Zhadnov V.V., Tikhmenev A.N.

SIMULATION MODELLING IN ESTIMATING RELIABILITY OF FAIL-SAFE ELECTRONIC EQUIPMENT

Enterprises of Russia's radio industry engaged in development and production of electronic instrumentation (EI) for space vehicles (SV), face problems of insuring reliability and, first of all, problems of failure-free operation. Failures during EI acceptance tests and accidents at SV operation are real evidences of mentioned problems. One of the reasons of such situation is application of out-of-date and inaccurate methods of estimating the reliability of SV EI at the design stage where developers embed the reliability that will be realized during production and supported at the operation stage.
On the other hand, use of "lower" estimates of failure-free operation parameters can lead to decrease of SV EI competitiveness, as this way in order to enhance reliability, manufacturers unreasonably use various additional ways that lead to deterioration of economic, mass-dimensional and other indices. Therefore, increase of accuracy of estimating the reliability of SV EI with long terms of active existence is a pressing problem, in particular for EI wherein redundancy as well as reconfiguration is used to ensure reliability.

Keywords*: reliability, electronic equipment, fail-safety, simulation modeling.*

Redundancy is one of the basic means to insure a required level of EI reliability with its insufficiently reliable constituents (C). The purpose of redundancy is to provide failure-free operation of EI as a whole, i.e. to keep its serviceability when there is a failure of one or several Cs. Together with «traditional» redundancy introducing additional (redundant) Cs, there are also other kinds of redundancy used. Among them, there is time redundancy (using time reserves), information redundancy (using reserves of information), functional redundancy when we use the ability of C to carry out additional functions or the ability of EI to redistribute functions between Cs, loading redundancy when the ability to take on additional loads exceeding nominal ones and the ability of EI to redistribute loads between Cs are used [1].

One of the ways of practical implementation of redundancy based on the EI ability to redistribute functions (or loads) between Cs is reconfiguration of its structure during failures. When using such redundancy, there occurs a problem of estimating the efficiency of reconfiguration algorithms, i.e. it is necessary to estimate how much the reliability parameters of EI have increased quantitatively.

In case of availability of structure reconfigurations during EI operation, to estimate reliability it is necessary to take into account not only possible combinations of working and not working Cs at the end of the time period of functioning, but also the sequence of their failures. It is caused by the fact that failures of some Cs can make other Cs change their operating modes, and consequently, their reliability characteristics [2].

The standard methods of analytical calculations (methods of minimal paths / cross sections, etc.) are of little use for such cases. To estimate reliability parameters by using an analytical method, we can build some mathematical model that takes into account the structural redundancy and possible failure scenarios and reconfigurations of EI with probabilities of each of them. Such a model is developed on the basis of the theorem of total probability, and to be as much adequate as possible, should take into account all possible operation scenarios when EI serviceability is retained, otherwise results of calculation will be obviously approximate.

However, in practice with a lot of interrelated components and various reconfiguration algorithms it is extremely difficult to satisfy the given requirement when constructing a mathematical model due to a huge amount of alternatives, therefore one usually makes a number of assumptions that allow us to obtain the «lower» estimation of reliability.

The alternative to an analytical method is the method of simulation modelling. However, construction of a model, its verification and conduction of a simulation experiment are quite complicated and time-consuming operations requiring high qualifications of a researcher. Application of simulation modelling allows to very precisely estimate the reliability parameters of a complex EI due to the adequate description of its structure and reconfiguration algorithms. The basic complexity of application of this method consists not so much in construction of a formal model, but in its verification to confirm the correctness of obtained results.

In spite of universality of this research method, its application for reliability calculation is not systematical; a few articles on the topic are isolated and describe construction of models for particular EI structures [3, 4]. It leads to the necessity of recurrence of developing sufficiently similar models of EI reliability by

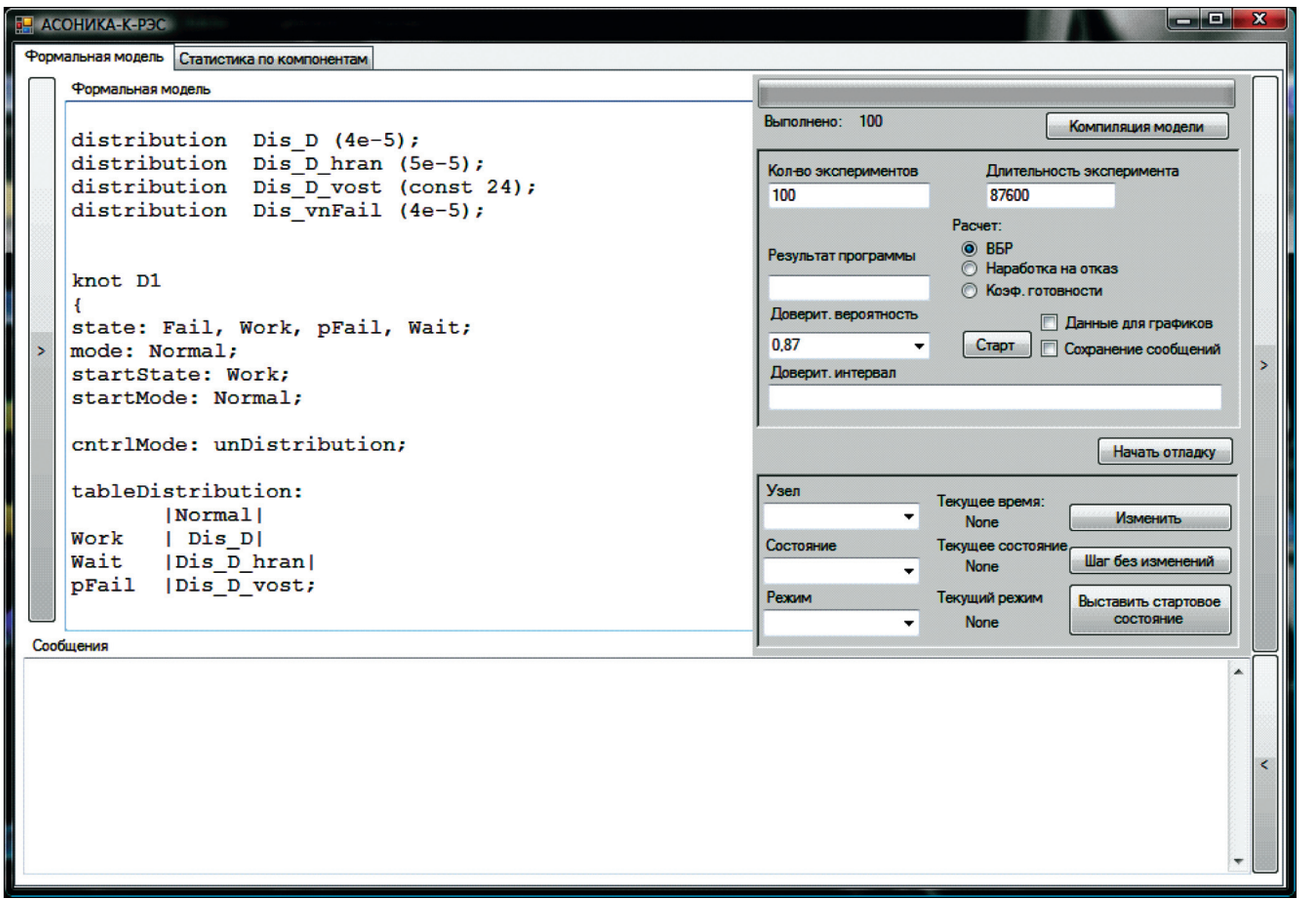

Fig. 1. The ASONIKA-K-RES system: user interface

means of various programming languages. Existing developments in the field of reliability simulation of complex systems concern the issues of maintenance service [5]. To solve these problems, there are also some specialized software products (for example, AvSim + system by Isograph company) with some sets of templates, and some universal languages of modelling (for example, a widely known GPSS language provides a possibility to describe sufficiently complex structure systems of spares [6]), which allow us to model a maintenance service system and estimate its efficiency. However, even application of flexible (as it seems at first glance) languages of simulation modelling does not allow us to essentially simplify the problem of constructing and verifying an EI model with a complicate reconfiguration algorithm.

In order to solve similar problems, the ASONIKA-K-RES system has been developed. The system enables to build models of reconfigurable EI using «standard» elements, by analogy to how models of queuing systems in the GPSS language are created. The system (see Fig. 1) includes a language compiler, model verification tools, means for carrying out simulation experiments and processing their results.

The specialized language for description of reconfigurable EI failures (ASONIKA-K-RES system input language) has been developed for model description. The language allows describing separately each component of EI through its list of states and modes, and also transitioning rates in between states. In compliance with the language semantics, the model of each component to some extent “lives its own life”, that is, after the beginning of a simulation experiment for each component we define time for which it should keep in initial state, and after that its states start to change in compliance with its description [7].

As an example, we shall consider the calculation problem of telemetry unit (TU) which is part of the onboard integrated computer complex (OICC) intended for use in near-Earth space environment as part of onboard computer networks of a space vehicle. To insure reliability requirements, a redundancy schematic and reconfiguration algorithm have been developed using structural features of TU.

TU is a complex product containing a big number of Cs, incorporated in redundancy groups at several downsizing levels. TU consists of 2 sets of modules. The same type modules are located in one cell, but are fed from various sources of power supply. TU has a local circuit of redundancy for supporting independent functioning, irrespective of serviceability of other parts of OICC. This circuit has 4 levels of redundancy and is presented in Fig. 2.

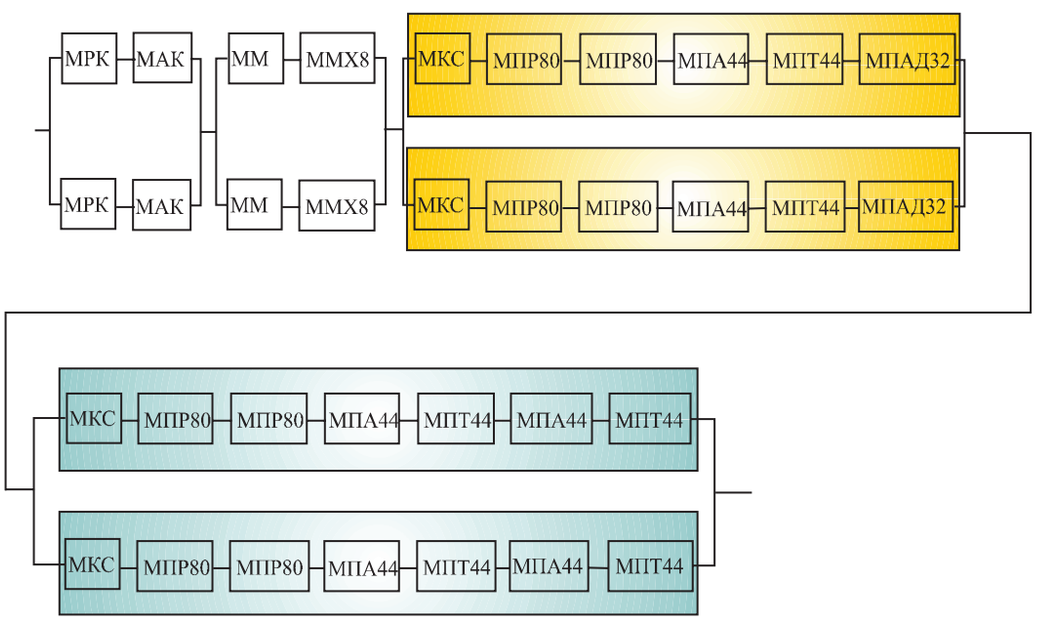

Fig. 2. Local circuit of TU redundancy

It is worth to note that for chains of components inside bars (see Fig. 2), failure of any component in each of them (except for МКС), or even several components, does not lead to total failure of the whole chain since if the same components remain efficient in a similar chain these failures can be parried by hardware-software means of TU without participation of external control (provided that power supply is sent onto both chains) and, thus, TU remains completely efficient.

Telemetry modules of half-sets A and B (see Fig. 2) function as follows:

- The MPS module (A) provides power supply to the following groups of modules:

• module of MM (A) + module MMH8 (A);

• 2 groups of modules МКПС(А);

• 11 groups of modules МУП2(А), and in this case each module МУП2(А) is connected over power supply circuits to one of measuring modules МПТ32(А), МПА64(А), МПЦ80(А), МПН32(А).

- Each of the two modules МКПС(А) is connected functionally to groups of measuring modules: the module МКПС1(А) is connected to the three modules МПТ32(А) (group of 1 measuring modules in Fig. 3), to the two modules МПЦ80(А) (group of 3 measuring modules in Fig. 3) and to the one module МПН32(А) (group of 4 measuring modules in Fig. 3);

- Module МКПС2(А) is connected to the two modules МПТ32(А) (group of 1 measuring modules in Fig. 3), to the one module МПА64(А) (group of 2 measuring modules in Fig. 3) and to the two modules МПЦ80(А) (group of 3 measuring modules in Fig. 3).

- Similarly the module МПС(В) provides power supply to such modules of the half-set B.

- When the module МПС(А) fails, all modules of the half-set A listed above are disconnected, and the module МПС(В) and all modules of the half-set are activated.

- When modules of MM (A) or MMX8 (A) fail, the module МПС(В) (B) and all modules of the half-set are activated, and modules of MM (B) and MMX8 (B) start to function instead of the switched-off modules of MM (A) and MMX8 (A).

- When one of the modules МКПС(А) fails, the module MKPS (B) and all modules of the half-set are activated, except for measuring modules and modules МУП2, connected to the module МКПС(В), corresponding to the serviceable module МКПС(А). Instead of the failed module МКПС(А) and the chain of measuring modules connected to it with their corresponding modules МУП2(А), the module МКПС(В) and the chain of measuring modules connected to it and modules МУП2(В) start to function.

- When one of the modules МУП2(А) or one of the measuring modules of the half-set A fail, the following modules are activated: (B), MM(B), MMX8(B), МКПС1(В), МКПС2(В), the measuring module of the half-set B together with the module МУП2 corresponding to the failed module of the half-set A. All other measuring modules and modules MUP2 of the half-set B corresponding to them keep switched-off. Instead of the failed module МУП2(А) or the measuring module of the half-set A, the corresponding measuring module of the half-set B and connected with it by power supply module МУП2(В) start to function.

The block diagram of TU reliability corresponding to these conditions of functioning is shown in Fig. 3.

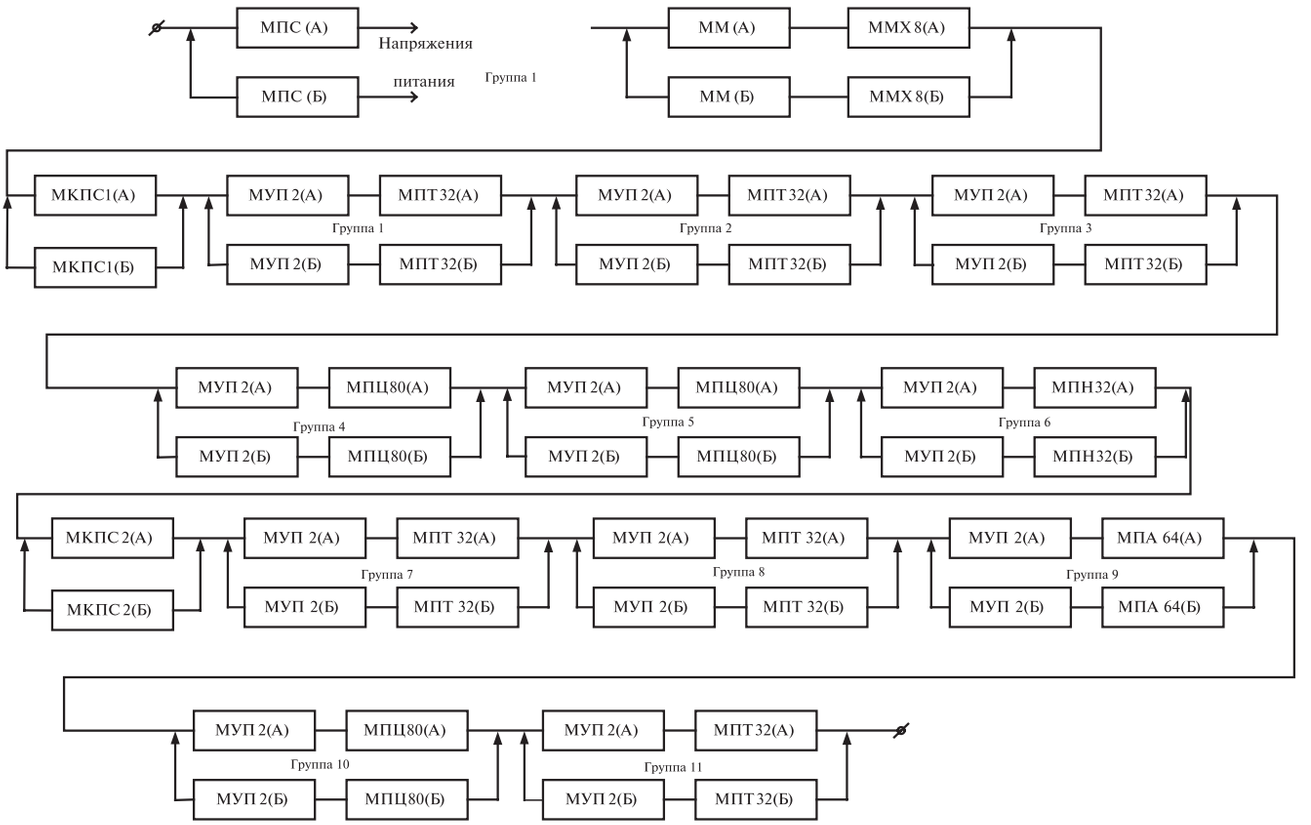

Fig. 3. The block diagram of TU reliability

The description of TU modules in the input language of system ASONIKA-K-RES is simple enough since all of them are no restorable and just operate to failure, and only for modules of the half-set B there are two modes: expectations (storage) and operation. Such process can be presented in the form of diagram shown in Fig. 4.

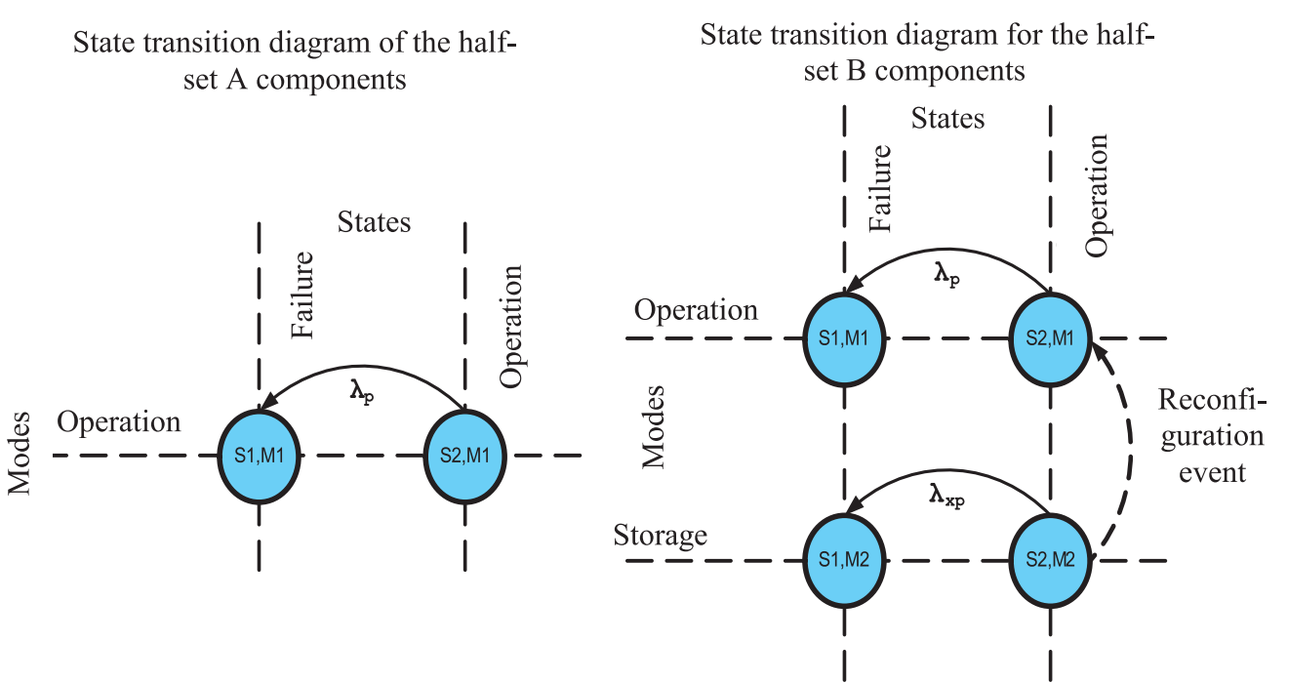

Fig. 4. Diagrams of transitions of TU modules

Transition of "elementary" components from one state to another is modeled through the laws of distribution. Transition into another state with the same mode is characterized by some density of probability in time. The density in formal model is set through the law of time distribution of a component being in each state.

Transition from one state into another can also take place as a result of any event in the model. And intensity induced transition cannot change a mode, only the state changes. An event can transfer a component in any pair "mode – state". The semantics of the standard model of a component assumes that the first state is a state of failure, from that state the transition in other state is impossible.

The formal model of a component looks more bulky, but still it is simple enough and logical:

```
knot MMX8_B
{
state: Fail, Work;
mode: Normal, Wait;
startState: Work;
startMode: Wait;
cntrlMode: unDistribution;
tableDistribution:
      |Normal |          Wait |
Work | Dis_MMX8|           Dis_MMX8_Wait;
tableStateChange:
         Normal |Wait
Work          |Fail    |Fail;
};
```

The presented description is universal and will consist of the following blocks:
- state <the list of possible states of a component>;
- mode <the list of possible modes of a component>;
- startState <starting condition>;
- startMode <starting mode>;
- cntrlMode <parameter determining the type of a component (elementary or compound)>;
- tableDistribution <table of time distributions of being in each pair (a mode; a state)>;
- tableStateChange < table of transition directions of each pair (a mode; a state)>.

Thus, the "text" model definitely describes the diagram form of transitions, shown in Fig. 4.

The exponential distribution is used in the given model, therefore there is no necessity to take into account the previous states of a component, and however, the possibility for considering other types of distribution is generally stipulated. Such models are described in [7].

Components are combined into a common model by using components of a higher downsizing level. So, either symbolic notation of a group of components included in the reserve or EI description as a whole can be used for this. A group of components is defined similarly as a single component but its state is determined not by the distribution, but as a function of the state of other components. Thus, an elementary component and a group of components can be both included in a state of group failure. This is why a component externally describing a group is characterized by the same parameters as an elementary one is characterized by a state and an operating mode [8].

When constructing a TU model, it is convenient enough to combine components into groups from half-sets A and B which back up each other. To describe failure criteria, logical and mathematical

operations over states of components are used. Generally, it can be a computing operation with its own local and global variables, cycles and ramifications. In the case of TU model, it is sufficient to use small expressions related to states of components. The result of such expression should be equal to «1" if the group is efficient, and to "0" in case of its failure. For any of redundant groups it is possible to write such an expression. The example of such an expression is shown below:

```
function FunctGroup2
{
return (MPS_A&MUP2_2_A &MPT32_2_A)|( MPS_B&MUP2_2_B&MPT32_2_B);
};
```

When calculating the state, names of components are replaced by "1" if the component is not in a failure state (the first state specified in the list of states), and by "0" otherwise. It is also possible to use the following writing: K1_1: Operation. This operator returns "1" if the component is in a "Operation" state and – "0" for any other state. Thus, the given expression remains equal to "1" until components remains efficient even in one half-set.

To describe the switching-on of redundant components and the switching-off of the basic ones, a specialized construction switch-event is used. This construction represents the pair "reconfiguration condition – reconfiguration action". To describe reconfiguration action, operators of state change and mode change are used. In the case of reconfiguration, logical and mathematical operations over the states of components in the model are also used. However, to simplify the task, operators for defining the time of transition of a component from one state into another have been added. To describe reconfigurations inside a TU, it is necessary to create many reconfiguration actions but they supplement each other. Each of actions describes reconfiguration in case of failure of one component; therefore, it includes just a few operations. The example of one such construction is shown below:

```
switch_Event MUP_1_A_FAIL  (->MUP2_1_A:Fail|->MPT32_1_A:Fail)
{
set_mode (MPS_B:Normal);
set_mode(MM_B:Normal);
set_mode(MMX8_B:Normal);
set_mode(MKPS1_B:Normal);
set_mode(MKPS2_B:Normal);
set_mode(MUP2_1_B:Normal);
set_mode(MPT32_1_B:Normal);
};
```

In the given example the condition for the beginning of reconfiguration is transition of the component МУП2 or a component in МПТ32 into failure state. Action consists in changing modes of those components which should be put into operation according to the description: these are the common components of the half-set and the redundant group for failed components. It is not difficult to make other reconfiguration actions by analogy as they completely repeat the description of TU structure.

After programming of the description of the formal model, its verification is required since if we have not verified the adequacy of the programmed reconfiguration algorithms and failure criteria, it is impossible to be confident that the results of modelling will be reliable.

At the initial stage for verification we used the results of probability calculation of failure-free operation (P_{BT}) obtained under the following mathematical model:

$$P_{БТ}(t) = e^{-\lambda_{A(Э)}t} + \sum_{i=1}^{10} \lambda_{Mi(Э)} \int_0^t e^{-\lambda_{Б(x)}\tau} \cdot e^{-\lambda_{A(Э)}\tau} \cdot P_{рез(i)}(t-\tau)d\tau, \quad (1)$$

where $\lambda_{A(Э)}$ is failure rate of all the modules of the half-set A being in the switched-on state; i is number of a reconfiguration script corresponding to failure at the moment of time τ of the i-th module from the half-set A; $\lambda_{Mi(Э)}$ is failure rate of the i-th module of the half-set A being in the switched-on state; $\lambda_{Б(x)}$ is failure rate of all the modules of the half-set B being in the switched-on state; $P_{рез(i)}$ is probability of failure-free operation of the redundant system of telemetry modules during the time t, after failure at the moment of time τ of the i-th module of the half-set A provided that before the moment of time τ all modules of the half-set B were serviceable.

Model (1) has a number of restrictions, in particular it was accepted that the half-set B should be completely serviceable for replacement of any failed module of the half-set A. In reality, however, it is required that only those units which are directly involved in operation according to the reconfiguration script should function, and only one of the scripts needs a full-function complete set B, i.e. failure of МПС(А), while the others tolerate the possibility of failure of some components pertaining to the half-set B. In addition, (1) takes into account reconfiguration of TU only at the first failure, and any subsequent failure is considered as failure of all TU which also does not correspond to the real algorithm of functioning.

Despite of these restrictions, it is obvious that the value P_{BT} obtained as a result of simulation modelling cannot be lower than that calculated as to model (1). Besides, the ASONIKA-K-RES system provides the opportunity of conducting a controlled experiment to verify the model. In this case the user on his/her own defines the sequence of failures of components and controls a model's state after each failure (Fig. 5).

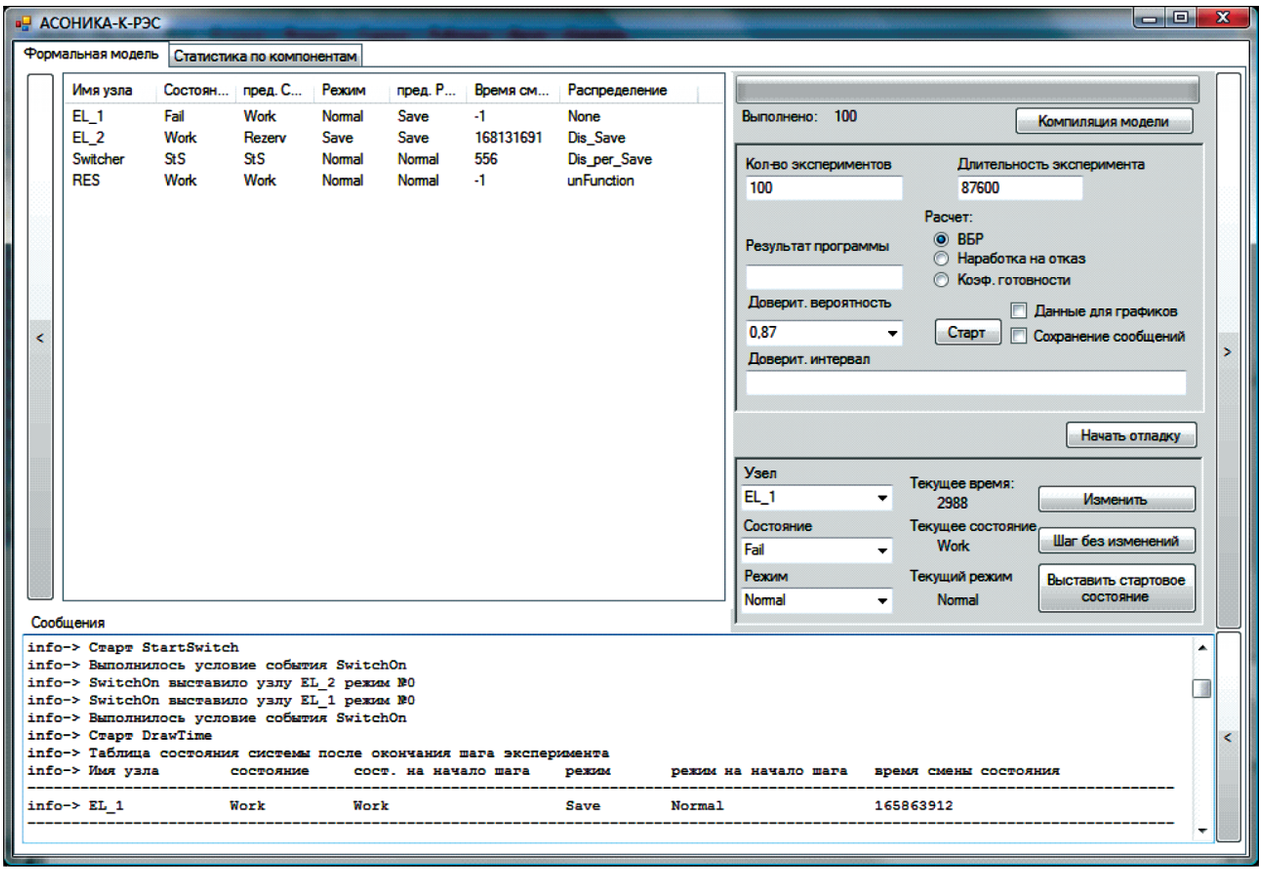

Fig. 5. The ASONIKA-K-RES system: process of model verification

In case of mismatch of a model's reaction to the description of TU operation, the error can be found with the help of the analysis of the log file as to execution of an experiment's step, which contains data about which conditions pertaining to which reconfiguration events have been satisfied and which operations over a model's components have been made. An example of such log file is presented in Fig. 6.

```
 |     Шаг отладки  №   7      |
  \_____________________________/
info-> Часы сдвинуты на 330 часов
info-> Часы системы выставленны на значение 2988 часов
info-> Изменяет сотояние узел Switcher
info-> Узлу Switcher присвоенно состояние StS
info-> Старт StartSwitch
info-> Выполнилось условие события SwitchOn
info-> SwitchOn выставило узлу EL_2 режим №0
info-> SwitchOn выставило узлу EL_1 режим №0
info-> Выполнилось условие события SwitchOn
info-> Старт DrawTime
info-> Таблица состояния системы после окончания шага эксперимента
info-> Имя узла        состояние     сост. на начало шага    режим       режим на начало шага   время смены состояния
-------------------------------------------------------------------------------------------------------------------------
info-> EL_1            Work          Work                    Save        Normal                 19813522
-------------------------------------------------------------------------------------------------------------------------
info-> EL_2            Rezerv        Rezerv                  Save        Normal                 81382895
-------------------------------------------------------------------------------------------------------------------------
info-> Switcher        StS           StW                     Normal      Normal                 3544
-------------------------------------------------------------------------------------------------------------------------
info-> RES             Work          Work                    Normal      Normal                 -1
-------------------------------------------------------------------------------------------------------------------------

  /  ____________________________\
 |      Шаг отладки      №8      ||
  \_____________________________/
info-> Узлу EL_1 присвоенно состояние Fail режим Work
info-> Старт StartSwitch
info-> Выполнилось условие события EL_1_fail
info-> EL_1_fail выставило узлу EL_2 состояние №1
info-> Старт DrawTime
info-> Таблица состояния системы после окончания шага эксперимента
info-> Имя узла        состояние     сост. на начало шага    режим       режим на начало шага   время смены состояния
-------------------------------------------------------------------------------------------------------------------------
info-> EL_1            Fail          Work                    Normal      Save                   -1
```

Fig. 6. The ASONIKA-K-RES system: log file of a controlled experiment

As reconfiguration events usually have sufficiently simple conditions and perform not so many actions, then based on this log file and print-out of components states before and after change, it is possible to easily determine the source of errors and to make corrections to the program (model). It should be noted that generally it is always recommended to verify a model with the participation of an expert who knows the object of research and has not been involved directly in the development of a model, as this essentially facilitates process of verification and promotes fast search and elimination of errors.

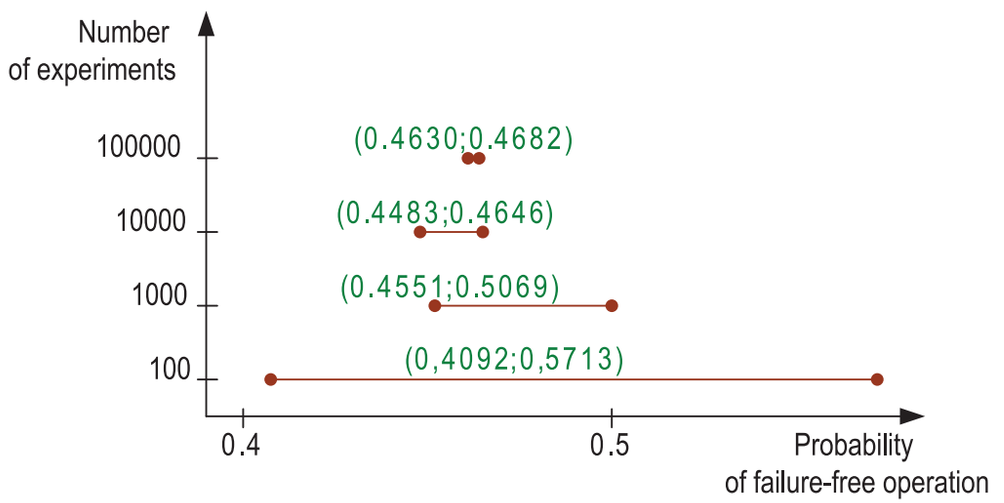

Fig. 7. Relation between the width of the P_{BT} confidential interval and the number of experiments

However, a verified model cannot provide a "precise" estimation of the probability of failure-free operation (or mean time to failure) even in case of a significant number of virtual experiments (tests of a model), therefore, in order to calculate reliability parameters, the ASONIKA-K-RES system calculates a confidential interval for a confidential probability specified by the user. It is obvious that the increase of the number of experiments leads to the increase of estimation accuracy of reliability parameters of EI in question. The diagrams that characterize reduction of the relative width of a confidential interval for P_{BT} in case of increase of the number of experiments are shown in Fig. 7.

The P_{BT} estimation obtained as a result of simulation modelling was 17 % higher than the results of the analytical calculation using the model (1), and that proved the efficiency of TU reconfiguration algorithm. In addition to that, according to statistics of TU failure times collected during experiments, time dependences of P_{BT} (Fig. 8) and failure rates (Fig. 9) have been constructed.

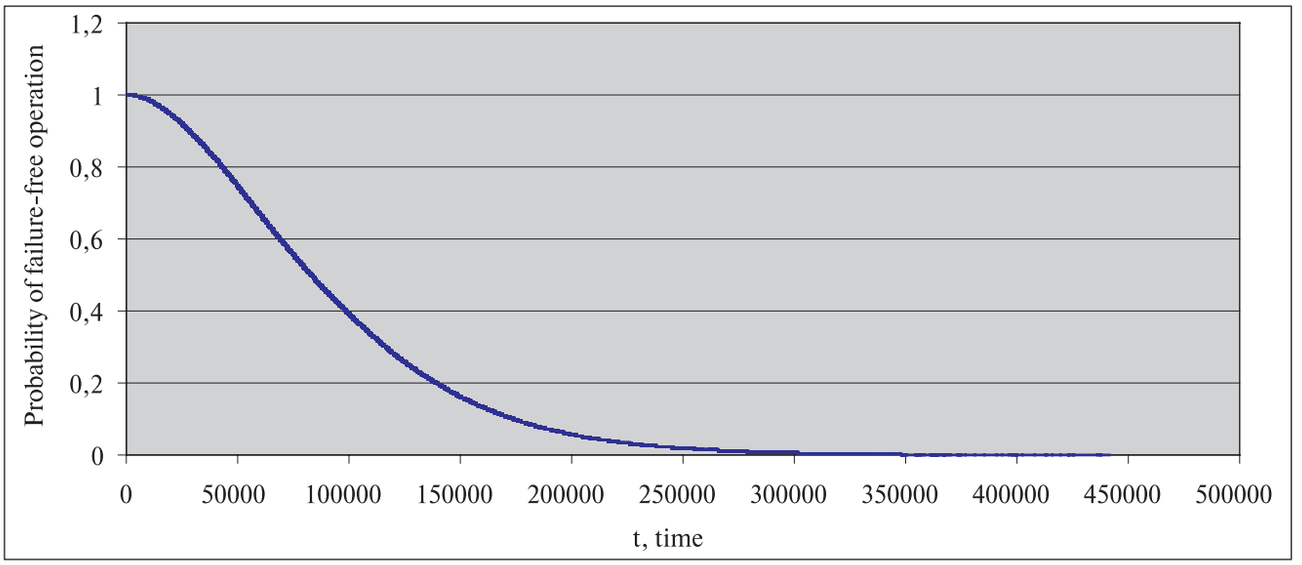

Fig. 8. ASONIKA-K-RES system: Chart of P_{BT} dependence of time

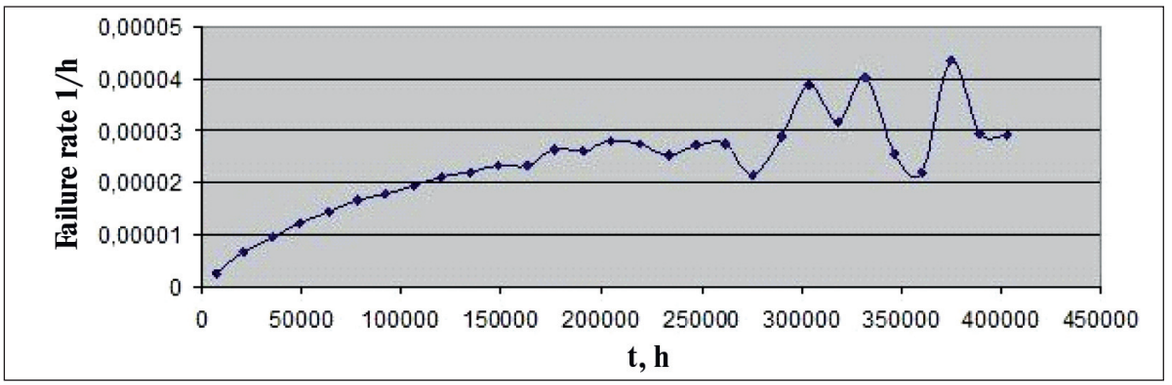

Fig. 9. ASONIKA-K-RES system: Chart of failure rate dependence of time

These charts are of interest for EI reliability studies and consequently included in the structure of service functions of the ASONIKA-K-RES system.

One more useful supplement to the method of simulation modelling realized in the ASONIKA-K-RES system is the opportunity of gathering statistics about failure causes. It allows to carry out the

comparative analysis and to reveal not only the least reliable groups of components, but also vice verse, to define EI components possessing redundant reliability. Carrying out repeated calculations after model modifications enables to estimate the effect of these changes and, thus, to optimize EI according to reliability criterion.

Thus, in the conclusion it is possible to ascertain that the developed language for the description of the reconfiguration process of EI in case of failures of its components and the software designed to work with it are efficient and perspective tools for reliability study. ASONIKA-K-RES application allows not only to raise accuracy of calculations due to the adequate description of structure and EI reconfiguration algorithms, but also to carry out researches aimed at optimization of their structure in terms of reliability insuring by engineers-developers from whom no profound knowledge either in the field of simulation modelling or in the theory of reliability is required.

References

1. GOST 27.002-89. Reliability in technical equipment. Terms and definitions.

2. **Zhadnov V.V., Lasarev D.V.** Simulator of electronic radio equipment reliability characteristics of components. / Reliability: Scientific and technical journal. No. 4 (11), 2004. – pp. 15-23.

3. **Feduhin A.V.** Modelling of a restorable redundant system with the structure like “k out of n”. / Mathematical machines and systems, 2008, No. 4.

4. **Zadorozhny V.N., Rafalovich S.A.** Solving equations in switching functions on GPSS WORLD. / Automated systems of information processing and management in UNIPS university: Collection of reports of theoretical and practical workshop. – Omsk: OmGTU, 2007. – pp. 31-34.

5. **John J. Black, Mejabi O.O.** Simulation of Complex Manufacturing Equipment Reliability Using Object Oriented Methods. / Reliability Engineering and System Safety, 2004.

6. **Tikhmenev A.N.** Application of GPSS WORLD language for failure modelling of electronic instrumentation with complex structure of redundancy. / Reliability and quality: Conference proceedings of the International symposium: in 2 v. // Edited by N.K.Jurkov. – Penza: PGU, 2011 – 1 v. -pp. 333-335.

7. **Tihmenev A.N.** Language for failure description of electronic instrumentation with reconfigurable structure. / Scientific and technical conference of students, post-graduate students and young experts MIEM: Brief outline reports – M.: MIEM, 2010. – p. 137.

8. **Zhadnov V.V., Tikhmenev A.N.** Modelling of electronic instrumentation components with reconfigurable structure. / Reliability and quality: Conference proceedings of the International symposium: in 2 v. // Edited by N.K.Jurkov. – Penza: PGU, – 1 v. – pp. 330-331.

9. **Zhadnov V.V., Polessky S.N., Tikhmenev A.N.** Development of reliability models for design researches of radio-electronic equipment reliability. / Radio altimeter 2010: Proceedings. The third All-Russia scientific and technical conference. // Edited by. A.A.Iofina, L.I.Ponomareva. – Ekaterinburg: Publishing House “Fort Dialogue-Iset”, 2010. – pp. 200-201.