be so with some probabilistic statistical behavior model (where would it come from for a one-of-a-kind product) with questionable distribution parameters being applied (operation is carried out in the space environment, and therefore it is, by definition, difficult to obtain experimental data with the necessary level of trust).

On the other hand, when an existing mathematical model has to be adjusted to a real physical object, assumptions and schematization of physical states and processes are always used and then are balanced out (adjusted) by selecting the model's parameters (that is the foundation engineering calculations). These parameters are selected based on a long-term observation and research practice. When it comes to unique highly vital products, for which there cannot be any reliable statistics, the assumption that the product is operational before the start of operation (i.e., that there are no fundamental errors in the technical documentation or manufacturing defects) is at least controversial. In the case of batch products that means "turning a blind eye" to the fact that the developer or manufacturer, like all people, can make mistakes. These mistakes lead to any product having a heredity of failures long before the start of operation, which can manifest itself in the

course of operation. Moreover, each stage of the product life cycle, starting with the preparation of the design and operational requirements, has a certain degree of criticality of hereditary factors due to the probability of loss of function, while the heredity itself is subject to the laws of realization. As shown in [5, 9], the conditional reliability of products defined by the failure heredity factors, has a tendency to accumulate before the end of the design stage, reaching its local maximum, and to spend starting from the stage of preproduction engineering, reaching a certain local minimum by the time of operation. That minimum should be taken as the initial conditions in the development of highly vital products.

It is important to understand that any development testing is a sort of quasi-operation (usually carried out under tougher conditions compared to normal operation) that is performed on a limited number of test objects (for financial and economic reasons). This suggests that for the purpose of justifying the target reliability the sample size may simply not be sufficient for evaluation of the test results with the required level of confidence (even given the tough testing). That is due to the fact that in the course of operation a combination of product technical statеы, operating modes, external loads and effects may occur that was not covered or technically infeasible during simulation at the testing stage.

Hence is the task of identifying and eliminating the potential hazard of improbable failures at the early stages of unique highly vital systems development. That can only be achieved by considering the genesis of their dependability [5, 9].

Problem 3: How to prevent improbable failures? The conclusion that the performance demonstration during testing does not guarantee the absence of failures during operation directly follows from the total probability formula

$$R(t)+Q(t)=1. \qquad (1)$$

Obviously, the dependability function $R(t)$ in formula (1) is defined by the up state of an object, while the failure (undependability) function $Q(t)$ is defined (similarly to the dependability function) by the *fallible state* of the object. If not proven otherwise, an object by default can simultaneously be in two states at any moment in time: up state and fallible state. For some reason, this obviously and important fact is not reflected in the dependability terminology (the concept of "*fallible state"* is not used in the regulatory documentation).

An important conclusion follows from (1): any methods for performance parameter calculation and product testing with limited sampling provide only a certain extremum of the dependability function $R(t)$ (which is not known in advance). This is a consequence of the ever-present uncertainty of the total probability's second component, the failure function $Q(t)$ that characterizes the occurrence of improbable events. For example, failure statistics for USV deployable structures [9] shows that, in practice, the existing modern computational and experimental methods allow achieving a dependability level of no more than 0.996 (while the acceptable requirement is at least 0.999). Therefore, in no case dependability can be evaluated (even indirectly) based on positive results of computational and experimental testing. It can only be argued that, for example, the successful experimental development (including flight tests) showed that the product demonstrated its performance n times successively.

If the specified dependability level $R(t) > \underline{R}$ has to be demonstrated, objective evidence must be provided to prove that

$$Q(t) < 1 - \underline{R}. \qquad (2)$$

The fulfillment of condition (2) obviously cannot be confirmed only by computational and experimental identification of the performance parameters.

Thus, for highly vital systems, the *direct* methods of confirming the specified level of the failure function (non-dependability) (2) must be used in addition to the computational and experimental demonstration of the performance parameters. The easiest solution is to carry out dependability tests, however, for financial and economic reasons they are not acceptable for costly highly vital one-of-a-kind products. All that is left to do is perform additional analysis to identify improbable failures, which should be carried out in parallel with the computational and experimental performance assurance (preferably with the use of a single data base). That requires the appropriate methodological framework for such analysis, which is not yet provided for in the regulatory documentation on dependability.

Problem 4: Fuzziness of dependability terminology. We are not even talking about the term "dependability" (its functional and parametric definition [6, 9 – 11]) that did not become clearer with the introduction of the new standard GOST 27.002–2015. In view of the above, it is much more important and useful to consider the term "up state". It is the author's opinion that one of the main problems of dependability of unique highly vital systems lies in the fuzziness of this term's definition. Let us put aside the vague definition in the new standard and assume that its essence has not changed with the introduction of the notes (clarifications), and therefore we can use a clearer definition of the term from the repealed standard. Thus, up state is *"a state of an object, in which the values of all parameters characterizing the ability to fulfil the specified functions comply with the requirements of regulatory and technical and/or design (project) documentation"*. In other words, in order to identify the up state one must not only identify "*the values of all parameters…"*, but also make sure that each of these parameters complies with "*the requirements of regulatory and technical and/or design (project) documentation"*, which should be timely speci-

fied there in advance (not after the failures occur, but at the end of the documentation development).

Here, the author sees semantic inconsistencies at the system methodology level. It is quite clear that in order to manufacture and operate a product in accordance with the design documentation (this particular documentation, not some "other documentation", as the new standard GOST 27.002–2015 interprets, since *design documentation* ***alone*** can be the basis for the manufacture of a product), it should contain all the necessary and sufficient requirements. Moreover, in order to develop error-free design documentation, the engineer must determine all the necessary and sufficient design parameters that characterize the ability to fulfil the specified functions, demonstrate the values of the chosen parameters and establish necessary and sufficient requirements for the manufacture that strictly correspond to the chosen design parameters. Not being able to perform any of these actions and/or to establish their criteria may lead to failures. However, these highly important concepts (how to identify all the necessary and sufficient parameters and ensure that they are relevant to the established requirements) are not reflected in any way in the terminology or in other provisions of the "Dependability in technics" series of standards.

Moreover, it is clear that in order to fulfil the specified functions, the values of a structure's design parameters must lie within the permissible limits during operation, ensuring its up state. It is also obvious that a state when the parameters' values are at the boundaries of the permissible range is a limit state; and a state when the parameters' values are outside of the permissible range is beyond the limit (disabled state). The transition of the parameters' values across the boundaries of the permissible range is called a failure. Thus, the limit state is determined by the formula

$$X_{lim} = \begin{cases} \overline{X} \\ \underline{X} \end{cases}. \tag{3}$$

From (3) follows the formula of the up state:

$$\underline{X} \le X \le \overline{X}. \tag{4}$$

From (3) – (4) follows the formula of the disabled state, which leads to failure:

$$X \in \left\{ \left(X < \underline{X} \right) \vee \left(X > \overline{X} \right) \right\}. \tag{5}$$

Formulas (3) – (5) clearly show that the concept of "limit state" not only plays a key role in determining the durability property (as interpreted by modern dependability terminology), but it is also directly related to dependability in general and, first and foremost, to fail-free operation.

Problem 5: How quality and dependability are related. Today, there is a firm understanding – at the level of regulatory documents – that quality among other things is characterized by dependability indicators. In other words, dependability is an integral part of quality. However, this is not quite so [3, 9]. Quality, as well as all its lower level properties, is determined by the relations of things in the form of collocation, interconnections and interactions, i.e. in the current state. At the same time, these relations themselves have a tendency to change over time, and it is this property that we call dependability. It characterizes in time the quality of products and, accordingly, each of the properties of quality individually.

With the definition of the term "operation" (GOST 22487–77) being a process of manifestation of the required properties in accordance with a given algorithm, the expression (4) can be interpreted as a formula for the quality of a product in up state. Thus, the dependability formula is

$$\underline{X} \le X(t) \le \overline{X}. \tag{6}$$

In a parametric form, formula (6) can be written as follows:

$$X(t) \in D = \left\{ X_i(t) \middle| \underline{X}_i \le X_i(t) \le \overline{X}_i ; t \in \left[\underline{t}, \overline{t} \right]; \forall i = \left[1, \overline{n} \right] \right\}, \tag{7}$$

where D is the domain, inside which the general dependability parameter $X(t)$ lies.

Taking into account (6) – (7), full dependability can be calculated as follows[1]:

$$R(t) = P\left\{ X(t) \in D; t \in \left[\underline{t}, \overline{t} \right] \right\} \tag{8}$$

Formula (7) conforms with the definition of the term "dependability" according to GOST 27.002 (old and new editions), and formula (8) conforms with the conclusions of the general dependability theory for mechanical systems of V.V. Bolotin [12].

The connection between quality (4) and dependability (6) is naturally determined using the dependence [9]

$$X = \lim_{\Delta t \to 0} X(t + \Delta t). \tag{9}$$

Formula (9) shows that dependability is a continuous function of time, and quality is some kind of a point locus on a dependability function curve. There is no "frozen" quality (inherent to the product once and for all), it constantly changes over time due to physicochemical processes, and it is exactly in relation to this change that quality is characterized by dependability. Quality can be identified at any fixed moment in time, for example, by means of direct or indirect measurements of product parameters with non-destructive testing. Dependability cannot be measured, it can only be predicted based on calculations (8) or by identifying the probability of each of the parameters' values being within a given range (6)

$$R_i(t) = P\left\{ \underline{X}_i \le X_i(t) \le \overline{X}_i ; t \in \left[\underline{t}, \overline{t} \right] \right\}. \tag{10}$$

[1] R – Reliability (dependability); P – Probability

For products with a serial connection of critical elements (if their parameters are independent in terms of dependability), full dependability with regard to (10) is calculated using the formula

$$R(t) = \prod_{i=1}^{n} R_i(t). \quad (11)$$

Solutions to the considered problems of dependability. Formulas (6) – (11) allow analyzing and synthesizing dependability by performance parameters, which makes it possible to move away from probabilistic statistical approaches and move on to ensuring dependability based on physicality (laws of cause-and-effect relationships) and physical necessity (non-contradiction to the laws of nature) of failure causes.

Analysis and synthesis of dependability by performance parameters (at least for highly vital products) should be obviously carried out taking conditions (1) – (2) into account. In order to do so, a full parameterization procedure is performed, during which the drawing and technical documentation is presented in the form of column vector of performance parameters characterizing the full functionality of the product structure in the following form

$$X = \left(X_1, X_2, \ldots, X_i\right)^{\mathrm{T}} \ \forall i = \left[1, \overline{n}\right]. \quad (12)$$

Column vector (12) is the basis of the parametric representation of the structure (7) and does not take into account the differences in ranking (for example, the frequency of events: never, rarely, frequently) and/or in significance (for example, the severity of malfunction: significant, insignificant, critical, catastrophic) between possible failures as events not being able to fulfil specified or intended functions (this is the only way improbable failures can be identified). The construction of the column vector in practice is done by performing successively the following procedures of dependability engineering and design analysis (DEAD) [4, 7-9]:

• identify functions that ensure the performance of the structure, which must be taken into account when making engineering decisions, and identify failures as hypothetical situations that interfere with the fulfilment of each of the functions in question;

• identify causes, directly leading to failures, which occur, exist and develop in environmental conditions as a combination of environmental factors and operating modes, taking the worst possible combinations into account;

• determine the properties of critical structural elements, which make each of the failure causes impossible (the failure causes are countered by the prescribed properties of the corresponding critical elements);

• each of the properties of critical elements is quantified using parameters (indicators), which ultimately belong to the desired column vector (12).

After the column vector is determined, the D (7) domain is defined. For that purpose, each parameter (indicator) is assigned a range of its permissible values based on the development (product design from the customer's point of view, specified requirement) and structural design (product design from the developer's point of view, implied requirement) requirements specification.

Then, dependability is calculated by formula (8) or (11), using stochastic methods to evaluate whether parameters' values of the structure lie within the permissible range (for example, individual design dependability method [13], which takes into account individual statistical characteristics of the parameters' distribution under specific production conditions). The other way is to ensure performance parameters margin by design so that they would fall in a given range with a permissible confidence level (for example, DEAD [4, 7-9]). The dependability calculated in this way shows how much the selected performance parameters comply with the requirements of the technical specification for dependability (basically, this is the expected or design dependability).

It should be noted that with a proper choice of the performance parameters margins (when DEAD is used), the expected dependability is $R(t) \equiv 1$. In order to translate this dependability into practice, error-free design and technical documentation should be developed, and critical defects should be eliminated at the production stage. For that purpose, DEAD provides certain procedures for verification of parameters' compliance with specified requirements in regulatory, design and technical documentation, as well as compliance control procedures. Dependability calculations are adjusted based on the results of these procedures, and final conclusions on the compliance with the dependability requirements are made [4, 7-9].

Thus, not only the dependability problems listed above are solved, but also some problems beyond the dependability.

Problem 6: Why doesn't the quality management system always guarantee quality and dependability? A quality management system (QMS), for example, ISO 9001 is a set of procedures (methods of carrying out activities), which allow converting drawing and technical documentation into an end product during the manufacture in strict accordance with the established requirements.

QMS can be visualized as millstones. If you add grain, you get flour; if you add garbage, you get the same garbage. The reason is that there are no formalized procedures that would separate (sort the "grain" from the "garbage") correct (sufficient) requirements from incorrect (insufficient) ones. Obviously, technical quality management procedures (that are rarely mentioned in the present day) should be applied together with the QMS procedures formalized in the ISO 9001 standards.

The DEAD procedures, namely parameterization (12); substantiation of parameters' values being within the permissible range (4) and (6); regulatory and technical documentation requirements definition; verification of parameters' compliance with specified requirements, fulfil a function of technical quality management [4; 7-9].

Problem 7: How does dependability affects development costs? It is generally believed that the development costs directly depend on the values of the specified dependability indicators (it is assumed that heavy expenses are the price paid for high dependability). This seemingly obvious connection is in fact a delusion in some way. If we proceed from mathematics, then everything seems to be true. According to the classic concepts of the dependability theory [14], the lower one-sided confidence limit for estimating the probability of failure-free operation when conducting a series of tests without failures is calculated by the formula:

$$\hat{P}_{н} = (1-\gamma)^{1/n}. \qquad (13)$$

From (13) it follows that, for example, with a dependability confidence level of $\gamma = 0.9$, the demonstration of no-failure operation $P = 0.9$ will require a minimum of $n = 22$ independent tests of homogeneous products; if $P = 0.99$ $n = 230$; if $P = 0.999$ $n = 2302$; if $P = 0.9999$ $n = 23025$. Hence the conclusion that with each "extra" nine the development cost should increase by an order of magnitude. However, such "accounting approach" is not always reasonable in real life, because, according to (6) – (12), future production costs can be significantly and effectively reduced at the earliest stages of the life cycle by developing error-free design documentation (with mandatory use of DEAD) and organizing defect-free manufacturing by QMS methods, for example, ISO 9001.

Moreover, this early stage failures prevention technology is fully consistent with the well-known "tenfold cost rule" (if there is an error at one of the stages of the product life cycle, which was detected at the next stage, fixing it will cost 10 times more than if it was detected on time).

Conclusion

The application of design methods for the dependability analysis (assessment) allows – within the framework of existing views, yet with certain corrections – solving dependability-related problems without the use of the mathematics of the classic dependability theory. High dependability can be achieved by the same ways as non-dependability comes about, i.e. through design and process engineering solutions. The analysis, substantiation of engineering solutions and specification of necessary and sufficient requirements for the manufacturing process allows achieving the target dependability by engineering means through higher quality of design and process engineering.

If we regard dependability as a multiparametric property, parametric models of products (statistical, mathematical, physical, virtual or digital) can be developed that enable the evaluation of the temporal stability of parameter values using methods of individual design dependability [13] and/or DEAD [4, 7-9]. The principles of unity of the design concept and its implementation in manufacture enables the development of products and assessment of their dependability based on a single foundation, i.e. the design and process engineering solutions directly associated with the capabilities of a specific manufacturing facility.

References

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

[2] Pokhabov Yu.P., Ushakov I.A. 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].

[3] Pokhabov Yu.P. About the philosophical aspect of dependability exemplified by unique mission critical systems. Dependability 2015;3:22-27.

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

[5] Pokhabov Yu.P., Valishevsky O.K. Genesis of dependability of unique safety critical systems. Dependability 2016;16(3):47-53.

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

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

[8] 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.

[9] Pokhabov Yu.P. 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].

[10] Netes V.A., Tarasiev Yu.I., Shper V.L. Current issues of terminology standardization in dependability. Dependability 2014;2:120-123.

[11] Netes V.A., Tarasyev Yu.I., Shper V.L. How we should define what «dependability» is. Dependability 2014;4:15-26.

[12] Bolotin V.V. Prognozirovanie resoursa mashin i konstruktsiy [Lifetime forecasting of machines and structures]. Moscow: Mashinostroenie, 1984 [in Russian].

[13] Timashev S.A., Pokhabov Yu.P. 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].

[14] Volkov L.I., Shishkevich A.M. Nadiozhnost letatelnykh apparatov [Aircraft dependability]. Moscow: Vyshaya shkola; 1975 [in Russian].

About the author

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

Received on: 16.08.2018