ACTIVE FAULT PROTECTION IN COMPUTER SYSTEMS
WHERE JOB PROCESSING TIME IS COMPARABLE WITH
INTERARRIVAL TIME

I. B. Shubinskii and N. P. Vasil'ev

Principles of active fault protection in computer systems are presented. The probability of successful adaptation of the system to faulty modules is estimated as a function of information load, time reserve, number of modules, and regularity of the distribution of the relevant random variables in the system.

INTRODUCTION

Structural redundancy is a popular technique for fault tolerance in real-time computing systems. But inherent restrictions of fault checking facilities essentially reduce the effectiveness of redundancy. To achieve the required levels of fault tolerance in modular real-time computing systems, we have developed methods of active protection against faults [1-3].

1. During the active protection interval, a standby module performs parallel processing with all the main modules in prescribed order. This allows external checking of normal operation of all modules, including the standby module, classification of permanent and transient faults, elimination of errors, location of the faulty module, automatic replacement of the faulty module with the standby module, disconnection of the faulty standby module for the duration of its repair or for replacement with a normally operating unit, and finally restart of the computational process from the last check point.

2. The classification of permanent and transient faults and the location of the faulty module require no fewer than \( m = 2 \) main modules and one standby module. With simple organization of active fault protection, the standby module runs in parallel with the first main module in the first active protection interval, and then it runs in parallel with the second main module in the second protection interval (or after an interval). If the results produced by the pair of computing modules in the previous interval do not match, the computation is repeated, which eliminates the effect of a transient fault or establishes that one of the modules is faulty (if the results again do not match). The faulty module is located from the results of parallel processing of the standby module with the second main module. If the results match, then the decision is that the first main module is faulty; if the results do not match, then the decision is that the standby module is faulty.

3. The possibilities of active protection largely depend on the mean length of the protection interval \( \tau \). The value of \( \tau \) should be chosen so that during the time \( T_a^* = T_a - \tau \) the faulty module is located with a given degree of confidence and is replaced with the nonfaulty standby module. Here \( T_a \) is the admissible time during which processing may be interrupted. The time \( \tau \) is the recovery time of the computational process from the last check point with appropriately organized active

Fig. 1. Time diagram of fault checking in a computer system with active protection when the job processing time is comparable with interarrival time: a) the standby module is connected to the assigned main module between job arrivals; b) the standby module is connected to the assigned main module while a job is processing.

Statement of the Problem

We consider a computer system consisting of $m + 1$ identical modules. The $m$ main modules process stationary job streams. The random interarrival times $\vartheta_1$ and the random job processing times $\vartheta_2$ are identically distributed for all modules. Moreover, these random variables are commensurable and small, which avoids the need for providing fault protection intervals inside the processing intervals (in this case, we may take $\tau = \vartheta_2$). The standby module provides one-level active protection in the system (dynamic reconfiguring, fault detection, location of the faulty module, replacement of the faulty module with the standby module, and recovery of the interrupted service). Dynamic reconfiguring either takes the time $\psi_1 + \vartheta_1$ if the standby module is connected to the $(i + 1)$-th main module between arrivals (hypothesis $H_1$) and waits during the random time $\psi_1$ for parallel operation to start (Fig. 1a) or takes the time $\psi_2 + \vartheta_1 + \vartheta_2$ if the standby module is connected while a job is being processed (hypothesis $H_2$) and waits for parallel operation to start during the random time $\psi_2 + \vartheta_1$ (Fig. 1b).

It is required to estimate the ability of the system to adapt to faults in the sense of the criterion of successful adaptation.

Probability of Successful Adaptation of the System to Faulty Modules

This probability is defined as

$$\beta = P\{\nu \leq T_a - t_\beta\},$$

where $\nu$ is the random latency time of a fault.

To solve this problem, we need to find the density function of the random variable $\nu$. To this end, we first determine the density function of the random time $\xi$ from the instant when the free standby module is connected to the next main module to the instant when parallel processing with the standby module ends. We assume that the random times $\vartheta_1$ and $\vartheta_2$ follow Erlang distributions of order $a_1$ and $a_2$ with intensities $\lambda_1$ and $\lambda_2$, respectively. We denote the density functions of these times by $\varphi_i(t)$ ($i = 1, 2$).

According to Fig. 1, the random variable $\xi$ is expressed as

$$\xi = I_{H_1}(\psi_1 + \vartheta_1) + I_{H_2}(\psi_2 + \vartheta_1 + \vartheta_2).$$

Here $I_{H_1}$ ($I_{H_2}$) are the indicators of the hypotheses $H_1$ ($H_2$), which take the value 1 if the hypothesis is true and 0 otherwise. If the process is ergodic, the probabilities of the hypotheses $H_1$ and $H_2$ are calculated from the following relationships:

$$P_{H_1} = \frac{(a_1 + 1)/\lambda_1}{(a_1 + 1)/\lambda_1 + (a_2 + 1)/\lambda_2}, \quad P_{H_2} = 1 - P_{H_1}. $$

509