The method providing fault-tolerance for information and control systems of the industrial mechatronic objects

E V Melnik, A B Klimenko and V V Korobkin

1 Southern Scientific Center of the Russian Academy of Sciences, 41, Chekhov Str., Rostov-on-Don, 344006, Russia
2 Scientific Research Institute of multiprocessor computing systems, Southern Federal University, 2, gsp-284, Chekhov Str., Taganrog, 347900, Russia

E-mail: anna_klimenko@mail.ru

Abstract. The paper deals with the provision of information and control system fault-tolerance. Nowadays, a huge quantity of industrial mechatronic objects operate within hazardous environments, where the human is not supposed to be. So the question of fault-tolerant information and control system design and development becomes the cornerstone of a large amount of industrial mechatronic objects. Within this paper, a new complex method of providing the reconfigurable systems fault-tolerance is represented. It bases on performance redundancy and decentralized dispatching principles. The key term within the method presented is a ‘configuration’, so the model of the configuration forming problem is represented too, and simulation results are given and discussed briefly.

1. Introduction

Nowadays, industrial mechatronic objects (IMOs) are widespread within such areas as nuclear energy plants, autonomous production, hazardous industry, etc. IMOs are used frequently in industries with hazardous environments where IMOs have to operate without maintenance for a long period of time [1]. So, IMO reliability becomes the cornerstone of an important practical and scientific direction. IMOs in general are considered as systems of sensors, actuators, communication environment, power and a control system. According to this IMO representation, the typologies of IMO faults are made: as an example, figure 1 represents the percentile values of the IMO subsystem impact onto the IMO mission success, while figure 2 contains the typology of IMO failure sources [2].

![Figure 1. The IMO subsystem impact onto the mission success.](image1)

![Figure 2. The IMO failures sources typology.](image2)
As it is shown in Figures 1 and 2, the faults of physical IMO subsystems have a great impact on the system operability. In the scope of this paper, the IMO control systems (more precisely - information and control systems (ICSs)) are under consideration: it is obvious, that the reliability of ICS is one of the most important aspects of the reliable IMO design and development.

Contemporary ICSs are the complexes of computational units, communicational environment and software. The ICS hardware components are developed, verified and tested; there are some prospective methodologies and techniques for very-large-scale integration (VLSI) devices development and verification: for instance, VHDL, Verilog, SystemC. Using appropriate coverage metrics, VLSI is verified, but it is useful to remember that, for example, for most coverage metrics, constrained random verification achieves 80% of coverage rapidly and then asymptotically approaches 100% with test redundancy and time overheads [3]. The slow convergence of random conditions to complete coverage is well known and referred to as the ‘coupon collector problem’ [4]. As the reliability of IMOs is incredibly important, and it is almost impossible to provide full verification coverage, it is necessary to provide additional methods and techniques for the ICS fault-tolerance providing.

The basis of the fault-tolerant reconfigurable IMO systems is the redundancy. Until recently, the structural redundancy was the key method for the fault-tolerance via reconfiguration provision, but contemporary hardware and software allow using another redundancy type – the performance one [5, 6]. Besides performance redundancy, decentralized dispatching methods for the net-centric ICSs were synthesized and used [5, 6], so the main bottleneck of the centralized dispatching was taken away. Within this paper, the method of IMO ICS fault-tolerance provision is represented. The subsequent sections contain a brief review of the performance redundancy concept, the formalization of the configuration forming problem, an algorithmic description of the reconfiguration procedure and some experimental results and discussion.

2. Performance redundancy and decentralized dispatching principles

Structural redundancy is well-known and used widely in different types of ICSs. For instance, almost all modern aircrafts such as Boeing 777 and Airbus A320/330/340 have used triplex- or quadruplex-redundant activation systems, flight control computer and databus systems [7, 8]. Performance redundancy is an alternative way to organize a redundancy in the system: instead of reserve computational units (CUs), there is a performance redundancy within each CU. So, in case of CU fault, monitoring and control tasks can be re-launched on the operational nodes. To minimize the impact of faulted CU onto the system, the fault-tolerance providing method is enriched by the decentralized dispatching principles: every CU is controlled by its own software agent, which is a special type of the monitoring and control task. The problem to be solved by agents is to provide the reconfiguration via the cooperative action.

The basis of fault-tolerance provision presented within this paper is a combination of the performance redundancy and decentralized dispatching.

However, to reconfigure IMO ICS, there must be a set of pre-defined and verified system states described according to the fault-tree analysis – a set of configurations. Within this paper, a term ‘configuration’ means a control and monitoring tasks (CMTs) distribution among the CUs. The configuration forming problem is multiobjective and multiconstraint; the configuration set is designed and verified at the system design stage.

A generalized model of the configuration forming problem is represented in the next section.

3. The model of the configuration forming problem

Let the input data be the following:

- A set of CMTs $G = \{x_i\}, i = 1 \ldots N$, where $x_i$ – the size of task $i$, $N$ – the number of tasks.
• Let \( G = G_c \cup G_{nc} \), \( G_c \cap G_{nc} = \emptyset \), where \( G_c \) – a subset of critical CMTs, \( G_{nc} \) – a subset of non-critical ones. Non-critical CMTs can be stopped or eliminated from the system during reconfiguration. The number of critical CMTs is \( N_c \), the number of non-critical CMTs \( N_{nc} \);

• Let \( G_f \) be the set of CMTs from the faulted CU. \( G_f \subseteq G \), \( G_p \) are the performing tasks, \( G_p \subseteq G \), \( G_p \cap G_f = \emptyset \).

• A planned completion time for set \( G \) is \( T_{plan} \).

• The number of CUs is \( M \) with equal performance \( p \).

Let us take into consideration the fact that we have to allocate the CMTs from set \( G_f \) within the system of operational CUs, on which the tasks from set \( G_p \) are allocated with the constraint of completion time \( T_{plan} \). Let the resource allocated by CU \( j \) for subtask \( i \) be \( \lambda_i^j \). The tasks allocation before the failure is described by matrix \( R \):

\[
R = \begin{bmatrix}
  r_{11} & r_{12} & r_{1M} \\
  \vdots & \vdots & \vdots \\
  r_{N1} & r_{NM}
\end{bmatrix}
\]  

where \( r_i = f(\frac{x_i}{\lambda_i^j}p) \), \( f(\frac{x_i}{\lambda_i^j}p) = \begin{cases} \frac{x_i}{\lambda_i^j}p, & \text{if } x_i \text{ is running on CU } j, \\ 0, & \text{otherwise.} \end{cases} \)

Let the failure occurred on the CU with number \( d \). Column \( d \) of matrix \( R \) is deleted, so there are \( M-1 \) columns and \( N-|G_f| \) lines in new matrix \( R_f \). Renumber the elements of \( R_f \) in the following way, saving the indexes from matrix \( R \) in the upper positions:

\[
R_f = \begin{bmatrix}
  r_{11}^f & r_{12}^f & r_{1(M-1)}^f \\
  \vdots & \vdots & \vdots \\
  r_{N-|G_f|}^f & r_{(N-|G_f|)(M-1)}^f
\end{bmatrix}
\]  

\( R_f \) describes the system state before the reconfiguration and contains the allocation of the operational tasks among the operational CUs. \( R_r \) will be the allocation of task set \( G \) on the \( M-1 \) CUs. Formally, subset \( G_f \) will be added to \( G_p \) with the number of CU \( s = M - 1 \):

\[
R = \begin{bmatrix}
  r_{11}^f & r_{12}^f & r_{1(M-1)}^f \\
  \vdots & \vdots & \vdots \\
  r_{N1}^f & r_{N(M-1)}^f
\end{bmatrix};
\]

\[ r_i^f = f(\frac{x_i}{\lambda_i^j}g(x_i)) \] ;

\[ g(x_i) = \begin{cases} 0, & \text{if } x_i \in G_{nc} \text{ and removed from the system,} \\ 1, & \text{otherwise.} \end{cases} \]  

Let us consider matrix \( \Phi \).

\[
\Phi = \begin{bmatrix}
\varphi(x_{11}^f) & \varphi(x_{12}^f) & \cdots & \varphi(x_{1M}^f)
\end{bmatrix}
\]
where \( \varphi(x^k_j) = \begin{cases} 0, & l = j, \\ \xi, & \text{otherwise} \end{cases} \)

\( k, l \) – the saved indexes of matrix \( R \), \( j \) – the number of CU in matrix \( R_r \), \( \xi \) – the integer number.

Matrix \( \Phi \) describes whether the CMT \( x_i \) was relocated from CU \( l \) to CU \( j \).

The first objective function can be written in the following manner:

\[
F_1 = \sum_{i=1}^{N} \varphi(x^k_j) \rightarrow \text{MIN}.
\]

The maximum number of non-critical tasks running equals the maximum sum of all \( g(x_i) \) in matrix \( R_r \). The next objective function component can be presented as following:

\[
F_2 = - \sum_{i=1}^{N} g(x_i) \rightarrow \text{MIN}.
\]

Herewith, the time constraint must be satisfied:

\[
\forall j: \sum_{i=1}^{N} r_{ij}^* \leq T_{\text{plan}}^i, \ j \in [1..M], \ r_{ij}^* \in R_r.
\]

Then, another criterion must be added to our model – a load-balancing objective function. As it was shown in [5-7], load balancing has a great impact onto the reliability function of CUs and, hence, onto the system reliability. It can be put in the following way:

\[
F_3 = \text{MAX}\left(\sum_{i=1}^{N} \lambda_{id} - \sum_{i=1}^{N} \lambda_{id}' \right) \rightarrow \text{MIN}, \ \forall k, l, \lambda_{id} \in R_r.
\]

With expression (9), the multicriteria configuration forming problem can be written as a one-criteria optimization problem:

\[
F = \sum_{i=1}^{N} \varphi(x^k_j) \rightarrow \text{MIN};
\]

\[
\text{MAX}\left(\sum_{i=1}^{N} \lambda_{id} - \sum_{i=1}^{N} \lambda_{id}' \right) \leq \gamma; \ \sum_{i=1}^{N} g(x_i) \leq \mu; \ \forall j: \sum_{i=1}^{N} r_{ij}^* \leq T_{\text{plan}}^i, \ j \in [1..M];
\]

\( x_i > 0; \ 0 < \lambda_{id} < 1 \), where \( 0 < \gamma < 1 \) is the assumed level of load dispersing, \( \mu \) is the constraint for the eliminated non-critical tasks.

4. The reconfiguration method and the configuration forming problem

The general reconfiguration method on the basis of performance redundancy and decentralized dispatching is described below. Every CU controlling agent gets the configuration tables through the system initialization. Also, we assume that all agents are fully interconnected and sent to the communicational network with a ‘presence’ sign. When the failure occurs, each agent is informed about the fault, and the new appropriate configuration is loaded from the agent’s own configuration storage. If the new configuration is adequate to the system state (all agents are active), control and
monitoring tasks from the faulted node are run on the other nodes according to the configuration due to the performance redundancy.

A set of configurations is a key of a reconfiguring procedure, and has to be designed according to the fault-tree analysis. As it was shown in the previous section, the configuration forming problem is multiobjective, has constraints and, in general, np-hard. So, the forming of the configuration set can take unacceptable periods of time.

In order to reduce this time-consuming procedure, the parallel stochastic search was used, more precisely – asynchronous parallel simulated annealing via parallel multistart. Simulated annealing in general has slow convergency, but some modified methods allow obtaining the solution within the satisfactory time period [9-11]. To solve the configuration forming problem described above, we used a parallel multistart search with a quenching temperature scheme. This kind of modification of SA allows us to obtain the local minimas in the acceptable time period, and the best solution among the local ones is chosen.

5. Simulation results

Within this paper, two types of simulation were made: the first one demonstrates the convergency speed of the SA with the quenching temperature scheme, and the second one contains aggregated results of the parallel SA search procedure.

During the first simulation, a set of 50 monitoring and control tasks with randomized laboriousness was taken. The objective function was minimizing the eliminated non-critical tasks (other objective functions were transformed into constraints). In figure 3, the tracing results of SA are represented: it is seen that the quenching temperature scheme allows us to obtain solutions with a satisfactory quality within 10-20 iterations. Such results make SA the prospective technique in the area of configuration forming.

![Figure 3. Simulation annealing convergency with quenching ratios 0.9, 0.8, 0.7.](image)

![Figure 4. Solution quality for the 2, 5, 10 parallel search procedures.](image)

The next simulation is for the comparison of different numbers of search processes of solution quality: 2, 5 and 10 parallel searches. As shown in figure 4, the best results are obtained by 10 parallel searches on 10 CUs. These results are rather expectable: with the increasing of the initial search points number, the search results become better. With 50 control and monitoring tasks (30 critical, 20 non-critical), the task distribution with 3 eliminated tasks was obtained. It can be just an example of the local optimum, and, possibly, the better solution exists, but this type of solution was accepted by the authors of this paper as satisfactory.
6. Conclusions
A problem of fault-tolerance of IMO information and control systems is one of the contemporary fundamental science problems. Fault-tolerant reconfigurable systems, in general, use the structural redundancy, which can be inconvenient in many aspects: too expensive in development and maintenance, with the deficiency of proper dependability characteristics. Within this paper, the new fault-tolerance providing method based on performance redundancy and decentralized dispatching is presented.

The reconfiguration procedure of IMO ICS needs the set of configurations, which must be designed and verified at the design system stage. The configuration forming problem is non-trivial and time-consuming, so it is expedient to develop fast procedures to obtain the solutions. Parallel simulated annealing with the quenching temperature scheme allows one to obtain solutions of a satisfactory quality within the acceptable time periods, so these search techniques are prospective for the configuration forming.

As a conclusion, we can state that the area of IMO ICS research is developing intensively, so we look forward to the new principles, methods and techniques of IMO ICS fault-tolerance provision.

Acknowledgments
The reported study was funded by SSC RAS projects 0256-2014-0082, 0256-2015-0008 and by RFBR project 16-58-00191 bel-a.

References
[1] Zhang Y and Jiang J 2008 Annu. Rev. Control, 32(2) 229-52
[2] Carlson J, Murphy R 2005 IEEE Trans. Robot. 21(3) 423-37
[3] Jerinic V, Langer J, Heinkel U and Miller D 2006 Des. Aut. Test. Europe 1 1-6
[4] Blom G, Holst L and Sandell D 2004 Probl. and Snapshots from the World of Probab. 191 85
[5] Melnik E, Klimenko A and Korobkin V 2015 Proc. 10th Int. Conf. Application of Information and Communication Technologies (Baku) (New York: IEEE) p 274
[6] Melnik E, Klimenko A and Korovin I 2016 Lecture Notes in Comput. Sci. 9812 9-17
[7] Bartley G 2001 Boeing B-777: fly-by-wire flight controls The Avionics Handbook ed Spitzer C R (Boca Raton: CRC Press)
[8] Biere D, Favre C and Traverse P 2001 Electrical flight controls, from Airbus A320/330/340 to future military transport aircraft: a family of fault-tolerant systems The Avionic Handbook (Boca Raton: CRC Press)
[9] Kirkpatrick S, Gelatt C and Vecchi M 1983 Science 220 (4598) 671-80
[10] Ingber L 1993 Mathl. Comput. Modelling 18 29-57
[11] Azencott R 1992 Simulated Annealing: Parallelization Techniques (New York: John Wiley and Sons)