Original article
https://doi.org/10.21683/1729-2646-2021-21-3-3-12

On the dependability of highly critical non-recoverable space entities with short operation life. Case study of single-use mechanical devices

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 consider matters of dependability of highly critical non-recoverable space products with short operation life, whose failures are primarily caused by design and process engineering errors, manufacturing defects in the course of single-unit or small-scale production, as well as to define the methodological approach to ensuring the required reliability.* **Methods.** *Options were analysed for improving the dependability of entities with short operation life using the case study of single-use mechanical devices and the statistical approaches of the modern dependability theory, special methods of dependability of actuated mechanical assemblies, FMEA, Stage-Gate and ground experiments on single workout equivalents for each type of effect.* **Results.** *It was concluded that additional procedures need to be conducted for the purpose of predicting, mitigation and (or) eliminating possible failures as part of the design process using exactly the same approaches that cause failures, i.e., those of design and process engineering. The engineering approaches to dependability are based on early identification of possible causes of failures, which requires a qualified and systemic analysis aimed at identifying the functionality, performance and dependability of an entity, taking into account critical output parameters and probabilistic indicators that affect the performance of the required functions with the allowable probability of failure. The solution is found using a generalized parametric model of operation and design engineering analysis of dependability.* **Conclusion.** *For highly critical non-recoverable space entities with short operation life, the reliability requirements should be considered primarily in terms financial, economic, safety-related and reputational risks associated with the loss of spacecraft. From a design engineer's standpoint, the number of nines after the decimal point (rounded to a smaller number of nines for increased confidence) should be seen as the indicator for the application of the appropriate approaches to ensuring the required reliability at the stage of product design. In case of two nines after the decimal point it is quite acceptable to use analytical and experimental verification techniques common to the aerospace industry, i.e., dependability calculations using the statistical methods of the modern dependability theory and performance indicators, FMEA and Stage-Gate, ground experiments on single workout equivalents for each type of effect. As the required number of nines grows, it is advisable to also use early failure prevention methods, one of which is the design engineering analysis of dependability that enables designers to adopt substantiated design solutions on the basis of engineering disciplines and design and process engineering methods of ensuring quality and dependability. The choice of either of the above dependability strategies is determined solely by the developer's awareness and understanding of potential hazards, which allows managing the risk of potential rare failures or reasonably refusing to do so.*

Keywords: *dependability calculation, Stage-Gate, FMEA, actuated mechanical assemblies, single-use devices, spacecraft, design engineering analysis of dependability (DEAD).*

For citation: *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;3: 3-12. https://doi.org/10.21683/1729-2646-2021-21-3-3-12*

Received on: *26.05.2021* / **Upon revision:** *15.07.2021* / **For printing:** *17.09.2021.*

Introduction

In the process of insertion, the configuration of a modern spacecraft undergoes four changes of its kinematic state [1]:

1) operation as part of the launch vehicle with compactly folded structures in the launching position (the satellite is installed on the rocket and its folding structures are arranged within specified dimensions and fixed on the body);

2) separation from the launch vehicle and orbital flight with folding structures in the launch position (the satellite is decoupled and is at a safe distance from the rocket, yet its structures remain arranged and fixed on the body until the preparation to deployment is complete);

3) deployment of the structures from the launch position to service position by means of mechanical devices (the mechanical connections to the body housing are removed and the structural elements execute the required motions taking the specified cantilever position relative to the body);

4) the operation of the on-board systems and satellite equipment for the intended purpose during the specified lifetime of active existence with the open structures in the working position.

The above sequence of satellite state changes is defined by the conditions and restrictions for its delivery to Earth orbit by a multiple-stage rocket [2]. Only after all the mechanisms have operated – separated and deployed the folding structures in the specified configuration – the spacecraft is able to operate normally in orbit. Otherwise, all the efforts associated with the construction and launch of a spacecraft-carrying rocket lose their effectiveness, sometimes even their meaning.

Space-based mechanisms are non-recoverable systems, therefore the cost of failure in the process of separation from the launch vehicle and deployment of mechanical devices is a partial or complete loss of spacecraft functionality even before the start of the operation it was created and launched for [3]. As the history of space launches shows, failures of single-use mechanical devices are not very rare. For instance, the proportion of failures at the stage of satellite deployment may be as high as 10.05%, and 12.8% at the stage of separation from the launch vehicle [4]. At the same time, practically every time the satellite sustains various degrees of damage (except in cases of self-deployment after failures caused by thermal effects, for example, when Kiku 8 deployed its antennas). For example, three months of spin-up manoeuvres following the non-deployment of the C-band antenna on Anik E2 resulted in excess consumption of an amount of fuel corresponding to one year of normal in-orbit operation. The incomplete deployment of solar arrays on Telstar 14, Telstar 14R and Intelsat 19 caused power shortages, which entailed a forced shutdown of a part of the transmitter-receiver devices of the payload (for example, on Telstar 14R, 17 transponders out of 41 were disabled). The non-deployment of solar arrays caused the loss of the $190-mil. Sinosat 2 and the $250-mil. Chinasat 18 that could not commence their intended operation. Every year, in the world there are at least 1 or 2 failures of single-use mechanical devices in the course of spacecraft separation and deployment in the orbital phase of the flight, while the average probability of failure is as high as 0.004 per year [5]. At the same time, according to OST 92-4339, the reliability of the deployment and retention mechanisms is to be not less than 0.999 with the confidence level of 90%, while the specified pointwise value of probability of devices operation for modern long-operation spacecraft is 0.9995 [6-8].

The conclusions are simple and disappointing. In more than 60 years of space exploration, no scientifically substantiated methods have been developed for designing and building single-operation mechanisms with the required reliability. Additionally, even a long (over the last 20÷30 years) lack of failures of the separation and deployment mechanisms designed by certain manufacturers cannot be considered as indisputable evidence of the faultless methods of ensuring dependability due to the small samples of statistical data. In particular, given the required reliability of mechanical devices over 0.9995, the accident-free launch of up to 10 devices per year (maximum about 300 devices over 30 years), which is the standard volume of production of one of Russia's largest developers, by itself does not guarantee a reliability level of 0.9995 even with the confidence level of 15% [5, 9, 10]. That is assuming that losses of single-use mechanisms are practically unaffected by such sources of uncertainty as the ageing and degradation of materials and connections resulting from long exposure to space flight factors. In most cases, the time to failure of such products is minimal. That is the time of launching into orbit and deployment from the launch position that, in total, does not exceed dozens of minutes and does not suppose reactivation in orbit [5, 8]. Accordingly, the failures of mechanical devices are determined mainly by design and manufacturing errors, as well as non-observance of the conditions of zero-defect production of single and/or small-batch products [5, 11-14]. The prevention[1] of such failures mainly depends on the degree of substantiation and establishment of the indispensable and sufficient requirements in the

[1] Prevention of failures: The implementation – in the course of the construction (upgrade), manufacture and operation of products – of a set of managerial and technical measures enabling the prevention, detection, investigation and elimination of the causes of product failures [OST 134-1012-97, Section 4].

design documentation for the purpose of manufacture and appropriate supervision of the key values of critical elements at all life cycle stages [15].

Given the above circumstances, let us consider ways of increasing the dependability of highly critical non-recoverable products with short operation life and one of the methodological approaches to ensuring the required functional reliability of single-use mechanical devices of spacecraft.

Capabilities of the modern dependability theory

First, literally all regulatory documents and scientific and methodological literature require calculating the dependability on the basis of undependability known from experience, i.e., a posteriori knowledge on possible failures [16, 17]. It is believed that dependability calculation is to be based on the presumption of failures, that are allegedly inevitable by definition, therefore, in order to calculate the dependability, it is required to know the statistical probability of failure of the entire product or at least the actual undependability of its components and elements in the specified modes and conditions of application [18]. If there are no known dependability (in reality, undependability) indicators, then, according to the modern dependability theory, they should be produced using statistical methods [19-21]. No other way is allowed by the requirements of such standards as, for example, GOST 27.002, GOST 27.301, GOST RO 1410-001, etc.[1]

Second, as regards single-use mechanical devices of spacecraft, ensuring a reliability of, e.g., 0.9995 it is required to hold at least 9995 independent tests (experiments) under uniform conditions. In other words, according to regulatory documents, it is required to deploy in orbit (not on the ground, otherwise the uniform conditions will not be observed) at least 9995 mechanical devices (not testing one device 9995 times, otherwise the test independence is not observed). All of that is only to confirm, that a single normal opening will occur with the required dependability. Let us assume a 0.9995 reliability would be sufficient with a confidence level of 0.9, but even then, the number of independent tests in uniform conditions must not be less than 4605 [22] (see example in GOST R 27.003 for identifying the minimal scope of statistical tests as part of dependability-related contracts). If we use the dependability calculation method based on known dependability indicators of components and elements, the number of required statistical tests in outer space will be considerably higher than for the mechanical devices themselves, since they consist of tens and hundreds of components in the form of the simplest mechanisms and devices, the number of requirements to the dependability of which grows exponentially with respect to the number of functional elements that affect the overall dependability of the system [23]. It is obvious that it is almost impossible to obtain reliable data for calculating the dependability of highly vital mechanical devices using statistical methods of the modern dependability theory due to financial and economic reasons (as of 2018, the cost of launching 1 kg of freight was $20-30 ths, as of 2020, it was $15-17 ths [24]).

Third, the humanity simply does not possess the required numbers of equivalent items to calculate the dependability of mechanical devices with a reliability close to 0.9999. The total number of satellites successfully launched worldwide between 1958 and 2010 is 6264 [25]. Between 2011 and 2016, 1153 more spacecraft were launched [5]. Even if we ignore the requirement of sample homogeneity, we still cannot rely on the reliability of statistical data for the purpose of calculating the reliability of deployment of, for example, solar panels (installed on almost every satellite) at the level of 0.9995.

Fourth, in the aerospace industry it is conventionally believed that flight-qualified products are dependable [9]. However, the high requirements for the dependability indicators in cases of small sample sizes do not correspond to the statistical approaches of the modern dependability theory. A failure that is acceptable, for example, for 10000 tests (experiments), may occur at the time of any of the tests, and, let us suppose, if 100 successive tests went successfully, there is no guarantee the 101-th does not end in a failure. In this case, it can be said that the product has confirmed its performance 100 successive times (but in no case conclusions concerning dependability can be made). Therefore, without the scientific and methodological substantiation of the feasibility of the required reliability (i.e., without additional analysis and/or simulations confirming the performance of the required functions with no failures), from an engineer's standpoint, it would be simply careless to draw any conclusions regarding the dependability of highly vital products in cases of low operation life.

Thus, using the statistical approaches of the modern dependability theory alone is not acceptable for the purposes of ensuring high operational dependability of single-use mechanical systems. Obviously, in this case the causes, rather than the consequences (statistics) of failures must be first identified. Therefore, methods of engineering analysis and dependability calculation are required that would be based on the physical phenomena described by physical theories. That would enable the construction of mathematical models of loss (or retention) of an object's performance with the change of its internal state in the specified modes and conditions of application [26].

[1] See terms related to the methods for dependability identification [articles 3.7.9-3.7.11].

Special methods for ensuring the dependability of single-use mechanical devices

The method of dependability calculation of the mechanical parts of moving structures of spacecraft was first published in 1978-1979 [27, 28]. In addition to the durability, the dependability calculation was proposed that is based on identifying the probability of excess drive moments (forces) of actuators over the resistance moments (forces) in the path of motion of the executive devices, as well as the calculation of the overall dependability of mechanisms on the basis of the phantom item (unit) model [28]. Later, mechanism dependability was calculated taking into account the margin of drive moments (forces) [29-33] similarly to the deterministic calculations for strength based on the safety factors and safety margin [34]. Abroad, the compliance with requirements for margin of drive moments (forces) is an integral part of all standards for designing moving mechanical assemblies (MMA) intended for space application. In 1975, the standard values of the margin of drive moments (forces) were specified in the military standard MIL-A-83577, later, in the civil standards AIAA S-114-2005, NASA-STD-5017A and ECSS-E-ST-33-01C. In Russia, there are no official standards (GOST, GOST R, OST, STP, STO) for designing mechanical devices taking into account the margin of drive moments (forces), but the years-old application practice is that deployment drives are selected on the basis of the requirement of a margin of drive moments (forces) not less than 100% (2:1 ratio) of the worst value of the resistance moments (forces) at any point of the path of motion assuming zero kinetic energy [32, 33]. It is commonly believed that if the specified reliability coefficients, strength margins, drive moments (forces) and conditions of successful confirmation of the criteria of experimental optimization (as defined in GOST R 58630) are observed, the specified reliability of deployment and retention of mechanical devices is ensured by default [29-31].

However, studies of the actual causes of failure show that in the vast majority of cases they are rare in terms of their nature that is defined by an unfavourable combination of manufacturing tolerances, unaccounted factors of technological heredity, application modes and external effects [5, 15]. Such failures can be caused, for example, by sudden disappearance of gaps in kinematic pairs (Kiku 8, Soyuz TMA-17M), unfavourable combination of production factors (Intelsat 19), manufacturing defects (Kanopus-ST, Progress M-19M), foreign objects in the deployment mechanism (Skylab, Telstar 14, Telstar 14R), failures of deployment actuators (EchoStar 4), unauthorized deployment (Resurs-P no. 3), design and manufacturing errors (Mayak), cold welding (Galileo), etc. The practice shows that dependability calculations using the statistical methods of the modern dependability theory and performance parameters (from the recommended list in OST 92-0290), as well as successful ground experiments on single workout equivalents for each type of effect, are unable to prevent the risk of rare failures [16, 35]. Modern methods of experimental optimization are not intended for identifying and emulating loading cases that correspond to critical combinations of critical states of a product, factors of modes and external effects [5]. Moreover, for small probabilities of failures (not more than 0.01), the total error of dependability evaluation based on the results of experimental optimization can be as high as an order of magnitude of the valid digit, while in terms of engineering calculations an error of not more than 5÷10% [5, 36-38] is acceptable.

The Stage-Gate concept

According to the Stage-Gate concept, the execution of any project[1] is defined by sequential execution of cross-functional actions and activities (stage) separated from each other with decision points (gate) that lead to the next stage of the work plan (in the stage-gate system) [39].

In fact, it refers to process project management standards that, unlike those adopted in Russia (GOST, GOST R, OST, STP, STO), establish the order and procedures for appropriate decisions and actions. In particular, the process principle is at the foundation of the ESA standards intended for the purpose of management, engineering and quality assurance in space projects, for instance for space mechanisms (ECSS-E-ST-33-01C).

Despite the obvious benefits of the Stage-Gate-based process standards, i.e., the availability to “average” engineers for the purpose of achieving the required quality and dependability, when all of their decisions and actions are regulated by a set of pre-defined (by someone else) procedures, a thoughtless execution of formalized instructions can lead to the loss of the physical significance of decisions and the purpose of actions. For example, in the process of development of a mechanism with any particular principle of action, process standards are certainly useful, but if the physical principles of such mechanism’s operation change, it becomes necessary to promptly compensate the shortcomings of the used procedures in the standards. This can be made possible by applying engineering techniques based on strictly defined algorithm-based procedures or by the engineers’ heuristics. In the first case, that means a quick adjustment of the existing engineering methodology, in the second case, that means a relatively long way of trial and error

[1] Project: A temporary enterprise aimed at creating a unique product, service or deliverable [PMBOK, Glossary].

involving the accumulation and generalization of the behaviour patterns of new products for the purpose of enabling the required properties [40].

The FMEA analysis

The purpose of failure mode and effects analysis (FMEA) is to enable the detection and elimination of technical problems within complex systems by examining each type of failure of any critical component. FMEA and its versions: DFMEA, PFMEA, and MFMEA are based on brainstorming or expert evaluation of the types and consequences of failures of critical elements, complemented, if required, by failure mode, effects and criticality analysis (FMECA) or failure modes, effects and diagnostic analysis (FMEDA).

The FME[C,D]A method involves the following steps:

- definition of the structure of the analysed object (structural analysis);
- identification of the possible critical event scenarios (functional analysis);
- execution of the analysis to determine the types, effects and causes of failures with risk assessment for the purpose of preventive or corrective action (FMEA), FMEA-based calculation of safety indicators, i.e., risk priority or failure criticality (FMECA), FME[C]A-based identification of the failure rate (FMEDA) for dependability calculation;
- evaluation and documentation of analysis results (FMEA, FMECA or FMEDA).

FME[C,D]A analysis is performed by a cross-functional team of domain experts (e.g. designer, engineering technologist, assembler, tester, supervisor, etc.) of up to 7 or 8 people who possess practical experience and high level of professionalism [41]. The principles of FMEA team building and work organization are defined in standards and guidelines, e.g., GOST R 51814.2, STB 1506, RD 03-418-01, etc.

FMEA analysis and its extended variants (FMECA, FMEDA) are performed by experts using formalized algorithms and procedures for obtaining subjective semi-quantitative estimates (based on consequence significance ratings, probability of occurrence and detection) of potential failures (faults). The experts normally have different professional views on the analysed object that does not always correspond to the understanding of how exactly and in what conditions such object operates [42]. Experts do not know (they do not have to know according to FMEA standards) the design concept aimed at solving specific technical problems, therefore they evaluate the consequences of defects on the basis of external features (indicators) that a consumer can notice and the experts can understand from the standpoint of personal professional qualities (knowledge, qualification and experience).

Meanwhile, the designers' intent is very closely associated with establishing and substantiating the output parameters of critical elements of an object within the permissible range of values [17, 36, 37]. Moreover, if the FMEA standards (for example, GOST R 51814.2) require defining the types of potential failures in physical and technical terms (crack, deformation, jamming, destruction, leakage, etc.), then the consequences of failures are recommended to be described in the consumer's language (what he/she can notice or experience), e.g., noise, incorrect operation, instability, intermittent operation, etc. [43]. The FMEA results are either not at all or indirectly related to the output parameters and their allowable ranges that are in one way or another defined by the designer.

The approach to ensuring the dependability of single-use mechanical devices

Given that the methods of the modern dependability theory do not enable a sufficiently accurate solution of the problems of dependability of highly vital products with short operation life due to non-applicability of statistical approaches, while special and auxiliary methods are not designed for identifying the causes and assessing the risks of rare failures, it is only left to predict, mitigate or prevent possible failures at the design stage using exactly the same approaches that cause failures, i.e., those of design and process engineering.

According to the principles of rational design, a design[1] and any of its structural elements should be considered from the standpoint of them performing strictly defined functions that were originally conceived and implemented by the designer by adopting and executing specific solutions (design, engineering, design and engineering, process engineering)[2]. Such solutions are based on a physical understanding of the world and the use of design and engineering methods for their implementation as part of technical objects. In this case, each of the designer's decisions that are potentially capable of causing a failure must be substantiated. Each argument must be compliant with the designer's logic of reasoning that he/she understands in the context of ensuring a failure-free operation of the product.

It may be advisable to use methods of parametric modelling of products based on the available diagrams

[1] Design: A device, the mutual arrangement of parts of an object, machine, instrument defined by its purpose and involving a method of ensuring the connection, interaction of parts, as well as the material the individual parts (elements) must be made of [GOST R 57945-2017, Article 2.66].

[2] According to definitions of the respective terms associated with the word "decision" per GOST R 57945.

(design layout, structural, etc.), sketches, drawings, 3D models in order to confirm the solutions. In this case, any graphic, text-and-graphics or digital design models must be represented in the form of a parametric model, the modification of whose parameters enables the fulfilment by the product of all required functions.

Based on the principles of physicality (causal connections)[1] and physical necessity (consistency with the laws of nature)[2] it is not difficult to represent the performance of the required functions by the product on the basis of the parametric model that describes its functionality, performance and dependability [17, 36, 37, 44]. The logical sequence of reasoning is as follows. If the design is represented as a set of output parameters that characterize the performance of the required functions (i.e. the functionality), each design parameter is defined based on a combination of the modes and conditions of application (i.e., performance), while the modification of the values of the design parameters over time is restricted within the allowable range (i.e., dependability), a generalized parametric model of the product's operation can be obtained, in which the criteria for required functions performance (output parameters and their allowable ranges) are interrelated, mutually conditioned and dedicated to achieving the specified performance and dependability [44]. Since recently, this approach complies with the logic of the "Space Systems and Complexes" series of standards developed by TsNIIMash in 2019 and 2020.

1. After the introduction of the state standard GOST R 58629, one of the tasks of the failure mode, effects and criticality analysis of space products and processes is aimed at identifying the key design (functional and physical) characteristics of the critical elements and their testability. However, the standard does not establish the method for solving the problem of identification of such key characteristics (although based on the general concept of FMEA, it can be assumed that they are identified, for example, by the method of expert evaluation). Additionally, it is not perfectly clear what should be done if the fulfilment of the required functions cannot be expressed in physical values, but can be characterized with the qualitative features of a product that are described by probabilities (as the degree of confidence that under the specified conditions an event will occur). Nevertheless, in general, the requirements of GOST R 58629 for the identification of the key characteristics of critical elements comply with the concept of functionality identification in the generalized parametric model of product operation [44].

2. Worst case analysis according to GOST R 58626 allows defining and sets forth a list of formalized analysis procedures that include the quantification of the tolerances of value changes of the output parameters of the object of analysis depending on the possible values of its internal and input parameters. This procedure is the definition of product performance under the worst combinations of the modes and conditions of application in the generalized parametric model of product operation [44]. However, according to GOST R 58626, such analysis is conducted on the basis of the results of FMECA (FMEA) performed in accordance with the requirements of GOST R 58629, i.e., using the method of expert assessment based on experts' opinions for the purpose of subsequent decision-making, which is not a sufficient condition for establishing a complete list of worst cases. Additionally, due to the insufficient maturity of certain terms, for example, "mode" and "emergence" [44, 45], the approach to the worst case analysis according to GOST R 58626 remains uncertain in terms of calculation of the maximum and minimum values of allowable deviations (the worst case) of the output parameters.

3. According to the explanations in the reference annex to GOST 27.002-89, it is not customary to distinguish between the indicator of the probability of no-failure in terms of the strength on the basis of statistical data and the probability of that within the specified period of time the strength values will be within the acceptable limits taking into account the safety factors and strength margins [18]. In fact, this approach to assessing the probability of no-failure corresponds to the definition of dependability taking into account the design margins in such a way as to, with a reliable confidence, guarantee that the values of the examined parameters are within the allowable area [17, 44].

Thus, the key task associated with the identification of possible causes of rare failures consists in conducting a systematic and qualified analysis for identifying the functionality, performance and dependability of a product taking into account critical output parameters and probabilistic indicators that affect the performance of the required functions with the allowable probability of failure. The solution is found using a generalized parametric model of operation and design engineering analysis of dependability.

Ways of achieving systemic analysis

The analysis of the functionality, performance and dependability of products is done based on the information on the modes and conditions of such product's

[1] Principle of physicality: The principle, according to which inherent to any system (regardless of its nature) are laws (regularities), perhaps unique, that define the internal causal relations of its existence and operation.

[2] Physical necessity: The actual causality between a phenomenon and certain natural circumstances that is unambiguously predictable within the knowledge of it (as opposed to randomness).

application, as well as the current state of the design documentation ("as is") taking into account its requirements for the manufacturing process and technical oversight [5]. The efficiency of such analysis is the highest if it is made on the basis of the intended use, i.e., the key purpose the product is created for that includes (besides the general design goals) all the additional conditions, limitations and requirements that quantify and specify such purpose [46]. After the intended use has been established, a task tree is built for the product's components that enable the key purpose. Based on each task, the required functions are formulated (defined by the question: "What does an object or its individual elements do?"), each of which is an external manifestation of the product's properties of a strictly defined physical nature within the given modes and conditions of application. The resulting tree of required functions is the necessary and sufficient condition for substantiating the specified performance and dependability of the product on the basis of the engineering disciplines and methods of ensuring dependability.

After the tree of required functions has been constructed, it becomes possible to identify potential failures in the form of a verbal description of hypothetical events that prevent the performance of the respective functions. Then, the conditions that make failures impossible are defined (failure-free conditions). Such conditions are found using the method of antithesis. The logical design of this method is based on a biased judgement, according to which a failure of any critical element has already "occurred". If, in the course of design, the required and sufficient measures for eliminating the cause of a possible failure have been taken and documented, that serves as evidence that the above negative judgement is false and, therefore, the condition of reliability has been ensured. The condition of reliability is understood as each of the properties of a particular critical element that makes the corresponding cause of failure impossible [47]. Importantly, under this approach, the properties of critical elements that define their reliability are identified automatically based of strictly engineering techniques (with no regard for the subjective opinion of "experts").

The list of properties of critical elements itself allows characterizing each critical element quantitatively depending on the selected functional model, i.e., stochastic or physical [17]. Additionally, if the behaviour of a critical element can be characterized in physical values, the description of the properties of a critical element is based on output parameters that best describe the physical nature within the specific system of relations of a specific element in the product and between the entire product and the external environment. This procedure fully complies with the requirements of GOST R 58629. If the model does not allow characterizing the operation of a critical element through physical values (due to the insufficiency of knowledge regarding the physical nature of failures), the properties of such element are described through an indicator in the form of the probability of failures in the course of performance of the required function based on a "black box" or logical and probabilistic models. If required, the parameters and probabilistic functional indicators of the item can be reduced to a consistent dimensionless form (when the parameters can be represented as the probability of value variation within the allowed range similarly to the explanation given in the Reference Annex to GOST 27.002-89 [18]). That allows estimating the predicted (planned) dependability of the product using the method of dependability calculation based on the probability of performance by components and elements of their required functions [17].

Dependability analysis of highly critical non-recoverable products with short operation life

Based on the above approach, the method of design engineering analysis of dependability (DEAD) [5, 15-17, 36, 37, 44] has been developed, whose application does not cancel any engineering practices, but develops and complements them, enabling the following:

- abandoning the concept of randomness of the causes of failures and establishing their logical and mathematical relationship with the design and engineering factors;
- identifying the relationships between the output operational parameters and the probability of failure;
- identifying the design and manufacturing risks associated with failures that cannot be identified through the conventional methods of analytical and experimental verification;
- timely detecting rare causes of possible failures;
- reducing the number of potential structural failures at early life cycle stages, etc.

Despite the fact that the method of design engineering analysis of dependability (DEAD) implies dependability estimation (calculation), in should be above all considered as a system of design engineering and managerial measures aimed at eliminating (reducing the probability) of failures based on the analysis of the engineering documentation that includes:

- definition of the calculation task (required and sufficient calculations of the performance and dependability parameters according to specified criteria for maximum possible reduction of the probability of unreasonable risks of failures);
- experimental program definition, including experimental identification of the values that cannot be calculated due to the lack of required data and confirmation of the specified performance parameters in the course of

ground experiments, when the number of items submitted for testing is limited due to financial and economic reasons;

- definition of the necessary and sufficient requirements in the design documentation for the manufacture and operation of products;
- development of a check list of output parameters used in the process of quality and dependability verification of products;
- planning of measures to prevent design failures at all life cycle stages;
- iterative calculation of predicted dependability as the result of the required measures to prevent design failures;
- evaluation of design and process engineering solutions for compliance with the specified dependability requirements.

The use of design engineering analysis of dependability (DEAD) creates conditions, in which ensuring dependability is a natural and integral part of a designer's work enabling engineering decision-making in accordance with the specified dependability requirements (rather than in isolation, as it is the case when statistical approaches to dependability are used). However, unlike in the case of failure mode, effects and criticality analysis (FMECA) that is intended for identifying and assessing the criticality of product defects and inadequacies (based on the result of business processes or procedures), DEAD serves to verify designer solutions subject to process constraints (aimed at preventing the causes of possible failures at the physical level before the product has been manufactured).

DEAD has been tested in the design of single-use mechanical space devices and hydraulic assemblies of oil well equipment [5, 15]. Such analysis was in all cases carried out after the experimental activities (and even flight qualification) adopted by the company that developed the mechanisms in accordance with the required regulatory documentation. Nevertheless, the analysis enabled a practically substantiated identification of design and process engineering errors in the design documentation; an evaluation of the effectiveness of the existing computational and experimental optimization of product design; assessment of the adequacy of the established requirements in the design documentation; identification of unacceptable combinations of structural parameters based on the design constraints, actual manufacturing and control conditions; drawing conclusions regarding the products' propensity to failure; predicting the compliance to the specified dependability requirements; providing recommendations regarding design modifications to ensure specified dependability of products. In fact, DEAD allows identifying and eliminating the shortcomings of the conventional methods of design, project engineering and experimental optimization to achieve the specified dependability [5, 15].

Conclusion

For highly critical non-recoverable space entities with short operation life (principally, single-use mechanical devices of spacecraft), the reliability requirements should be considered primarily in terms financial, economic, safety-related and reputational risks associated with the loss of spacecraft. From a design engineer's standpoint, the number of nines after the decimal point (rounded to a smaller number of nines for increased confidence) should be seen as the indicator for the application of the appropriate approaches to ensuring the required reliability at the stage of product design.

In case of two nines after the decimal point it is quite acceptable to use analytical and experimental verification techniques common to the aerospace industry, i.e., dependability calculations using the statistical methods of the modern dependability theory and performance indicators (out of the recommended list according to OST 92-0290), FMEA and Stage-Gate, ground experiments on single workout equivalents for each type of effect [5-8, 27-31, 35, 38-43].

As the required number of nines grows, it is advisable to also use early failure prevention methods, one of which is DEAD that enables designers to adopt substantiated design solutions on the basis of engineering disciplines and design and process engineering methods of ensuring quality and dependability [5, 15-17, 36, 37, 44].

The choice of either of the above dependability strategies is determined solely by the developer's awareness and understanding of potential hazards, which allows managing the risk of potential rare failures or reasonably refusing to do so.

References

1. Fortescue P., Stark J., Swinerd G. Spacecraft systems engineering. NJ: John Wiley & Sons; 2003.

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

3. Sevastyanov N.N. Reliability control in spacecraft with long service life. *Cosmonautics and rocket engineering* 2017;3:133-148. (in Russ.)

4. Gorbenko A.V., Zasukha S.O., Ruban V.I. et al. Safety of rocket-space engineering and reliability if computer systems: 2000-2009 years. *Aerospace technic and technology* 2011;1:9-20. (in Russ.)

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

6. Patraev V.E. [Methods of ensuring and assessing the dependability of long active life spacecraft]. Krasnoyarsk: SibGAU; 2010. (in Russ.)

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

8. Patraev V.E., Shangina E.A. [Dependability of technical systems of spacecraft]. Krasnoyarsk: SFU; 2019. (in Russ.)

9. Spacecraft [Electronic Resource]. ISS-Reshetnev. [accessed: 15.03.2021]. Available at: iss-reshetnev.ru. (in Russ.)

10. Launches: a database [Electronic Resource]. [Launch vehicles, satellites, airplanes, instruments]. [accessed: 15.03.2021]. Available at: http://ecoruspace.me. (in Russ.)

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

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

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

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

15. [Model and methodology for assessing the impact of scheduled activities for the prevention of structurally defined failures on the dependability of spacecraft in terms of failures of the single-use mechanical devices]. IDN 532-OT-MKB-0031-19. No. GR 192073020089221700024185 1. Zheleznogorsk: AO NPO PM MKB; 2019. (in Russ.)

16. Pokhabov Yu.P. Problems of dependability and possible solutions in the context of unique highly vital systems design. *Dependability* 2019;19(1):10-17.

17. Pokhabov Yu.P. Dependability from a designer's standpoint. *Dependability* 2020;4: 13– 20.

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

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

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

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

22. Volkov L.I., Shishkevich A.M. [Aircraft dependability]. Moscow: Vyshaya shkola; 1975. (in Russ.)

23. Timashev S.A., Pokhabov Yu.P. [New methods of analysing and evaluating the dependability of aerospace products]. In: [Safety and monitoring of man-made and natural systems: materials and presentations. VI All-Russian Conference (September 18-21, 2018, Krasnoyarsk). Krasnoyarsk: SFU;2018:254-259. (in Russ.)

24. [Roscosmos to cut launch prices by 30% due to Musk's SpaceX dumping]. RosBusinessConsulting. (accessed 15.03.2021). Available at: https://www.rbc.ru/technology_and_media/10/04/2020/5e90869c9a7947d4640156b7. (in Russ.)

25. Krylov A.M. [Comparative analysis of space activities of Russia, China and India]. MKK. (accessed 15.03.2021). Available at: http://mosspaceclub.ru/base/base.php. (in Russ.)

26. Belozertsev A.I., El-Salim S.Z. [Deterministic model of improved dependability of analytical systems]. In: [Dependability and quality: proceedings of the international symposium] 2017;2:396-399. (in Russ.)

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

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

29. Shatrov A.K., Nazarova L.P., Mashukov A.V. [Mechanical devices of spacecraft. Design solutions and dynamic characteristics]. Krasnoyarsk: SibGAU; 2006. (in Russ.)

30. Shatrov A.K., Nazarova L.P., Mashukov A.V. [Introduction to the design of mechanical devices of spacecraft. Design solutions, dynamic characteristics]. Krasnoyarsk: SibGAU; 2009. (in Russ.)

31. Romanov A.V., Testoedov N.A. [Introduction to the design of information management and mechanical systems of spacecraft]. Saint Petersburg: Professional; 2015. (in Russ.)

32. Postma R.W. Force and torque margins for complex mechanical systems. In: Proceedings of the 37th Aerospace Mechanisms Symposium, Johnson Space Flight Center, May 19–21; 2004. P. 107-118.

33. Conley P.L., editor. Space vehicle mechanisms – Elements of successful design. NJ: John Wiley & Sons; 1998.

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

35. Kolobov A.Yu., Dikoun E.V. Interval estimation of reliability of one-off spacecraft. *Dependability* 2017;4:23-26.

36. Pokhabov Yu.P. Dependability from a designer's standpoint. *Dependability* 2020;2:3-11.

37. Pokhabov Yu.P. Designing complex products with small probability of failure in the context of Industry 4.0. *Ontology of Designing* 2019;9(1):24-35. (in Russ.)

38. [Milestones in space: collection of research papers dedicated to the 50-th anniversary of ISS-Reshetnev]. Krasnoyarsk: IP Sukhovolskaya Yu.P.; 2009. (in Russ.)

39. Crowe D. et al., editors. Design for dependability. NJ: CRC PRESS LLC; 2001.

40. Doronin S.V., Pokhabov Yu.P. [Approaches to the selection of loading cases of load-bearing structures of technical objects]. In: Moskvichiov V.V., editor. [Safety and monitoring of natural and man-made systems: materials and presentations. VII All-Russian Conference (October 5-9, 2020, Kemerovo)]. Novosibirsk: FRC ICT; 2020. P. 43-46. (in Russ.)

41. Pistsova Yu.P., Nikolaeva N.G., Priymak E.V. et al. [Failure mode and effects analysis (FMEA) of design documentation]. *[Bulletin of the Kazan Technological University]* 2004;1:411-415. (in Russ.)

42. Isaev S.V. [We don't need such FMEA! (Difficulties of deployment and infancy mistakes)]. *[Quality management methods]* 2008; 3:30-32. (in Russ.)

43. Stengach M.S., Gorbunov A.A., Kobzev V.N., compilers. [Failure (defect) mode and effects analysis, FMEA]. Samara; 2011.

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

45. Tarasenko F.P. [Applied systems analysis]. Moscow: KNORUS; 2017. (in Russ.)

46. Baranchukova I.M., Gusev A.S., Kramarenko Yu.B. et al. [Designing automated machine-building processes]. Moscow: Vysshaya Shkola; 1999. (in Russ.)

47. Gersevanov N.M. [Application of mathematical logic to structural analysis. Volume 1]. Moscow: Stroyvoenmorizdat; 1948. (in Russ.)

About the author

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

The author's contribution

The paper considers the matters associated with ensuring the dependability of highly critical non-recoverable entities with short operation life based on one of the methods of early prevention of structurally-defined failures. The paper builds upon the author's ideas set forth in the Dependability Journal nos. 2 and 4, 2020.

Conflict of interests

The author declares the absence of a conflict of interests.