Ensuring the quality of the materials used in the spacecraft engineering

V E Patraev¹, E A Shangina¹, V V Dvirny¹, A A Voroshilova²,³,⁴ and S A Borisov²

¹ JSC “Academician M F Reshetnev Information satellite systems”, 52 Lenin street, Zheleznogorsk, Krasnoyarsk region, 662972, Russia
² Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russia
³ Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations, 61 Uritskogo street, Krasnoyarsk, 660049, Russia
⁴ E-mail: anvoroshilova@gmail.com

Abstract. The paper represents the principles and methods of perspective spacecraft quality assurance. The results of flight tests and operation of modern domestic and foreign spacecraft are taken into account. It is established that when planning scientific and methodological works aimed at ensuring the reliability of the spacecraft at the design stage, it is necessary to proceed from a number of principles that determine the order of spacecraft reliability index formation and constructive methods of ensuring reliability. The author's methodology includes an analysis of the main functions and their corresponding functional circuits. It is shown that when carrying out the functional analysis, special attention should be paid to identifying the mutual influence of the elements involved in performing various functions.

1. Introduction

In modern spacecraft (SC) development, only qualified materials are used in accordance with the mechanical, technological and physical properties of materials and operating conditions of equipment on the basis of an approved list of materials allowed for use in spacecraft developed by the space technology manufacturing organizations [1].

During SC development, the compliance of materials used by designers and subcontractors with external influencing factors, including active life, radiation, temperature loads, etc., is under strict control. When using materials that are not on the restrictive list, the results of the materials qualification, the sufficiency of the program and the amount of their testing are monitored. Permission to use materials in flight equipment is given only after completion of qualification [2].

2. Methodology of ensuring reliability at design stages

Constructive methods of ensuring reliability are based on the tests at all stages of the equipment design including both system and SC design [3]. The set of the analysis methods includes:

- functional analysis (at the level of equipment and systems);
- analysis (calculation) of reliability (at the level of equipment, systems and SC);
- failure mode, effects and critical analysis (FMECA) (at the level of equipment, systems and space vehicles);
- structural load analysis (at the equipment level);
• worst-case analysis (at the equipment level);
• resource provision and maintainability analysis (at the equipment level);
• extraordinary and emergency situation analysis (at the SC level);
• safety analysis (at the level of equipment and systems).

The purpose of the reliability analysis is to identify critical elements, to include them into the list of critical elements, to develop and implement a program of their control in order to eliminate criticality and ensure the reliability of the SC as a whole.

Other design tests include:
• analysis of electromagnetic compatibility by fields at the level of on-board equipment and space vehicles;
• analysis of conductive electromagnetic compatibility at the level of on-board equipment and space vehicles;
• thermal analysis;
• mechanical analysis;
• analysis (calculation) of radiation resistance to the effects of space factors.

The methodology of carrying out the reliability analysis includes certain requirements [4].

2.1. Functional analysis.
It is carried out to determine the impact of the loss of an individual function on the operability of equipment and systems, as well as to find each function of the criteria for allowable losses and the general criterion for the failure of equipment and systems for use in other reliability analyzes [5].

For each equipment or system, the main functions and the corresponding functional circuits are analyzed. For each functional chain associated with the main function, during analysis all the elements involved and the effect of their loss on the performance of the main function are determined.

As a result of the functional analysis, the structural diagram of the equipment or system in all modes of operation should be specified and its tabular description presented with the reflection of all available functional elements, their purpose and interfaces between them. When conducting a functional analysis, special attention should be paid to identifying the mutual influence of the elements involved in performing various functions.

For the equipment level, the block diagram should cover the level of the function blocks. For relay-switching single-type devices, it is advisable to consider the structural unit as a functional block. Functional blocks should be analyzed to the level of the main functional elements that realize the function of this block.

2.2. Reliability analysis (evaluation).
It is carried out for the equipment, systems and SC as a whole in order to confirm that their calculated probability of failure-free operation for the period of active life will not be lower than required [6].

The initial data for the analysis of reliability are the results of functional analysis.

When analyzing the reliability of equipment, system, SC, the following assumptions are accepted:
• the analyzed equipment, the system, SC are considered in their regular execution;
• stages of functioning are independent of each other. Loads of elements tested during the stage do not affect the failure rate at subsequent stages;
• the failure rates of electro-radio products are constant throughout the SC period of active existence, and their wear is not taken into account during the required period, unless otherwise specified;
• the reliability of the structural elements is taken equal to one subject to the completion of their qualifications and with a confirmed margin of safety in accordance with the strength standards;
• failures of individual components do not depend on each other;
• component parts and materials are qualified for their application and environment;
• production processes and tests do not introduce unknown mechanisms, hidden damages or failures and are approved for use in the project.

Reliability analysis must include:
• data sources used for the analysis;
• a structural diagram in all operating modes with its brief description and reflection of the existing interrelations of the elements;
• structural reliability scheme, corresponding to the structural scheme and reflecting all types of used reservation with their description;
• methodology and mathematical model for the calculation of failure-free operation probability, the corresponding structural reliability scheme;
• initial data and results of failure-free operation probability calculation;
• conclusion on the compliance of the calculated failure-free operation probability with the required value.

2.3. Failure mode, effects and critical analysis.
It is carried out in order to determine the possible types of failures for each piece of equipment, the system within its function and assess the impact of each type of possible failure on the specified characteristics of equipment, systems and SC.

Failure mode, effects and critical analysis (FMECA) must be carried out in order to determine:
• possible types of failures in the functional blocks of the SC equipment and the resulting consequences of failures in equipment, systems and SC;
• points of single failures and measures to mitigate their consequences or reduce the likelihood of their consequences from critical failures in order to concentrate efforts in the sphere of quality, inspections, control during manufacture;
• the need for more reliable developments, changes in design affecting components, materials or processes, the possibilities of project simplification and/or implementation of redundancy and cross-linking.

FMECA has to consider:
• types of failures caused by equipment failures;
• software crashes;
• failures of interface exchange between elements;
• personnel errors during operation, ground tests, transportation and storage.

For electronic and electromechanical equipment of a SC having internal redundancy, the types of failures caused by the construction and physical interaction between the components and equipment should be analyzed, although they can be isolated from each other from a functional point of view (project FMECA). In this case, the following should be determined:
• single points of failure (SPOF), caused by individual components related to elements with multiple applications (dual-purpose resistors that feed signals to a pair of redundant circuits, redundant circuits in the same hybrid integrated circuit (IC), etc.)
• SPOF relating to conductors, connector leads, soldered joints, jumpers, etc.

It is necessary to conduct FMECA of interfaces between the redundant circuits performed at the level of the component elements.

As a result of FMECA the following items should be defined:
• SPOF;
• elements single failure of which can spread and nullify the appropriate reservation or protection;
• critical elements for which detection and recovery should be carried out at a time shorter than the response of the ground station;
• elements in which influence of the single failure on the interface is not allowed by Terms of
Reference (TOR):
- failures causing breaks in work;
- failures causing safety level reduction;
- commands, unauthorized issuance of which can lead to negative impact;
- shortcomings of the project, equipment design (if identified) to ensure necessary reliability;
- availability of appropriate capabilities, such as telemetry information and control commands, to identify and counter the detected failures;
- ways of checking all reserve elements when simulating possible types of failures to the maximum possible depth at the appropriate integration levels;
- the necessary work in operation for the prevention and elimination of failures, included in the operating instructions.

The basis for carrying out FMECA of the equipment and the system is the result of functional analysis, i.e. the structural diagram of equipment and system, which is given in the report on FMECA. For each function, all possible types of functional devices failures and connections between them responsible for their execution should be determined.

The level of criticality of each type of failure is determined by the most severe consequences (the worst case) in accordance with Table 1.

Criticality level is added by “SPOF” index for single failure points, “S” index if the element is critical in safety, “B” index if the failure causes breaks in work and “R” index if reservation is provided.

**Table 1. Failure criticality levels.**

| Criticality level | Failure effect                                           |
|-------------------|---------------------------------------------------------|
| 1                 | The failure causes complete failure of the equipment, system or spacecraft |
| 2                 | The failure causes serious violations in the equipment or system functioning, constant limitation in SC work |
| 3                 | The failure causes losses of some operating properties of the equipment or system, leads to breaks in SC work |
| 4                 | The failure does not cause loss of the operating properties of the system (equipment), but it causes reducing the level of reservation or telemetric (TM) control |

The elements identified by the results of FMECA, assigned to the category of criticality 1 and 2 in table 1, are subject to mandatory inclusion into the list and control program for critical elements.

2.4. Structural load analysis.
It is carried out for electronic, electrical and electromechanical equipment in order to compare the actual load factors of the components at the maximum loads in the steady and transient modes, including the maximum thermal loads, with the established values of the load factors when using electrical and radio devices (ERD) in light modes.

If the equipment has internal redundancy, the analysis of the loads on the component parts must cover the failure conditions in addition to the standard configuration. If failure conditions change the load applied to a workable redundant side, the risk of failure propagation should be determined due to the increased voltage on the components (the performance values for the components are not exceeded if properly functioning, if the failed function can be disabled).

The calculation of the actual load factors of the ERD is carried out by comparing the calculated or measured ERD regimes with the regimes allowed in the technical specifications (TS) for ERD, taking into account the requirements for reducing loads.

If there are inconsistencies in the actual loads of components, measures should be taken to reduce
the loads of components to the established limits. The list of components that exceed the load criteria must be presented in the analysis of the loads on the component parts.

2.5. **Worst-case analysis (WCA).**

It is carried out for equipment to ensure that the equipment meets the requirements specified in the terms of reference (TOR) under the worst operating conditions at the end of the active life. The analysis is carried out for critical elements of equipment, or elements that fall under the requirements for accuracy, or sensitive to environmental conditions.

The analysis takes into account:

- changes in the parameters of the components due to the influence of destabilizing factors: temperature, aging (storage taking into account the active life), radiation in combination with a full range of supply voltage, temperatures, loads and input signals;
- modes of operation in transient processes, including failures of redundant circuits, transitions from mode to mode, on-off. WCA is a thorough evaluation of the technical characteristics of electrical circuits under conditions of external influence, operating conditions and conditions for changing parameters in the worst case, including:
  - changes in acceptable limits of components;
  - degradation due to aging (aging time is equal to active life);
  - extreme temperature values (temperature limits);
  - degradation due to radiation (the time of exposure to radiation is active life);
  - change in input power to upper / lower acceptable limits;
  - change of voltage to upper / lower acceptable limits;
  - sources of signals, with a deviation to the upper / lower acceptable limits;
  - changes in current loads, as a result of deviation to their upper / lower permissible limits;
  - changes in the components or in the scheme, depending on the external impact;
  - operating mode of the circuit in the worst case (regular, emergency operation modes, transients when switching on / off, during current surges, etc.);
  - loading of electrical circuits, control actions on the circuit, potential conditions of motion (delay mismatch).

2.6. **Resource provision and maintainability analysis.**

It is carried out at the equipment level to identify elements critical for resource and storage, and to determine the components of equipment that require resource tests (accelerated resource tests) and retention tests (accelerated storage tests).

As a rule, resource tests and storage tests are used to check the equipment or its components which are subject to deterioration or degradation of characteristics. First of all, they are used to check resource-critical elements, in order to confirm the given resource and reserves for the resource. These tests are usually used for Wave Tube Amplifiers (TWTAs), solid-state amplifiers, frequency standards, batteries, electromechanical and mechanical devices, etc.

For the rest of the equipment, the required resource and maintainability are confirmed by an analysis of the provision of resource and storageability on the basis of data and guarantees of the applied components and materials, assessing the possibility of degradation of characteristics during the operational active life, taking into account the WCA and the available developments of analogs and prototypes.

The analysis is carried out by reviewing and identifying resource-critical components of the equipment based on the data evaluation of the characteristics established in the ERB lists, qualification decisions and other documents, as well as statistical data on the prototypes and analogues in previous projects.

Analysis of resource provision and maintainability should be carried out taking into account the results of the equipment and components WCA: the maximum initial tolerance for characteristics, the
qualification range of operating temperatures and supply voltage, the effect of radiation and aging factors on the end of the operational active life. Based on the results of the resource provision and storage analysis, critical (degrading) components of equipment are identified that require resource tests and storage tests.

In conclusion, based on the analysis results the following items are stated:

- a list of elements that are resource and storage critical (if identified) that are to be included into the list and critical element control program as resource-critical and persistence-critical elements for criticality reduction activities;
- a list of equipment component parts that require resource tests (accelerated resource tests) and persistence tests (accelerated persistence tests) for inclusion into a Reliability Program (RP) and a General Development Test Programme (GDT) of the equipment.

2.7. Work interruption analysis.

It is carried out for the equipment and SC in order to:

- identify cases related to the total or partial loss of the target functions of the systems and SC as a whole;
- find elements, failures or malfunctions of which cause these cases;
- provide data about the work interruptions to test SC readiness;
- to define measures to minimize the occurrence of work interruptions and their duration.

For each event associated with the occurrence of work interruption, it is necessary to determine the possibility of its occurrence or its failure rate, the way to restore serviceability and the possible duration of interruptions, including ground tests and issuing commands [2]. The initial data of the work interruption analysis include FMECA and reliability analysis.

Work interruption analysis is carried out for redundant elements and unforeseen cases associated with interruptions, with nominal command submission and removal of telemetric information.

2.8. Extraordinary and emergency situation analysis.

It is carried out for the SC with the purpose of determining the algorithm of actions for the analysis and restoration of the SC operability for its use in operational documentation for spacecraft control.

The analysis considers non-emergency and emergency situations, elimination of which is possible only from the Earth.

Extraordinary and emergency situations analysis is the basis for the development of operational documentation for the SC control.

Extraordinary and emergency situations analysis should contain the following information:

- worksheets for all possible SC extraordinary and emergency situations analysis;
- worksheets for all possible on-board system extraordinary and emergency situations analysis;
- conclusions on the adequacy of the measures taken to parry extraordinary and emergency situations and developed exit algorithms to maintain the survivability of SC;
- recommendations, if required, for their application in operational documentation.

2.9. Safety analysis.

It is carried out for equipment and systems to identify and eliminate factors that can lead to injury or death of personnel, damage or loss of equipment, as well as to develop safety measures and actions of the maintenance personnel to prevent and eliminate hazardous situations and their consequences at all stages of work with equipment and systems. The following steps are taken into account:

- electric and other types of tests in the manufacturing organizations and on the technical complex;
- transportation and loading;
- repair and maintenance work.

In the safety analysis, the following hazards are considered:

- electrical (increased value of voltage, current in the electrical circuit, etc.);
• fire, explosion;
• thermal (elevated or lower temperatures of equipment surfaces);
• high-frequency, ionizing radiation, etc.;
• dangerous materials (flammable, high gas emission, toxic, etc.);
• mechanical (random activation of mechanical devices, moving aggregates and mechanisms, transfer of products, etc.);
• pressure (overpressure);
• operational (errors of the operator, maintenance personnel);
• electrostatic discharges;
• mental and physiological (mental and physical overload).

For each hazardous factor, the causes of the hazard, the possible consequences for personnel and equipment, as well as the measures taken to prevent (protect) the hazard, should be analyzed in relation to the equipment in question.

The hazard level is determined by the most severe consequences (worst case) in accordance with the categories given in Table 2.

### Table 2. Categories and levels of danger.

| Category   | Level | Possible consequences                                              |
|------------|-------|-------------------------------------------------------------------|
| Catalytic  | 1     | Death                                                             |
|            |       | Death threat                                                      |
|            |       | Permanent disability                                             |
|            |       | Professional diseases                                            |
|            |       | Temporary disability without death threat                         |
|            |       | Temporary professional disease, serious injure                   |
| Critical   | 2     | Loss, damage of SC, SC equipment or on-ground equipment           |
|            |       | Loss or big damage of public or private property                  |
|            |       | Long-term damage to the environment                               |
|            |       | Minor injures                                                    |
| Significant| 3     | Minor damages of other equipment                                  |
|            |       | Minor damage of public or private property                        |
|            |       | Temporary damage to environment                                   |
| Minor      | 4     | No consequences                                                   |

Identified dangerous elements related to the level of danger 1 and 2 are to be included into the list and the control program for critical elements as "Element critical for safety" [3].

### 3. Conclusion.

The analysis of the principles and methods for ensuring the reliability of perspective SC, taking into account the results of flight tests and operation of modern domestic and foreign SC has been done. It is found out that while planning scientific, methodological and other works devoted to the problem of ensuring SC reliability at the design stage, it is necessary to proceed from a number of principles. Such principles are the procedure for forming the composition of SC reliability indicators and constructive methods for ensuring reliability, which include:

• use (selection) of ERD for the integration of on-board SC equipment only of the highest quality level, the qualification of ERD for the forthcoming use;
• use of stable, wear-resistant and resistant to external influences materials used in the design of SC and on-board systems;
• use of optimal circuit solutions based on the perspective methodology of reliability analysis at design stages.

The methodology provides: functional analysis (at the level of equipment and systems); analysis (calculation) of reliability (at the level of equipment, systems and spacecraft); FMECA (at the level of equipment, systems and space vehicles); analysis of loads on component parts (at the equipment level); analysis of the worst case (at the equipment level); analysis of resource provision and maintainability (at the equipment level); readiness analysis (at SC level); analysis of extraordinary and emergency situations (at SC level); safety analysis (at the level of equipment and systems).

References

[1] Arzamasov B N et al 2008 Materials Science ed B N Arzamasov and G G Mukhina (Moscow: MSTU)
[2] Galochkin S 2011 Application of Microsatellites for Monitoring Natural Disaster Results in Siberia and for Education purposes Digest of the 8th International Symposium of the Intern. Acad. of Astronautics (Apr. 4-8, 2011, Berlin) pp 8-15
[3] Patraev V E 2014 Fundamentals of SC reliability (Krasnoyarsk: SibSAU)
[4] Saleh J H 2011 Spacecraft Reliability and Multi-State Failures (J-F: Castet Ltd ) pp 20-40
[5] Kuznetsov P A, Kovalev I V, Losev V V, Kalinin A O and Murygin A V 2016 IOP Conf. Ser.: Mater. Sci. Eng. 122 012020 doi:10.1088/1757-899X/122/1/012020.
[6] Kovalev I V, Losev V V, Saramud M V and Petrosyan M A 2017 MATEC Web of Conferences 132 04011 doi: 10.1051/matecconf/201713204011