DOI: http://doi.org/10.25728/cs.2023.5.7

COMPONENT MONITORING TO MANAGE THE REDUNDANCY OF AN ONBOARD EQUIPMENT COMPLEX

V.N. Bukov[1], A.M. Bronnikov[2], A.V. Vorob'ev[1], A.S. Popov[3], and V.A. Shurman[4]

[1] Institute of Aircraft Equipment, Zhukovsky, Russia
[2] Bauman Moscow State Technical University, Moscow, Russia
[3] Zhukovsky–Gagarin Air Force Academy, Voronezh, Russia
[4] Ramenskoe Instrument-Making Design Bureau, Zhukovsky Branch, Zhukovsky, Russia

✉ v_bukov@mail.ru, ✉ bronnikov_a_m@mail.ru, ✉ vorobiev@niiao.ru, ✉ saga30@yandex.ru, ✉ vshurman@rpkb.ru

Abstract. This paper considers the technical condition monitoring problem for the components of an onboard equipment complex to perform its real-time reconfiguration. The idea is to use at least three levels of monitoring systems: the nearest perspective, only traditional built-in control (BiC) to detect faults; the next level, BiC together with auxiliary means to increase the fidelity of technical diagnosis, including mutual cross-pair monitoring; the distant perspective, logical processing algorithms for system observations as a whole based on the normalized rules of failure mode and effects analysis (FMEA) of aircraft equipment. Mathematically, the pair monitoring of component conditions consists in forming the so-called preference matrices; their values and special tables are used to determine the condition of diagnosed objects with high reliability and, moreover, to evaluate possible errors of diagnostic tools. For third-level methods, an action sequence is proposed as follows: the reverse and direct logical models reproducing the dependencies of faulty states based on FMEA results are alternatively initiated. An updated methodology for handling triplex logical models is proposed. The main advantages of logical models—significant simplicity and universality—ensure their effectiveness in a wide range of dynamic systems of varying complexity. A methodological example illustrates the application of logical triplex models.

Keywords: onboard equipment complex, technical monitoring, logical pair monitoring, logical triplex models, analysis of functional failures, redundancy management.

INTRODUCTION

The creation of redundant reconfigurable onboard equipment complexes (OECs) for mobile objects is a non-alternative way to achieve the maximum possible reliability of these complexes under the limited reliability of the components used and a wide range of external factors. According to the paper [1], the concept of Active Fault-Tolerant Control Systems (AFTCS) implies the joint operation of at least three subsystems as follows. The first subsystem is the reconfigurable or adaptable part of the equipment (Reconfigurable Control System, RCS; in our case, the equipment of the complex); the second subsystem detects (monitors) and diagnoses faults of this complex (Fault Detection and Diagnosis, FDD); the third subsystem implements the so-called Reconfiguration Mechanism (RM).

Reconfigurability means that an OEC has the properties to purposefully change its parametric and structural characteristics in real time.

By definition, redundancy management is assigned to the second and third subsystems mentioned above.

Historically, research works on monitoring, diagnosis, and reconfiguration of technical systems have been isolated from each other. On the one hand, the known solutions in the field of monitoring and diagnosis [2–9] are not related to the subsequent use of their results in real time. On the other hand, the reconfiguration approaches proposed in [10–14] proceed from monitoring results as a given. This situation has obvi-

ous disadvantages since the following questions remain open: What is the actual necessity of real-time diagnosis? What are the mutual requirements of diagnosis and reconfiguration? How can their interaction be systematically analyzed?

Nevertheless, separate solutions of monitoring, diagnosis, and reconfiguration problems have been prevailing in the scientific literature and practice so far.

This paper is devoted to the technical condition (operability) monitoring problem for the components of a reconfigurable complex within the redundancy management approach based on the supervisory configuration control method [15]. Here, we consider a broader problem statement: the readiness monitoring of an OEC, which covers (along with operability) the completion of all real-time preparations of OEC components for the intended use.

1. THE FUNCTIONS AND GENERATIONS OF MONITORING MEANS

In the emerging applied theory of redundancy management [15], monitoring means have to determine, for each available (hardware or software) component, its availability index (AI) and functional efficiency (FEI) for use in periodic arbitration of configurations.

By assumption, monitoring is performed in three main steps as follows:

- data acquisition from components (either by sending special requests or intercepting data translation implemented by components independently);
- data processing, including initial mathematical treatment, if they come from several sources and belong to one component, and preparation of the results (generation of AI and FEI) for transmission;
- transfer of the results (AI and FEI) to the redundancy management level by supervisor requests or by translation over a shared local area network.

As the theory and applications evolve [15], different monitoring methods in terms of principles and algorithms can be used; they form three main levels summarized in Table 1.

The first monitoring level is basic and involves only the existing built-in control (BiC) or new means created by component developers. The effect is to ensure equipment control in accordance with industry regulations determining the depth and quality of control procedures [16, 17].

Along with the existing BiC, the second level involves effective algorithmic solutions with mutual control of redundant components having BiC, e.g., logical pair monitoring (LPM) procedures [18]. The corresponding implementation is possible in onboard automated control systems (OACSs) and onboard maintenance systems (OMSs) [17].

In the case of heterogeneous[1] objects and their BiCs, it is possible to assess the operability of the functional part of the components and BiC with maximum reliability.

The third level involves more complex (most importantly, independent of BiC) algorithms and monitoring strategies based on the analysis of processes in the "object + OEC" system using various concepts and models, including state forecasting. In particular, the matter concerns logical models based on the so-called directed triplex graphs [19].

Table 1

Development of monitoring methods for redundant OECs

No.	Level	Means	Toolkit	Effect
1	Basic	Traditional BiC	Autonomous monitoring	Ensuring equipment control in accordance with industry regulations
2	Next-generation	Integration with OACSs, use of LPM	Integration into the architecture of existing (currently developed) OACSs (OMSs)	More comprehensive and complementary equipment control based on various engineering and algorithmic solutions
3	Next-generation	Independent monitoring algorithms	Application of more sophisticated monitoring algorithms and strategies (logical models, state forecasting)	The qualitatively new level and high fidelity of control, multiple fault detection and diagnosis

[1] Nodes of the same purpose are created by different developers and (or) are based on different engineering solutions.

2. MONITORING BASED ON BUILT-IN CONTROL

BiC is a set of hardware or software components introduced into systems, their parts, or functional assemblies (FAs). As a rule, they do not participate in the work of functional modules (FMs) of the system or its FAs on purpose but collect and summarize various data that objectively reflect the operability of these modules in the developer's opinion.

There are two significantly different organizational approaches to the operation of BiC:

– test control of equipment operability, which requires a temporary "withdrawal" of the controlled object from its intended-purpose operation;

– functional control, which is performed during the intended-purpose operation of the controlled object.

Functional control is generally implemented based on two main principles as follows:

• *Use of different voting schemes.* Here, a common solution is the so-called quorum elements (QEs), which identify faulty modules by the processing of voting results of several connected FMs. The operability of an FM is judged by a significant deviation of its output from those of same-type modules (the largest deviation or that exceeding a given threshold) [20].

The main features of the quorum-based method include:

– the assumption that the technical state of an FM remains unchanged within each cycle;

– the assumption that a QE is operable (never fails);

– applicability to three or more FMs (in the case of two FMs, a pair of FMs becomes the controlled object, not each FM separately);

– the assumption that within the voting rules (equal, weighted, with discriminations, etc.), the operable FMs within each cycle dominate over the faulty ones and the latter can be disconnected;

– a common data flow for all FMs.

A peculiar form of voting is widely implemented in the so-called self-checking systems [9]: a set of same-type modules subjected to identical input actions is divided into pairs, and the outputs within each pair are compared with each other. A pair with matching outputs is considered to be operable; otherwise, both modules of the pair are considered to be inoperable.

• *Use of fidelity rules.* Depending on particular conditions and solutions, such rules can be as follows: comparing with reference models, detecting violations of given time and (or) parametric intervals (control by parameter tolerance [20]), checking logical and other relations, calculating different-order invariants, etc.

The main features of the method of fidelity rules include the following:

– Within each cycle, the operability of an FM does not change.

– By assumption, an element implementing fidelity rules is operable. (If there is a reference model, it is operable.)

– This method is applicable to any number of FMs.

– By assumption, the input and output data contain sufficient information.

– Each FM has a separate data flow.

The technical condition of computing units in the OEC central computing system is monitored by combining the methods described above.

In accordance with the ARINC 653 standard, a health monitor is a system function responsible for monitoring and reporting errors in the operation of hardware means, application software, and the operating system. The information about the technical condition of the computer during normal operation is finally collected by operating system kernel mechanisms and (or) a special section of system software.

The resulting information of the health monitor is transmitted to the OMS and communication channels with ground facilities or is processed by the operating system. This information is generated from the following input data:

• the results of built-in control tests, which check equipment operability in the background mode during specially allocated time intervals;

• the output data of event handlers; an event is a "special case" detected by hardware means when executing functional applications, usually a programming error detected or a protocol violation during data reception in the input channels of an external interface;

• the information of functional applications about errors and incorrect input or output data.

The recent direction [21] stands somewhat apart. It can be called FM monitoring based on operational data. By assumption, a special element (chip) is structurally and functionally connected directly to an FM to gather and accumulate data on the conditions of its use and storage. Such a chip stores different parameters (FM data) and sends them to the monitoring module, in particular:

– passport information,

– test results at different stages of the life cycle,

– statistics of operation indicators and characteristics (estimates of the achieved accuracy, remaining life, energy indicators, etc.),

– statistics of external impacts during intended use, storage, and routine maintenance.

The monitoring module is responsible for analyzing the incoming data and judging about FM operability based on the analysis results.

Thus, we summarize the common features (limitations) of BiC with different degrees of occurrence:

– weak[2] assumptions about the unchanged operability of the controlled devices within the monitoring cycle;

– strong[3] assumptions about the operability of control systems or their major devices;

– the requirement on a minimum admissible or large number of FMs (in the case of quorum or majority control);

– the requirement that operable FMs dominate over inoperable FMs;

– the fast disconnection of faulty FMs;

– the requirement on sufficient informativeness for all processes in FMs.

The main advantage of using BiC (in the current form) to monitor the components of a redundant OEC is the well-established technologies of their creation and application in practice.

Analytical monitoring and diagnosis methods [5–7] are being intensively developed. They further refine the concept of fidelity rules and are based on theoretical patterns and peculiarities in the operation of dynamic systems.

3. USE OF LOGICAL PAIR MONITORING

A common drawback of using BiC is the forced trust in these diagnosis means, i.e., the a priori assumption of their infallibility [22–24]. According to the studies [15], without considering the inevitable limited capabilities of control (monitoring) means, factual fault tolerance can be significantly inferior to expectations.

One remedy is logical pair monitoring (LPM) procedures [18]: both autonomous monitoring and mutual cross-monitoring are performed for two FMs of the same functional purpose. By assumption, all structurally isolated functional assemblies "FM + BiC," comparable in purpose and operation principles, are designed so that the BiC of each assembly can access the FM of any other assembly[4] (Fig. 1).

This figure has the following notations: τ is the current time (monitoring cycle number); v_τ is input data; y_τ is output data; p_τ is controlled parameters (possibly, they include v_τ and y_τ); s_τ^{i-j} is the operability assessment of the i th FM (FMi) generated by the j th BiC (BiCj). Binary operability assessments (1—"operable" and 0—"inoperable") form an indicator matrix (IM).

Monitoring is performed under several assumptions:

- Same-type data flows through different FAs are not connected with each other (the functional autonomy of FAs).
- Each functional node "FM + BiC" is implemented on a technological base and supported by infrastructural means independently of the base and means of other FAs (the technical heterogeneity of FAs).
- FMs may be independently operable or inoperable (the independence of FM operability).
- Only one element in a pair of BiC can have a simple error, i.e., a false assessment of "operable" or "inoperable" (the error-free operation of at least one BiC).
- The monitoring process is divided into cycles within which FM operability and the errors of BiC are unchanged (the stationary operability of FAs).

Under these assumptions, the full group of different IM values makes up 13 matrices uniquely related to the operable or inoperable state of both FAs; for details, see [18]. In accordance with the LPM indicator rule [18] (Table 2 below), each IM value unambiguously determines the technical condition of both each FM and each BiC. The only exception is the IM value

$$S_\tau^{\text{ind}} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

which describes the operability of both FMs or the inoperability of one BiC in the form of a false assessment of "operable." But this ambiguity does not concern FM operability; in the part of BiC, it can be considered by design solutions.

Also, the publication [25] presented a more complicated version of LPM with the possible presence of the so-called gray zone. This zone appears when some part of BiC participating in monitoring cannot be separated from the FM in terms of data passage. In this case, to implement LPM, BiC has to be dissected along the boundary between the grey zone and the analytical segment. As a result, the indicator rule is modified and, generally, the efficiency of monitoring is reduced: the operability of the grey zone becomes indistinguishable from that of the FM, and error identification refers to the analytical segment only.

[2] This assumption is not crucial in practice.

[3] This assumption significantly narrows the applicability of the approach.

[4] The complete adoption of such an idea may cause significant difficulties. As a compromise solution, limited access may be implemented at the developer's discretion.

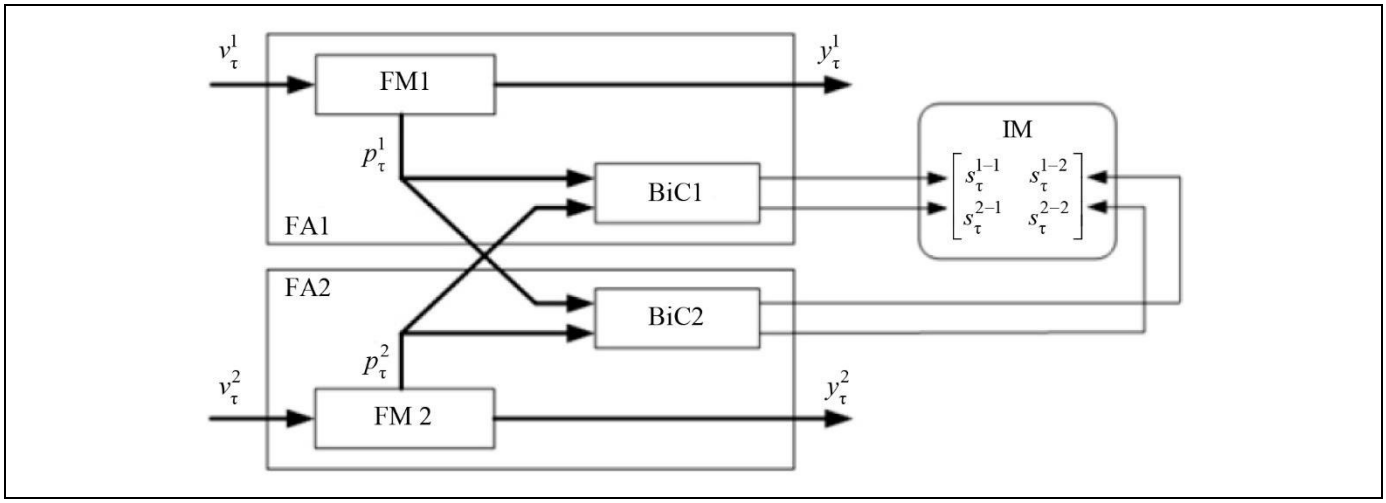

Fig. 1. The schematic diagram of functional assemblies for LPM.

Table 2

IM values obtained by LPM

Inoperable FM	Errors in BiC				
	Errors in BiC1		Errors in BiC2		No errors
	False "1"	False "0"	False "1"	False "0"	
Inoperable FM1	$\begin{bmatrix}1&0\\1&1\end{bmatrix}$	$\begin{bmatrix}0&0\\0&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}0&0\\1&0\end{bmatrix}$	$\begin{bmatrix}0&0\\1&1\end{bmatrix}$
Inoperable FM2	$\begin{bmatrix}1&1\\1&0\end{bmatrix}$	$\begin{bmatrix}0&1\\0&0\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\end{bmatrix}$	$\begin{bmatrix}1&0\\0&0\end{bmatrix}$	$\begin{bmatrix}1&1\\0&0\end{bmatrix}$
Both operable	–	$\begin{bmatrix}0&1\\0&1\end{bmatrix}$	–	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$

4. DIRECT AND REVERSE LOGICAL MODELS

The publications [20, 26] introduced a logical models-based approach to operability control of technical systems. When applied to the monitoring of components in a complex with managed redundancy, this approach is as follows.

According to [27], the OEC designer performs failure mode and effects analysis (FMEA) of aircraft equipment. Such failures include completely terminated operation, loss of capability to meet the requirements, intermittent operation, unnecessary operation, etc. The assessment results are a list of typical equipment failures causing functional faults, including the description of their relationships and consequences. In most cases, failure consequences are divided into local (i.e., characteristic of the component itself), those of the next higher level, and those at the highest level (the entire system, e.g., an aircraft). It is necessary to identify failure consequences at the highest level for comparing the criticality of failures of all components included in the OEC. Usually, FMEA results are presented in the form of tables of possible failures and their consequences.

FMEA may be not comprehensive, i.e., may be performed partially considering the criticality of failures of different parts of the systems.

This approach implies passing from descriptive (qualitative) FMEA results to the construction of two types of formalized logical failure propagation models for the object of diagnosis with triplex variables: 0—"no failure or its impact," 1—"failure or its impact exists," and &—"indefinite state."

The original methodology of building and using triplex models was described in [20, 26]. It has a low level of formalization (a system of decision rules), which creates difficulties in practice. Below we propose a deeper approach largely devoid of this drawback.

The idea is to model failure impact propagation (from causes to manifestations) in an OEC using a logical network containing generalized elements with

the following logical operators: ORi (an analog of disjunction) or ANDi (an analog of conjunction) at the input and ORo or ANDo at the output; see Fig. 2. In this case, the element's state x_{id} is given by the values of triplex variables at its inputs, x_{in}^{j}, in accordance with causal relation formulas: $x_{in}^{1} + x_{in}^{2} \to x_{id}$ for the ORi operator or $x_{in}^{1} \times x_{in}^{2} \to x_{id}$ for the ANDi operator. It also determines the value of such variables at the outputs: $x_{id} \to x_{out}^{1} + x_{out}^{2}$ for the ORo operator or $x_{id} \to x_{out}^{1} \times x_{out}^{2}$ for the ANDo operator.

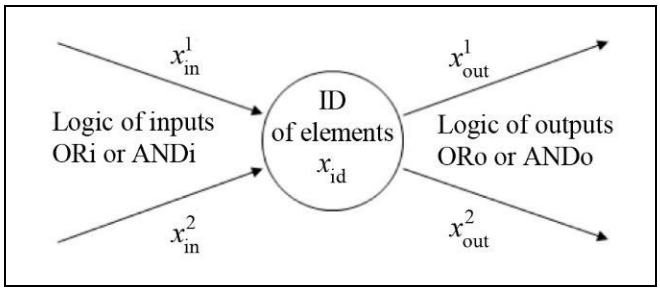

Fig. 2. An element of the logical network (failure impact propagation models for OEC).

The ORo operator must be provided with a description of output switching conditions (by an external impact, by definite characteristics of the logical network state, etc.).

Note an important aspect: when constructing the logical network by the artificial division of the models of real devices, each network element must be assigned at most one input and at most one output operator.

Note that the arithmetic of such triplex variables is not conventional, and each causal transition between the elements of the proposed logical network (the direct logical model) is performed according to the rules summarized in Table 3. The additional symbol ∇, also called an operator, denotes the absence of an alternative.

For example, the formulas in cells 1-2 (row 1, column 2) and 1-4 of Table 3 should be interpreted as follows: the presence of at least one signal $x_{in}^{j} = 1$ (failure impact) at the inputs of a logical network element with the ORi logic brings this element to the state $x_{id} = 1$ (it is prone to failure impact). This corresponds to failure state evolution in non-redundant functional devices of the OEC. The cells of row 2, on the other hand, are associated with the ANDi logic, characteristic of redundant devices.

The cells highlighted in yellow in Table 3 describe the propagation of the indefiniteness & over the triplex logical network. The remaining cells reflect the unambiguous development of the situation: the propagation (1) or non-propagation (0) of failure impact.

The process of analyzing system failures is associated with the reverse logic that determines transitions from failure manifestations to their causes. The corresponding transitions (the reverse logical model, the left "effect-to-cause" arrows) $x_{in}^{1} + x_{in}^{2} \leftarrow x_{id}$, $x_{in}^{1} \times x_{in}^{2} \leftarrow x_{id}$, and $x_{id} \leftarrow x_{out}^{1} \times x_{out}^{2}$ are presented in Table 4. For example, the formula in cell 2-1 of this table is interpreted as follows: the state $x_{id} = 1$ of an element with the ANDi operator was a consequence of the simultaneous presence of 1 at its inputs.

Reverse logic is used to judge about the input given a known output. For operators at the input, it is required to determine possible combinations at the input of a logical network element by its state; for operators at the output, it is required to determine the state of a logical network element by the combination at the output.

Table 3

Direct logic arithmetic

Operators and row numbers		Column numbers and formulas								
		1	2	3	4	5	6	7	8	9
ORi	1	1 + 1 → 1	1 + 0 → 1	1 + & → 1	0 + 1 → 1	0 + 0 → 0	0 + & → &	& + 1 → 1	& + 0 → &	& + & → &
ANDi	2	1 × 1 → 1	1 × 0 → 0	1 × & → &	0 × 1 → 0	0 × 0 → 0	0 × & → 0	& × 1 → &	& × 0 → 0	& × & → &
ORo	3	-	1 → 1 + 0	-	1 → 0 + 1	0 → 0 + 0	& → 0 + &	-	& → & + 0	-
ANDo	4	1 → 1 × 1			0 → 0 × 0			& → & × &		
∇	5	1 → 1			0 → 0			& → &		

Table 4

Reverse logic arithmetic

Operators and row numbers		Column numbers and formulas		
		1	2	3
rORi	1	0 + 0 ← 0	(1 + 1 ← 1 or 1 + 0 ← 1 or 0 + 1 ← 1 or)* 1 + & ← 1 or & + 1 ← 1	0 + & ← & or & + 0 ← & or & + & ← &
rAN Di	2	1 × 1 ← 1	(0 × 0 ← 0 or 1 × 0 ← 0 or 0 × 1 ← 0 or)* 0 × & ← 0 or & × 0 ← 0	1 × & ← & or & × 1 ← & or & × & ← &
rORo	3	0 ← 0 + 0	1 ← 1 + 1 or 1 ← 1 + 0 or 1 ← 0 + 1 or 1 ← 1 + & or 1 ← & + 1	& ← 0 + & or & ← & + 0 or & ← & + &
rAN Do	4	1 ← 1 × 1	0 ← 1 × 0 or 0 ← 0 × 1 or 0 ← 0 × 0 or 0 ← & × 0 or 0 ← 0 × &	& ← 1 × & or & ← & × 1 or & ← & × &
∇	5	1 ← 1	0 ← 0	& ← &

* If "indefinite" is conceptually identified with "any," then the formulas in brackets should be ignored.

The formulas in Table 4 can be justified using the following explanations for row 4:

a) If a combination of 1 and 1 is detected at the outputs of a logical network element (both are prone to failure impact), then due to the logic of the AND operator, this element is prone to failure impact.

b) If a combination of 1 and 0 is detected at the outputs of a logical network element (one output is prone to failure impact, whereas the other is not), then this element is resistive to failure impact, and the failure has occurred in the chain of elements following the output with a value of 1.

c) If a combination of 0 and 1 is detected, then the result is the same as in item *b*).

d) If a combination of 0 and 0 is detected, then the element is resistive to failure impact.

e) If a combination of & and 0 is detected, then the element is resistive to failure impact for any value of & (see item *a*) or *c*)).

f) If a combination of 0 and & is detected, then the result is the same as in item *e*).

g) If a combination of & and & is detected, then the element has the indefinite state.

h) If a combination of & and 1 is detected, then the element has the indefinite state since the element is resistive to failure impact for & = 0 (by item *b*)) but is prone to failure impact for & = 1 (by item *f*)).

i) If a combination of 1 and & is detected, then the result is the same as in item *h*).

In Table 4, the cells generating ambiguity are highlighted in yellow; it is therefore required to analyze in parallel each of the possible variants. For example, according to the formulas in cell 1-2 (analysis of rORi, i.e., the ORi operator in the reverse direction), the state $x_{\text{id}} = 1$ may be a consequence of signal indefiniteness at any input, even though the other input may be resistive to failure impact. Bold boxes indicate cells with different combinations of output signals corresponding to the same element state. For example, according to cell 3-2, an element with the ORo operator is prone to failure impact if any of its outputs has this property.

The formulas of Tables 3 and 4 can be obviously extended to the cases of three or more inputs and outputs.

5. FORMULAS OF TRIPLEX MODELS

The direct analysis of the logical network is to model cycle-to-cycle failure impact propagation among elements. The corresponding relations of state dynamics and output have the form

$$X_{k+1} = \text{DM} \vec{\Diamond} X_k + X_{\text{init}},\ Y_k = \text{EM} \times X_k,\quad k = 1, 2, ..., \tag{1}$$

with the following notations: X_k is the n-dimensional vector of OEC component failures at calculation cycle k with values 1, 0, or &, assigned to each logical network element; X_{init} is the initial state of the vector X_k; DM is the direct dependency matrix, filled with unities and empty elements[5] $\odot$ according to FMEA results; EM is the exit matrix, which highlights the elements of the OEC model with directly observed failures (is filled with zeros and unities); Y_k is the m-

[5] Not a zero value (no failure), but an indication of being eliminated from consideration.

dimensional output vector of directly observed failures (or their absence). Here, the signs $\times$ and $+$ indicate the extended conjunction and disjunction, respectively (Table 3); the sign $\vec{\Diamond}$ means their simultaneous use according to the special methodology described in Section 6. The first formula in (1) is not algebraic in the conventional sense.

To explain the expression (1), we consider an illustrative example with five elements. The state of one element is directly observed. Figure 3 shows the graph of the corresponding logical network.

The graph of this example is described by the following relations (1):

$$\underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}_{k+1}}_{X_{k+1}} = \underbrace{\begin{array}{c} \\ \vee \\ \text{ANDi} \\ = \text{ORi} \\ \vee \\ \vee \\ \text{ANDo} \end{array} \begin{bmatrix} \odot & \odot & \odot & 1 & \odot \\ 1 & \odot & \odot & 1 & \odot \\ 1 & 1 & \odot & \odot & \odot \\ \odot & \odot & 1 & \odot & \odot \\ 1 & \odot & \odot & \odot & \odot \end{bmatrix}}_{\text{DM}} \begin{array}{c} \\ \\ \\ \vec{\Diamond} \\ \\ \\ \\ \vee \end{array} \vee \quad \vee \quad \text{ORo} \quad \vee$$

$$\vec{\Diamond} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}_k + \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}_{\text{HO}}, \qquad (2)$$

$$\underbrace{[y]_k}_{Y_k} = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix}}_{\text{EM}} \times \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}_k}_{X_k},$$

in DM, the corresponding input operators are given to the left of the rows, and the corresponding output operators are given under the columns; in addition, x_i denotes the states of logical network elements with values 1, 0, or &.

The cyclic use of formulas (1) (in the illustrative example, formulas (2)) for $k = 0, 1, 2, \ldots$ allows modeling the cycle-to-cycle impact propagation of the initial failure X_{init} over all logical network elements.

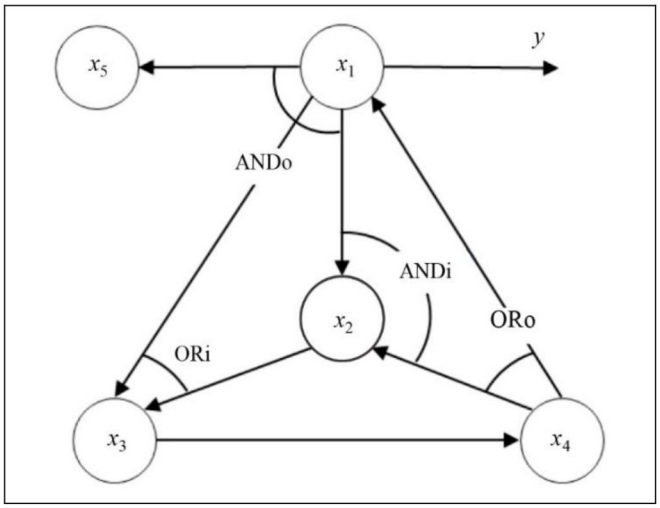

Fig. 3. An illustrative example of a logical network.

The reverse analysis is to find the root cause of failures by their manifestations. The corresponding iterative formulas for the initial and subsequent assessments have the general form

$$\hat{X}_0 = \text{EM}^{\text{T}} \times Y_k + \overline{\text{EM}}^{\text{R}} \times \mu(\&),$$

$$\hat{X}_{\tau+1} = \text{rDM} \overleftarrow{\Diamond} \hat{X}_\tau + \text{EM}^{\text{T}} \times Y_k, \ \tau = 0, 1, 2, \ldots, \qquad (3)$$

with the following notations: $\hat{X}_\tau$ is the estimated component failure vector at cycle τ with the initial estimate $\hat{X}_0$; $\overline{\text{EM}}^{\text{R}}$ is the matrix right divisor of zero of maximum rank for EM [28]; $\mu(\&)$ is a matrix of compatible dimensions with arbitrary elements, denoted by &. Here, the transposition of the binary matrix EM with linearly independent rows replaces the canonizer (a more complex universal matrix structure [28]), and the sign $\overleftarrow{\Diamond}$ means the reverse analysis operations for failure impact propagation (see the formulas in Table 4), which are performed using the special methodology described in Section 6.

The reversed dependency matrix (rDM) is obtained from DM by applying transposition, replacing the operators ORi $(x_{\text{in}}^1 + x_{\text{in}}^2 \to x_{\text{id}})$, ANDi $(x_{\text{in}}^1 \times x_{\text{in}}^2 \to x_{\text{id}})$, ORo $(x_{\text{id}} \to x_{\text{out}}^1 + x_{\text{out}}^2)$, and ANDo $(x_{\text{id}} \to x_{\text{out}}^1 \times x_{\text{out}}^2)$ by the operators rORi $(x_{\text{in}}^1 + x_{\text{in}}^2 \leftarrow x_{\text{id}})$, rANDi $(x_{\text{in}}^1 \times x_{\text{in}}^2 \leftarrow x_{\text{id}})$, rORo $(x_{\text{id}} \leftarrow x_{\text{out}}^1 + x_{\text{out}}^2)$, and rANDo $(x_{\text{id}} \leftarrow x_{\text{out}}^1 \times x_{\text{out}}^2)$, respectively, and adding 1 to the diagonal position of

each row corresponding to the null row[6] of the combined matrix $\left[\mathrm{DM}^{\mathrm{T}} \quad \mathrm{EM}^{\mathrm{T}}\right]$.

Thus, the direct logical model (2) relates to the reverse logical model (3) of the form

$$\underbrace{\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\\ \hat{x}_4\\ \hat{x}_5\end{bmatrix}_0}_{X_0} = \underbrace{\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix}}_{\mathrm{EM}^{\mathrm{T}}} \times \underbrace{y_k}_{Y_k} + \underbrace{\begin{bmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}}_{\overline{\mathrm{EM}}^{\mathrm{R}}} \times \underbrace{\begin{bmatrix}\&\\\&\\\&\\\&\end{bmatrix}}_{\mu(\&)}, \tag{4}$$

$$\underbrace{\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\\ \hat{x}_4\\ \hat{x}_5\end{bmatrix}_{\tau+1}}_{\dot{X}_{\tau+1}} =$$

$$= \underbrace{\begin{matrix}\mathrm{rANDo}\\ \nabla\\ \nabla\\ \mathrm{rORo}\\ \nabla\end{matrix}\begin{bmatrix}\odot&1&1&\odot&1\\ \odot&\odot&1&\odot&\odot\\ \odot&\odot&\odot&1&\odot\\ 1&1&\odot&\odot&\odot\\ \odot&\odot&\odot&\odot&\mathbf{1}\end{bmatrix}}_{\mathrm{rDM}} \vec{\Diamond} \underbrace{\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\\ \hat{x}_4\\ \hat{x}_5\end{bmatrix}_{\tau}}_{\dot{X}_{\tau}} + \underbrace{\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix}}_{\mathrm{EM}^{\mathrm{T}}} \times y_k, \tag{5}$$

$$\begin{matrix}\nabla & \mathrm{rANDi} & \mathrm{rORi} & \nabla & \nabla\end{matrix}$$

where bold type sets off the diagonal element 1 added by the rDM formation rule.

The peculiarities[7] of handling the matrices DM and rDM are discussed in Section 6.

6. THE METHODOLOGY FOR HANDLING TRIPLEX MODELS

In the direct logical failure impact propagation model (1), the operation $\vec{\Diamond}$ remotely resembles the multiplication of a square matrix by a column matrix on the right. These operations are not identical due to binding different rows and columns of the matrix DM to different input and output logical operators of the logical network and the presence of empty elements (see model (2) in the illustrative example).

Let $\mathrm{DM}_{i.j}$ denote the binary element of the ith row and jth column of the matrix DM. In the direct logical model, the operation $\vec{\Diamond}$ implies the sequential composition[8] of the elements $x_{j.k}$ of the column matrix X_k with the elements $\mathrm{DM}_{i.j}$ for each i. The element $\mathrm{DM}_{i.j} = 1$ corresponds to using the triplex value of the variable $x_{j.k}$ whereas $\mathrm{DM}_{i.j} = \odot$ to ignoring the latter. An operator associated with a row of the matrix DM prescribes the type of formulas from Table 3, combining the elements of this row. An operator associated with a column of the matrix DM prescribes preliminary actions with the triplex variable as follows: the operators ∇ and ANDo prescribe no actions; the operator ORo prescribes introducing the distinction of the variables $x_{j.k}$ used in this column according to the switching conditions in the logical network. These compositions of each row are combined according to the operators indicated for the rows of DM.

For example, the first formula in (2) is equivalent to

$$\begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{bmatrix}_{k+1}$$

$$\begin{matrix}\nabla\\ \mathrm{ANDi}\\ =\ \mathrm{ORi}\\ \nabla\\ \nabla\end{matrix}\begin{bmatrix}\odot&\odot&\odot&x_4(\mathrm{ORo})&\odot\\ x_1&\odot&\odot&x_4(\mathrm{ORo})&\odot\\ x_1&x_2&\odot&\odot&\odot\\ \odot&\odot&x_3&\odot&\odot\\ x_1&\odot&\odot&\odot&\odot\end{bmatrix}_k$$

$$+\begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{bmatrix}_{\mathrm{init}} = \begin{bmatrix}x_{4.k}(\mathrm{ORo}) + x_{1.\mathrm{init}}\\ x_{1.k} \times x_{4.k}(\mathrm{ORo}) + x_{2.\mathrm{init}}\\ x_{1.k} + x_{2.k} + x_{3.\mathrm{init}}\\ x_{3.k} + x_{4.\mathrm{init}}\\ x_{1.k} + x_{5.\mathrm{init}}\end{bmatrix}. \tag{6}$$

[6] A null row contains empty and zero elements only.

[7] They express the novelty of the methodology presented.

[8] This term is used here in the universal sense for extended conjunctions and disjunctions.

Here, the notation $x_{4.k}(\mathrm{ORo})$ refers to cycle k and is interpreted as follows: according to the switching rule at the output of element 4 (Fig. 3), the current value $x_{4.k}$ is considered in either the first $(x_{1,k+1})$ or second $(x_{2,k+1})$ row of (6) only. The alternative to the value $x_{4.k}$ is 0.

With $x_{1.k} = \&$, $x_{2.\mathrm{init}} = 1$, and $x_{4.k} = 1$, the row for $x_{2.k+1}$ gives

$$\text{for } x_4 \xrightarrow{\mathrm{ORo}} x_1,\ x_{2.k+1} = \underbrace{\underbrace{(\& \times \mathbf{0})}_{0\ (3/2\text{-}6)} + 1}_{1\ (3/1\text{-}4)} = 1;$$

$$\text{for } x_4 \xrightarrow{\mathrm{ORo}} x_2,\ x_{2.k+1} = \underbrace{\underbrace{(\& \times \mathbf{1})}_{\&\ (3/2\text{-}7)} + 1}_{1\ (3/1\text{-}7)} = 1.$$

Hereinafter, the subscripts in brackets indicate the cell address: table/row-column.

In the reverse logical failure cause analysis model (3), the operation $\overleftarrow{\Diamond}$ is interpreted as follows. Sequential composition is performed for the elements $\hat{x}_{j.\tau}$ of the column matrix $\hat{X}_\tau$ with the elements $\mathrm{rDM}_{i.j}$ for each i. The element $\mathrm{rDM}_{i.j} = 1$ corresponds to using the triplex value of the variable $\hat{x}_{j.\tau}$ whereas $\mathrm{rDM}_{i.j} = \odot$ to ignoring the latter (but according to other rules). An operator associated with a column of the matrix rDM prescribes the type of formulas from Table 4. An operator associated with a row of the matrix DM prescribes combining the elements of this row and preliminary actions with the triplex variable as follows: the operators ∇ and rANDo prescribe no actions; the operator rORo prescribes introducing the distinction of the variables $x_{j.\tau}$ used in this column according to the switching conditions in the logical network.

The actions with rDM are explained by the following generalized notation, valid for any element rDM_{ij}:

$$\begin{aligned}\left[\hat{x}_i\right]_{\tau+1} &= \mathrm{rOPo}\left[\ldots 1_{ij} \ldots\right] \overleftarrow{\Diamond} \left[\hat{x}_j\right]_\tau + \ldots \\ &= \Big[\ldots \underset{\mathrm{rOPi}}{\mathrm{rOPo}} \quad (?\,\underset{\mathrm{rOPi}}{?} \leftarrow \hat{x}_{j.\tau})_{\text{table 4}} \quad \mathrm{rOPo} \ldots\Big] + \ldots,\end{aligned} \tag{7}$$

where rOPi outside square brackets denotes the operators rORi, rANDi, and ∇ at the input of the element, and rOPo outside square brackets denotes the operators rORo, rANDo, and ∇ at the output of the element. Inside square brackets, these notations represent the corresponding operations: + (in the case of OR), × (in the case of AND), or no operations (in the case of ∇). Question marks indicate the values 1, 0, or & read from Table 4 for particular rOPi and $\hat{x}_j$.

For example, the expression (8) is equivalent to formula (5). Here, the notations $x_{1.\tau}(\mathrm{rORo})$ and $x_{2.\tau}(\mathrm{rORo})$ are interpreted as follows: according to the switching rule at the output of element 4 (Fig. 3), either the value $\left(\hat{x}_{1,\tau}\right)$ or the value $(\hat{x}_{2,\tau})$ is used in the line for $\hat{x}_{4.\tau+1}$. The alternative is the value 0.

The ambiguities in formula (8) are resolved by harmonizing the logical formulas or require additional investigation of the variants.

$$\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\\ \hat{x}_4\\ \hat{x}_5\end{bmatrix}_{\tau+1} = \begin{bmatrix} \odot & \times & ?\times ? \leftarrow \hat{x}_{2.\tau} & \times & ?+ ? \leftarrow \hat{x}_{3.\tau} & \times & \odot & \times & \hat{x}_{5.\tau} \\ \odot & & \odot & & ?+ ? \leftarrow \hat{x}_{3.\tau} & & \odot & & \odot \\ \odot & & \odot & & \odot & & \hat{x}_{4.\tau} & & \odot \\ \hat{x}_{1.\tau}(\mathrm{rORo}) & + & ?\times ? \leftarrow \hat{x}_{2.\tau}(\mathrm{rORo}) & + & \odot & + & \odot & + & \odot \\ \odot & & \odot & & \odot & & \odot & & \hat{x}_{5.\tau} \end{bmatrix} + \begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix} \times y_k . \tag{8}$$

With $\hat{x}_{2.\tau} = 1$, $\hat{x}_{3.\tau} = 0$, and $y_k = 1$, the row for $\hat{x}_{1.\tau+1}$ gives

$$\hat{x}_{1.\tau+1} = \underbrace{\underbrace{\underbrace{1}_{1\,(4/2-1)} \times 1 \leftarrow \underbrace{1}_{}}_{} \times \underbrace{\underbrace{0}_{0\,(4/1-1)} + 0 \leftarrow \underbrace{0}_{}}_{0\,(4/4-2)}}_{1\,(4/3-2)} + 1 = 1,$$

which agrees with the direct analysis of the graph in Fig. 3.

7. THE GENERAL LOGIC OF USING TRIPLEX MODELS

The failures of OEC components during their operation are diagnosed as follows. The proposed approach is based on the assumption that any technical system (the object of diagnosis) contains three groups of parts.

The first group includes various OEC components (hardware and software) whose failures are significant (critical) and are covered by FMEA.

Communication channels can be either physical (wired or wireless communication between components) or virtual (routed digital communication).

The third group includes OEC components to identify (observe) the correctness or incorrectness of OEC operation directly. As a rule, the final effects of functional failures are manifested in such components.

The three groups of components are characterized in Table 5.

The proposed approach is to use the direct and reverse logical models alternately and repeatedly. It has the following features:

Table 5

The capabilities and features of logical models

Characterization		The group of system parts		
		System components where failures may occur	Links between components (the propagation channels of failure impacts)	The locations of failure manifestations (the devices whose behavior can be observed to detect the occurrence of failures)
Features regarding the occurrence and manifestation of failures		Failures can be in any of the components analyzed.	The links can be arbitrary within known structures.	The locations of failure manifestations, as well as the forms of these manifestations, are precisely known.
The capabilities of logical models	Direct logical model	As a rule, the locations of expected failures (the vector X_k) are unknown and are given approximately.	The links must be determined precisely.	The locations of failure manifestations are calculated, but they possibly differ from the really observed ones due to erroneous specification of failure locations. Therefore, the modeling process is repeatedly initiated with varying the expected failures. The accuracy criterion of failure specification is the coincidence of the calculated and measured output vectors Y_k.
	Reverse logical model	Failure locations are determined from calculation results, but there is no confidence due to model ambiguities.	The links are determined by the logical reversion of the direct model.	The locations of failure manifestations are specified according to the observation results.

• Due to its exceptional simplicity, the logical failure impact propagation model in the form of a logical network yields computationally simple algorithms even for very complex OEC architectures.

• Model building is based on FMEA, a well-mastered methodology for the aircraft industry with acceptable depth and breadth of coverage for the operation conditions of OECs.

• The operability of components is described using triplex variables to reduce the number of variants under analysis when executing the algorithms.

• The models are alternated to proceed with the following steps.

Step 0. The initial failure vector estimate $\hat{X}_{\tau=0}$ is determined by formula (3) from the known output vector Y_0 (the vector of directly observed failures). The estimate $\hat{X}_{\tau=0}$ contains the components of the vector Y_0 in the form of 0 and 1; the other components are indefinite.

Step 1. The reverse logical model is used from the locations of failure manifestations $\hat{X}_{\tau=0}$ to expected failures to divide the components $\hat{X}_{\tau=1,\,2,\ldots}$ into definitely operable (0), definitely inoperable (1), and indefinite (&). The indefinite states either pass through the branches of the reverse logical model unchanged or change to definite states. The number τ of cycles implemented must be sufficient to reach a "stationary point," i.e., the invariable vector $\hat{X}_{\tau}$.

Step 2. The direct logical model is used from the expected failures $\hat{X}_{k=0} = \hat{X}_{\tau}$ to the corresponding estimates $\hat{Y}_{k=1,2,\ldots} = \mathrm{EM} \times \hat{X}_{k=1,2,\ldots}$ of their manifestations to confirm the adequacy of these estimates or to refine the indefinite states. The number *k* of cycles implemented must be sufficient to reach a "stationary point," i.e., the invariable vector $\hat{X}_{k=1,2,\ldots}$.

Steps 1 and 2 are alternated until stabilizing the estimate $\hat{X}_{k=1,2,\ldots}$.

The problem of calculating the estimate $\hat{X}_{k=1,2,\ldots}$ from the vector Y_0 has no analytical solution so far. Hence, it can be obtained by numerical iterative methods only. Various computational algorithms, rational and effective to a greater or lesser extent, can be applied here. One possible algorithm was presented in [19].

8. A METHODICAL EXAMPLE

In [29], the failures in helicopter altitude and speed parameters were detected using the algorithm [19]. The paper [30] considered the problem of detecting failures in a redundant electrohydraulic actuator. Due to the voluminous nature of applications and the limited scope of the presentation, we will demonstrate the approach of this paper on a simplified example.

Consider a partially redundant OEC fragment (Fig. 4). Here, drive 1 is controlled by computing units 1 and 2 (the drive becomes inoperable in the case of failures of both units); drives 2 and 3 are controlled by computing unit 2; power unit 1 feeds computing units 1 and 2; power unit 2 feeds drives 1 and 2; finally, power unit 3 feeds drive 3. For the sake of a compact problem statement, neither power supply buses nor digital and analog communication lines are considered. The directly observable data are the drive failures, which are assessed by the current positions of the rods relative to the set positions within a given tolerance.

We introduce the following notations of the states: x_1 (drive 1), x_2 (drive 2), x_3 (drive 3), x_4 (computing unit 1), x_5 (computing unit 2), x_6 (power unit 1), x_7 (power unit 2), and x_8 (power unit 3). The output vector consists of $y_1 = x_1$, $y_2 = x_2$, and $y_3 = x_3$. Drive 1 is conventionally divided into two elements x_1 and x_9 to distinguish the operators ORi and ANDi that formalize failure impact at its input $((x_4 \times x_5) + x_7)$.

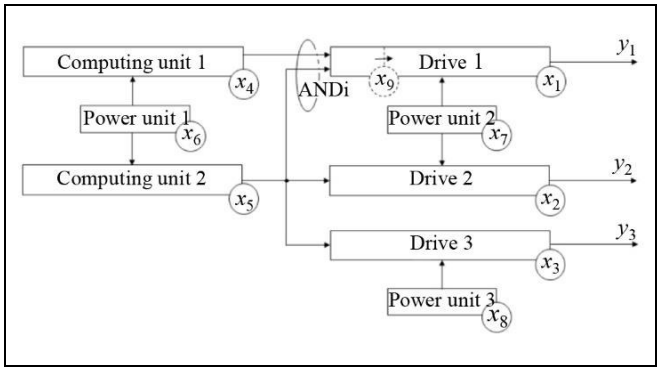

Fig. 4. The functional diagram of the OEC fragment.

The diagram in Fig. 4 is described by the direct logical model (2) of the form

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix}_{k+1} = \underbrace{\begin{matrix} \text{ORi} \\ \text{ORi} \\ \text{ORi} \\ \nabla \\ \nabla \\ \nabla \\ \nabla \\ \nabla \\ \text{ANDi} \end{matrix} \begin{bmatrix} \odot & \odot & \odot & \odot & \odot & \odot & 1 & \odot & 1 \\ \odot & \odot & \odot & \odot & 1 & \odot & 1 & \odot & \odot \\ \odot & \odot & \odot & \odot & 1 & \odot & \odot & 1 & \odot \\ \odot & \odot & \odot & \odot & \odot & 1 & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & 1 & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & 1 & 1 & \odot & \odot & \odot & \odot \end{bmatrix}}_{\text{DM}} \vec{\Diamond} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix}_k + \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix}_{\text{init}}, \quad (9)$$

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}_k = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{\text{EM}} \times \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 \end{bmatrix}_k^{\text{T}} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}_k. \quad (10)$$

The corresponding reverse model (3) is

$$\underbrace{\begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \\ \hat{x}_4 \\ \hat{x}_5 \\ \hat{x}_6 \\ \hat{x}_7 \\ \hat{x}_8 \\ \hat{x}_9 \end{bmatrix}_0}_{X_0} = \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{\text{EM}^{\text{T}}} \times \underbrace{\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}}_{Y_k} + \underbrace{\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}}_{\overline{\text{EM}}^{\text{R}}} \times \underbrace{\begin{bmatrix} \& \\ \& \\ \& \\ \& \\ \& \\ \& \end{bmatrix}}_{\mu(\&)} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \& \\ \& \\ \& \\ \& \\ \& \\ \& \end{bmatrix}, \quad (11)$$

$$\begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \\ \hat{x}_4 \\ \hat{x}_5 \\ \hat{x}_6 \\ \hat{x}_7 \\ \hat{x}_8 \\ \hat{x}_9 \end{bmatrix}_{\tau+1} = \underbrace{\begin{matrix} \nabla \\ \nabla \\ \nabla \\ \nabla \\ \text{rANDo} \\ \text{rANDo} \\ \text{rANDo} \\ \nabla \\ \nabla \end{matrix} \begin{bmatrix} \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & 1 \\ \odot & 1 & 1 & \odot & \odot & \odot & \odot & \odot & 1 \\ \odot & \odot & \odot & 1 & 1 & \odot & \odot & \odot & \odot \\ 1 & 1 & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & 1 & \odot & \odot & \odot & \odot & \odot & \odot \\ 1 & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \end{bmatrix}}_{\text{rDM}} \vec{\Diamond} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \\ \hat{x}_4 \\ \hat{x}_5 \\ \hat{x}_6 \\ \hat{x}_7 \\ \hat{x}_8 \\ \hat{x}_9 \end{bmatrix}_{\tau} + \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{\text{EM}^{\text{T}}} \times \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}. \quad (12)$$

Consider the failure of power unit 3 ($x_{8.0}=1$), starting from the direct failure propagation model (9), (10). The corresponding calculations can be performed by the reader independently. At the first step, we obtain $x_{3.1}=1$. At all subsequent steps, $x_{3.k}=1$ and $x_{8.k}=1$. The output vector becomes

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}_k = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \qquad (13)$$

i.e., the failure manifests itself as a malfunction of drive 3.

Now we localize the failure using triplex models.

Step 0. We calculate the initial estimate $\hat{X}_0$ of the failure vector by formula (11):

$$\hat{X}_0 = [0 \;\; 0 \;\; 1 \;\; \& \;\; \& \;\; \& \;\; \& \;\; \& \;\; \&]^{\mathrm{T}}. \qquad (14)$$

According to this estimate, the first and second elements of the logical network (drives 1 and 2) are resistive to failure impact whereas the third element (drive 3) is prone to it (the location of the failure remains unclear), which does not contradict the problem condition. The other elements of the logical network (from the fourth to the ninth) have the indefinite state.

Step 1. We substitute the vector (14) into formula (12). For τ = 0 (see the note to Table 4), the first cycle results in

$$\begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \\ \hat{x}_4 \\ \hat{x}_5 \\ \hat{x}_6 \\ \hat{x}_7 \\ \hat{x}_8 \\ \hat{x}_9 \end{bmatrix}_1 = \underbrace{\begin{matrix} \nabla \\ \nabla \\ \nabla \\ \nabla \\ =\text{rANDo} \\ \text{rANDo} \\ \text{rANDo} \\ \nabla \\ \nabla \end{matrix} \begin{bmatrix} \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & 1 \\ \odot & 1 & 1 & \odot & \odot & \odot & \odot & \odot & 1 \\ \odot & \odot & \odot & 1 & 1 & \odot & \odot & \odot & \odot \\ 1 & 1 & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & 1 & \odot & \odot & \odot & \odot & \odot & \odot \\ 1 & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \end{bmatrix}}_{\text{rDM}} \overset{\leftarrow}{\Diamond} \begin{bmatrix} 0 \\ 0 \\ 1 \\ \& \\ \& \\ \& \\ \& \\ \& \\ \& \end{bmatrix}_0 + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{matrix} \text{rORi} & \text{rORi} & \text{rORi} & \nabla & \nabla & \nabla & \nabla & \nabla & \text{rANDi} \end{matrix}$$

$$\begin{matrix} \nabla \\ \nabla \\ \nabla \\ \nabla \\ =\text{rANDo} \\ \text{rANDo} \\ \text{rANDo} \\ \nabla \\ \nabla \end{matrix} \begin{bmatrix} \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \&\times\&\leftarrow\& \\ \odot & 0+0\leftarrow 0 & \frac{1+\&\leftarrow 1}{\&+1\leftarrow 1} & \odot & \odot & \odot & \odot & \odot & \&\times\&\leftarrow\& \\ \odot & \odot & \odot & \& & \& & \odot & \odot & \odot & \odot \\ 0+0\leftarrow 0 & 0+0\leftarrow 0 & \odot & \odot & \odot & \odot & \odot & \odot & \odot \\ \odot & \odot & \frac{\&+1\leftarrow 1}{1+\&\leftarrow 1} & \odot & \odot & \odot & \odot & \odot & \odot \\ 0+0\leftarrow 0 & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot \end{bmatrix}_0 + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

In the scalar notations, using Table 4 (table/row-column), we obtain

$$\hat{x}_1 = 0,$$

$$\hat{x}_2 = 0,$$

$$\hat{x}_3 = 1,$$

$$\hat{x}_4 = \underbrace{\mathbf{\&}\times\&_5 \leftarrow \&}_{\&\ (4/2\text{-}3)} = \&,$$

$$\hat{x}_5 = \underbrace{\underbrace{(\mathbf{0}+0_7\leftarrow 0)}_{0\ (4/1\text{-}1)} \times \underbrace{(\frac{\mathbf{1}+\&_8\leftarrow 1}{\mathbf{\&}+1_8\leftarrow 1})}_{1\text{ или }\&\ (4/1\text{-}2)}}_{0(4/4\text{-}2)} \times \underbrace{(\&_4\times\mathbf{\&}\leftarrow\&)}_{\&\ (4/1\text{-}3)} = 0,$$

$$\hat{x}_6 = \underbrace{\& \times \&}_{\&\ (4/4\text{-}3)} = \&,$$

$$\hat{x}_7 = \underbrace{\underbrace{(\mathbf{0}+0_9\leftarrow 0)}_{0\text{ или }\&\ (4/2\text{-}2)} \times \underbrace{(0_5+\mathbf{0}\leftarrow 0)}_{\&\text{ или }0\ (4/2\text{-}2)}}_{0\ (4/4\text{-}2)} = 0,$$

$$\hat{x}_8 = \underbrace{\frac{\mathbf{1}+\&_9\leftarrow 1}{\mathbf{\&}+1_9\leftarrow 1}}_{(4/1\text{-}2)} = 1 \text{ или } \&,$$

$$\hat{x}_9 = \underbrace{0_7+\mathbf{0}\leftarrow 0}_{0\ (4/1\text{-}1)},$$

Here, the possible variants for $\hat{x}_j$ (Table 4) are shown by the fractional line; the values related to $\hat{x}_j$ are set in bold; the values $\hat{x}_q$ appearing in the formulas of Table 4 jointly with $\hat{x}_j$ are indicated by the subscripts q. Note that in the formula for $\hat{x}_5$, the multiplication of variants according to cell 4-2 in Table 4 is canceled; in the formula for $\hat{x}_8$, it is preserved.

Thus, after the first cycle, the system state has the estimate

$$\begin{bmatrix}\hat{x}_1\\ \hat{x}_2\\ \hat{x}_3\\ \hat{x}_4\\ \hat{x}_5\\ \hat{x}_6\\ \hat{x}_7\\ \hat{x}_8\\ \hat{x}_9\end{bmatrix}_1 = \begin{bmatrix}0\\ 0\\ 1\\ \&\\ 0\\ \&\\ 0\\ 1\text{ or }\&\\ 0\end{bmatrix} \begin{matrix}\text{– no failure,}\\ \text{– no failure,}\\ \text{– failure,}\\ \text{– indefinite state,}\\ \text{– no failure,}\\ \text{– indefinite state,}\\ \text{– no failure,}\\ \text{– indefinite state,}\\ \text{– no failure.}\end{matrix}$$

The estimation procedure can be continued in different directions due to the ambiguous estimate $\hat{x}_{8.1}$. It is possible to analyze each of the options $\hat{x}_{8.1}=1$ and $\hat{x}_{8.1}=\&$, thereby increasing the amount of calculations, or to accept $\hat{x}_{8.1}=\&$. The advantage of each option seems unobvious and needs to be studied in a particular case. Let us select the second option.

Then, after the second cycle of the reverse triplex model, we obtain

$$\hat{X}_2=\begin{bmatrix}0 & 0 & 1 & 0 & 0 & \& & 0 & \& & 0\end{bmatrix}^{\mathrm{T}};$$

after the third cycle, the estimation takes the final form

$$\hat{X}_3=\begin{bmatrix}0 & 0 & 1 & 0 & 0 & 0 & 0 & \& & 0\end{bmatrix}^{\mathrm{T}},$$

remaining invariable at the subsequent cycles.

Step 2. In this result, one component $\hat{x}_8$ has the indefinite value: it can be either 1 (failure) or 0 (no failure). To clarify the situation, we use the direct logical model (9), substituting alternately $\hat{x}_8=1$ and $\hat{x}_8=0$. In the first case,

$$\hat{X}'$$

$$= \begin{array}{c} \\ \text{ORi}\\ \text{ORi}\\ \text{ORi}\\ \nabla\\ \nabla\\ \nabla\\ \nabla\\ \nabla\\ \text{ANDi}\\ \\ \end{array}\!\!\begin{bmatrix}\odot & \odot & \odot & \odot & \odot & \odot & 1 & \odot & 1\\ \odot & \odot & \odot & \odot & 1 & \odot & 1 & \odot & \odot\\ \odot & \odot & \odot & \odot & 1 & \odot & \odot & 1 & \odot\\ \odot & \odot & \odot & \odot & \odot & 1 & \odot & \odot & \odot\\ \odot & \odot & \odot & \odot & \odot & 1 & \odot & \odot & \odot\\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot\\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot\\ \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot & \odot\\ \odot & \odot & \odot & 1 & 1 & \odot & \odot & \odot & \odot\\ \nabla & \nabla & \nabla & \nabla & \text{ANDo} & \text{ANDo} & \text{ANDo} & \nabla & \nabla\end{bmatrix}$$

DM

$$\vec{\Diamond}\begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\1\\0\end{bmatrix}_0 + \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\1\\0\end{bmatrix}_0 = \begin{bmatrix}0\\0\\1\\0\\0\\0\\0\\1\\0\end{bmatrix}.$$

The reader can verify that the second case gives $\hat{X}''=\begin{bmatrix}0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}^{\mathrm{T}}$. In both cases, there is an observation of failure (10), (13), which confirms the possible failures of drive 3 (x_3) and power unit 3 (x_8) in the first case and the possible failure of drive 3 (x_3) in the second case.

This methodical example is simple, and the cause of the failure of drive 3 (x_3) can be established by the reader independently. Two variants are possible here: either drive 3 (x_3) has failed under the indefinite state of power unit 3 (x_8) or power unit 3 (x_8) has failed, causing drive 3 (x_3) to fail as well.

Thus, the modeling result obtained in this example does not contradict the engineering analysis.

CONCLUSIONS

This paper has considered three solutions to monitor the technical condition of components in reconfigurable redundant OECs. The choice of an appropriate variant depends on different factors, including the level of theoretical and applied development, the goals

and capabilities of the OEC developer, the criticality of systems under diagnosis, etc.

The most accessible solution is using BiC in the nearest perspective. The next level implies the supplementary application of logical pair monitoring to increase the reliability of diagnosis results significantly under the inevitable errors of diagnostic means. In the distant perspective, it seems reasonable to add algorithms based on the logical failure impact propagation models of OECs.

The algorithms with logical (triplex) models have several features that make the approach attractive:

- Due to their exceptional simplicity, logical models can be effectively applied even for very complex OEC architectures.
- Model building is based on FMEA, a well-mastered methodology for the aircraft industry with acceptable depth and breadth of coverage for the operation conditions of OECs.
- Triplex models are handled using special constructs similar to matrix ones; appropriate methods and software tools have to be developed.

Further research will focus on the analytical determination of the failure estimate vector to reduce the number of iterations when identifying the operable state of OECs.

Acknowledgments. *The authors are grateful to A.M. Ageev for his invaluable contribution to separate aspects of the proposed approach.*

REFERENCES

1. Zhang, Y. and Jiang, J., Bibliographical Review on Reconfigurable Fault-Tolerant Control Systems, *Proc. the 5th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, Washington, DC, 2003, pp. 265–276.
2. Willsky, A.S., A Survey of Design Methods for Failure Detection in Dynamic Systems, *Automatica*, 1976, no. 12, pp. 601–611.
3. Patton, R.J., Frank, P.M., and Clark, R.N., *Issues of Fault Diagnosis for Dynamic Systems*, London: Springer, 2000.
4. Bukirev, A.S., Savchenko, A.Y., Yatsechko, M.I., and Malyshev, V.A., Diagnostic System for the Technical Condition of the Aircraft Avionics Complex Based on Intelligent Information Technologies, *Modeling, Optimization and Information Technology*, 2020, vol. 8, no. 1(28), pp. 12–24. (In Russian.)
5. *Diagnosis and Fault-tolerant Control. Vol. 1: Data-driven and Model-based Fault Diagnosis Techniques*, coordinated by V. Puig and S. Simani, London: ISTE Ltd; Hoboken: John Wiley & Sons, 2021.
6. *Diagnosis and Fault-tolerant Control. Vol. 2: From Fault Diagnosis to Fault-tolerant Control*, coordinated by V. Puig and S. Simani, London: ISTE Ltd; Hoboken: John Wiley & Sons, 2021.
7. Zhao, R., Yan, R., Chen, Z., et al., Deep Learning and Its Applications to Machine Health Monitoring, *Mechanical Systems and Signal Processing*, 2019, no. 115, pp. 213–237.
8. Parkhomenko, P.P. and Sogomonyan, E.S., *Osnovy tekhnicheskoi diagnostiki* (*optimizatsiya algoritmov diagnostirovaniya, apparatnye sredstva*) (Foundations of Technical Diagnosis (Optimization of Diagnostic Algorithms, Hardware)), Moscow: Energoatomizdat, 1981. (In Russian.)
9. Sapozhnikov, V.V., Sapozhnikov, Vl.V., and Efanov, D.V., Synthesis of a Built-in Control Circuit for Multi-Output Combinational Devices Based on Logical Complement and Signal Compression, *Journal of Instrument Engineering*, 2020, vol. 63, no. 7, pp. 583–599. (In Russian.)
10. Ageev, A.M., Principles of Storing and Monitoring Configuration Information in the Task of On-Board Equipment Complex Redundancy Managing, *Mechatronics, Automation, Control*, 2022, vol. 23, no. 1, pp. 45–55. (In Russian.)
11. Chandler, P.R., Self-repairing Flight Control System Reliability and Maintainability Program Executive Overview, *Proc. IEEE National Aerospace and Electronics Conf.*, Dayton, 1984, pp. 586–590.
12. Nishiyama, T., Suzuki, Sh., Sato, M., and Masui, K., Simple Adaptive Control with PID for MIMO Fault Tolerant Flight Control Design, *AIAA*, 2016, art. no. 0132.
13. Mel'nik, E.V., Methods and Software Tools for Increasing the Reliability of Network Information and Control Systems Based on Computer Resource Reconfiguration, *Doctoral (Eng.) Dissertation*, Taganrog: Research Institute of Multiprocessor Computing Systems, Southern Federal University, 2014. (In Russian.)
14. Zaets, V.F., Abdulin, R.R., Kulabuzov, V.S., et al., RF Patent 2629454 S2, *Byull. Izobret.*, 2017, no. 8.
15. Bukov, V.N., Ageev, A.M., Evgenov, A.V., and Shurman, V.A., *Upravlenie izbytochnost'yu tekhnicheskikh sistem. Supervizornyi sposob upravleniya konfiguratsiyami* (Redundancy Management of Technical Systems. The Supervision Method of Configuration Management), Moscow: INFRA-M, 2023. (In Russian.)
16. *GOST* (State Standard) *R 55255–2012: Air Transport. Maintenance and Repair System for Aircraft Equipment. Organization of Works to Diagnose the Technical Condition of Aircraft Equipment*, Moscow: Standartinform, 2020.
17. Bolelov, E.A., Matyukhin, K.N., Prokhorov, A.V., and Prokof'ev, I.O., *Tekhnicheskie sredstva kontrolya pri ekspluatatsii radioelektronnogo oborudovaniya vozdushnogo transporta* (Technical Means of Control in the Operation of Radio-Electronic Equipment of Air Transport), Moscow: Zhukovsky Academy, 2018. (In Russian.)
18. Bukov, V.N., Ozerov, E.V., and Shurman, V.A., Pair Monitoring of Redundant Technical Systems, *Automation and Remote Control*, 2020, vol. 81, no. 1, pp. 74–93.
19. Bukov, V.N., Bronikov, A.M., and Sel'vesyuk, N.I., An Algorithm to Localize Onboard Complex Failures Based on Mixed Directed Graphs, *Problemy Bezopasnosti Poletov*, 2010, no. 2, pp. 57–71. (In Russian.)
20. *Diagnostirovanie i prognozirovanie tekhnicheskogo sostoyaniya aviatsionnogo oborudovaniya* (Technical Condition Diagnosis and Forecasting for Aircraft Equipment), Sindeev, I.M., Ed., Moscow: Transport, 1984. (In Russian.)
21. Dzhandzhgava, G.I., Dyadischev, A.V., and Garifov, R.Sh., On a Concept for Technical Condition Monitoring of Methods

Used for Analyzing Physical Media, *Ideas and Innovations*, 2018, vol. 6, no. 3, pp. 64–68. (In Russian.)
22. Mozgalevskii, A.V. and Kalyavin, V.P., *Sistemy diagnostirovaniya sudovogo oborudovaniya* (Diagnosis Systems for Shipboard Equipment), Leningrad: Sudostroenie, 1987. (In Russian.)
23. Sokolov, N.L., The Basic Principles of Diagnostics of Serviceability of the Onboard Equipment Automatic (SV) and Development of the Recommendations on Elimination of Not Regular Situations, *Advances in Current Natural Sciences*, 2007, no. 6, pp. 16–20. (In Russian.)
24. Baranovsky, A.M. and Privalov, A.E., Onboard Monitoring and Diagnostic System of Small Space Vehicles, *Journal of Instrument Engineering*, 2009, vol. 52, no. 4, pp. 51–65. (In Russian.)
25. Bukov, V.N., Ozerov, E.V., and Shurman, V.A., Logical Pair Monitoring That Accounts for the Grey Zone, *Automation and Remote Control*, 2020, vol. 81, no. 6, pp. 1037–1050.
26. Bukov V.N., Aver'yanov I.N., Bronnikov A.M., et al., RF Patent 2557441 S2, *Byull. Izobret.*, 2015, no. 7.
27. *GOST* (State Standard) *R 27.606-2013: Reliability in Engineering. Reliability Management. Safety-Oriented Maintenance*, Moscow: Standartinform, 2014.
28. Bukov, V.N., *Vlozhenie sistem. Analiticheskii podkhod k analizu i sintezu matrichnykh sistem* (Nested Systems. An Analytical Approach to the Analysis and Design of Matrix Systems), Kaluga: Bochkareva's Press, 2006. (In Russian.)
29. Bukov, V.N., Bronnikov, A.M., and Sel'vesyuk, N.I., A Failure Propagation Model for the Helicopter Altitude-Velocity Channel, *Problemy Bezopasnosti Poletov*, 2010, no. 10, pp. 39–51. (In Russian.)
30. Bronnikov, A.M. and Morozov, D.V., Troubleshooting of Directly not Observable Failures of Airborne Systems Based on Mixed Directed Graph, *Mekhatronika, Avtomatizatsiya, Upravlenie*, 2013, no. 1, pp. 62–66. (In Russian.)

This paper was recommended for publication by V.G. Lebedev, a member of the Editorial Board.

Received June 11, 2023,
and revised September 24, 2023.
Accepted September 28, 2023.

Author information

Bukov, Valentin Nikolaevich. Dr. Sci. (Eng.), Institute of Aircraft Equipment, Zhukovsky, Russia
✉ v_bukov@mail.ru
ORCID iD: https://orcid.org/0000-0002-5194-8251

Bronnikov, Andrei Mikhailovich. Dr. Sci. (Eng.), Bauman Moscow State Technical University, Moscow, Russia
✉ bronnikov_a_m@mail.ru

Vorob'ev, Aleksandr Vladimirovich. Dr. Sci. (Eng.), Institute of Aircraft Equipment, Zhukovsky, Russia
✉ vorobiev@niiao.ru

Popov, Aleksandr Sergeevich. Cand. Sci. (Eng.), Zhukovsky–Gagarin Air Force Academy, Voronezh, Russia
✉ saga30@yandex.ru

Shurman, Vladimir Aleksandrovich. Ramenskoe Instrument-Making Design Bureau, Zhukovsky Branch, Zhukovsky, Russia
✉ vshurman@rpkb.ru

Cite this paper
Bukov, V.N., Bronnikov, A.M., Vorob'ev, A.V., Popov, A.S., and Shurman, V.A., Component Monitoring to Manage the Redundancy of an Onboard Equipment Complex. *Control Sciences* **5,** 75–91 (2023). http://doi.org/10.25728/cs.2023.5.7

Original Russian Text © Bukov, V.N., Bronnikov, A.M., Vorob'ev, A.V., Popov, A.S., Shurman, V.A., 2023, published in *Problemy Upravleniya*, 2023, no. 5, pp. 91–109.

Translated into English by *Alexander Yu. Mazurov*,
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com