High-level testing of distributed systems based on a link model without loss of information

Gruzlikov A.V.¹, Kolesov N.V.² and Tolmacheva M.V.³

1 Candidate of Technical Sciences, Head of Department, Concern CSRI Elektropribor, Saint Petersburg, Russia
2 Doctor of Technical Sciences, Associate Professor, Chief Researcher, Concern CSRI Elektropribor, Saint Petersburg, Russia
3 Candidate of Technical Sciences, Senior Researcher, Concern CSRI Elektropribor, Saint Petersburg, Russia

E-mail: agruzlikov@yandex.ru

Abstract. A new dynamic model of a distributed real-time computing system is investigated. The model is embedded in the system software and is intended for test diagnostics of violations in addressing exchanges between the system software modules. The questions of observability and controllability of the proposed model are discussed for the case when models of links are used without loss of information.

Introduction
Consideration of diagnostic issues is important in the design of integrated navigation systems (INS), since the quality of their solutions depends on the reliability and fault tolerance of systems. The solutions used in practice are based on the techniques of functional and test diagnostics [1-3]. One of the features of modern INS is real-time operation with the use of distributed information processing. In this paper, the object of high-level diagnostics is an arbitrary distributed real-time computing system, which can be represented as a set of functionally related program modules (PM) assigned on processors and exchanging the necessary information asynchronously. The feature of the proposed approach that distinguishes it from the majority of known approaches is that every program module includes program redundancy, which allows increasing the efficiency of testing and applying the approach not only during debugging but also at the stage of operation of the system for its intended purpose. The introduced program redundancy is actually a system model calculated in parallel with the main program. In this paper, we propose to use the data flow model. From the point of view of the considered class of failures, this diagnostic model can be attributed to discrete event systems [4], when the system operation is described in the language of sequences of certain events. Such models are widely used in the analysis and testing of complex systems.

1. Preliminary Information and Problem Statement
The model synthesis algorithm described in this paper is based on the results of [5], which, unfortunately, are not sufficiently general. We will give them a brief review. This algorithm is valid for any distributed real-time computing systems and consists of two stages.

At the first stage, the structure of the model is created. For this, a set of computational paths is formed based on the well-known algorithms. These paths make up the coverage of the graph directed...
links of data flow. In this context, a computational path is used in reference to a sequence of triggered PMs that connects a certain input with an output. Then, a chain, including as many dynamic links as the number of PMs through which the path passes, is assigned to each path. After the described procedures, the system model is represented as a set of functionally independent chains, and the diagnostic problem can be reduced to the diagnosis of individual chains.

At the second stage of model formation, the type of dynamic links is determined. In this case, the fundamental fact is that the sought dynamic model of the system is further used to construct tests. It is known that the procedure for constructing tests is simplified if the model of the system is, firstly, linear, and, secondly, controllable and observable. Hence, we can formulate a requirement for the links of the chains of the model. They must be linear. In addition, the links should be such that the system model would be controllable and observable.

Diagnostic Tools (DT) generate test data, include it in the system input and examine the test output. In each of the PM, real information words are processed by main algorithms. In parallel with this, test information words are processed by special algorithms that react to events of information transmission and the results of their processing are included as a part of the output data. Since the mechanism for exchanging real and test data in the system is common, it becomes possible, based on the test results obtained during operation, to make a conclusion on the presence or absence of faults in the addressing of data transmission. Note that distortions of real data during the exchange process are not included in the class of faults considered here. Thus, the problem consists in designing algorithms for test processing in the PM, as well as designing the tests in accordance with the content of the algorithms. Only the first problem is considered in the paper. The test data processing algorithm is an event model of the system. In terms of this model, the class of considered violations is defined as all possible distortions of the matrices of this model.

Dynamic description of a chain is obtained in accordance with the following rules. Assume that only one exchange takes place in a system at each instant of time. Then, state vector \( x(t) \) is formed, which is composed of the state vectors of links \( x_i(t) \) included in this model. Matrices \( F(t), G(t), H(t) \) are used to describe the transfer of information between the PM and the DT in each \( j \)-th information exchange. Note that in this paper we consider real-time systems that are characterized by a periodic process of information processing, and, therefore, periodic exchange processes. Therefore, the matrices \( F(t), G(t), H(t) \) will be periodically repeated, and the system model will be periodically non-stationary. In this regard, we associate each sequence of matrices with its own sequence of indices, the set of which is denoted by \( \Gamma = \{ \gamma_s^j | r = 1, L+1 \} \). Their initial segments on an interval with a duration of a period are obtained as a result of a cyclic shift of the sequence of indices \( 1, 2, ..., L+1 \). For \( L = 2 \), we have three sequences of indices: \( \Gamma = \{1, 2, 3; 2, 3, 1; 3, 1, 2\} \). Then

\[
x(t+1) = F(\gamma_s(j))x(t) + G(\gamma_s(j))u(t), \quad y(t) = H(\gamma_s(j))x(t) \quad j = 1, L+1.
\]

These equations describe L-1 exchanges between PMs and two exchanges with DT (receiving and sending test information). The second stage of synthesis of dynamic diagnostic model data flow graph is considered below. At the same time, it is proposed to perform it using dynamic systems as links without loss of information. This makes it easier in some cases than in the General case to find the desired solutions. We introduce the concept of a system without loss of information.

**Definition 1.** A linear dynamical system is called a system without loss of information if the input sequence can be reconstructed based on the results of the analysis of its output sequence.

2. **The Conditions of Observability and Controllability of Chain**

Let us formulate the conditions that the links of the model must satisfy and under which the model of the system will be observable and controllable.

**Statement 1.** A chain composed of observable links without loss of information is observable.
The proof is fairly obvious. Indeed, a chain composed of one link is observable by condition. Let the chain be composed of two links. The second (output) link is observed in the chain by condition. The first link is observable in the chain, since its output sequence, by Definition 1, is determined by the chain output. This reasoning continues by induction.

**Statement 2.** A link \((f, g, h)\) is observable and controllable if the matrix \(f\) is a low row Frobenius form, i.e.

\[
f = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
-\alpha_0 & -\alpha_1 & -\alpha_2 & \ldots & -\alpha_{n-1}
\end{bmatrix},
\]

and also one of the conditions is fulfilled:

\[
h = [h_{00} \ 0 \ \ldots \ 0 \ 0], \quad g = [0 \ 0 \ \ldots \ 0 \ 0 \ g_{m-1,0}]^T, \quad h = g = E,
\]

\[
h = E, \quad g = [0 \ 0 \ \ldots \ 0 \ 0 \ g_{m-1,0}]^T, \quad h = [h_{00} \ 0 \ \ldots \ 0 \ 0].
\]

**Statement 3.** The observable nonsingular link \((f, g, h)\) of dimension \(m\) describing a low row Frobenius form dynamics matrix is a link without loss of information in the following cases:

\[
h = [h_{00} \ 0 \ \ldots \ 0 \ 0], \quad g = [0 \ 0 \ \ldots \ 0 \ 0 \ g_{m-1,0}]^T, \quad h = E, \quad g = E.
\]

**Statement 4.** A chain made up of observable links without loss of information of types 1 and 3 (Statement 3) is observable and controllable.

This statement is quite obvious. Indeed, the observability of the chain is shown in Statement 1. The controllability of the chain in both cases is easy to verify if you go to the dual system. The latter will be a chain of the same type as the original one, since the matrices \(h\) and \(g\) are connected in both cases by a transpose relation. This indicates the observability of dual systems, which, in turn, indicates the controllability of the original systems.

3. **Conclusion**

This paper considers the synthesis of a diagnostic model of a distributed real-time computing system. The system implements parallel asynchronous computations. The model is intended to be used for high-level test diagnosis, when the model is integrated in the system and executed in parallel with the main software. The paper proposes an algorithm for model synthesis that uses links without loss of information. For the resulting models, sufficient conditions for observability and controllability have been formulated.

This work was supported by the Russian Foundation for Basic Research, project no. 19-08-00052.

**References**

[1] Isermann, R., Fault-Diagnosis Applications: Model-Based Condition Monitoring: Actuators, Drives, Machinery, Plants, Sensors, and Fault-Tolerant Systems, Springer Science & Business Media, 2011.
[2] Patton, R.J., Frank P.M., Clark R.N., Eds., Issues of Fault Diagnosis for Dynamic Systems, Springer Science & Business Media, 2013.

[3] Kolesov, N.V., Tolmacheva, M.V., and Yukhta, P.V., Sistemy real’nogo vremeni. Planirovanie, analiz, diagnostirovanie (Real Time Systems. Planning, Analysis, Diagnostics), St. Petersburg: Concern CSRI Elektropribor, 2014.

[4] Cassandras, C.G. and Lafortune, S., Introduction to Discrete Event Systems, Springer Science & Business Media, 2009.

[5] Gruzlikov, A.M. and Kolesov, N.V., Discrete-event diagnostic model for a distributed computational system. Independent chains, Autom Remote Control, 2016, 77, pp. 1805–1817.