Original article
https://doi.org/10.21683/1729-2646-2020-20-2-3-11

Dependability in digital technology

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

Yuri P. Pokhabov

Abstract. Aim. *The migration towards the Industry 4.0 digital technology will soon enable "right first time" (virtually with no material expenditures for experimental testing and subsequent design improvement) creation of increasing numbers of entities with unique application properties. Calculating the dependability indicators of such entities based on reliable statistical data will be greatly challenging. However, the need for dependable entities will remain. Additionally, the approaches to digital technology based on physical models and engineering knowledge enable the creation of predictive dependability methods (based on the assumption of non-acceptability or, contrarily, intentional programming of failures). That inevitably causes a paradigm shift in the modern dependability theory associated with a forced deviation from the mathematical models as the basis of the dependability theory.* **Methods.** *According to the Russian tradition, dependability is normally defined by specifying the required functions through a set of parameters that characterize the ability to perform them and the allowable variation limits of the parameter values. If the criteria of some required functions cannot be specified through parameters, a technique can be used, whereas the operation of the item is substituted with an information model in the form of a black box, in which the performance of the required functions is characterized by probabilistic indicators of failures (statistical, logical, Bayesian, subjective). In order to account for the parameters and probabilities of performance of the required functions in a coordinated manner, finding the values of the parameters within the allowed range can be characterized by the probability as the degree of confidence in the occurrence of such event, for example accounting for design reserves. In this case the performance of all the required functions can be characterized by an additive dependability indicator that is identified using the method of dependability structure diagram. This indicator completely characterizes the predicted dependability level.* **Results.** *Predicted dependability is estimated using the method of design engineering analysis of dependability (DEAD). This method allows using a set of algorithm-based techniques to present the design (per GOST 2.102) and process control (per GOST 3.1102) documentation for a technical item in the form of a generalized parametric model of operation. Such model allows taking into consideration the individual specificity of the design of entities based on the unity of functionality, operability and dependability, and thereupon estimating the probability of failures. DEAD and digital design algorithms are completely compatible and driven by common problems related to the substantiation of design solutions for the purpose of elimination (reduction of probability) of errors able to cause failures based on analytical, computational and experimental verification.* **Conclusions.** *Digital technology provides a tangible opportunity of predicting, reducing the impact or eliminating possible failures. That can be achieved through the same means that often cause failures, i.e. design engineering. For that purpose, it is required to create new applications of the modern dependability theory based on engineering disciplines and design engineering methods developed for ensuring quality and dependability of entities.*

Keywords: *digital technology, dependability theory, dependability prediction, unique highly vital system, design engineering analysis of dependability (DEAD).*

For citation: *Pokhabov Yu.P. Dependability in digital technology. Dependability. 2020;2: 3-11. https://doi.org/10.21683/1729-2646-2020-20-2-3-11*

Received on: *24.01.2020* / **Upon revision:** *17.04.2020* / **For printing:** *17.06.2020.*

Introduction

During the closing of the MMR-2004 conference in Santa Fe (US), a discussion titled "Is Reliability Theory Still Alive?" was held that defined the theme of Igor A. Ushakov's article that concluded: "The need for pure theory may be not as pressing as it used to be, yet the need for applications of the dependability theory for solving practical tasks was, is and always will be!" [1]. The list of problems that can be solved through the development of new applications of the dependability theory was published four years ago at the plenary meeting of the MMR-2000 conference in Bordeaux (France) in the presentation titled "Dependability: past, present, future" [2]. Despite the efforts made, some of the mentioned problems of the dependability theory are still unsolved, including, for instance, dependability of unique highly vital systems (entities, items) [3].

Over the past years, the fourth industrial revolution added new unsolved problems to that list [4]. Todays' generation of engineers can hardly imagine the technological changes caused by the results of this revolution, but we must start preparing for it right now. Meanwhile, as a forerunner of the predicted future, new directions in engineering have emerged and have been developing: system engineering ("right first time" design) [5] and Industry 4.0 digital technologies ("right first time" entity development) [3]. A trend is becoming popular, whereas the dependability indicators in digital engineering are not considered as a target. It is thought that if target values of operational integrity and resource limitations (time, financial, technological, industrial, etc.) are achieved, the dependability is ensured by default [5, 6]. For example, the residual life of an entity can now be set and defined in an explicit form (parametric form) according to the results of numerical simulation of physical processes resulting in its loss. The term "dependability" becomes blurry: dependability seemingly still exist in digital technology (it still needs to be ensured), but it is not clear how to control the dependability indicators (most processes related to the development and optimization of entities are transferred into a virtual computing environment, production of material objects for – primarily – experimental testing is minimized, and the mathematics of the modern dependability theory are not adapted to this). However, the most important is that the basic principle of the modern dependability theory, that, according to Alexander S. Pronikov, consists in the *statement of a certain level of dependability for a machine with expired service life* [7] is not good for anyone even today.

If, as part of finding solutions to future problems, the approaches to dependability do not change, then for the next generation of engineers the value of the modern dependability theory may die down, as it does not contribute to the development of new engineering ideas. Nothing can be done about it, it has been and remains: "*We know that every age has its own problems, which the following age either solves or casts aside as profitless and replaces by new ones*" [8]. And it's time to ask a question much more dramatic than in the early 2000s: Do we really need a dependability theory in the digital age?[1] By asking such a provocative question, the author does not in any way reject the dependability theory, strength of materials or any other engineering (technical) disciplines, and therefore asks another question: What requirements should the dependability theory applications and other engineering disciplines meet in the digital age?

Problems of the dependability theory for digital technologies

Since any technical entities are developed by engineers working on computers, it would be fair to suppose that in the digital era the skills and knowledge related to calculating formulas are also necessary and important, just like before the advent of computer technology (at least for the purpose of evaluating the effectiveness of own activity). The more so since a computer is just a high-performance calculation device (whether it is used for drafting or finite-element calculations). When solving engineering problems, a computer does not independently search for areas where the end result should be, but only performs specified calculations using established algorithms. The human prerogative is to apply the available computing resources to the required area to obtain the most optimal result by setting the appropriate initial data [10]. Without the knowledge of the principles of natural science, engineering disciplines and the ability to do elementary engineering calculations, that problem can hardly be solved adequately. The more so since (according to one of the definitions in GOST 27.002–2015) dependability is intended to be somewhat of the pinnacle of engineering (in order to define "**the values of all parameters** *that characterize…* **required functions**"), and in the age of computers dependability acquires even greater significance, not the other way around. First, the items' ability to perform the required function with specified dependability will remain the main goal of any development. Second, failures in operation (depending on the purpose of the items) must become predictable (unacceptable or, conversely, intentionally programmed). Digital technologies are intended exactly for that, i.e. to simulate adverse events and thereby enable the selection of optimal results. In the author's opinion, new applications of modern dependability theory should be applied to those problems in order to prove useful in the implementation of digital technology.

[1] Though this question might seem unreasonable, today the idea is seriously discussed that a modern engineer who is involved with computing does need no knowledge on strength of materials as that will be replaced by software [9].

Barriers of modern dependability theory on the way of digital technology

Computer calculations are performed according to the established algorithms (exact requirements that define the sequence of elementary operations with initial data), be it simple arithmetic operations or numerical solutions of differential equations. It is impossible to directly calculate dependability using computer calculations, since it cannot be expressed, calculated or measured using physical values, primarily, due to the multifactorial and interdisciplinary nature of the causes of possible failures that cannot be algorithmized. For this reason, before the age of computers, special mathematics were developed for the purpose of calculating dependability indicators; they allow identifying dependability using a posteriori knowledge about possible failures, i.e., in fact, through the experience of undependability. The result is an endless vicious circle, whereas it is required to know a technical item's undependability to calculate its dependability. The availability of appropriate failure statistics makes it easy; difficulties start when there is no database to obtain failure statistics, for example, if there are no prototypes, the items are one-of-a-kind (unique)[1] or failures are unacceptable under the operating conditions. There are no regulations or guidelines on dependability that could provide guidance on what to do in this case.

The Reference Annex of GOST 27.002-89[2] explicitly states that the area of dependability indicators calculations (according to the rules of the statistical theory of dependability) is limited to large-series items only. For unique and small-series items, calculations using methods of the statistical dependability theory are limited to only the cases when the dependability indicators can be calculated according to known dependability indicators of components and elements. In [11] the feasibility is substantiated, but it requires data on the dependability of components and elements that can be obtained from statistical tests in the amount of parent universe, which, for example, is almost impossible in the case of unique highly vital systems due to financial limitations [12].

With the deployment of digital technology, the problem of dependability calculation based on statistical dependability theory is exacerbated, since the number of test (engineering) models used in the development and commencement of product manufacture will inevitably reduce due to the virtualization of real processes (actions, inspections and tests) related to material objects [6]. Thus, the basis of statistical methods of the dependability theory, i.e. accumulation and processing of statistical information on item failures, disappears due to the application of digital technology. There is no point in setting probabilistic dependability indicators as input data for digital computing not only from the standpoint of the fundamental principles of the statistical dependability theory (due to the lack of information on failures). The probability itself is not subject to direct computer calculations, as it is a numerical measure of the events that is independent from the algorithm of their occurrence.

Nevertheless, if it is possible to calculate the value of a certain parameter and correlate it with limit permissible parameters, then we can talk about the probability of finding the value of this parameter within a permissible region (as a degree of confidence in the occurrence of such event[3]). If a technical item can be represented with a set of parameters and permissible limit values, then this makes it possible to identify its dependability as an additive indicator that characterizes the performance of the required intended function when modeling possible scenarios of events in operation (essentially, as an indicator of predicted dependability). It is not difficult for modern computers to calculate the favorable (unfavorable) outcomes, provided an appropriate calculation algorithm is defined. However, modern applications of the dependability theory do not provide such algorithms.

Current quality of the solution of highly vital item dependability problems

The barriers of the modern dependability theory on the way of digital transformation equally impede the development of highly vital items without prototypes. The lack of the required statistical data and difficulty of calculation of dependability indicators lead to the realization of the fact that calculations themselves only serve an auxiliary function in the adoption of engineering solutions in the course of development, leaving the leading role to the methods of expert assessment and verification, which is reflected in foreign regulatory and literary sources:

- *NOTE The "probability of failure" and its corresponding reliability index are only notional values that do not necessarily represent the actual failure rates but are used as operational values for code calibration purposes and comparison of reliability levels of structures.* This is one of the explanations in the Eurocode EN 1990:2002 standard of the European design system;

[1] A one-of-a-kind (unique) product is a product that is one of a kind in terms of its design or unique in its extreme rarity/significance [OST 134-1032–2003, article 3.1].

[2] GOST 27.002–89 was cancelled in 2017 but the Reference Annex can be considered as a separate source, since it was written based on 12 publications, most of which constitute the very foundations of the modern dependability theory.

[3] Probability is a real number ranging from 0 to 1 related to a random event. Note: the number may indicate a relative frequency in a series of observations or the degree of confidence that some event will occur. The probability is close to 1 for a high degree of confidence [GOST P 50779.10–2000, article 1.1].

- *…it is more important to identify and, if possible, mitigate the consequences of failure modes by design measures than to know the probability of their occurrence.* That is an explanation of the definition of failure modes in IEC 60812:2006;
- "*…all methods of reliability assessment require expert evaluation. When we approach that, the probability values are much like a label that an engineer put on a structure to show what he thinks about its reliability*", said Charles Harlan, former Director, Safety, Reliability and Quality Assurance of the Space Shuttle program [13].

The above views were put into practice in the NASA and ESA standards, where calculations are part of the processes of analytical and experimental verification of rocket and space technology. However, in practice, the results of such verification still leave much to be desired. For example, after the crash of the STS-51L Challenger Shuttle, the application of one of the main tools of analytical verification (the FMEA method) was sharply criticized in the US engineering circles [13]. According to the results of preliminary analysis of possible failures and their consequences, only one out 10.000 flights was supposed to end in a crash. However, in practice, two shuttles crashed as a result of 135 flights (Challenger in 1986 and Columbia in 2003). That constitutes an unprecedented catastrophic error in the practice of FMEA application: the actual fail-safety was 0.985 instead of the predicted 0.999 9. A similar result follows from the 2009 – 2016 failure statistics of deployed structures on foreign and Russian spacecraft. The average fail-safety of deployment mechanisms did not exceed 0.996 instead of the permissible fail-safety of at least 0.999 5 (with reservations assuming that this assessment is overestimated due to incomplete failure statistics) [14]. It should be taken into account that, in practice, in each case the results of dependability calculation (verification) in accordance with the current regulations must confirm the above permissible fail-safety, otherwise the spacecraft would not have been launched due to design insufficiencies. The investigation of the real causes of failures was carried out to clarify why the results of dependability assessment do not correspond to reality. The investigation results showed that in most cases the causes are rare in their nature that, in turn, is defined by an unfavorable combination of manufacturing tolerances, unaccounted factors of technological heredity, as well as external effects that today's dependability verification methods do not consider [14]. It was also revealed that for highly vital products, any rare cause of failure can reduce the accuracy of the dependability assessment, while, in practice, the total calculation error can reach at least a magnitude order of the significant figure[1], which is confirmed by the above examples.

Approach to predicting the dependability of highly vital items

Let us assume that the operation of any item can be represented with a set of parameters, the values of which can vary within the given ranges (i.e. in strict accordance with one of the definitions of dependability). Each of these parameters is considered from the standpoint of resilience to possible failures under external effects that, in turn, determine the limits of value variation of the analyzed parameters [15]. In this case, combining the effect and resilience parameters it is possible to build a fail-safety operation model based on physical laws that takes into account the temporal variation of the limit values of the considered parameters. Such model, as opposed to mathematical models of the dependability theory is suitable for predicting dependability (an example of a similar model for spacecraft rotating rod is provided in [16]). In such model, the list of these parameters characterizes the item's functionality (properties determined by the presence and set of capabilities to perform the required functions), the specified range of parameter values variation characterizes its operational integrity (a state in which an item can perform the required functions), and the probability of the parameter values being within the given range during operation characterizes the dependability (the ability to maintain the performance of the required functions in specified modes and conditions of operation) [16].

Based on the fact that all item failures occur due to the physicality (causal connections) and physical necessity (consistency with the laws of nature) of the causes that generate them (whether we know these causes or not), then based on the knowledge of the laws of physics, it is possible to build a parametric model of the item operation that determines its functionality, operational integrity and dependability based on a single database of parameters and ranges of their permissible values. The construction of such model is based on the knowledge of the physical principles of nature at the levels of micro world (the world of elementary particles, atoms, molecules and molecular compounds), macro world (the world of persistent forms and values commensurate to human) and the mega world (the surrounding world commensurate to the universe). The values of the parameters of the parametric operation model are calculated by known methods of engineering disciplines, i.e. the theory of mechanisms and machinery, theory of theoretical mechanics, material resistance, machine components, etc.

If there are not enough knowledge and understanding at any level of the world structure to calculate the values of the parameters of the parametric model of item

[1] By analogy with engineering calculations, this corresponds to the accuracy of the sought result not by percentage points (usually, the error is 5÷10%), not even several times (for example, two or three times), but by orders of magnitude, i.e. not less than ten to a hundred times (!).

operation, it is possible to use the well-known technique, according to which the operation of any of the components of the item is replaced with the information model in the form of a black box where the performance of the required functions is characterized by probabilistic failure rates (statistical, logical, Bayesian, subjective). It is necessary to bring the values of parameters and probabilistic indicators to a consistent nondimensional form in order to take into account the probabilistic indicators of such information models and calculate the dependability using a generalized parametric model of item operation. For this purpose, the probability of the parameter values being within the acceptable range is identified (based on their physical understanding [16]), upon which all probabilities regardless of their origins (based on physical or information models) will be available to calculate the dependability using the method of structural dependability scheme [14, 16]. At the same time, this does not contradict the idea of calculating the dependability of unique and small-series items according to known dependability indicators of components and elements.

Two interchangeable methods can be used to determine the probabilities of parameter values being within the allowable range: deterministic (setting the design margins for each of the parameters in such a way as to guarantee with certain confidence that their values are within the allowable range) [14] and stochastic (for example, by assessing the individual structural dependability [17], i.e. calculating the probabilities of parameters being within the allowable areas based on individual characteristics of materials, loading/impact processes and product manufacturing processes). The interchangeability of these methods can be explained through the example of a strength calculating model of the “load parameter – strength parameter” type, whereas the probability of failure-free operation equals the probability that the value of the load parameter will never exceed the value of the strength parameter within a given period of time. Moreover, even if both parameters are random functions of time, it is possible to solve the dependability problem in a deterministic statement of the calculated values of the load and safety margins [16] by applying structural margins according to GOST R 56514–2015, i.e. by “expanding” the range of real values of the “load parameter” with safety factors and/or “narrowing” the allowable range of the “strength parameter” using safety margins. This method is widely used in the rocket and space industry.

Examples of structural margins used in practice in the form of redundancy, safety factors, safety margins and drive torque (forces), parametric redundancy, power and thermal decoupling, procedures for obtaining guaranteed results, for example, using minimax criteria or engineering psychology factors, are provided in [14, 16]. All structural margins are assigned based on the rules of the statistical dependability theory (for example, safety factors and safety margins [18]), proven application practices (for example, margins of drive torque (forces) [14, 19–20]), design methods aimed at removing limitations on output parameters variation (for example, by using power and thermal decoupling [21–22]), or other organizational and technical actions that reduce or eliminate the probability of failures.

In the general case, for example, for deploying structures of spacecraft, the dependability in terms of strength can be calculated using the deterministic method according to GOST R 56514–2015, and dependability in terms of operation can be calculated using the stochastic method [20], or in any other combinations [14, 17]. Furthermore, the use of structural margins for solving dependability problems in a deterministic formulation not only simplifies the selection and substantiation of parameters when designing items, it is also one of the important conditions for compiling the initial data for digital design in the form of a matrix of target indicators and their limitations [6].

Design engineering methods for solving the dependability problems of highly vital items

Various aspects of the above parametric approach to solving the dependability problems of highly vital items (philosophy, genesis, definitions, theoretical issues, models, calculations, practical applications, etc.) were considered in detail in [14]. They served as the basis for the design of the method of engineering analysis of dependability. That technique, relying both on engineering disciplines and the mathematical foundations of the dependability theory (if acceptable and justified), allows analyzing and taking into account individual design features of products, which makes it possible to predict dependability in the design and construction of technical objects without prototypes.

DEAD is based on a generalized parametric model of operation in the form of [16]

$$\left\{X_i\right\} = \left(X_1, X_2, \ldots, X_i\right)^T \ \forall i = \overline{1,n}; \tag{1}$$

$$D_x = \left\{X_i\left(t\right) \mid \alpha_i \le X_i\left(t\right) \le \beta_i\right\}; \tag{2}$$

$$R = P\left\{X_i\left(t\right) \in D_x,\ 0 < t < t_к\right\}, \tag{3}$$

where $\{X_i\}$ is a set of output parameters X_i, that determine the performance of the required functions in the form of a column-vector (functionality of the object); D_x is the acceptable region of output parameters $X_i(t)$ (operational integrity of the object in the permissible ranges of parameter values α_i and β_i); R is the dependability of the object as the probability P of values of the output parameters $X_i(t)$ being within the region of their permissible values of D_x within the time to failure $t_к$.

DEAD is a sequential set of algorithmic methods that allow presenting the design (in accordance with GOST 2.102) and process engineering (in accordance with GOST 3.1102) documentation of a technical item (i.e. its text-and-graphic or digital model depending on the development method) in the form of a generalized parametric model of operation (1) – (3). The procedures of the technique allow (in a generalized form):

- initialization of the item in the form of parameterization (turning it into a set of parameters and permissible ranges of their variation), which is carried out to establish conditions (1) – (2);
- calculations of theoretical dependability by design parameters carried out according to (3);
- providing evidence that the analysis (assessment) of dependability corresponds to the reality (the requirements of design and technological documentation, production conditions, quality control methods), for which the relevant risks assessment is carried out [23].

The application of the generalized parametric model of operation (1) – (3) and the DEAD [16] does not violate the basic principles of dependability theory. Along with the applied methods of the dependability theory (mathematical, statistical and physical), design engineering methods allow expanding the capabilities of the dependability theory for predicting the dependability of technical objects and making dependability problems understandable and accessible for engineers. DEAD was tested in the design of single-use mechanical space devices and hydraulic assemblies of oil well equipment [14], which allowed:

- detecting design and process engineering errors in the technical documentation;
- evaluating the effectiveness of the existing computational and experimental optimization of product design;
- assessing the adequacy of the established requirements in the design documentation;
- identifying unacceptable combinations of structural parameters based on the design constraints, actual manufacturing and control conditions;
- drawing conclusions regarding the propensity to failure of products;
- predicting the compliance to the specified dependability requirements;
- providing recommendations regarding design modifications to ensure specified dependability of products.

Comparability of DEAD with existing predictive approaches to dependability

The idea of dependability analysis (evaluation) with account of design and technological factors is not new. Its relevance was repeatedly noted and demonstrated, for example, in [24–26]. However, analysis and evaluation methods for design engineering factors that allow designers of highly vital systems making their decisions taking the dependability into account are yet to be developed (as far as the author knows).

Certain aspects of accounting for design factors that affect dependability are well known in the literature. For example, the basics of calculating the dependability by strength are set forth in [27], and approaches to calculating the dependability of the mechanical parts of an aircraft subject to the requirements of strength and undisturbed operation in case of deployment mechanisms actuation, are shown in [28, 29]. The parameters by which dependability is calculated in the indicated examples are part of the column-vector (1). Operational integrity and dependability are calculated using formulas (2) – (3), taking into account the physical foundations of ensuring the desired parameters. However, as practice shows [14], when calculating highly vital systems, it is required to take into account additional factors affecting dependability. Such factors may include, for example, sudden disappearance of gaps in kinematic pairs, insufficient vibration resistance of joints, presence of foreign objects in deployment mechanisms (components or adjacent parts of structures), instability of the mechanism settings, insufficient actuator stroke, critical operation execution modes being violated or not set etc. [14, 16–17, 23].

In order to establish the output parameters that affect dependability, a design engineering analysis of dependability is performed [14, 16] that produces a parametric description of the functionality (1), operational integrity (2) and dependability (3) of the structure. Moreover, the application of the method of mitigation [14, 16] that allows translating possible failures into the desired output parameters, actually allows considering model (1) – (3) as a condition for the failure-free operation of the structure. This greatly increases the effectiveness of analytical verification, for example, using FMECA [30], which is based on identifying undesirable failures by the severity of their consequences and conducting expert assessments of the risks of possible failures, but does not provide an answer on how to prevent the very possibility of failures. The use of DEAD allows managing failures by selecting the values of the design parameters under the conditions of given restrictions (modes and conditions of use) based on mathematical equations (1) – (3) that reflect the set of knowledge, ideas and hypotheses when implementing output effects based on the physical laws of nature.

When it comes to DEAD, it should be understood that it does not replace or undermine the existing foundations of dependability (generally accepted standards of dependability should be followed where possible). However, when there is no information on the dependability of components and statistical data on product failures is insufficient, this method allows avoiding a significant part of design errors, including those that cause unlikely failures. The use of DEAD puts the notion that dependability calculations are impossible and even meaningless

[12] for highly vital systems (0.997 and higher) into question. In the framework of DEAD, calculations of the dependability of highly vital systems are critical, but its procedure requires standardization [23].

Moreover, the use of DEAD in itself is a necessary, but insufficient condition for creating highly vital systems. Like any other tool, it requires skill. In this case, that is the knowledge of the physical principles of operation of technical items, the fundamentals of engineering disciplines and methods of design for ensuring quality and dependability. Furthermore, all the same is required when using digital design technologies. Fortunately, the need to follow the established DEAD algorithm together with the possibility of obtaining a posteriori knowledge (from the results of testing and operation) allows accumulating knowledge with each iterative cycle of analysis and, if necessary, creating check lists of design principles and design rules [14, 28], corresponding to a specific subject area of development (which only enhances the effectiveness of the method).

Compatibility and conditionality of DEAD and digital technologies

From the standpoint of being focused on dependability prediction, DEAD and digital design methods use common procedures, i.e. substantiation of design solutions in order to eliminate (reduce the probability of) errors that can cause failures based on analytical, computational and experimental verification.

DEAD is within the authority of the human dependability expert. It is therefore instrumental in compiling the initial data for computer calculations in the human – computer system, since the effectiveness of digital technology itself directly depends on their completeness and reliability.

Today, in the course of construction of a matrix of target indicators and limitations, as well as validation of the calculation results, each iteration would involve experts who rely only on their own knowledge and experience [6]. The use of DEAD enables algorithmized preparation and verification of input data for computer calculations using formulas (1) – (2) and validation of their results according to (3). Thus, two problems are solved:

- there is no need to search for unique and costly experts (who may just not be around at the right time);
- engineers in the human – computer system are able to use a system approach that increases the efficiency of their decisions and allows for effective actions when preparing and conducting computer calculations.

The benefits of the latter cannot be overestimated. The capabilities of computer hardware and software are constantly growing, while the human capabilities in terms of technology development have been deteriorating in recent years: the quality of thinking does not improve, analytical abilities do not increase and the educational level has noticeably degraded. If knowledge is not enhanced and human actions are not further algorithmized, an ever-widening gap in the human – computer system may lead to unpredictable consequences, the most harmless of which may be Robert Sheckley’s prophecy in Ask a Foolish Question.

In theory, a generalized parametric model of operation (1) – (3) consisting solely of parameters can be obtained by simulating the operation of technical items at the micro-, macro- and megaworld levels (the principles of constructing digital models allow for that and are limited only by the available computational power). In this case, only an automated option is required, that would enable additive calculation of the predicted dependability resulting from the required measures aimed at preventing structural failures. Otherwise (if human knowledge or computing capabilities are insufficient), human participation is required for adjusting the calculation of predicted dependability by taking into account factors that require probabilistic assessment based on information models in the form of a black box.

The use of DEAD in digital technology may be essential for topological optimization of structures. In that case, it is important to distinguish between the goals of the tasks being solved. It is one thing when topological optimization is carried out to reduce production costs, while if the reduction of such costs may cause risks of excessively larger losses than the benefit of the savings is a totally different matter. For example, the mass of a mechanical spacecraft device can be reduced by 1 kg through topological optimization, which leads to savings of about 10^3 dollars based on the market price of blanks and the cost of manufacture. However, the failure of the mechanism in orbit as a result of the topological optimization can lead not only to losses of about 10^6 dollars, corresponding to the unit cost of payload deployment, but also to much more critical losses in the form of the cost of the lost spacecraft and the time of its creation, the cost of repeated satellite manufacture and financial losses due to potential reputational costs (for example, increasing cost of space risk insurance). In this case, predicting the dependability becomes a top priority that must be addressed using scientific methods.

Conclusions

Digital technology provides a tangible opportunity of predicting, reducing the impact or eliminating possible failures. That can be achieved through the same means that often cause failures, i.e. design engineering. For that purpose, it is required to create new applications of the modern dependability theory based on engineering disciplines and design engineering methods developed for ensuring quality and dependability of products.

Anyone interested in the problems described in the article are kindly asked to express their opinions, including personally at pokhabov_yury@mail.ru.

References

1. Ushakov I.A. Is Reliability Theory Still Alive? *Reliability: Theory & Applications.* 2017;3(46):45-68. [accessed 15.04.2020]. Available at: https://cyberleninka.ru/article/n/is-reliability-theory-still-alive-1/viewer.

2. Ushakov I.A. [Dependability: past, present, future: keynote speech of the opening of Mathematical Methods in Reliability (MMR–2000) conference, Bordeau, France, 2000]. *Reliability: Theory & Applications*. 2016;1(1):17-27. (in Russ.) (accessed 15.04.2020). Available at: http://www.gnedenko.net/Journal/2006/RTA_1_2006.pdf. (in Russ.)

3. Pokhabov Yu.P., Ushakov I.A. [On the fail-safety of unique highly vital systems]. *Metody menedzhmenta kachestva.* 2014;11:50-56. (in Russ.)

4. Schwab K. The fourth industrial revolution. Moscow: Eksmo; 2016.

5. Levenchuk A. [Systems engineering thinking in life cycle management]. (accessed 15.04.2020). Available at: https://ailev.livejournal.com/1121478.html. (in Russ.)

6. Borovkov A.I., Riabov Yu.A., Kukushkin K.V. [Digital tweens and the digital transformation of defense industry companies]. *Oboronnya teknika*. 2018;1:6-33. (in Russ.)

7. Pronikov A.S. [Dependability of machines]. Moscow: Mashinostroenie; 1978. (in Russ.)

8. Hilbert D. Mathematical Problems. *Bulletin of the American Mathematical Society: journal*. 1902;8(10):437-479.

9. Kuleshov A.P. [To overcome the resistance of materials: February 2, 2018 interview]. *Stimul: zhurnal ob innovatsiyakh v Rossii*. (accessed 15.04.2020). Available at: https://stimul.online/articles/interview/preodolet-soprotivlenie-materialov/?sphrase_id=1295. (in Russ.)

10. Doronin S.V., Pokhabov Yu.P. [Improving the reliability of structural strength estimates of technical items]. *Vestnik mashinostroyeniya*. 2013;6:85-88. (in Russ.)

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

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

13. Lerner E. [Alternative to “starting at haphazard”]. *Aerokosmicheskaya tekhnika*. 1987;9:157-160. (in Russ.)

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

15. 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.)

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

17. Timashev S.A., Pokhabov Yu.P. [Problems of comprehensive analysis and assessment of individual design dependability of spacecraft (with the example of rotating structures)]. Ekaterinburg: AMB; 2018. (in Russ.)

18. Gladky V.F. [Probabilistic methods of aircraft structural design]. Moscow: Nauka; 1982. (in Russ.)

19. Zolotov A.A., Pokhabov Yu.P., Ensuring the design reliability of unfolding structures spacecraft. *Polet*. 2018;7:36-45. (in Russ.)

20. Pokhabov Yu.P. [Method of selection of the servo for rotation of a structure in an articulated joint: pat. 2198387 Russian Federation. No. 2000129330/28; claim 23.11.2000; publ. 10.02.2003, bul. no. 4]. (in Russ.)

21. Pokhabov Yu.P. [Method of fastening items: pat. 2230945 Russian Federation. No. 2002113143/11; claim 18.05.2002; publ. 20.06.2004, bul. no. 17]. (in Russ.)

22. Pokhabov Yu.P., Nagovitsin V.N. [Method of fastening items with a statistically indeterminate system of connections: pat. 2125528 Russian Federation. No. 5067373/28; claim 29.09.1992; publ. 27.01.1999, bul. no. 3]. (in Russ.)

23. 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.

24. Hecht H., Hecht M. Reliability prediction for spacecraft: Report prepared for Rome Air Development Center: no. RADC-TR-85-229, Dec. Rome Air Development Center; 1985.

25. Saleh J.H., Caster J.-F. Reliability and Multi-State Failures: A Statistical Approach, First Edition. NJ: John Wiley & Sons; 2011.

26. Testoedov N.A., Mikhnev M.M., Mikheev A.E. et al. [Spacecraft manufacturing process]. Krasnoyarsk: SibSAU; 2009. (in Russ.)

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

28. Bowden M.L. Peter L. Conley, editor. Deployment devices. Space Vehicle Mechanisms: Elements of Successful Design. NJ: John Wiley & Sons; 1998.

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

30. ECSS Standard. Space product assurance. Failure modes, effects (and criticality) analysis (FMEA/FMECA). ECSS Secretariat, ESA ECSS-Q-ST-30-02C.

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, Russia, Krasnoyarsk Krai, Zheleznogorsk, e-mail: pokhabov_yury@mail.ru.

The author's contribution

The paper is the result of a long practice (since 1982) of design and assurance of dependability of space structure deployment mechanisms. Using the patented method of design engineering analysis of dependability (DEAD), between 2014 and 2019 expert assessment of the susceptibility to failure of structure-deploying mechanisms of spacecraft was conducted by leading Russian developers (with publication of scientific technical reports), that identified the insufficiency of todays' methods of analytical and experimental verification of dependability in the aerospace industry in terms of ensuring the required reliability above 0.999 and, paradoxically, reduced quality of the designs in terms of dependability subject to the application of digital design technology.