THE ADAPTIVE APPROACH TO ACTIVE FAULT TOLERANCE MAINTENANCE OF AUTOMATIC CONTROL SYSTEMS

O. Gavrilenko, A. Kulik, O. Reznikova

National aerospace university "Kharkiv Aviation Institute"
61070, street Chkalov, 17, faculty of aircraft control systems (301)
Ph.: +3 8 (057) 707-43-01; fax: +3 8 (057) 744-11-33; e-mail:gvrol@d3.khai.edu

Abstract: In the article the well known approaches to fault tolerance maintenance, based on diagnosing and functional condition recovery of automatic control systems technologies, are analyzed. The features of the adaptive approach maintenance active fault tolerance by means of interconnected technologies of deep diagnosing of spacecraft stabilization system are considered.

Keywords: the adaptive approach, active fault tolerance, deep diagnosing, flexible recovery, diagnostic model.

1 THE CONDITION OF PROBLEM OF ACTIVE FAULT TOLERANCE MAINTENANCE OF AUTOMATIC CONTROL SYSTEMS

The industrial development period of society has resulted in creation of technical systems carrying potential threat to both a society and its environment. The majority of recent failures and accidents have man-caused character. Their consequences result in multimillion losses, ecological accidents (for example Chernobyl), and in the worse case to human victims. Analyzing the reasons of recent failures and accidents it is possible to make a conclusion, that four basic reasons, namely: technologies imperfection, human factor, vital subsystems faults and the external revolting influences, - are the preconditions for their occurrence. All this testifies to the unsufficient safety, survivability, fault tolerance level of created technical systems, and, first of all, of their automatic control systems (ACS).

Under fault tolerance we usually understand the system property to keep and automatically restore for the limited time an efficient condition at its element faults from the given set without essential functioning quality reduction (Patton, 1997).

Let's consider the available approaches to fault tolerance maintenance. According to diagnosing and recovery technologies used the well known approaches to ACS fault tolerance maintenance can be presented by such two: passive and active.

In the basis of the passive approach is the reason of maintenance robust of closed loop automatic control system to parametrical and signal uncertainty, caused by not certain types of faults. The various reservation methods widely used in the theory and practice of ACS construction are the common representatives of this approach. Its characteristics are use of not intellectual managing devices, which are selectively tolerant to certain faults types, absence of constructive diagnostic information reception procedures (fact of occurrence of a fault type, characteristic of a fault type), that allows to speak about fault tolerance in narrow sense (Patton, 1997, Demirci, and Kerestecioglu, 2003).

The active fault tolerance methods provide automatic control system „adaptation" to arising in it faults types in a mode of real time. The approaches to active fault tolerance maintenance are characterized by use of the advanced diagnosing and systems functional condition recovery procedures (Patton, 1997; Kulik, 2000).
Under active fault tolerance systems the authors understand its ability to carry out automatic deep diagnosing and flexible functional condition recovery satisfying to the required quality's parameters(Kulik,1994; Kulik, and Gavrilenko,2004).

The advantages of active fault tolerance are: smaller volume of used hardware and, as a consequence, smaller expenses for manufacture and more rational mass characteristics; the control is based on digital computing use (processors and microprocessors), that expands ACS opportunities, gives flexibility to developed control algorithms.

According to control formation the active fault tolerance methods can be divided into the following groups: preliminary (off-line) control laws formation, adaptation to faults in real time. Preliminary (off-line) control laws formation is elementary way of active fault tolerance maintenance, which disadvantages are the rigid law structure, depth of diagnosing up to a place of faults, adaptation elements absence to varied external conditions (Chen , *et al*., 1998; Zhang, and Jiang J, 2002).

The real time fault adaptation is deprived of these disadvantages. A plenty of approaches to active fault tolerance control formation in real time have appeared recently. They are Feedback Linearisation (Meyer, Smith, Ochi), and Model-following Approaches (Huang, Morse), and Pseudo-inverse modeling methods or reconfigurable management methods (Gao, Ostroff, Zhao) and Hybrid Adaptive Linear Quadratic Control (Ahmed-Zaid) and many others. The basic advantage of these approaches consists in use of diagnosing results for re-structuring or reconfigurable control. Nevertheless, these approaches are not deprived of disadvantages, namely: the questions of the redundancy analysis and control by it, absence of the forms description and features of restoration models (behind exception reconfigurable control) are not considered. The majority of the authors in the researches consider automatic control system elements (gauges, drives), instead of considering the system as a whole. All this allows making a conclusion, that in this area there are still more intuitive engineering decisions, than theoretically proved ones.

As it was said, in using active fault tolerance the first stage is functional condition diagnosing. In the sense of diagnosing depth tasks of the control (fault detection) and diagnostics (localization of a fault type) are distinguished. Now there are a large number of control and diagnostics methods, based on a number of classification attributes. Let's consider existing methods of diagnosing in the sense of their applicability to active fault tolerance maintenance.

As attributes of classification we shall allocate: a type of mathematical models of diagnosing object; diagnostic attributes character; a principle of diagnosing, depth of diagnosing.

Depending on the type of used mathematical models we can distinguish methods of diagnosing in time and frequency domains, static and dynamic, determined and stochastic methods.

According to the principle of diagnosing the control and diagnostics methods can be divided into three large groups - methods based on the invariants theory, on application of models and on introduction and use of analytical redundancy.

The methods based on application of the invariants theory. The given group of methods requires diagnosing object invariants knowledge. Some object characteristics remaining constant at normal object functioning and varying at faults occurrence are defined. These characteristics (invariants) are used further as direct or indirect diagnostic attributes. Invariants can be of two types - parametrical and signal. The basic difficulty at the control on parametrical invariants is connected to complexity of real parameters meanings measurement, whereas their rating value is known. At the control on signal invariants the main problem is the necessity of continuous theoretical target signals meanings definition, proceeding from known current meanings of entrance signals. For definition of real meanings parametrical invariants it is possible to take results advantage of the identification theory. At the signal invariant control the check of some algebraic control conditions is carried out which should satisfy input signals of object at the absence of faults.

The methods based on use of models. The given group of methods is one of most frequently used in technical diagnostics. The advantages of these methods are their universality and presentation.

In the elemental case of diagnosing with use of model as reference one the second copy of object, on which the same input signals are acts.

The control is made by comparison of outputs of the diagnosing object and the model. For hardware redundancy reduction it is possible to use not the duplicate of the object, but its mathematical model. Usually it is realized with the help of computer equipment. A number of mobile objects control methods are based on use of the so-called state observers. This term used for Kalman filters, Luenberger observers and other devices intended for estimation of linear dynamic systems condition state vector (Jiang, and Zhao, 1998; Demirci, and Kerestecioglu, 2003).

Methods based on use of analytical redundancy. The third control principle is connected to use of analytical redundancy (Patton, 1997). According to this principle the system diagnosing is carried out on the basis of analytical dependences check existing between measuring inputs and outputs of the system. Such dependences (control conditions, either equations or the parities) can connect signals related to the same moment of time - in this case we can speak about algebraic invariants, or to the different moments - then we speak about dynamic invariants or temporary redundancy (temporal redundancy). Among other types of redundancy there are geometrical one, reflecting presence kinematics parities between mechanical systems variables; structural one (arises at presence of measuring gauges superfluous number) and the information redundancy (takes into account presence apriority information). If the natural redundancy is absent, the artificial redundancy introduction is applied to get the invariant parities. The given methods are rather sensitive to the unmeasured disturbances of object (Jiang, and Zhao, 1998; Patton, 1997; Demirci, and Kerestecioglu, 2003).

It is important to notice, that all three allocated principles are not isolated, and act in close interaction. So, for example, the organization of the control is always accompanied by introduction and use of hardware, temporary or informational redundancy, which enables to receive the information on faults arising in system. In many methods this redundancy acts as this or that model used for obtaining control parities, invariant to input signals, or for calculation of diagnostic attributes, for which signal or parametrical invariants serve.

To disadvantages of the considered methods it is possible to relate: the authors do not consider an opportunity of „adaptation" of models and diagnosing methods to the recovery problem decision, in the majority they consider open-loop ACS diagnosing, use linear models; the considered methods provide small diagnosing depth (usually detection or place of faults).

2. THE NEW CONTRIBUTION TO ACTIVE FAULT TOLERANCE MAINTENANCE BY MEANS OF ADAPTATION

Theoretical and experimental researches carried out by the authors have allowed to generate the new adaptive approach to automatic control systems active fault tolerance maintenance (fig. 1).

The feature of this approach is that the basic principles and results of the modern automatic control theory are applied to solving a fault tolerance problem, as well as methods of systems signal-parametrical diagnosing (Kulik, 2000).

The modern methods of the automatic control theory are also based on using models of object or controlled process. These models have only information character - dependence of an object output on input influence. The models used in the adaptive approach are more complete, allow to simulate object, both in nominal, and in emergency operation. The methods of faults parrying include the available redundancy analysis and control methods. Using methods of redundancy control, the synthesis of algorithms is carried out with diagnostic models used at the first stage. Thus, the adaptive approach to fault tolerance maintenance provides adaptation, structural and semantic models integrity and, accordingly, algorithms used at all stages of active fault tolerance control.

The account of faults influence on ACS serviceability has resulted in necessity of considerating system with faults as one of its possible states. As a result of automatic control system research for considered set of fault types D = {d_1, d_2, …, d_q} it is necessary to establish direct diagnostic attributes for each basic task of diagnosing, namely: α_i - for a class determine task, β_i - for a place determine task, γ_i - for a location task. For each generalized diagnostic parameter $\lambda_i \in \{\alpha_i, \beta_i, \gamma_i\}$ the set of its possible values is established, and the model describing certain emergency operating mode is constructed. For the effective faults parrying the estimation of natural redundancy and depths of automatic control systems diagnosing will be carried out with the help of maintainability criteria of a structural-analytical ACS analysis method. Such analysis is carried out in two stages. The first stage is definition of hardware and functional resources of system based on tabulated model of ACS graph nodes connections. The second stage is definition of system information resources to form signal and parametrical tuning algorithms based on characteristic vectors. To formalize of hardware, functional and information redundancy existence conditions a number of constructive criteria is used.

The construction of adequate mathematical model of diagnosed object is one of the basic tasks of the diagnostic maintenance developer. In emergency and nominal modes ACS in a general view is described in states space by the following equations:

$$\begin{cases} \tilde{\mathbf{x}}(k+1) = \phi\left[\tilde{\mathbf{x}}(k), \mathbf{u}(k), \boldsymbol{\lambda}, \boldsymbol{\xi}(k)\right] \\ \tilde{\mathbf{y}}(k) = g\left[\tilde{\mathbf{x}}(k), \mathbf{u}(k), \boldsymbol{\lambda}, \boldsymbol{\eta}(k)\right] \end{cases}, \quad (1)$$

where $\tilde{\mathbf{x}}(k)$ is a state vector of a diagnosed object with faults; $\mathbf{u}(k)$ is a vector of input influences; $\tilde{\mathbf{y}}(k)$ is a vector of measurable object variables; $\boldsymbol{\xi}(k)$ and $\boldsymbol{\eta}(k)$ are the vectors of simulating noises and errors; $\phi[\cdot]$ and $g[\cdot]$ are nonlinear functions, λ – non-measurable generalized diagnostic parameter.

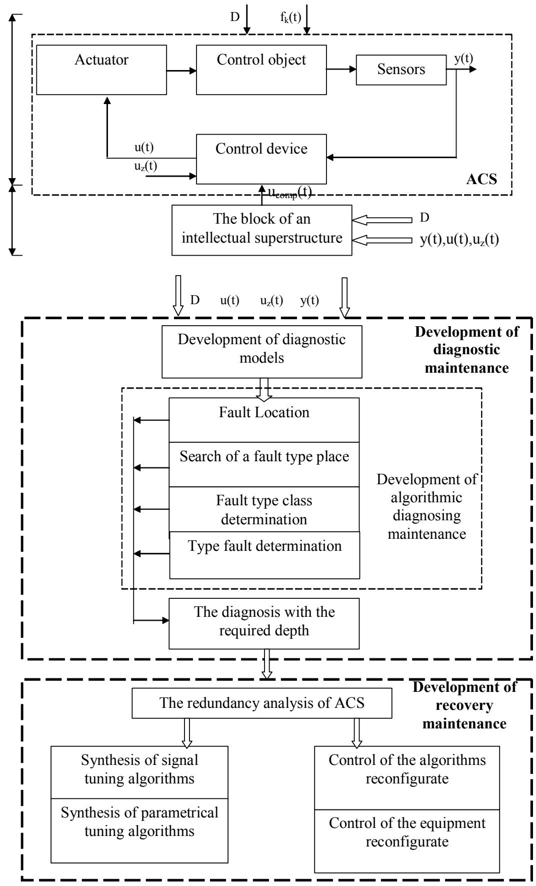

Fig. 1. Generalized circuit of the adaptive approach

The choice of diagnostic model depends on a task being solved and requirements, made to the time, quality and quantity diagnosing characteristics.

Within the framework of the adaptive approach the signal-parametrical methods, that allow ensuring diagnosing depth adapted to available resources, are developed (Kulik, 2000). The diagnosing is carried out stage by stage. At the first stage fault location is carried out (the fault location is a diagnosing stage on which the fact of operating break is established); at the second stage the search of fault type place is carried out (the diagnosing stage connected with finding of a structurally completed system unit or an element, in which a fault from the given fault types set occurred); at the third stage the fault type class is determined (the diagnosing stage connected with clearly recognizing of an occurring fault type class from the given set; a fault type class is a group of fault types described by the same display); at the fourth stage the fault type is determined (the diagnosis stage connected with clearly recognizing of certain physical fault display).

For the diagnosing realization the special diagnostic models are created. Diagnostic model (DM) is a formalized description of object necessary for the diagnosing tasks solving, connecting direct non-measurable object attributes with indirect measurable ones. Generally diagnostic model looks like:

$$\begin{cases} \Delta\mathbf{x}(k+1) = \Psi\left[\tilde{\mathbf{x}}(k), \Delta\mathbf{x}(k), \mathbf{u}(k), \Delta\lambda_i, \boldsymbol{\upsilon}(k)\right] \\ \Delta\mathbf{y}(k) = \Theta\left[\tilde{\mathbf{x}}(k), \Delta\mathbf{x}(k), \mathbf{u}(k), \Delta\lambda_i, \boldsymbol{\tau}(k)\right] \end{cases}, \quad (2)$$

where $\Psi[\cdot]$ and $\Theta[\cdot]$ is a nonlinear functions, which kind depends on a used model construction method, $\mathbf{\upsilon}(k)$ and $\mathbf{\tau}(k)$ are vectors of simulating noises and errors, $\Delta\mathbf{x}(k)=\tilde{\mathbf{x}}(k)-\hat{\mathbf{x}}(k)$, $\hat{\mathbf{x}}(k)$ is a rating value of a states vector of diagnosed object, $\Delta\mathbf{y}(k)=\tilde{\mathbf{y}}(k)-\hat{\mathbf{y}}(k)$, $\Delta\lambda_i(k)=\tilde{\lambda}_i(k)-\hat{\lambda}_i(k)$.

It is necessary to note, that on the each of the above-stated stages its own DM type is used, it reflects only given task features. DM data are connected with one another in hierarchy system, in which at the top level there are DM, used for fault location, at the middle level there are DM, used for fault places search, and at last, third level are DM, suitable for the each fault class determination task solving.

A matter of principle at development of diagnostic maintenance is the creation of diagnosis conditions. The diagnosed and recovered object properties depend either on its structure, or on states caused by external controlling and disturbance actions, therefore it is expedient to analyze both structural and signal ACS properties using appropriate constructive criteria.
The initial data for development of automatic control system diagnosing models and tools are the diagnosed object research results, namely: diagnostic models hierarchy, requirements to the depth of diagnosing, to the time of diagnosing, to the reliability of the diagnosis, set of initial signals and requirements to character of input signals. The results of the basic tasks solving should be submitted in the form of computer-oriented algorithms, and the whole ACS diagnosis process - as treelike product knowledge base. In nodes of the tree the appropriate attributes are placed representing two-place predicate equations on the set of measurable discrete system signals values arrays:

$$\mu_j = S_2\left[\Delta\mathbf{y}(k), \mathbf{V}_\lambda(k), \sigma_j\right], \qquad (3)$$

where $\mathbf{V}_\lambda(k)$ is a sensitivity function of diagnostic parameter λ_i, σ_j is a threshold ratio within the sign of predicate $S_2[\cdot]$.

Such equations are solved on the appropriate arrays of discrete values using of certain factor of trust reducing influence of the destabilizing factors (as is measurement noises, signal noises, simulating errors) on quality of the decision. As a result of predicate equation solving the value 0 or 1 is taken, determining a direction of the further tree passing. The tree ends with the leafs which correspond to possible states and given ACS faults types.
Solving diagnosis tasks and consistently removing uncertainty, concerned with the occurrence time, occurrence place and size of the fault the characteristics of fault type are established. The recovery could be carried out so that to reduce to a minimum the consequences of fault type occurrence. The initial data for development of ACS recovery tools are the results of diagnosed object research, namely: the diagnosis, types of available resources, characteristics of resources, principle of action, requirements to recovery time, transient processes nature, recovery model. The basic result of this stage is the effective recovery resource definition task solving as optimizing task of a multi-criterion choice. For private criteria formation it is offered to use major (for the given task) properties of the considered system, such as recovery quality by the given resource, recovery time using the given resource, ability of additional using the given resource. Then, taking into account the rigid requirements to recovery time expenses, and also assuming, that worse emergency hasn't been held yet, it is possible to generate criteria of optimization (Gavrilenko, 2003):

$$\begin{cases} K_1(R_i) \to \max\limits_{\psi} \; R_i(\psi_i, t_i, \tau_i);\; i=\overline{1,3}; \\ K_2(R_i) \to \min\limits_{t} \; R_i(\psi_i, t_i, \tau_i);\; i=\overline{1,3}; \\ K_3(R_i) \to \max\limits_{\tau} \; R_i(\psi_i, t_i, \tau_i);\; i=\overline{1,3}, \end{cases} \qquad (4)$$

where ψ_i – ACS recovery quality by the *i* resource; t_i – recovery time by the *i* resource; τ_i - possibility of additional use *i* resource, R - decision determined on allowable set of the decisions {R}, K = {K_1, K_2, K_3} - set of private criteria.
The private criteria allow to range allowable alternatives only on the set of the subordinated decisions, when criterion consistent, otherwise there is a task of the "best" compromise decision choice:

$$R^o = \arg\max_{R\in\{R\}}\left[\sum_{i=1}^{n} p_i \cdot K_i(R_i)\right],\; i=\overline{1,n}., \qquad (5)$$

where $P=\{p_1,p_2,p_3\}$ - relative importance of private criteria.

The weight factors quantitative meanings of private criteria importance p_i are determined by the developer originating from the requirements of the task and a considered class systems operation experience. It is necessary to take into account, that the resources have a final opportunity of additional use. Therefore, parameter τ dynamically changes during use of resources.

The set of possible models factors meanings of recovery is determined by stability areas construction in a plane of appropriate factor and direct attribute of fault. Thus, that part of D-splitting curve is considered only which is responsible for stability range. The consideration fault tolerant ACS as systems with delay, allows to determine admitted temporary resource of diagnosing and recovery.

For a quantitative estimation of a fault tolerance level relatively to a direct attribute of a fault type the constructive criterion based on fault tolerant graph model ACS is used (Gavrilenko, 2003; Kulik, and Gavrilenko,2004). Such model is represented as oriented graph G: where predicates displaying hierarchy of diagnosing and recovery tasks correspond to graph node G_I, and the arches G_{IJ} have the weights, appropriate to their situation: t1 - time of search of fault type place, t2 - time of a fault type class determination, t3 - time of fault type determination, t4 - time of a recovery resource choice, t5 - time of recovery by the given type of a resource.

3 PRACTICAL APPLICATION

The developed adaptive approach to active fault tolerance ACS maintenance was used for solving of such practical task as diagnostic support for the spacecraft stabilization system. For fault tolerance maintenance in the given example the intellectual microprocessor system realizing developed algorithm was used.

Let's consider in more detail realization of the developed adaptive approach.

Among firsts the research bench of the seminatural modeling of diagnostic maintains was created, its structure includes block of the momentum wheels, microcontroller system and personal computer, where the mathematical model of the spacecraft is realized (fig. 2). The developed diagnostic maintenance allows to determine 6 fault classes and 9 fault places.

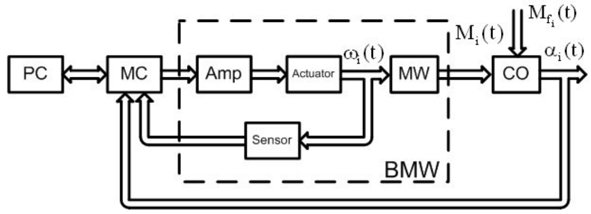

Fig.2. Functional diagram of the bench

As a result of the solution of the primal diagnosing problems of the spacecraft stabilization system generated the dichotomizing tree, showed in fig. 3.

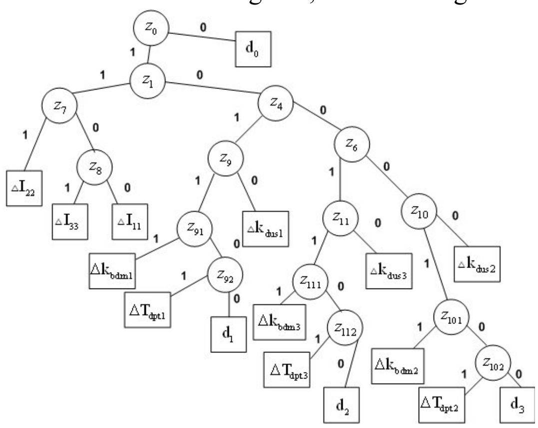

Fig. 3. Dichotomizing tree of the system diagnosing.

With the help of indications predicate equations (6, 7) and the dichotomizing tree formatted the algorithmic modules, permitting to compute the corresponding characteristics of faults and establishing of the fault classes in the spacecraft stabilization system. The influence 12 unitary faults types in various system elements were investigated. The diagnostic maintenance allows to determine the fault place and class in every fault case (fig. 4).

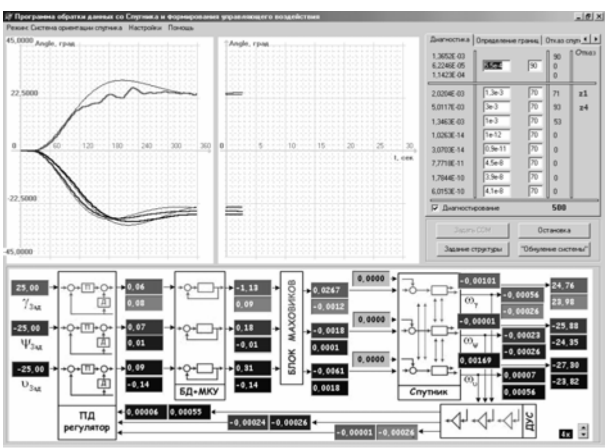

Fig. 4. The diagnostic maintain window.

$$z_0 = S_2[(\left|\Delta \mathbf{U}_{avs}(s^*)\right| - \delta) \cup (\left|\Delta \mathbf{M}_{bdm}(s^*)\right| - \delta)];$$

$$z_1 = S_2[\left|\Delta U_{avs1}(s^*)\right| - \delta];$$

$$z_4 = S_2[\left|\Delta M_{bdm1}(s^*)\right| - \delta];$$

$$z_5 = S_2[\left|\Delta M_{bdm2}(s^*)\right| - \delta];$$

$$z_6 = S_2[\left|\Delta M_{bdm3}(s^*)\right| - \delta];$$

$$z_7 = S_2[\delta - \left|\begin{matrix}\Delta U_{avs2}(s_1^*)\cdot\varphi_{I_{22}}(s_2^*) - \\ -\Delta U_{avs2}(s_2^*)\cdot\varphi_{I_{22}}(s_1^*)\end{matrix}\right|];$$

$$z_8 = S_2[\delta - \left|\begin{matrix}\Delta U_{avs3}(s_1^*)\cdot\varphi_{I_{33}}(s_2^*) - \\ -\Delta U_{avs3}(s_2^*)\cdot\varphi_{I_{33}}(s_1^*)\end{matrix}\right|];$$

$$z_9 = S_2[\delta - \left|\begin{matrix}\Delta M_{bdm1}(s_1^*)\cdot\varphi_{k_{bdm1}}(s_2^*) - \\ -\Delta M_{bdm1}(s_2^*)\cdot\varphi_{k_{bdm1}}(s_1^*)\end{matrix}\right|];$$

$$z_{10} = S_2[\delta - \left|\begin{matrix}\Delta M_{bdm2}(s_1^*)\cdot\varphi_{k_{bdm2}}(s_2^*) - \\ -\Delta M_{bdm2}(s_2^*)\cdot\varphi_{k_{bdm2}}(s_1^*)\end{matrix}\right|];$$

$$z_{11} = S_2[\delta - \left|\begin{matrix}\Delta M_{bdm3}(s_1^*)\cdot\varphi_{k_{bdm3}}(s_2^*) - \\ -\Delta M_{bdm3}(s_2^*)\cdot\varphi_{k_{bdm3}}(s_1^*)\end{matrix}\right|]. \qquad (6)$$

$$z_{91} = z_{101} = z_{111} = S_2\left[\delta - \left|\Delta\hat{\alpha}_1(k)\right|\right];$$
$$z_{92} = z_{102} = z_{112} = S_2\left[\delta - \left|\Delta\hat{\alpha}_2(k)\right|\right]. \qquad (7)$$

The fault location in the considered system is determined after 10 seconds. Then begin to work the algorithm of the place searching. The fault place is determined after 50 seconds and the fault class – after 55 seconds.

The results of researches have proved expediency and constructability of the offered approach. The functioning quality analysis of the developed fault tolerant systems testifies to their higher efficiency in comparison with traditional ones.

REFERENCES:

Demirci U., Kerestecioglu K. (2003) Fault Tolerant Reconfiguring Sliding Mode Controller. In: *Proc. Eleco 03 Conference,* Bursa, pp.279-283.

Gavrilenko O. I. (2003) Active fault tolerance support of statically unstable dynamic objects. Master's thesis. Kharkiv Aviation Institute. Kharkiv. Ukraine.

Jiang J., Zhao Q. (1998) Fault tolerant control systems synthesis using imprecise fault identification and reconfigurable control. In: *IEEE ISIC/CIRA/ISAS Joint Conference.* Gaithersburg (USA). pp. 169-174.

Kulik A. S. (1994) Control Systems Fault Tolerant Ensuring by means of Fault Diagnosis and Counteracting. In: *Proc. IFAC Symposium SAFEPROCESS 94.* Espo (Finland). **Vol.1**. pp. 157 - 162.

Kulik A. S., Gavrilenko O. I. (2002) Maintenance of the fault tolerance of control systems of statically unstable dynamic objects. In: *Successes of modern radio electronics*. Moscow. №2. pp 52-75.

Kulik A. (2000) *Signal-parametric diagnosing of control systems.* Byseness Inform, KhAI, Kharkov (Ukraine).

Patton R.J. (1997) Fault tolerant control: the 1997 situation. In: *IFAC SAFEPROCESS ' 97.* Hull (U.K.). pp. 1033-1055.