Design and technology reliability analysis: fork

A G Artyushenko and Yu P Pokhabov

JSC “NPO PM Small Design Bureau”, 55a, Lenin Str., Zheleznogorsk, Krasnoyarsk region, 662972, Russian Federation

E-mail: pokhabov_yury@mail.ru

Abstract. While space system functioning, faults are unacceptable. The price of any early failure in the operation of a spacecraft is much higher than the cost of the development and manufacture of the failed element. Modern verification methods do not provide the required reliability. For the mechanisms of spacecraft, a methodology of design and technology reliability analysis has been developed, which allows one to achieve reliability, which is not available for modern verification methods. The article provides the purpose of the new analysis, the basic foundations and a brief description of the analysis methodology. The technique was tested in the development of space-based mechanisms and hydraulic automation for oil equipment that operate without human intervention once during the service life. The basic approaches to the implementation of the design and technology reliability analysis make it possible to develop many branches (fork version) to solve problems of ensuring the quality and reliability of products for various purposes, increasing the efficiency of development and professional skill of designers.

1. Introduction

Reliability characterizes the failure-free performance of the required functions during a given service life, which is one of the main properties of technical objects. Any equipment manufacturer who cares about his image is obliged to do everything possible to produce high-quality and reliable products. To do this, as a rule, it is enough to strictly comply with the requirements of modern quality management systems, which, through the use of established verification procedures, force the developer to timely correct critical errors that can lead to failures. However, in practice, there is a threshold of required reliability, to achieve which even scrupulous fulfillment of the quality management systems requirements is not enough.

For example, the most reliable technical objects on spacecraft (SC) are moving mechanical assemblies of deployable structures. Their faults can lead to partial or complete failure of the satellite even before the start of work. According to existing standards, the reliability of operation of the deployable structures cannot be lower than 0.999. However, as failure statistics for 2009–2016 show, the average value of this indicator for foreign and domestic spacecraft did not exceed 0.996 [1]. It follows that the modern methods of analytical and experimental verification used by NASA, ESA, CNSA and Roscosmos do not allow reaching reliability rates in excess of 0.999 (although for long-term spacecraft these indices should be provided at the level of 0.999 5 and higher). This gap between expectation and actual execution is explained by the fact that in the arsenal of leading developers of movable mechanical units there are no verification methods capable of identifying rare causes of possible failures, which often cannot be detected right up to the very fact of their manifestation [1].
In 2014–2019 a methodology of design and technology reliability analysis (DTRA) was developed [1-3], which allows one to eliminate the imperfections of verification procedures. Initially, it was intended to identify possible causes of rare structural failures in the design of single-acting mechanical devices. The technique has been tested in practice in the design of various mechanisms for space purposes and hydraulic automation of oil equipment, which should operate once without human intervention in space or deep underground. As a result of practical application, a number of possibilities of the new technique were identified:

- detect rare causes of potential failures;
- determine the design and technology risks of failures that cannot be identified by traditional verification methods;
- move away from the concept of randomness of the failure-causing problems and find their logical and mathematical connection with structural and technological factors;
- establish the relationship between the output parameters of the operation with the probability of failure;
- reduce the number of potential structural failures at early stages of the lifecycle, etc.

At the same time, it was found that the introduction of digital design technologies without changing approaches to verification and validation of the quality and reliability of structures is not able to exclude design errors; the new methodology for analyzing and assessing reliability does not correspond to the paradigm of interstate standards 27, based on the rules of the statistical theory of reliability; reliability terminology base is not intended for use in creating unique highly responsible systems; DTRA can serve as an alternative to the use of FMECA for products whose reliability is determined by rare failures. A generalization of the application experience and study of the results showed that the range of tasks using the DTRA technique can be significantly expanded. Keeping the basic foundation, analysis procedures can be used in new areas of its application, generalized by the concept of “fork”, known in programming as the operation of crushing a product into parallel branches, which continue to develop independently of each other. The following are the most important features of the DTRA methodology and additional features that allow it to be used in the development of complex highly responsible technical systems with specified reliability indicators.

2. The purpose of the new analysis
Design and technology reliability analysis is, first of all, a methodology for analyzing design decisions for early detection of failures which causes do not occur often. The essence of this analysis is reflected in the name itself: design (outgoing from the designer) and technological (taking into account the manufacturing technologies used) analysis (designed to verify and validate design decisions) reliability (as the ultimate goal of design - the failure-free operation of products for official purposes).

Despite the fact that the DTRA methodology involves the assessment (calculation) of reliability, first of all, it should be considered as a set of design, technological and organizational measures to eliminate (reduce the probability) of failures, based on the analysis of technical documentation, which includes:

- setting objectives for design verification (conducting the necessary and sufficient calculations of the performance and reliability parameters according to specified criteria to minimize the likelihood of unreasonable risks of possible failures);
- setting objectives for experimental verification, including the experimental determination of parameter values that cannot be obtained as a result of design verification due to a lack of necessary data, and confirmation of the required performance parameters for ground experimental testing based on the conditions for limiting the objects to be tested;
- setting the necessary and sufficient requirements in the design documentation for the manufacture and operation of products;
• obtaining a checklist of the output parameters of the design, which are used to verify the quality and reliability of products;
• planning of measures to prevent structural failures at all stages of the life cycle;
• iterative calculation of predicted reliability as a result of the required measures to prevent structural failures;
• assessment of design and technology solutions for compliance with the specified requirements for reliability.

In contrast to the mathematical methods of the theory of reliability, during the DTRA, the genesis of reliability is taken into account based on the requirements of technical documentation:

• design (obligatory);
• technological (if at the time of analysis this documentation was developed);
• regulatory and technical (if necessary).

The lack of necessary and sufficient requirements in the technical documentation, the incorrectness of their establishment and improper execution (including failure to carry out verification operations by means of non-destructive testing and control tests) are all considered from the standpoint of the risks of possible failures and evaluated using the DTRA procedures along with calculations of theoretical reliability for design product parameters, for example, strength [3].

3. The basis of DTRA technique
A starting point is the approach to design calculations of the reliability of the mechanical parts for the aircraft structure [4–6], which are carried out using the mathematical tools of the reliability theory according to two limiting states of the structure — strength (ensuring load-bearing capacity) and functioning, for example, when turning constructions (ensuring energy sufficiency of drives). Since the beginning of the 1980s, reliability calculations began to be carried out taking into account structural reserves - safety factors (when calculating strength) and driving torque reserves (for calculations on functioning when revealing rotary structures), assigned on the basis of statistical data [1, 7].

For relatively simple one-two-link rotary structures with low reliability requirements (with a given reliability of less than 0.999), this approach is more or less acceptable to ensure the accuracy of the calculation. With the complication of the deployable mechanisms (a significant increase in the operational life of a spacecraft up to 12–15 years and the requirement for failure-free deployment performance close to one), the reliability calculation method for two parameters — strength and driving torque reserves — is not able to provide the required accuracy.

Carrying out drawing-and-designing and design technology developments inevitably results in detailed design of the structure members, taking into account the technological features of production. At the same time, the design reliability indicators may deteriorate due to design errors associated with structural and technological factors that can lead to possible failures, for example, due to the sudden disappearance of gaps in kinematic pairs, insufficient vibration resistance of the joints, and intrusion of foreign objects (engineering elements) in the deployable mechanism or parts of the structure), instability of the mechanism settings, insufficient actuator motion, non-compliance or failure to establish processing modes for critical operations, etc. [1, 2]. Accordingly, to achieve the required reliability, it is necessary to justify (evaluate) design and technology solutions aimed at eliminating (reducing the probability) of errors that can cause failures. This requires consideration of a significantly larger number of design and technology parameters (in addition to the parameters of strength and functioning during deployment) than is used in modern methods of verification of deployable mechanisms in NASA, ESA, CNSA and Roscosmos. The number of parameters and the criteria for their implementation are individual for each mechanism and are determined during the initialization of the DTRA at the stage of parameterization of its design [3].
4. A brief description of the basics of the DTRA technique

The approach to eliminating (reducing the probability) of design errors is implemented on the basis of simulation (scenario) modeling of the possible causes of failures. Two models are used as initial concept, reflecting a priori design idea about the external environment and the real object:

- an information model of temporal factors and external influences on an object via interfaces in the form of operating modes and conditions specified in the technical requirements for a development, which during iterative analysis, as a rule, remain unchanged;
- a textographic (digital) model corresponding to the stationary stochastic model of the object in the form of design (drawing-technical) documentation, which can be iteratively refined (changed) until the product is put into operation, respectively, the stochastic model of the object at each iterative step of changing the technical documentation is considered as stationary in a state of "as it is."

A stationary stochastic model of an object is an abstract description of real or hypothetical (as yet unprepared) products that can be obtained as a result of repeated manufacture with unconditional compliance with all requirements in the design documentation. The tolerances of the design parameters within each iterative step are unchanged (stationary), but the values of these parameters can change randomly (stochastically) within the specified tolerances for each real or hypothetically possible embodiment, and, therefore, can be implemented and deployed in time. Thus, the number of hypothetical reproductions of homogeneous products \( \tau \) (made according to the same documentation, on the same equipment, by one specialist), at which they are able to ensure failure-free operation, is a random variable, which in meaning cannot be anything other than the time of failure-free operation of the product \( t \), in terms of the number of real reproductions. The indicated property of the stationary stochastic model of the object is fundamental for the implementation of the DTRA technique and meets the condition for ensuring reliability in the form \( R(t) = P(\tau > t) \).

The impact of the external environment on a real object during operation can be represented using two mathematical models that describe the performance of the required functions in the given modes and operating conditions:

- probabilistic-statistical, when the stationary stochastic model of an object is considered as an information model in the form of a black box, which implements output effects depending on the specified modes and operating conditions (based on mathematical processing of statistical information about the behavior of a real object or its physical models without taking into account the laws of nature);
- quasiphysical, when a stationary stochastic model of an object in given modes and operating conditions is considered as a system of corresponding mathematical equations that reflect the totality of knowledge, ideas and hypotheses when implementing output effects based on physical laws of nature.

These mathematical models correspond to reliability models, which are implied by the terminological definition of reliability according to GOST 27.002 (functional and parametric [8]):

- functional, when the required functions are characterized by probabilistic failure indicators (statistical, logical, Bayesian, subjective);
- parametric, when the required functions are presented in the form of a set of parameters characterizing the ability to perform them, and the permissible limits for changing the values of these parameters (the parameters are measurable or calculated physical quantities).

If necessary, the parameters and probabilistic indicators of the object operation can be reduced to a consistent dimensionless form (if the parameters are presented as the probability of a change in their
values within acceptable limits), which makes it possible to consider the functional reliability model as a special case of a single parametric reliability model that takes into account both physical and statistical (the mathematical) nature of things based on quasi-physical and probabilistic-statistical models [1-3].

Based on this approach, a generalized parametric model of functioning and the DTRA technique have been developed [3]. The generalized parametric model of functioning is determined by the following categories:

- functionality (a set of properties determined by the presence and set of capabilities to perform the required functions)

\[
\{X_i\} = (X_1, X_2, ..., X_i)^T \forall i = 1, n;
\]  

(1)

- operability (the state in which the object is able to perform the required functions)

\[
D_x = \{X_i(t)|\alpha_i \leq X_i(t) \leq \beta_i\};
\]

(2)

- reliability (the ability to save in time the performance of the required functions in the specified modes and operating conditions)

\[
R = P\{X_i(t) \in D_x, 0 < t < t_k\},
\]

(3)

where \(\{X_i\}\) – many output parameters that determine the performing the required functions in the form of a column vector; \(D_x\) – range of permissible values of output parameters \(X_i\); \(\alpha_i\) and \(\beta_i\) – valid parameter values \(X_i(t)\); \(t_k\) – time to failure.

The DTRA technique is described in detail in [1–3], but without going into details, it can be aggregated to the performance of three analysis procedures:

- initialization in the form of parameterization (turning an object into a set of parameters and permissible ranges of their change), which is done to establish conditions (1) - (2);
- calculations of theoretical reliability by design parameters performed according to (3);
- providing evidence that the reliability analysis (assessment) corresponds to reality (the requirements of design and technology documentation, production conditions, quality control methods).

Thus, DTRA is actually a roadmap for the design and construction of products with the required reliability, which allows, on the basis of parametric modeling, to select design parameters that ensure the unconditional fulfillment of the required functions, which must be performed and confirmed at the manufacturing stage.

5. Applicability of DTRA
Since the DTRA is based on the functional approach [9], which allows replacing the stationary stochastic model in the given modes and operating conditions with an equivalent set of required functions, it is possible to abstract from the concrete design of the object of analysis. Formulas (1) - (3) can be used to describe technical systems for various purposes, for example, reusable mechanisms, electromechanical devices, electronic assemblies, power and precision structures, etc.

Using the DTRA procedures, these functions can be represented by a set of parameters (indicators) in the form of a column vector (1), and taking into account the given modes and operating conditions, determine the operability of critical elements (2). In fact, using expressions (1) - (2), the initial data can be verified for design and construction, which becomes possible based on the establishment of parameters whose values are justified by calculation and experimental methods. Taking into account the formula (3), the development results are validated - confirmation that the design meets the development goals, namely: operability (2) according to the official purpose is achieved and the required reliability
(3) is ensured. Thus, DTRA can be used in solving a number of applied problems of designing and constructing practically any technical objects, for example:

- for the analysis and assessment of the reliability of electronic assemblies (electronic equipment);
- in the design and construction of precision large-sized cantilever structures for space purposes;
- when using digital design technologies;
- as an alternative to the reliability analysis of unique highly responsible systems using FMECA;
- to reduce the cost of design and experimental development of products;
- as a means of monitoring reliability in the planning of measures to prevent structural failures;
- as a means for self-training of engineers.

The solution to each of these problems is a branch of the technique (fork version), which not only does not prevent its use for its intended purpose - to analyze the reliability of single-acting mechanical devices, but makes it possible to significantly extend its scope.

References

[1] Pokhabov Yu P 2018 Theory and practice of ensuring the reliability of single-acting mechanical devices (Krasnoyarsk:SFU) p 338
[2] Pokhabov Yu P2018 What should mean dependability calculation of unique highly vital systems with regards to single-use mechanisms of spacecraft Dependability 18(4) 28-35
[3] Pokhabov Yu P 2019 Designing highly responsive systems with reliability in mind using the slewing rod as an example J.of SFU Technics and technology 12(7) 861-83
[4] Kuznetsov A A1978 Ballistic missile design reliability (Moscow: Mashinostroenie) p 256
[5] Kuznetsov A A, Zolotov A A and Komyagin V A 1979 Reliability of mechanical parts of aircraft construction (Moscow: Mashinostroenie) p 144
[6] Shatrov A K, Nazarova L P and Mashukov A V 2006 Mechanical devices of spacecraft. Design decisions and dynamic characteristics (Krasnoyarsk:SibSAU) p 84
[7] Zolotov A A, Pokhabov Yu P and Gusev E V 2018 Ensuring the design reliability of deployable designs of spacecraft Voyage 7 36-45
[8] Netes V A, Tarasyev Yu I and Shper V L 2014 How do we determine what reliability is Reliability 4 3-14
[9] Shcherbakov V A and Prikhodko E A 2003 Basis of financial functional-cost analysis (Novosibirsk:NSTU) p 164