Pokhabov Yu. P.

APPROACH TO ENSURING OF DEPENDABILITY OF UNIQUE SAFETY CRITICAL SYSTEMS EXAMPLIFIED BY LARGE TRANSFORMABLE STRUCTURES

This paper describes the approach to ensuring of reliability, capable of identifying and preventing potential failures of unique safety critical systems at the earliest stages of the life cycle by the example of large transformable spacecraft structures. Among other things, this approach gives a possibility to take account of design and technological factors affecting reliability.

Keywords: *unique safety critical systems, large transformable structure, spacecraft, reliability, failure-free operation, property, ability, parameter, index.*

Introduction

At the mundane level of understanding the reliable equipment must not fail, it must be maintainable and it must be long operable. At old times, we used to assess reliability and quality of goods by a workman's name or by a trade mark. A workman's or a trade mark served as a basis for emotional evaluation of quality and reliability of a product, and besides, it significantly determined a product's selling price.

As the equipment was getting more complicated and due to the growth of risk of social and economic effects of failures and accidents, it became necessary to assess reliability of technical objects in figures. Today the predetermined values of reliability indices are an integral part of technical tasks for the development of equipment objects, as well as they bring a certain frequency sense of acceptable losses, which can be tolerably suffered by people in case of failures and accidents. For hazardous facilities, an acceptable rate of accidents is determined by the standards GOST 12.1.010-76, GOST 12.1.004-91, GOST R 12.3.047-98, RD 03-418-01, GOST R 51901.1-2002, PB 12-609-03, etc.

For objective verification of reliability requirements, there occurred the necessity to develop methodologies of reliability calculations. Initially, the basis of such calculations was the probabilistic renditions of reliability indices, whose analogs are defined by methods of mathematical statistics. As the result of study of technical objects' reliability, experts came to the rules of statistic theory of reliability, which are nowadays fixed in the national standards of the 27th series "Dependability in technique". Formally, it limits the application of modern theory of reliability in technique by the following product categories [GOST 27.002-89, Attachment, clarification to the term "Reliability index"]:

– large-series objects produced and operated in statistically uniform conditions, for which a statistic interpretation of reliability is applicable;

– single recoverable objects where, in accordance with normative documentation, multiple failures are permitted – for the description of their sequence a model of random events stream is applicable;

– unique and small-series objects consisting of mass-production products, for which the reliability calculations are generally made based on the methods of statistic theory of reliability by the known reliability indices of elements and components.

Nowadays, however, more and more technical products do occur, which are to operate in unnatural environment, and (or) in ultra hard modes strictly different from usual conditions of operation of ground-based equipment, and which are produced in single quantities. Their behavior in operation is beyond the notions and models of the probability theory and mathematical statistics due to the absence of statistic data and more or less reasonable opinions about laws of distribution of probabilities of random variables. There are also the objects for which the models of the probability theory and mathematical statistics are generally acceptable, but the required accuracy of reliability calculations far exceeds the accuracy of input data.

The indicated technical objects are unique if there is no statistics, or they are mission critical if the probability of failure-free operation (FFO) is close to one, or they are both the first and the second ones simultaneously. The latter objects form the class of unique mission critical systems (UMCS), widely used in military, chemical, space, atomic technique, etc. Failures of such systems are highly undesirable due to significant financial losses, or they are unacceptable due to safety reasons.

In relation to mechanical devices of space technologies, primarily to the devices of single operation related to UMCS, the scientific and technical literature contains rather poor description of the scientifically sustainable engineering methods to ensure reliability. For retrospective reasons, papers [1–4] should be mentioned here.

Specification of large transformable structures from the reliability viewpoint

The UMCS specimens are the large transformable structures (LTS) of space crafts (SC). These are the solar panels, space radio telescopes and reflector elements consisting of dozens, hundreds and even thousands of interrelated elements ensuring the opening of structures in space environment (SE) (vacuum, weightlessness, nonstationary thermal gradients, abnormal temperatures, etc). Such structures are produced mostly in single quantities with maximum possible failure-free operation characteristics. Redundancy of critical elements (CE) of LTS are unacceptable due to practical reasons, or the application of them is rather limited due to dimensions, and repairs in case of failures during as intended operation are technically not feasible.

Difficulties when ensuring the LTS reliability are compounded by the following:

– simulation of cumulative SE factors (vacuum, weightlessness, nonstationary thermal gradients, abnormal temperatures, etc) is technically almost not feasible in ground-based testing;

– in view of natural gravitation, due to small overall dimensions and lower structural rigidity, it is rather difficult to perform a full ground-based experimental development of their opening;

– due to redundancy restrictions, the operation of devices becomes very sensitive to any faults occurred under design, production and operation.

The main difficulty when ensuring LTS reliability lies in a complicated and unobvious dependency of reliability on the variety of factors, each of which has different physical nature and development laws, though some factors can be in statistic dependency with unknown correlation factors which are almost impossible to define. This is due to the fact that LTS refer to technical objects with unstable structure caused by their multi-functionality during a life cycle. Initially, in view of the conditions under which LTS are transported to a low earth orbit, they are in a stowed stationary position, then they transform into operating configuration, when the structure elements in short time change their spatial attitude and eventually are fixed, forming a new stationary position. In any of the spatial attitudes, as well as under transfer from one position to another the structures are constantly under the effect of external conditions and operating modes typical of a certain life cycle stage. By contrast, it should be mentioned that other SC components and structures do not change their configuration during a life cycle. Their reliability is normally characterized by the strength in the only possible spatial attitude, though the external conditions and operating modes may change during a life cycle, but they remain uniform. As for LTS, the strength factor is considered as a particular case affecting the reliability together with the following groups of factors:

– design (design errors, imperfect design methods);

– technology (imperfections or violations of the established procedures, technological errors, insufficient range of adjustments and settings, uncontrolled installation impacts, etc.);

– geometry (choice of radial clearance, stroke margin and drive springs, etc.);

– tribologic factor (choice of tribocoupling materials, stability of lubricant characteristics, designation of thickness of solid lubricant coating, etc.);

– vibration resistance (self-unfastening of serrated joints, acceptable partial frequencies, acceptable vibratory displacement, etc.);

– thermophysical factor (temperature-induced variations, compatibility of materials by coefficients of heat linear extension, application of heat uncoupling at fastenings, etc.);

– physical and mechanical factors (choice of drive moments, acceptable opening speeds, required push-rod power values for the first breakaway, etc.);

– micrometric factor (accuracy and stability of positioning, absence of freeplay in operation conditions, etc.);

– organizational factor (applicable redundancy methods, provision of specified opening areas, observation of sequence of clamping of the opening stages, etc.);

– anthropogenic factor (countermeasures to undeliberate unauthorized actions and personnel negligence, factors

of engineering psychology complicating an incorrect assembly).

Under such complex dependency of reliability on various factors, it is not possible to bring LTS reliability to a single index, which can be defined based on an integral general model, as none of the known models is capable of consideration of the variety of different physical factors. However, we cannot allow us to miss any of the indicated factors regardless of knowledge of failure rate, present in any group of factors. In case FFO is set close to one, it is assumed that there shall be no failures during operation, or the probability is negligibly low.

Approach and preconditions to ensure reliability of large transformable structures

Philosophical aspect of UMCS reliability is described in paper [5]. It stipulates that the reliability of technical objects regardless of a life cycle stage could be considered as the property or as the ability. These notions are not opposed, but they do complement each other expressing the single essence of things.

Reliability as a property is considered from the point of keeping of stability of properties of technical objects, and failure-free operation – from the point of *continuous* keeping of stability of properties of technical objects. As the reliability is defined by an object's ability to operate, then in a narrow sense the reliability is the property of objects to keep stability of operable state in given conditions and operation modes during a certain period of operating time. In such case the task to ensure reliability is to find and eliminate potential instabilities of an object's operable state at every life cycle stage.

Understanding of reliability simultaneously as the property and as the ability makes it possible to solve the reliability problem on the system base from unified positions, when there is no object yet, but there are its heuristic or mathematical models, when the object in any of stationary states, as well as at the transfer from one state to another. In this case the functioning of LTS as the object with unstable structure is completely within one of the definitions of the notion "functioning" – *"performance on an object (system) of a process (processes) corresponding to a specified algorithm and (or) showing by an object of specified properties"* [GOST 22487-77 (invalid), Attachment 1 (informational), article 3]. In relation to LTS, the sense of such notions of reliability as «preservation» and «failure-free operation», if to consider the term "preservation" in the definition of an obsolete national standard: *"Preservation is an object's property to keep the indices values of failure free operation, longevity and maintainability during and after storage and (or) transportation"* [GOST 27.002-83 (invalid), article 5]. In relation to a target task which is to transform LTS into operating state, the functioning in a stowed position serves as showing of a preservation property, and when transforming from a stowed position into an operating one it serves as showing of a property of failure free operation. And there is no «breach of notions» here, as transportation is a *"**movement of products in specified state** with an application, if necessary, of transport and load-carrying devices, starting with an embarking and ending with an off-loading at a destination point"* [GOST 25866-83, article 14].

Accordingly, ensuring of reliability is aimed at the research of stability of the prescribed properties of material objects or abilities to show these properties during a life cycle. In relation to each group of factors (strength, construction, manufacturing, tribologic factor, etc.) the stability of showing of properties, or the properties themselves shall be studied using mathematical models and methods typical to the physics of failures, arising from the showing of certain properties relating to certain objects. In such formulation the reliability of objects is not substituted by the research of separate properties by strength, mechanics, tribology, etc., but is considered as a complex property as a whole under the influence of the variety of different actors. And the methodology to ensure LTS reliability is generally based on the following principles:

– a man must understand the principles of operation and organization of the "device" he produces based on the gained scientific knowledge, and in case of lack of knowledge as the result of the focused studies and experiments;

– functioning of any "device" can be represented as the system of properties;

– any properties of a "device" can be characterized quantitatively;

– operable state of a "device" can be set by a domain of quantitative values of variables characterizing its properties;

– a man is able to define the requirements to the engineering documentation for the production of a "device" in such a way that quantitative values of the variables belong to the operable state domain;

– a man is able to organize and realize the production in such a way that the requirements to engineering documentation (ED) are fulfilled under proper control during the production of a "device".

The realization of indicated principles of LTS reliability is based on the following conceptual basis:

1) Tectology by A.A. Bogdanov (1913);

2) Method for analysis of structures with mathematical logic by N.M. Gersevanov (1923);

3) System concept by L. von Bertalanffy (1947);

4) Paradigm by A.I. Uyomov about the trinity of philosophical categories: thing→relation→property (1963);

5) Theory of reliability of mechanical systems by V.V. Bolotin (1969);

6) Ideology of robust design by G. Taguchi (1976).

Basic method to ensure reliability of large transformable structures

A basic method to ensure LTS reliability is the method of design and technology analysis of reliability (DTAR). This method is based on the principle of coordination of design

and technological concepts on all stages of a life cycle from a technical intention up to the target task accomplishment, in accordance with which a developer, a process engineer and a manufacturer are obliged to have joint coordinated positions to understand and take all the required measures to meet the reliability requirements.

Based on the principle of the implementation of the indicated method, reliability assurance is not just formal single procedures, performed upon the completion of any life cycle stages, and not ceremonial calculations of the "amount of nines" in reliability indices. This process goes on constantly and in parallel with the design engineering process, and besides, according to a single objective of the development of reliable objects, the reliability assurance and design stage are equally relevant for the achievement of the prescribed reliability indices. The difference is in the goals and methods of their implementation, and, in psychological aspect as well, which is crucially important.

The aim of the design stage is to achieve an object's functional capability, the aim of the reliability assurance is to understand why something could fail, which effects it could have and which measures should be taken so that the object can anyway keep its functional capability. A design procedure is normally performed by heuristic methods, and the reliability assurance – by the methods developed on the basis of utilitarian scientific (system) approaches.

The psychological factor is a key factor in the process of reliability assurance. To think intentionally how an object will operate is one thing, and to think about the causes that may lead to its failure is another thing. A developer tends to protect its darling, "to turn a blind eye" to gaps and deficiencies, to regard the structure with a "blurred" sight, and humanly it is absolutely natural and normal. That is why it was called for analogies from legal practice of pleaders and prosecutors when one of them defends, and another one accuses, and both of them do render justice. The attention was repeatedly drawn to the necessity and expedience of split of functions of reliability assurance at the design stage. For instance, in some of the issues of the SC design guidelines *Mary L. Bowden* [6] pointed out: *"Fully examine whether anything can conceivably go wrong, note that an unbiased but critical reviewer must do this, not the designer or chief engineer, who cannot help but think of how the system will work rather than how it will not work»*. According to a figurative note made by I.A. Ryabinin, such a "critical auditor "whereby must have"*...a psychology of a "diversionist", i.e. think properly how... to bring the system into hazardous state"* [7].

DTAR is aimed at the provision of evidence and confirmations of an object's ability to show the prescribed properties or the ability to show them on the level of physical necessity.

DTAR methodology is based on the following basic principles:

1) Reliability, as a property of relations of material objects, by means of relative positions, interrelations and interoperations is an integrated result of the properties shown by CE (a term "critical element" is regarded here as per GOST 27.310-95, article 3.7) assuring functional capability of objects in time;

2) CE properties assuring functional capability of objects can always be discovered by methods of system analysis expressed through the system of indices and parameters and defined quantitatively by the respective values;

3) Any calculations made during the design and engineering works serve as validation of the ED requirements. While solving the reliability tasks, such calculations are made for quantitative estimation of any parameters, or indices, achievement of which shall ensure operable state of objects;

4) The ED requirements must be met under the manufacture of parts and components, assembly, installation and acceptance testing of products, as well as they must be controlled by a manufacture quality control department;

5) Simultaneous fulfillment of the conditions on foundation, determination, carrying out of the design and technological requirements serve to ensure prescribed reliability.

DTAR in relation to LTS is performed in the following sequence:

– to carry out the most accurate and distinct qualification of possible failures;

– to have a full understanding about the environment the failures occur, exist and develop in;

– to reveal certain causes that may directly generate failures;

– to define the list of CE LTS;

– to define CE properties assuring the specified functional capability of LTS, for example, by the method of negative judgements in the amount sufficient to make a complete description of any LTS state provided the failure infeasibility;

– properties assuring LTS functional capability are expressed through the corresponding indices and parameters necessary to make a decisive characterization of its functional capability, and convenient for consideration of the properties concerned;

– to substantiate the criteria of limit values of indices and parameters under which LTS functional capability is ensured;

– to define limit values of indices and parameters;

– to define requirements in ED, that ensure a decisive achievement of the specified values of indices and parameters.

Further DTAR procedures are intended to provide all the indicated ED requirements that find a clear reflection in technological and operational documentation, are accurately fulfilled and properly controlled.

Practice of application has shown a good compatibility of DTAR with widely spread engineering methods of reliability analysis [3–4]. Besides, as the result of performed analyses of reliability of mechanical devices of single operation it has been revealed that DTAR as a method of verification of reliability requirements has a number of possibilities and advantages in comparison to the famous types of analyses:

1) DTAR is an additional type of analysis that does not substitute the current LTS reliability analyses, but generalizes and summarizes them;

2) Application of DTAR enables to increase certainty of calculations made to ensure reliability by means of the procedures of compliance of those accepted during analyses with the calculations of admissions with actual design and technological performance of the objects;

3) DTAR can be considered as a mean of system planning of those calculations which are required to ensure a specified reliability (calculations of strength, thermal calculations, calculations of dimension chains, etc.);

4) DTAR enables to reduce financial expenditures on LTS manufacture due to design errors by the fact that if they are detected timely during a design stage, you need to spend the same amount of money to correct them as the amount spent on their "occurrence", opposed to the correction of the design errors detected on later stages of a life cycle;

5) DTAR enables to forecast and eliminate the conditions of possible failures on earlier development stages. It facilitates not only the reduction of LTS failures in flight practice, but also the reduction of material costs of ground experimental methods due to both structure improvements and correction of failure effects;

6) DTAR enables to formalize the design process and as the result to reduce complexity of design works;

7) DTAR can serve as a mean to teach young specialists the methods of design with specified reliability indices;

8) DTAR enables to reveal design and technological factors of reliability of the concerned objects which are impossible to indicate by any other types of analyses;

9) Application of DTAR enables to provide the specified functional capability by means of system design and technological solutions made to substantiate, define, fulfillment and control of the fulfillment of the requirements to CE by a decisive performance of the specified functions;

10) DTAR is an effective mean to verify reliability, as it enables to explain not only the reliability requirements to the structures, but also the causes of their occurrence.

Approach to carry out analysis of reliability assurance

To achieve and keep the FFO close to one, it is necessary to detect and prevent from all the possible LTS failures without separation according to causes (errors, imperfections of methods or breaches of rules under design, manufacture or usage), degree of function impairment (important, unimportant, critical, catastrophic), occurrence probability (probable, improbable, etc.). In practice FFO requirements close to one mean that based on the knowledge, experience and understanding that a developer does have at the moment of reliability analyses, there must be for sure no failures. At any rate under the LTS development it is obligatory to take all necessary and reasonable measures to exclude failures. Newly revealed circumstances during manufacture and operation of LTS that broaden the understanding of the possibility of failures require an immediate adjustment of reliability analyses.

Tasks of analyses to ensure reliability for the products with a high rate of failure free operation shall include:

– detection of unacceptable losses of operable state;

– analysis of operating conditions with identification of the worst cases of combination of external factors, operating modes and design and technological performance;

– detection of all causes of possible failures based on research and practice basis of gained knowledge;

– development of means to remove the causes of possible failures;

– assessment of calculated values of reliability indices as well as its correlation with the prescribed reliability requirements.

It is suggested to solve the indicated tasks within the application of the following types of reliability analyses:

1) Functional analysis carried out to estimate the loss of separate functions affecting functional capability of the devices, as well as to define the acceptable losses criteria for every function and total criterion of a device failures (results of functional analysis are used when carrying out the next reliability analyses);

2) Worst case analysis, carried out to define possible matches of the worst combinations of external actions, operating modes, changes and degradations of physical and mechanical characteristics of the materials and performance of geometry of components and elements (results of a worst case analysis are used when carrying out the next reliability analyses);

3) DTAR, carried out to define values of indices and parameters characterizing failure free operation of the devices, substantiation of the limits of their change to provide an operable state, determination of requirements in ED related to an absolute performance of the required functions, fulfillment of all engineering requirements under manufacturing and organization of technical control (DTAR results are necessary to assess reliability, as well as for planning and implementation of physical measures to ensure reliability);

4) Analysis (estimation) of failure free operation, carried out to confirm that the predicted FFO shall be lower than the specified one.

If after the reliability analyses the predicted FFO is lower than the required value, it is necessary to review design and technological requirements to functional capability with an adjustment of the limits of a range of indices or parameter values, to change a reliability structure model, to change the accepted design r technological solutions, etc. After that it is necessary to repeat the reliability analyses with an assessment of a predicted FFO value till the specified reliability conditions are fulfilled.

Approach to assess dependability

Assessment of LTS reliability is carried out based on identification and consideration of the assessments of particular probabilities of certain properties: design, technological, strength, thermal, etc. Assessment of certain

properties is made by methods of the scientific knowledge which is applicable for the research of these properties, for instance, for strength – these are the methods of such disciplines as structural resistance, structural mechanics, elasticity theory, etc. A criterion of such assessments is the probability to find the values of indices and parameters within the ranges of operable state of the structures. For a guaranteed assurance of criteria of the structure operable state, it is necessary to carry out all the above mentioned DTAR procedures. Failure to carry out any of DTAR procedures or negative analyses results mean the probability of a failed operable state in relation to the property under consideration.

Overall reliability assessment is an additive calculation of the results of assessment made in relation to the particular probabilities of certain properties with consideration of the method of reliability structure diagram [8]. Such assessment does not have any frequency sense in failure development, but it reflects a degree of confidence that all the required design and technological solutions aimed to achieve the prescribed result on the level of physical necessity, have been initiated and made. This technique is used to explain the paradox, that due to social and economic reasons, specified reliability requirements are assigned with a specific frequency meaning which, as the requirements of failure free operation are getting closer to one, turns out to be an absurdity when making different engineering calculation.

In this formulation, any required calculations take their appropriate place in the methodology of reliability assurance, including the calculations developed in engineering practice (strength, thermal, etc.). System analysis of an object's properties that are changing in time determinates a necessity and reasonability of some calculations which excludes a subjectivity factor when it is necessary to choose any of them.

Integral assessment of LTS reliability can be made based on the method of score estimations of failure criticality (GOST 27.310-95, Annex B, table. B.1) with the only difference that in case all the design and technological solutions are made and implemented to achieve the prescribed result on the level of physical necessity, then, table B.1 shall be supplemented with a type of failures by a probability of occurrence with an expected probability close to zero (failure is negligible), with FFO close to one, correspondingly.

Conclusion

This article provides an approach to ensure UMCS reliability by the example of LTS. The results of practical application of this approach for the analyses of transformable structures operating in different external environments (in space for locking clamps of SC solar panels and in oil wells for casing cement collars) showed the possibility of timely detection of potential failures and prevent them before they become real. Gained practice of application of this approach proves that it is promising to develop process algorithms and methodologies for UMCS reliability assurance.

References

1 **Kuznetsov A.A.** Dependability of ballistic missilery structures. – M: Machinery engineering, 1978. – 256 p.

2 **Kuznetsov A.A., Zolotov A.A., Komyagin B.A., Titov M.I.** Dependability of mechanical parts of flight vehicle structures. – M.: Machinery engineering, 1979. – 144 p.

3 **Shatrov A.K., Nazarova L.P., Mashukov A.V.** Mechanical devices of spacecrafts. Constructive solutions and dynamic characteristics. – Krasnoyarsk: SibSAU, 2006. – 84 p.

4 **Shatrov A.K., Nazarova L.P., Mashukov A.V.** Basis of engineering of mechanical devices of spacecrafts. Constructive solutions, dynamic characteristics. – Krasnoyarsk: SibSAU, 2009. – 144 p.

5 **Pokhabov Y.P.** About the philosophical aspect of reliability exemplified by unique mission-critical systems // Dependability. – 2015. – No. 3. – P. 16-27.

6 **Bowden M.L.** Deployment devices // Space Vehicle Mechanisms – Elements of Successful Design, Edited by Peter L. Conley. John Wiley & Sons, Inc., 1998. – P. 495-542.

7 **Ryabinin I.A.** Dependability and safety of structural complicated systems. – SPb.: Polittechnika, 2000. – 248 p.

8 **Pokhabov Y.P., Ushakov I.A.** About reliability of unique mission-critical system // Methods of quality management. – 2014. – No.11. – P.50-56.