Original article
https://doi.org/10.21683/1729-2646-2022-22-1-20-29

Design engineering approach to ensuring specified dependability. Case study of unique, highly critical systems with short operation life

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. *To examine the design engineering approach to ensuring specified dependability on the basis of engineering disciplines and design engineering methods of quality and dependability assurance using the case of unique, highly critical products with short operation life. Such approach, unlike the statistical procedures of modern dependability, allows associating the dependability indicator calculations with the calculated operability parameters and established design criteria that are to be met in order to confirm the specified dependability indicators for products with an indefinite number of critical elements, each of which operates according to a functional principle that is different in its nature.* **Methods.** *The paper examined the prerequisites for the implementation of the design engineering approach to dependability, such as the distinctive features of ensuring the dependability of unique, highly critical products with short operation life, the applicability of design engineering approach to dependability, the effect of the genesis on the assurance of design engineering dependability, behavioural models of technical products in terms of dependability and specifics of highly critical product calculation. It was identified that, for items with high specified probability of no failure exceeding three-sigma random value variation interval, dependability is to be calculated not by identifying the dependability function, but rather by proving that undependability function is below the acceptable value, which ultimately ensures the specified dependability. Such approach enables the development of methods of early failure prevention using procedures of design engineering analysis of dependability for the purpose of achieving the required parameters of functionality, operability and dependability of products on the basis of a generalised parametric functional model.* **Results.** *The design engineering analysis of dependability allows substantiating the criteria for error-free design (selection of sound principles of operability and validation of engineering solutions for achieving the required dependability indicators). The effect of the error-free engineering criteria combined with the criteria for defect-free engineering (observance of the generally accepted principles, rules, requirements, norms and standards of drawing generation) and defect-free manufacture (strict adherence to the requirements of drawings with no deviation permits) enables a designer to achieve the specified dependability values without using the statistical methods of the modern dependability theory.* **Conclusion.** *Dependability as a comprehensive property is characterised by a probability that, on the one hand, determines the rate of possible failures, and, on the other hand, indicates the number of errors that were made by engineers during the design, manufacture and operation of products and can lead to failures. Additionally, the failure rate is determined by the engineers' efforts to eliminate or mitigate the consequences of possible failures at each life cycle stage. The greater and earlier are such efforts adopted, the higher the product's dependability will be. Ultimately, dependability is determined by consistent and rigorous implementation of error-free design, defect-free design and defect-free manufacture procedures whose efficiency is in no way associated with the number of manufactured products. Their efficiency and effectiveness are determined by specific decisions and actions by the engineers who make sure that the product performs the required functions with the specified dependability in the established modes and conditions of operation. Ensuring that only takes using engineering disciplines, as well as design engineering methods for quality and dependability assurance.*

Keywords: *dependability calculation, error-free design, defect-free design, defect-free manufacture, spacecraft, design engineering analysis of dependability (DEAD).*

For citation: *Pokhabov Yu.P. Design engineering approach to ensuring specified dependability. Case study of unique, highly critical systems with short operation life. Dependability 2022;1: 20-29. https://doi.org/10.21683/1729-2646-2022-22-1-20-29*

Received on: *18.12.2021* / **Revised on:** *21.01.2022* / **For printing:** *18.03.2022.*

1. Introduction

Ensuring faultless operation of single-use mechanical devices of spacecraft normally involves using methods of analytical and experimental verification that, in practice, have little in common with the stochastic methods of modern dependability [1, Chapters 16, 22]. Additionally, the methodological gap is so great that designers simply do not understand and are not aware of the relationship between the decisions they make and the specified dependability indicators, while the results of practical activities and calculations of dependability indicators do not correspond to each other so much that the founding fathers of the Russian aerospace industry generated a meme: "Dependability is calculated by people who cannot achieve it". It is still true today.

This practice is primarily due to the fact that calculations of dependability indicators are in no way associated with the types and tasks of parameter calculations (kinematic, electrical, thermal, hydraulic, pneumatic, etc.) that confirm the operability of products and serve as a ground for design solutions. The only exception is the dependability problems, in which the reliability indicators depend only on the strength parameters. In this case, it is normally considered that the *probability of no failure is identical to the probability that, within a specified time interval, the value of the loading parameter will never exceed the value that the strength parameter takes* ([2][1], see Reference Annex, comment on term "Reliability measure"), while strength calculations are performed taking into account the specified safety factors and strength margins that ensure the required probability of random parameters of loads and strength being within the acceptable range of values [3]. However, in most cases, the dependability objectives go beyond the matters of strength. The strength-specific dependability is regarded only as a conditional probability of failure that is based on the assumption that all other factors that can affect dependability are not critical.

It is still being debated in the research and engineering community as to what calculations of operability parameters and design criteria (apart from strength) are to be performed in order to confirm the specified dependability indicators for products with an uncertain number of critical elements, each of which operates according to principles that are different in their nature [4]. Ultimately, this problem is one of the causes of the widespread use of the statistical methods of modern dependability, as such methods do not require engineering analysis of the operability parameters of critical elements with different nature of operation. However, after the emergence of unique, highly critical products[2], the use of statistical methods eventually not only aggravated the problem due to the requirement to ensure the dependability of almost failsafe products, but also caused a complete misunderstanding of how to verify dependability in the situation of unavailable or insufficient failure statistics. Within the scope of the generally accepted approaches to dependability, there is still no scientifically substantiated solution for the problem of dependability of unique, highly critical products, which is confirmed by such regulatory documents as GOST RO 1410-001-2009, GOST 27.301-95, RD 50-476-84, etc. Additionally, the national standard GOST R 27.013-2019 clearly states that "*the probability of no failure is an indicator that cannot be evaluated using data for a single item.*" Regulatory documents do not clarify how to proceed, if the manufacturing procedure requires assessing the dependability of a product that was manufactured in a single instance and has no comparable items.

The paper presents and substantiates an approach to ensuring specified dependability based on engineering disciplines and design engineering methods of quality and dependability assurance using the case of unique, highly critical products with short operation time [5–7]. If required, the laws of the presented approaches allow extending them to any other technical products as forks [8].

2. Prerequisites for implementing the approach to design engineering dependability

Literally all engineering practices are based on the confirmation of physical principles of item operation and the application of design engineering methods of quality and dependability assurance, while no one doubts that this is the only way to achieve the required level of dependability. Nevertheless, designers continue using such approaches to dependability that do not allow understanding what dependability indicators can be achieved, given certain engineering practices, without involving the statistical methods of modern dependability. However, the statistical rules of dependability are only a consequence of an engineering practice in the form of quantitative interpretation of adverse events that allow judging upon product dependability based on data regarding failures that have already affected similar items. Additionally, if statistics are not available, such rules are of no practical importance, while if dependability requirements are high (with the probability above the three-sigma range of random value variation), obtaining the required reliable statistics may prove to be impossible. In particular,

[1] GOST 27.002-89 that is referred to herein is historical and has been replaced by GOST 27.002-2015 with removal of the reference annex, whose contents are of interest as regards the matters considered in this paper.

[2] Unique highly vital products are understood as virtually failsafe products that are unique (rare) in terms of their design, manufactured not more than in small series and operating in unique environmental conditions.

in case of unique, highly critical systems, it is virtually impossible to identify the dependability indicators using statistical methods due to financial/economic and/or physical/technical considerations (e.g., due to the large number of required test items and/or the need to conduct the tests in conditions drastically different from those on Earth, for example, in zero gravity and/or in increased radiation) [4].

At the same time, it is known that dependability as a property remains relevant for single or mass-produced items, with a long or short operation time, regardless of the availability of failure statistics [9]. Everything is defined by the ability of items to retain their properties over time under given modes and conditions of operation. The difference is that in the case of failures associated with long periods of operation, we are dealing with unacceptable (fatal) deterioration of functional properties of items over time, and in the case of short periods of operation the matter consists in various errors, i.e., actions or inaction of people (designers, fabricators, operators) that cause unintended results and eventually failures. Any unacceptable deterioration of item properties under the specified (known at the beginning of development) modes and conditions of operation are also errors, only associated with insufficient knowledge regarding the item operation, both in terms of its design (internal structure of elements and their interaction) and environmental conditions of application. Accordingly, statistical dependability may well be used to characterise cumulative errors that unintentionally occur in the course of design, development, manufacture and operation of products.

It is obvious that the case of unique, highly critical systems with short operation time simplified the identification of the effect of design engineering factors on dependability, as for such systems the reliability depends on a single performance of the required functions, rather than on the duration of operation exposed to the effect of modes and conditions of operation, which in itself is a complex scientific and technical problem (that distracts from the assessment of the criticality of human errors). Failures of products with short operation time are defined by the substantiated quality of the engineers' decisions and most often manifest as professional errors unlike failures caused by long deterioration of product characteristics over time that leads to gradual (implicit) decline in performance. However, in both cases, failures can be represented by a universally applicable diagram that describes the performance values of critical components going outside the admissible domain. The only difference is that the process may be sudden (instantaneous) or gradual (monotonous), which is determined by the physical processes that accompany the performance of the required functions by items. That is the context, in which are examined the various aspects of design engineering analysis of dependability of unique, highly critical systems that go beyond the statistical approaches of modern dependability [5].

3. Specificity of ensuring the dependability of unique, highly critical systems with short operation times

Virtually each spacecraft (being, in terms of its design, a rare and valuable product) in the orbit needs to deploy its folded structures (solar panels, antennas, reflectors, rods, etc.) into the operational position and only then is able to become fully functional for its intended purpose, e.g., as a repeater satellite [10–12]. The reliability requirements for such mechanical devices are so high that without using the engineering methods of identifying the potential critical failure hazards there is no point in creating spacecraft at all, which is evidenced by the fatal outcomes of the SinoSat 2 (2006), Kanopus-ST (2015), Mayak (2017), Zuma (2018), ChinaSat-18 (2019) missions, as well as the launches of many other artificial satellites and space devices [13–17].

The folded structures can deploy and assume their operational position in orbit only after the completion of a number of successive stages of spacecraft operation:

- ground transport and storage during and after exposure to transport loads and ground climatic conditions;
- final check of the mechanisms' operation in the technical area, where the "last draw" takes effect (possible unintentional disruption of mechanisms' operation before the flight as the result of personnel's action);
- flight as part of the launch vehicle during and after exposure to quasi-static, acoustic and vibration loads;
- separation from the last stage of the launch vehicle during and after impact loads;
- orbital flight in a folded position, when space factors that are sharply different from the atmospheric conditions on Earth (abnormally low or high temperature, temperature gradients, thermocycling, vacuum, microgravity, etc.) begin manifesting themselves;
- automatic deployment of mechanisms in presence of unstationary thermal processes of outer space and possible changes of dynamic dimensions of adjacent structures caused by microgravity (creating conditions for entanglement of moving parts);
- locking in the operating position with exposure to dynamic loads at the moment of end position lock operation.

The above sequence of events and states of mechanical devices of spacecraft is associated with integrated effects of modes and conditions of operation, which requires ensuring necessary and sufficient redundancy of product design to enable the specified dependability and is a complex engineering problem. It should also be taken into consideration that the products are manufactured in single instances, which is associated with a predominant share of manual labour in the assembly of unique systems (may result in anthropogenic risks of defects), the effect of technological heredity on the operation of mechanisms (in the form of assembly stresses, errors in the settings and adjustments of mechanisms, errors in the assembly operations, etc.), the practical impossibility of ensuring redundancy of functional elements due to the high cost of the launched payload and strict weight and dimension restrictions on the satellite design, as well as the non-availability of reliable statistics on the operation of functional units in outer space. All of the above features apply to space structures that deploy immediately after launching into the orbit, unlike, e.g., delayed deployment after a long stay in outer space [18–19] or deployment of mechanical devices of landing modules on destination planets exposed to climatic, atmospheric and gravitational effects of poorly studied environments that require taking into account additional environmental effects affecting the reliability [20].

The special methods of calculating the dependability of deploying spacecraft structures (that, along with strength, take into account the requirement of mechanical unit mobility) were developed in the late 1970s [21–22], but largely lost their relevance due to the increased dependability requirements, which is evidenced by the mechanical failure statistics of space launches over the last few years [23–25]. The existing dependability requirements (about 0.999÷0.9999 and higher) create an objective need to take into account the design engineering factors of dependability assurance that guarantee maximum reliability of highly critical products manufactured virtually in a single instance with no critical element redundancy [23]. Additionally, when it is required due to practical considerations, it is important not to reject the statistical theory of dependability (at least, as one of the starting points), as mechanisms may include components and elements that obey statistical rules of modern dependability, e.g., pyrotechnic devices or electrical and electronic components [5]. The legitimacy of using statistical approaches to dependability is thoroughly substantiated in the reference annex to GOST 27.002-89 [2]. However, the difficulty of applying the statistical rules of modern dependability to deploying space structures consists in the fact that such rules are at the foundation of the series of standards 27, R 27, RV 27 and many other standards that do not imply other approaches even if no failure statistics are available. At the same time, the demand for complex, unique, highly critical systems complying with the specified dependability indicators for the military, nuclear and space industries is on a constant rise [26].

4. On the applicability of the design engineering approach to dependability

In practice, failures of unique, highly critical systems show that dependability problems exist not only for systems with long operating lives, but also for those with single operation [23]. Moreover, in the first case, the failures are primarily caused by various factors of damage to the structure of materials and joint assemblies, i.e., ageing, degradation, fatigue, wear, etc., while in the second case, those are mainly due to erroneous design solutions adopted on the basis of the distinctive features of the manufacturing process (design engineering solutions) [27–29]. Assuming that the causes of failures in both cases are inferior design or process engineering solutions [27], it is always possible to identify and apply those out of them that allow eliminating failures or reduce their probability. Accordingly, since the designer proceeds from the knowledge available to him/her under the process-specific constraints of production, the product's dependability will be fully defined by the designer's decisions. Moreover, design engineering methods allow handling failures of any nature (physical, stochastic, design engineering), which enables the migration from failure simulation using stochastic methods of modern dependability to managing failures at the physical level by choosing the required product parameters.

The fact that the modern research and engineering literature on dependability, with rare exceptions [30–31], does not discuss design factors (i.e., those associated with the designer) of dependability assurance can be easily explained. The designer's work in any field of technical activity is, by its nature, difficult to understand by those who are not directly involved in it. Moreover, the further from the drawing board, the more, at best, is visible only the tangible result of the designer's work – the drawings – yet the process of their conception, i.e., the origin and substantiation of the design concept that most often defines the causes of future failures, is completely incomprehensible (and indifferent). The design concept is the cumulative result of the use of a person's natural abilities and individual knowledge that he/she accumulates, preserves and applies to the creation of technical items throughout the professional life. It has nothing to do with the computerisation of business that aims to reduce the share of routine operations, therefore substituting the designer's knowledge and skills with computer capabilities cannot improve the dependability of developed technology [32–34].

No educational and academic institution or industrial agency has or is not involved with the development of scientific and methodological foundations of dependability assurance at the stage of design. In Soviet times, it was believed that fundamental engineering education was sufficient for designers to be able to develop quality and dependable equipment. Nevertheless, every major company created specialised engineering schools continuously enriched by the experience and knowledge of many generations of engineers that, for various reasons, was not properly formalized, but passed on by word of mouth from generation to generation [23]. At the same time, all research in the field of dependability assumed that the operability of products by the beginning of operation is ensured by default (due to the high qualification of designers), i.e., virtually out of the context of the genesis of dependability. In the modern world, the hopes are set on the computer-assisted design in belief that computers do not make mistakes and, therefore, design ensures dependability automatically [32]. However, the fact is ignored that this dramatically increases the computational potential of technology and (through a misunderstanding) the educational level of engineers is unjustifiably reduced. In the author's opinion, that is a thoughtless mistake that needs to be addressed as soon as possible, but without developing and applying research and methodological approaches to dependability based on design engineering methods that would be almost impossible to do [33–34].

5. Genesis of the foundations of design engineering dependability

Philosophically speaking, all technical items that man creates are, in a sense, "prosthetics", devices that replace unobtainable functions or compensate for those that are not characteristic and difficult to achieve for a human being, e.g., to move in space (technical devices for transporting people and goods), communicate at a distance (means of telecommunication), live in comfortable climatic and other conditions (housing), etc. "Prosthetics", in the broad meaning of this word, that are commonly called technical items, are not the creation of nature existing by its laws, but something people artificially create owing to an understanding of the laws of nature (sometimes incorrectly or incompletely comprehended). Technical items make human life convenient, complete and comfortable, but are totally alien to the world around us and even ultimately harmful to humans when it comes to their disposal, and if so, then technical items are required and are created solely to satisfy the human needs[1]. Only man is able to conceive and impart to them a certain (required for him) functionality as a *set of properties defined by the presence and specific features of a set of functions capable of meeting given or implied needs* (GOST 28806-90). Moreover, such functionality of technical items must from the beginning (before their creation) be known and clear to man, otherwise significant safety risks may arise, if control is lost. The same principle applies to assembly drawings. All, even the smallest parts (e.g., bolts, nuts and washers) must be specified, each fulfilling a strictly defined function, for which they are all used. Each such function does not just (and only) exist, but can be formalised by a third person who is not directly associated with the design concept for the purpose of independent substantiation of its performance.

The understanding of functionality as the presence of a set of required functions ultimately underpins dependability that can only be achieved by focused and consistent human actions. Accordingly, without formalising what the required functionality is, it is virtually impossible to achieve dependability close to one.

6. Behaviour models of technical products in terms of dependability

In principle, any manufacture of products is organised in such a way that there are two ways of producing something. The first is "jury-rigging" according to the principle "good as done". The second one involves following a pre-designed plan, for which are used drawings of products with clear and known functionality, primarily as regards durability [35]. Drawings are important due to the fact that prior to the commencement of production, the information contained within them can be used to conduct the required engineering calculations, thus reducing the risk of errors, and to plan the production to improve its efficiency. The purpose of drawings is that they contain complete information on the performance by the product of its required functions, as well as the obligatory and sufficient requirements for its manufacture and operation. The absence or insufficiency of such information in the drawings inevitably reduces the product's dependability (the whole matter consists in the extent of such reduction). There are also two models of product behaviour in terms of dependability that are associated with drawings.

When no drawings for a product are available (they are not provided to the operator or they simply do not exist, e.g., they have been lost), the model of its behaviour in terms of dependability can only be identified by observing its operation (or through statistical tests). Such behaviour can be described using failure statistics, processing which using mathematical methods various dependability indicators can be obtained. For the purpose of implementing such approach, the methods of modern dependability were created, when it is not relevant which of a product's components causes failure or why the failure even occurs. Here, a person is only an observer who studies and generalises the laws of technical items' behaviour based on the results of their operation.

The fact that statistical methods of dependability are a special case of the physical understanding of various processes and phenomena was repeatedly pointed out by Soviet scientists A.I. Berg [36], V.V. Bolotin [9, 37], A.S. Pronikov [38–39], A.M. Polovko [4], I.A. Ushakov [40] and many others, but no fundamental changes have taken place yet. Various predictions of a product's future behaviour are usually based on the data on technical items that came to the end of their useful lives [39], while no effective methods of failure management at the earliest possible stages of newly created items' life cycle, primarily in mechanical engineering, have yet appeared [41]. There are only general guidelines for the design and development of products that have been worked-out on the basis of a long practical activity of engineers, following which high performance and dependability can be ensured [42–46]. However, such guidelines have

[1] By the way, the proverbial artificial intelligence does not need the human "prosthetics" either. And why would an artificial intelligence create technical objects that humans need (the "prosthetics") if it does not need those, and why would it know better than humans what humans need (the same is the case for any digital technology, primarily, in the area of design).

nothing to do with providing evidence of the achieved/not achieved product dependability indicators based on specific decisions made by the designer in the course of product development, i.e., they do not answer the question: "How much the designer's mistakes may weigh in terms of dependability indicator reduction" [7]. Consequently, various assumptions and restrictions inevitably arise that are associated with the concepts of early failure prevention models. For instance, it is assumed that, at the initial moment of operation, an automatic spacecraft is operable (GOST R 56526-2015), it is impossible to describe the first hump of the *U*-shaped dependability curve by mathematical formulae suitable for engineering calculations [47], the dependability of power structures of spacecraft is close to one, if their strength has the required safety coefficients [48], system dependability is the higher the less functional elements it contains [4], etc.

The second model of technical system dependability-specific behaviour is based on the fact that the drawing contains all the obligatory and sufficient requirements for manufacturing and operating the product that, within the specified operation time, in the given modes and conditions of application, will work without failure. Virtually, the point is that the design of such products is based on the assumption of unacceptable failures, or acceptable risks of failures, in the worst-case scenario. The premises of that approach are described in the foundations of dependability-specific design, when it is required to observe the principle of redundancy in order to eliminate (or reduce) the uncertainty between the "required" product structure and the "randomness" of environmental factors, whereas the degree of redundancy defines the acceptable ratio between the specified dependability and the possible undependability [49]. That should mean that if no errors were made in the process of design and development, the manufacture was done without damage or defects, while, in operation, the requirements of the operational documentation were not violated, then failures simply cannot occur. Should deviations occur at any of the life cycle stages, a risk of failure appears. Therefore, the primary problem of any development is to prevent design and development errors and to take measures to prevent defects in the manufacture and operation of products. The solution of the problem is examined in detail using the case of deployable spacecraft structures in papers that can serve as guidelines for engineers for using design engineering approaches to dependability assurance suitable for practical application (implementation) [5, 23]. In this case, it can be considered that technical documentation (design and process engineering) is a textual model of the product that contains all the required and sufficient information for the performance of the required functions. In particular, the geometric parameters correspond to the specified dimensions and tolerances, the choice of materials is made based on scientifically substantiated physical and mechanical characteristics and established safety margins, the structural depths and wall thickness of structural elements are selected subject to the specified safety coefficients, etc., therefore, the output parameters of any actual implementation of the product in the course of manufacture will meet the requirements of the design documentation, and the product itself, accordingly, will operate as the designer intended it to. A logical result of this model of dependability-specific product behaviour are the well-known methods of defect-free design (compliance with the generally accepted principles, rules, requirements, norms and standards of drawing development) and defect-free manufacture (work in strict compliance with drawing requirements without deviation permission cards) [50–51].

If the second, technical documentation-based model of dependability-specific product behaviour is used, three problems arise [23]:

1) identifying its dependability using hard-copy (design and process engineering documentation) and electronic documents (e.g., an annotation 3D model);

2) defining the obligatory and sufficient requirements for the manufacture in the design and process engineering documentation to ensure its specified dependability;

3) conducting the required technical inspection of the defined requirements.

In a certain sense, such statement is a trivial engineering problem, the solution of which can be appropriately organized and directed, e.g., using the methods of early failure prevention. For example, using the procedures of design engineering analysis of dependability to achieve the required indicators of functionality, operability and dependability of products based on a generalized parametric model of operation [5–7, 23, 33–34]. Moreover, if economically and financially feasible, quantitative dependability indicators can be ensured as per the standards, based on the statistical approaches of modern dependability [52].

7. Specificity of highly critical product calculation

When it comes to ensuring reliability above three nines (i.e., 0.997, which corresponds to the three-sigma rule), any stochastics-based calculations become meaningless [4, Chapter 14]. All possible failures in this case will fall within the category of rare events that do not match statistical patterns due to the fact that any set will always be smaller than the required entire assembly. In fact, proper engineering analysis shows that such failures have perfectly rational causal relationships. The purpose of such analysis may be to prove that system undependability $Q(t)$ will be below a certain value

$$Q(t) \leq 1 - P(t).$$

The analysis should result in the planning and execution of calculations and tests aiming not so much to identify the dependability – as it is usually done in modern dependability – but to confirm the required undependability using the method of negative judgements (antitheses). In this case, if it is proven that the undependability is less than, e.g., 0.0001, then the dependability would indeed be greater than 0.9999 [23].

Are "black swans" possible in this case? Certainly, they are (no one is safe from errors), but their number will obviously be much lower if left unaddressed in the belief that it is impossible to avoid errors anyway or by neglecting the development of the methodological framework for such analyses. It is only a matter of choice, i.e., to manage the risks of possible rare failures, or to reasonably reject this opportunity [7]. For example, if the specified dependability is not higher than 0.99, the use of the methods of modern dependability may well be justified, but if it is 0.999, those will prove to be absolutely insufficient and additional methods of early failure prevention will have to be employed enabling the designer to make timely and substantiated technical decisions for the purpose of failure prevention based on engineering disciplines and design engineering methods of quality and dependability assurance.

8. On the requirement to apply the methods of design engineering analysis of dependability

As it is known, dependability is the property of an item to retain in time the ability to perform the required functions in the specified modes and conditions of operation, maintenance, storage and transportation [52]. If a product does not yet exist, but the design documentation has already been developed, its dependability is objectively determined by the technical requirements of the design documentation for the manufacture and operation that define the ability of the product to display the specified dependability. This ability does not appear out of nowhere. It is defined by the designer in the course of development as a result of heuristic thinking, knowledge of the process and conditions of operation, engineering logic, calculated decisions, engineering calculations and development tests. In the process of manufacture, this ability can be reduced due to manufacturing defects and damage, or retained at the level of the design concept, if the conditions of defect-free manufacture are fulfilled [23]. Deviations from the requirements of operational documentation in operation have a similar effect. That is why it is believed that *it is impossible to improve equipment dependability in the course of operation. It can only be ensured and maintained at the required level* [4]. In this context, the design and engineering solutions directly determine the ability of a product to achieve a specified dependability. It is those solutions that define the product's dependability at the beginning of operation (at the stage of running-in) that, in turn, corresponds to the first "hump" on the *U*-shaped dependability curve. If the dependability genesis factors are taken into consideration, there is no business secret about the causes of the first "hump", as it is mentioned in [47], as well as about the possibility to describe the first "hump" of the curve by "simple mathematical formulas suitable for engineering calculations". Everything depends on the efficiency of the early failure prevention methods that the designer does or does not use.

The concept of dependability as a property and the ability to manifest such property does not contradict the definition of the term "probability" in GOST R 50779.10, where probability is considered as a real number between 0 and 1 associated with a random event that may reflect the relative frequency in a series of observations or the degree of confidence that a certain event will take place. The performance of the required functions by a product is conventionally characterized with the probability of no failure, i.e., the frequency probability that no failure will occur within a given operation time. However, there are no reasons not to characterize the operation of future products – in the course of design documentation development – with the conditional probability that the logical or subjective probability of its operation – should it be manufactured in accordance with the design and manufacturing documentation – is ensured, if the conditions of defect-free and manufacture were fulfilled (i.e., with no deterioration of the product's ability to manifest dependability the way that the designer has intended) [50-51].

The duality of the concept of "probability" leads to two ways of designing and manufacturing products. In the first case (frequency probability), whatever happens during the product's design and manufacture, with or without the application of quality management standards, such as the ISO 9000 series, its reliability can be characterised by a frequency probability that, within a certain (economically substantiated) range, can be monitored using statistical testing.

In the second case (conditional probability), product dependability can be based on the designer's confidence that all the technical requirements that he/she established in the design documentation are sufficiently substantiated and allow an actual product manufactured defect-free performing the specified functions regardless of the number of manufactured products. Additionally, the validity of the technical requirements means that any of the hypothetical (i.e., possible, yet for some reason not implemented in manufacture) or actual (as the result of actual manufacture) states and successions of product-related events would allow (or will allow) performing the required functions if the conditions of defect-free manufacture are fulfilled. A formalized description of such states and successions of events in the form of a set of parameters that characterize the ability to perform the required functions and the allowable limits of parameter value variation is identical to the concept of the digital twin, i.e., *"a single model that reliably describes all characteristics, processes and relationships both for an individual item and for the entire business process"*

[53]. In practice, the above confidence is supported by a check list of evidence of, e.g., the selection of materials and non-acceptability of substitution, specified physical dimensions, tolerances and their unconditional observance, specification of functional characteristics and their confirmation in the design, coordination of design requirements and manufacturing capabilities and limitations, compliance of the technological heredity factors with the requirements specified in the design documentation, acceptance testing of acquired products for compliance with the specified requirements, etc. This approach enables an ultimate dependability of a product manufactured even in a single instance without recurring to critical element redundancy. However, in this case, a method is required that would enable error-free design, i.e., choosing substantiated principles of operability and confirming engineering solutions for the purpose of achieving the specified dependability indicators.

The meaning of error-free design can be shown by the example used by the English naturalist T.H. Huxley to describe the essence of mathematics. Defect-free design (as in Uniform System for Design Documentation) and defect-free manufacture (as in ISO 9000) are millstones. If we fill them with wheat grains (error-free design), we will produce flour. If we mix wheat grain with litter (faulty design solutions), will not produce flour. The millstones (defect-free design and defect-free manufacture) will obediently grind litter (faulty solutions), producing the same litter (products with uncontrollable dependability).

Defect-free design is enabled by unbiased substantiation of critical solutions based on the assessment of the risks associated with the performance of each required product function for strict execution of the documentation (as is). The model involves that the designer predefines the performance of the required functions by means of the conditions that he/she examines based on the design and process constraints and specifies them in the form of drawing specifications that must be fulfilled and supervised in production. In this case, the dependability assessment at the stage of documentation preparation and manufacture is done by means of dependability calculation based on the probabilities of performance of the required functions by components and elements using the method of structural dependability [7]. The above method of dependability calculation can only be used along with the method of design engineering analysis of dependability, which allows obtaining a complete list of critical parameters and calculation criteria that affect dependability. That allows defining the tasks for engineering calculation and perfection of critical parameters of product operation subject to the established design margins [5].

9. Conclusion

Dependability as a comprehensive property is characterised by a probability that, on the one hand, determines the rate of possible failures, and, on the other hand, indicates the number of errors that were made by engineers during the design, manufacture and operation of products and can lead to failures. Additionally, the failure rate is determined by the engineers' efforts to eliminate or mitigate the consequences of possible failures at each life cycle stage. The greater and earlier are such efforts adopted, the higher the product's dependability will be.

Ultimately, dependability is determined by consistent and rigorous implementation of error-free design, defect-free design and defect-free manufacture procedures whose efficiency is in no way associated with the number of manufactured products. Their efficiency and effectiveness are determined by specific decisions and actions by the engineers who make sure that the product performs the required functions with the specified dependability in the established modes and conditions of operation.

Procedures for error-free design, defect-free design and defect-free manufacture are based on the results of design and process dependability analysis designed to achieve the required functionality, operability and dependability of products based on a generalised parametric model of operation. The methodology of such analysis uses the required engineering disciplines and design engineering methods for quality and dependability assurance, and is not bound to statistical rules of modern dependability.

References

1. Conley P.L., editor. Space Vehicle Mechanisms – Elements of Successful Design. NJ: John Wiley & Sons; 1998.

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

3. Biriukov G.P., Kukushkin Yu.F., Torpachev A.V. [Fundamentals of dependability and safety of launch facilities]. Moscow: MAI Publishing; 2002. (in Russ.)

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

5. Pokhabov Yu.P. [Design engineering analysis of dependability. Guidelines. Case study of spacecraft separation system]. Zheleznogorsk: AO NPO PM MKB; 2020. [Issued certificate of copyright registration no. 3644 of 27.05.2020 registered by OOO Sibkopirait, Novosibirsk]. [accessed 20.10.2021]. Available at: https://gnedenko.net. (in Russ.)

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

7. Pokhabov Yu.P. On the dependability of highly critical non-recoverable space entities with short operation life. Case study of single-use mechanical devices. *Dependability* 2021;21(3):3-12.

8. Artyushenko A.G., Pokhabov Yu.P. Design and technology reliability analysis: fork. *IOP Conference Series: Materials Science and Engineering* 2020;862(2):022001(1–6). doi:10.1088/1757-899X/862/2/022001.

9. Bolotin V.V. [Application of probability theory and dependability theory methods in structural analysis]. Moscow: Izdatelstvo literatury po stroitelstvu; 1971. (in Russ.)

10. Always P. Rockets of the world. Saturn Press; 1999.

11. Fortescue P., Stark J., Swinerd G. Spacecraft Systems Engineering. NJ: John Wiley & Sons; 2003.

12. Testoyedov N.A., Kosenko V.E., Vygonsky Yu.G. et al. [Space relay systems]. Moscow: Radiotekhnika; 2017. (in Russ.)

13. Fusaro R.L. NASA Space Mechanisms Handbook – Lessons Learned Documented. *Research & Technology 1998. NASA/TM* 1999:138–140.

14. Shapiro W. et al. Space Mechanisms Lessons Learned Study, Volume I – Summary. NASA/TM-107046; 1995.

15. Shapiro W. et al. Space Mechanisms Lessons Learned Study, Volume II – Literature Review. NASA/TM-107047; 1995.

16. Gore B.W. Critical Clearances in Space Vehicles. The Aerospace Corporation ATR-2009(9369)-1; 2008.

17. Harland D.M., Lorenz R.D. Space systems failures: disasters and rescues of satellites, rockets and space probes. Berlin: Springer; 2005.

18. Shtokal A.O., Rykov E.V., Dobrosovestnov K.B. et al. Ways of dependability enhancement of spacecraft deployment units with suspended actuation operating. Vestnik NPO im. S.A. Lavochkina 2017;4:60-67. (in Russ.)

19. Merstallinger A., Sales M., Semerad E. et al. Assessment of Cold Welding between Separable Contact Surfaces due to Impact and Fretting under Vacuum. ESA STM-279. Nordwijk; 2009.

20. Pokhabov Yu.P., Makarov V.P., Kolobov A.Yu. et al. [Aspects of ensuring the operational dependability of the mechanical devices for deployment and locking of landing module structures]. *Aktualnye voprosy proektirovaniya kosmicheskikh sistem i kompleksov. Sbornik nauchnykh trudov* 2019;20:151-166. (in Russ.)

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

22. Kuznetsov A.A., Zolotov A.A., Komyagin V.A. et al. [Dependability of mechanical parts of aircraft design]. Moscow: Mashinostroenie; 1979. (in Russ.)

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

24. Saleh J.H., Caster J.-F. Reliability and multi-state failures: a statistical approach. First Edition. NJ: John Wiley & Sons; 2011.

25. [Failures of rocket and space technology]. [Launch vehicles, satellites, planes, devices: website]. [accessed 20.10.2021]. Available at: http://ecoruspace.me. (in Russ.)

26. Levenchuk A. [Systems engineering thinking in life cycle management]. [accessed 20.10.2021]. Available at: https://ailev.livejournal.com/1121478.html. (in Russ.)

27. 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.

28. Tumanov A.V., Zelentsov V.V., Shcheglov G.A. [Fundamentals of spacecraft on-board equipment layout design]. Moscow: Bauman MSTU Publishing; 2010. (in Russ.)

29. Sevastianov N.N., Andreev A.I. [Fundamentals of dependability management of spacecraft with long service life]. Tomsk: TSU Publishing; 2015. (in Russ.)

30. Van-Jelen V. [Physical theory of dependability]. Simferopol: Krym; 1998 [Russian].

31. Kurylenko A.M., Ledovsky A.D. [Quality of ship dynamic control systems]. Saint Petersburg: Sudostroyenie; 1994. (in Russ.)

32. Kuleshov A.P. To overcome the resistance of materials: February 2, 2018 interview]. *Stimul: zhurnal ob innovatsiyakh v Rossii*. [accesed 20.10.2021]. https://stimul.online/articles/interview/preodolet-soprotivlenie-materialov/?sphrase_id=1295. (in Russ.)

33. Pokhabov Yu.P. Dependability in digital technology. *Dependability* 2020;2:3-11.

34. Pokhabov Yu.P. Dependability from a designer’s standpoint. *Dependability* 2020;4:13-20.

35. Haeder H. Konstruieren und Rechnen für Praxis und Schule. Saint Petersburg: Izdatelstvo K. Rikkera; 1904.

36. Berg A.I. [Selected works]. Energia; 1964. (in Russ.)

37. Bolotin V.V. [Theory of dependability of mechanical systems with a finite number of degrees of freedom]. *Izvestiya AN SSSR. Mechanics of solids* 1969;5:74-81. (in Russ.)

38. Pronikov A.S. [Parametric dependability of machines]. Moscow: Bauman MSTU Publishing; 2002. (in Russ.)

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

40. 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. (accessed 20.10.2021). Available at: http://www.gnedenko.net/Journal/2006/RTA_1_2006.pdf. (in Russ.)

41. 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.)

42. Yendogur A.I. [Aeronautical structure design. Structural design of parts and units]. Moscow: Izdatelstvo MAI-PRINT; 2009. (in Russ.)

43. Orlov P.I. Uchaev P.N., editor. Introduction into design in 2 volumes. Volume 1]. Moscow: Mashinostoenie; 1988. (in Russ.)

44. Khoroshev A.N. [Introduction into the design management of mechanical systems]. Belgorod; 1999. (in Russ.)

45. Lelikov O.P. [Fundamentals of calculation and design of machine parts and assemblies]. Moscow: Mashinostroenie; 2007. (in Russ.)

46. Bushuev V.V. [Practice of machine design]. Moscow: Mashonostrienie; 2006. (in Russ.)

47. Timoshenkov S.P., Simonov B.M., Goroshko V.N. [Fundamentals of the dependability theory]. Moscow: Yurait; 2015. (in Russ.)

48. Patraev V.E., Khalimanovich V.I. [Dependability of support spacecraft]. Krasnoyarsk: SibGAU; 2016. (in Russ.)

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

50. Gorokhova V.V. [Application of the Saratov system in research and design]. Moscow: Izdatelstvo standartov; 1969. (in Russ.)

51. Dubovikov B.A. [Fundamentals of scientific quality management (practical experience and theoretical substantiation of the system for defect-free work organization). Moscow: Ekonomika; 1966. (in Russ.)

52. GOST 27.002-2015. Dependability in technics. General principles. Terms and definitions. Moscow: Standartinform; 2016. (in Russ.)

53. Borovkov A.I., Riabov Yu.A., Kukushkin K.V. et al. [Digital twins and the digital transformation of defense industry companies]. *Oboronnaya tekhnika* 2018;1:6-33. (in Russ.)

About the author

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

The author’s contribution

The paper continues the author’s 2015–2021 series of publications in the Dependability Journal dedicated to the dependability of unique, highly critical systems using design engineering analysis of dependability based on a generalized parametric model of operation.

Conflict of interests

The author declares the absence of a conflict of interests.