North-Holland
Microprocessing and Microprogramming 22 (1988) 273–275

On System Diagnosis for Transient Fault Situations

Franc Novak
Institute Jožef Stefan, Edvard Kardelj University, Ljubljana, Jamova 39, 61111 Ljubljana, Yugoslavia.

Sandi Klavžar
Department of Mathematics, Edvard Kardelj University, Ljubljana, Jadranska 19, 61111 Ljubljana, Yugoslavia.

Ludvik Gyergyek
Faculty of Electrical Engineering, Edvard Kardelj University, Ljubljana, Tržaška 25, 61111 Ljubljana, Yugoslavia.

The paper deals with the problem of diagnosability of one-step t-diagnosable systems for transient fault situations. Test invalidation problem is discussed and assumptions corresponding to transient fault situations are stated. Necessary and sufficient condition for one-step t-fault diagnosability of maximum connection assignment is presented.

Keywords: Fault tolerant computing, Fault identification for t-diagnosable systems.

1. Introduction

The problem of fault diagnosis in computer systems has been widely studied in the past twenty years. Several diagnostic models have been proposed, among them the well-known PMC model (proposed by Preparata, Metze and Chien [5]). In the PMC model, a system is abstracted as a set of units that are capable of testing each other. A global observer performs the system diagnosis, based on the result of the outcomes of the tests performed by the system units. The fault-test relation digraph, introduced by the PMC model, has been analyzed in numerous other models, in which a variety of system diagnosability definitions have been stated, due to the different assumptions on system behaviour in the presence of faults. Fault diagnosis in earlier models has been studied primarily for the case where faulty units are assumed to be permanently faulty. Mallela and Masson have extended the analysis to include intermittent faults [3], resulting in a diagnostic model for hybrid fault situations [4].

In this paper, an attempt is made towards the analysis of transient fault situations. Test invalidation due to the transient faults is presented, and the problem of identification of transiently faulty units is analyzed for the case of maximum connection assignment.

An alternative approach to the study of transient fault situations has been suggested dy Dahbura and Masson [2]. Identification of transiently faulty units is accomplished by a so-called greedy diagnosis based on comparison syndromes formed from comparisons of the results of jobs performed by pairs of units. The job-comparison approach is claimed to be more realistic than the conventional complete-test-sets approach, yet an assumption is presumed that when two transiently faulty units perform the same job, the results are necessarily not identical. Test invalidation assumption presented in this paper avoids this restriction.

2. Test Invalidation Assumptions

Diagnostic models presume assumptions on test invalidation in the presence of faulty units corresponding to one of the following two basic categories, depicted in *Fig. 1:*

- symmetric invalidation (proposed by Preparata et al. [5]),
- asymmetric invalidation (proposed by Barsi et al. [1]).

In *Fig. 1* an empty circle denotes a fault-free unit, a filled circle a faulty unit, while an arc from unit u to unit v denotes that u tests v (test result is evaluated by u). The associated weight indicates the test outcome, which is 0 if u evaluates v as fault-free, and 1 if u evaluates v as faulty.

Symmetric and asymmetric invalidation have been originally defined for permanent fault situations. If the test executions and the occurrence of a transient fault do not coincide, a fault is likely to

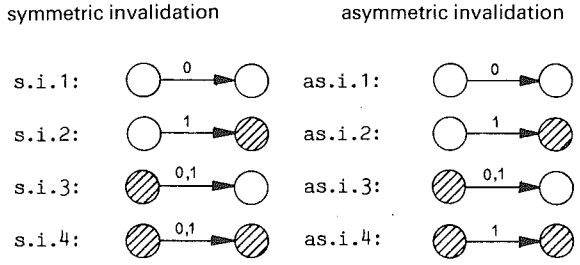

Fig. 1. Symmetric and asymmetric invalidation.

pass undetected. Hence, it may not be realistic to expect the assumption s.i.2 (or as.i.2) to be valid. Moreover, the restriction imposed by as.i.4 cannot be justified in practice for transient faults. Considering the nature of transient faults and the fact that a fault-free unit may fail to detect a transient fault in the tested unit, we get the assumptions for the test invalidation for transient fault situations, as shown in *Fig. 2*.

Apparently the test outcome 0 may result in any of the four possible situations thus disabling the performing of the diagnosis. Our aim is to explore additional conditions under which the identification of transiently faulty units becomes feasible.

3. Identification of Transiently Faulty Units

The problem of identification of transiently faulty units will be studied in terms of one-step t-diagnosability, as defined by Barsi et al. [1]. This definition is equivalent to the one originally proposed by Preparata et al. [5], yet we have chosen the formulation which is closer to the fault detection process presumed in our further discussion.

Definition. A system S is said to be one-step t-diagnosable if one application of tests is sufficient to identify all faulty units in S, provided that the number of faulty units does not exceed t.

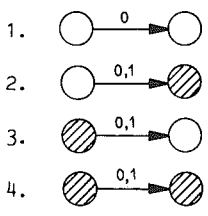

Fig. 2. Test invalidation for transient fault situations.

Consider a system S of n units with a maximum connection assignment (i.e. there exists a testing connection amont all ordered pairs of these n units). Let $\boldsymbol{F} \subseteq \boldsymbol{S}$ denote the set of units with transient faults and $\boldsymbol{T} \subseteq \boldsymbol{S}$ the set of fault-free units, where $\boldsymbol{S}$ is the set of all system units of the system S. For every v from $\boldsymbol{S}$ we introduce a function δ_v in the following way:

$$\delta_v : \boldsymbol{S} - \{v\} \to \{0, 1\}$$

$$\delta_v(w) = \begin{cases} 1, & \text{if } v \text{ identifies } w \text{ as faulty} \\ 0, & \text{otherwise.} \end{cases}$$

For every unit w we introduce its weight:

$$\text{weight}\,(w) = \sum_{v \in \boldsymbol{S} - \{w\}} \delta_v(w)$$

Theorem. Let the number of transiently faulty units in the system S not exceed t, $t + 2 \leqq n$. Then S is one-step t-diagnosable iff weight $(w) > t$ for every w from $\boldsymbol{F}$.

Proof. Assume that S is one-step t-diagnosable. Suppose there exists w from $\boldsymbol{F}$ such that weight $(w) = l \leqq t$, and let $\boldsymbol{F} = \{u_1, u_2, \ldots, u_{l-1}, w\}$. We are going to show that in this case S is not one-step t-diagnosable, by assuming the following possible (worst case) situation. Choose an arbitrary element v from $\boldsymbol{T}$ and assume:

$$\delta_{u_1}(w) = \ldots = \delta_{u_{l-1}}(w) = 1$$

$$\delta_{u_1}(v) = \ldots = \delta_{u_{l-1}}(v) = 1$$

and

$$\delta_v(w) = \delta_w(v) = 1.$$

All other test results are evaluated to be 0. If y is from $\boldsymbol{T} - \{v\}$ then it is obvious that y is not able to distinguish between v and w. Thus, S is not one-step t-diagnosable, proving the necessity part.

For the proof of sufficiency, let v belong to $\boldsymbol{T}$ and w to $\boldsymbol{F}$. We claim that weight $(w) > t \geqslant$ weight (v). The first inequality follows by assumption. Because v belongs to $\boldsymbol{T}$, identity $\delta_u(v) = 1$ is possible only if u is a transiently faulty unit. Since $|\boldsymbol{F}| \leqslant t$ we obtain weight $(v) \leqslant t$. So any y from $\boldsymbol{T} - \{v\}$ is able to distinguish between any v from $\boldsymbol{T}$ and any w from $\boldsymbol{F}$ by computing their weights, which completes the proof.

4. Conclusions

Specific nature of transient faults calls for different test invalidation assumptions than those proposed for permanent faults. The problem of diagnosability of one-step t-diagnosable systems cannot be solved for transient fault situations by merely limiting the maximum number of transiently faulty units. It is shown that even for the maximum connection assignment a transiently faulty unit can be identified only if at least $t + 1$ tests of the unit fail, where t is the maximum number of transiently faulty units in the system.

Acknowledgment

The authors wish to thank the referees for useful advice and suggestions.

References

[1] F. Barsi, F. Grandoni and P. Maestrini: 'A Theory of Diagnosibility of Digital Systems.' *IEEE Trans. on Comput.*, Vol. C-25 (June 1976) pp. 585–593.

[2] A.T. Dahbura, G.M. Masson: 'Greedy Diagnosis as the Basis of an Intermittent-Fault / Transient-Upset Tolerant System Design'. *IEEE Trans. on Comput.*, Vol. C-32 (October 1983) pp. 953–957.

[3] S. Mallela and G.M. Masson: 'Diagnosable Systems for Intermittent Faults'. *IEEE Trans. on Comput.*, Vol. C-27 (June 1978) pp. 560–566.

[4] S. Mallela and G.M. Masson: 'Diagnosis Without Repair for Hybrid Fault Situations'. *IEEE Trans. on Comput.*, Vol. C-29 (June 1980) pp. 461–470.

[5] F.P. Preparata, G. Metze and R.T. Chien: 'On the Connection Assignment Problem of Diagnosable Systems'. *IEEE Trans. Electron. Comput.*, Vol. EC-16 (December 1967), pp. 848–854.

F. Novak received B.Sc. degree in 1975 and M.Sc. degree in 1977 from the University of Ljubljana. He is currently working toward the Ph.D. degree. From 1975 on, he is a higher research associate at the Jožef Stefan Institute, Ljubljana.

L. Gyergyek received Ph.D. degree in 1957 from the Université Libre de Bruxelles. He is presently professor at the University in Ljubljana, Faculty of Electrical Engineering. He is also a member of Slovene Academy of Sciences and a senior member of IEEE.

S. Klavžar received B.Sc. degree in 1985 from the University in Ljubljana and is currently a M.Sc. student at the same university. He is assistant at the Department of Mathematics.