Conference on Computers
in Engineering, 1981,
Melbourne, 2-3 September

Easily Diagnosable Design at System Level

K.K. SALUJA
Lecturer, Department of Electrical and Computer Engineering, University of Newcastle
and
B.D.O. ANDERSON
Professor, Department of Electrical and Computer Engineering, University of Newcastle

SUMMARY In this paper we investigate diagnosis properties of large interconnected systems composed of small subsystems. We propose two diagnosable designs of systems along with diagnosis algorithms. We also define a new fault model which is based on interrelation between faulty subsystems and show that faults can be diagnosed in systems with relatively simpler structures.

1 INTRODUCTION

Investigation of faults in large interconnected systems composed of small subsystems or units (for example, interconnected microprocessor systems, a large number of interacting programs, large communication networks etc.) is drawing increasing attention of researchers and engineers. A number of models have been studied in the literature for such systems (see [1] for references). In this paper we shall address ourselves to the following problems which are based on one such model, called graph theoretic model as introduced by Preparata et al [2].

(i) We shall propose an algorithm to locate faulty units in a class of systems known as single loop systems.

(ii) We shall establish a bound on the number of units in a system such that a system meeting such a bound can be diagnosed with little additional hardware and/or algorithms of low complexity.

(iii) We shall propose a new fault model for interconnected systems which is applicable to both hardware and software systems. We shall, then, propose a system structure and investigate its diagnosis properties.

In Section 2 we give necessary preliminaries and define a new fault model. In Section 3 we discuss (i) and (ii) mentioned above and in Section 4 (iii) is discussed in depth.

2 PRELIMINARIES AND FAULT MODEL

A large interconnected system (hardware or software) is represented by a directed graph for the diagnosis purpose. Each unit u_i of the system is represented by a node u_i of the graph. A directed link, b_{ij}, is drawn from a node u_i to a node u_j if and only if unit u_i tests unit u_j. The outcome of a test applied by unit u_i to u_j is denoted by a binary variable a_{ij} where

$a_{ij} = 1$ if u_i is fault free and u_j is faulty
$a_{ij} = 0$ if u_i is fault free and u_j is fault free
$a_{ij} = d$ if u_i is faulty, where $d \in \{0,1\}$

Figure 1 shows a graph of a system with 6 units. A possible test outcome has been marked when units u_1 and u_4 are faulty. In the existing literature systems with n units having at most t faults (both n and t are integers and $t \leq \frac{n-1}{2}$) have been studied. No relations between faulty units have been assumed, in other words faulty units were assumed to be randomly distributed. However, in most practical systems, some relation(s) between faulty units can be established. For example, in software systems a corrupt program (or a program with bugs) can corrupt a called program(s) or a calling program(s). Similarly, in an interconnected hardware configuration a faulty unit u_i can cause a fault in a unit u_j if u_j is connected (physically or logically) to unit u_i. Thus a fault can spread

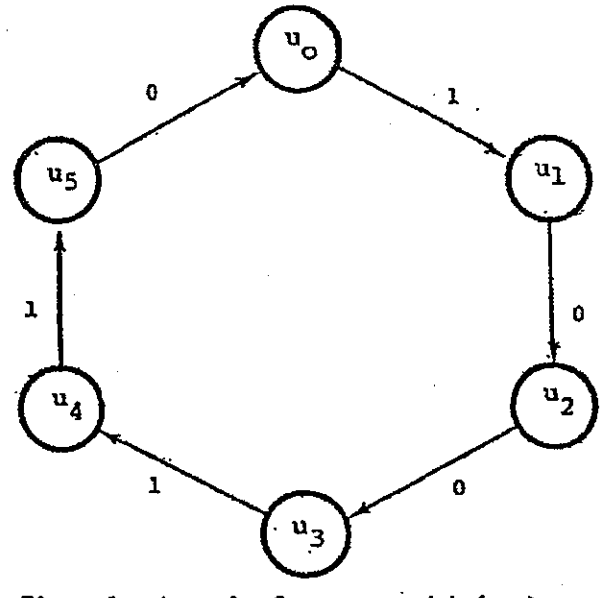

Figure 1 A graph of a system with 6 units

between interconnected units (nodes). Based on this explanation we define a new fault model as follows.

> A system S will be denoted by its diagnostic graph $G = (V,E)$, where V is set of nodes $\{u_0, u_1, \ldots, u_{n-1}\}$ and E is the set of directed links $\{b_{ij}\}$. If U is a set of nodes such that $U \subseteq V$ then $G_U = (U,E_U)$ is a subgraph of G generated by U, where $E_U = \{b_{ij}/u_i,u_j \in U \text{ and } b_{ij} \in E\}$. Clearly $E_U \subseteq E$. We shall call U a fault if all nodes in U are faulty.

Definition 1: A sequence of distinct nodes $u_0, u_1, \ldots, u_\ell$, $\ell \geq 1$ and $b_{i,i+1} \in E$ for $i = 0, 1, \ldots, \ell - 1$, is called a path ($[u_0,u_\ell]$-path).

A subgraph G_U is said to be connected if and only if either $|U|^1 = 1$ or for any pair of nodes $u_i, u_j \in U$ either there is a $[u_i,u_j]$-path or $[u_j,u_i]$-path.

Definition 2: A fault U is called a subgraph fault if G_U is connected. If G_U is not connected, instead it has α different unconnected components we call U to be a fault of order α.

Definition 3: If a fault U is such that G_U is a path then U is a Chain Fault (CF).

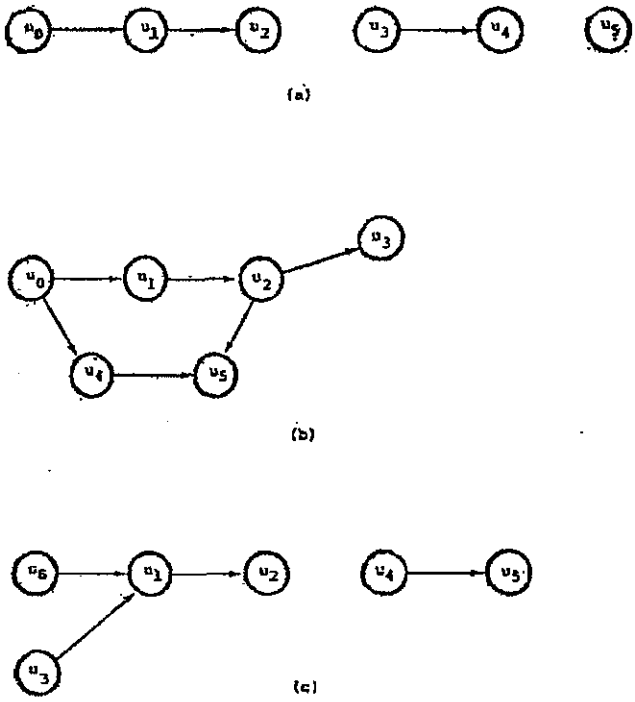

Figure 2 Subgraphs (a) G_{U_1} (b) G_{U_2} and (c) G_{U_3} for Example 1.

Definition 4: A fault U is said to be k-chain Fault (k-CF) if G_U satisfies one of the following conditions:

(i) G_U has exactly k components and each component is a path.

(ii) Number of distinct paths in G_U which cover all nodes of G_U are no less than k.

The following example clarifies the above definition and the remark following the example explains the significance of Definition 4.

Example 1

(a): For a subgraph G_{U_1} of Figure 2(a) k=3.

(b): For a subgraph G_{U_2} of Figure 2(b) k=2 because $[u_0,u_4,u_5]$ and $[u_1,u_2,u_3]$ are two distinct paths which cover all nodes of G_{U_2}.

(c): For a subgraph G_{U_3} of Figure 2(c) k=3 because $[u_0,u_1,u_2]$;$[u_3]$ and $[u_4,u_5]$ are least number of paths covering all nodes of G_{U_3}.

Remark:

The implication of condition (i) of Definition 4 is that a number of faults can occur in a system independently and randomly, i.e. without being related to each other and these faults can spread as chain faults. This can happen if a system is run for reasonably long duration without any repair. The implication of condition (ii) of Definition 4 can be best understood for software systems. A faulty program may be called by a program which in turn can be called by another program thus creating a chain fault. However, if a system is run long enough without repairing fault(s), an initially faulty program can corrupt many calling programs thus starting many chains. We observe that in either case parameter k is a measure of the period a system is run without undergoing a repair.

3 EASILY DIAGNOSABLE DESIGNS

In this section we shall consider occurrance of random faults. We shall employ the concept of one-step diagnosability and sequential diagnosability as defined by Preparata et al [2]. Fujiwara and Kinoshita [3] have studied the complexity of system diagnosis algorithms and have shown that single-loop-systems [2] are diagnosable (sequentially) by algorithms of complexity O(n). In what follows we shall propose two designs of systems which are one-step t-fault diagnosable by algorithms of complexity t O(n) and t+O(n). We first propose an algorithm to diagnose a faulty unit in a single-loop system. The algorithm is a direct consequence of the works of Preparata et al [2] and Saluja and Anderson [4]. Therefore the proof of the algorithm is not included. However, for the sake of completeness, certain definitions have been included here.

Definition 5 [2]: A system S is said to belong to a design D_{1t} when a link from u_i to u_j exists if and only if $j-i = m \pmod n$, $1 \le m \le t$. S is said to belong to a single loop design if m is a fixed constant equal to one.

Theorem 1 [2,4,6]: A single-loop system is sequentially t-fault diagnosable if and only if the number n of units it contains satisfies the following inequality

$$n \ge n_p^t = \left\lfloor \frac{t}{2} \right\rfloor \left(t - \left\lfloor \frac{t}{2} \right\rfloor\right) + t + 2$$

where $\lfloor x \rfloor$ denotes largest integer $\le x$.

We use the algorithm of Preparata et al [2] to partition a single loop system into sequences. The steps of the algorithm are given below.

(1) Choose a 0 test signal followed by a 1 (all zero condition means no fault).

(2) Mark with an x the test link following the link whose test signal is 1. If the link is already marked the algorithm terminates, otherwise go to step (3).

(3) Proceed in the direction of arrowhead. If the value of the test signal is 0, perform step (3), otherwise to to step (2).

Example 2

For the case of n = 10, t = 4 and the following fault pattern (written linearly), where F denotes a faulty unit and N denotes a fault-free unit, the x's are marked using the above steps.

u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9
N	N	N	F	N	N	N	F	F	F
0	0	1	1	0	0	1	0	0	1
x			x				x		

[1] $|x|$ denotes the cardinality of a set x.

Definition 6 [2]: A sequence consists of units comprised of two successive x-marked links.

Algorithm 1: In a single loop system meeting the bound given in Theorem 1, the last unit in a sequence of maximum length is faulty. If there are more than one maximum length sequences then an arbitrary choice of sequence can be made (in fact more than one unit can be diagnosed to be faulty).

In Example 2 above u_7 will be diagnosed to be faulty.

We point out that an earlier algorithm given by Karunanithi and Friedman (Strategy 3 [5]) will fail to diagnose a faulty unit under the fault condition given in Example 2.

We now present our first design which is applicable when $n \geq n_p^t$

Design 1: Let the n units be $u_0, u_1, \ldots, u_{n-1}$; $n \geq n_p^t$. Construct a D_{1t} system consisting of these units. We shall refer to this design as D_{1t}^1 system.

Lemma 1: Let us consider $k(\leq t)$ arbitrary units $u_{i_1}, u_{i_2}, \ldots, u_{i_k}$. In a D_{1t}^1 system there is embedded a single loop system containing $n-k$ units and not containing the above k units.

Proof: Let us put the above k units in ascending order. Now for every chain of the form $u_{i_j}, u_{i_j+1}, \ldots, u_{i_j+p}$, there is a link for u_{i_j-1} to u_{i_j+p+1}. We can thus find a single loop subsystem not containing any of the above units and all the other units.

VVV

The following algorithm can be used to diagnose a D_{1t}^1 design.

Algorithm 2: First consider a single loop containing all the units. Use Algorithm 1 to diagnose a faulty unit.

Consider a single loop embedded in the system containing all but those units which have already been diagnosed to be faulty. Use Algorithm 1 again to locate a faulty unit. Repeat this step until all the faults (at most t faults) have been located.

Theorem 2: D_{1t}^1 system can be diagnosed by an algorithm of complexity $t\,O(n)$.

Proof: Algorithm 2 can be used to diagnose a D_{1t}^1 system. Clearly Algorithm 2 is an application of Algorithm 1 at most t times.

VVV

In the above algorithms we have attempted to locate faulty units. However, if we could locate a non-faulty unit in the first instance it will simplify the location of faulty units because we could then move in the direction of the arrows from the non-faulty unit(s) and could discover the state of such units and thus proceed further and diagnose a system completely. The following algorithm can be used to locate faulty units in a D_{1t} system if a unit is known to be non-faulty.

Algorithm 3: Let us assume a unit u_i is known to be non-faulty. Move in the direction of the arrow from u_i to u_{i+1} to u_{i+2} etc. observing the result of the test. If u_k is the first such unit which is found to be faulty (i.e. u_{k-1} tests u_k giving a test outcome of 1) then check the link from u_{k-1} to u_{k+1} and repeat the process till all faults are located.

It is evident that to locate t faults by the above algorithm we need to observe at most $t+n$ test outcomes and each of the outcome once only. We can therefore state the following theorem.

Theorem 3: Complexity of Algorithm 3 is $t+O(n)$.

We now proceed to establish a bound on n such that the Algorithm 3 can be readily used, but we need some more results.

Lemma 2: In a D_{1t} system with no more than t faults, if all the incoming arcs to a unit u_i are zeros then u_i is fault free.

Proof: Assume to the contrary u_i is faulty. Then the t units testing u_i must all be faulty making total number of faults to be $t+1$.

VVV

Definition 7: Let A, B be two node sets such that $A \cap B = \emptyset$ and $|A \cup B| = |V| = n$. We define

$$E_{AB} = \{(a,b) \mid a \in A,\ b \in B \text{ and } (a,b) \in E\}.$$

We can similarly define E_{BA} and we denote the cardinality of these sets as follows

$$|A| = n_A;\ |B| = n_B;\ |E_{AB}| = n_{AB} \text{ and } |E|_{BA} = n_{BA}$$

Theorem 4: In a D_{1t} design of a system there exists a fault free unit in the system which is tested by t fault free units if and only if

$$n \geq t^2 + t + 1.$$

Proof: (Sufficiency) – Let there be $k(\leq t)$ faulty units in the system. We partition the units in the system into sets A and B such that A contains all the non-faulty units and B is the set of all faulty units. Clearly $n_{BA} \leq kt$.

Also $n \geq t^2+t+1 \Rightarrow n \geq kt+k+1\ ; \forall k \leq t$

$\Rightarrow n-k \geq kt+1$

$\Rightarrow n_A \geq n_{BA}+1$

$\Rightarrow n_A > n_{BA}$

Therefore there exists a unit u_i in the set A which is not tested by any unit of the set B. Thus u_i is tested by t units of the set A only. Thus unit u_i is tested by t fault-free units.

(Necessity) – Let us consider a D_{1t} system of t^2+t units in which units $u_0, u_{t+1}, u_{2t+2}, \ldots u_{t^2-1}$ are faulty and all other units are fault-free. Clearly in this condition every fault-free unit is tested by exactly one faulty unit.

VVV

Design 2: Construct a D_{1t} system of n units, where $n \geq t^2+t+1$. Also connect the incoming arcs to a unit u_i to a t input NOR gate G_i. We shall refer to this design as D_{1t}^2.

Theorem 5: D_{1t}^2 system can be diagnosed by an algorithm of complexity $t+O(n)$

Proof: By Theorem 4 in $D^2_{1,t}$ system there exists a fault-free unit u_i which is tested by fault-free units only. Thus the output of the corresponding gate C_i is 1 if and only if u_i is fault-free. Therefore a fault-free unit can be determined by observing n values and then we can use Algorithm 3 to determine t faulty units. Thus the total complexity of the diagnosis algorithm is $t+O(n)+O(n) = t+O(n)$.

VVV

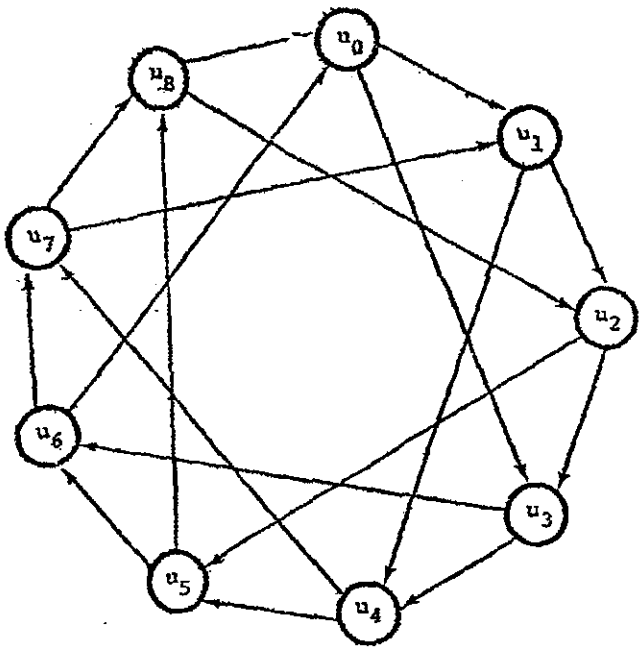

Figure 3 A $C^9_{1,3}$ graph

4 CF DIAGNOSABLE SYSTEMS

In this section we shall confine our attention to 1-CF t-fault diagnosable systems. Let us consider the system of Figure 3. In this system no unit is tested by more than two other units therefore this system is not one-step 3-fault diagnosable for random fault distribution. However, we shall show that the system of Figure 3 is 1-CF one-step 3-fault diagnosable. Clearly the chain faults in such a system can themselves be quite complex e.g. fault sets $\{u_1,u_2,u_3\}$;$\{u_1,u_4,u_5\}$$\{u_1,u_6,u_7\}$;$\{u_1,u_4\}$ are all 1-CF with total number of faults less than or equal to 3, whereas fault sets $\{u_1,u_3,u_4\}$; $\{u_1,u_3\}$ are not 1-CF.

Definition 8: Let $C^n_{1,t}$ be a graph consisting of n nodes $u_0,u_1,\ldots,u_{n-1}$ and links from u_i to u_j if and only if $j-i=1$ or t (modulo n). The graph of Figure 3 is a $C^9_{1,3}$.

We now give a number of properties of $C^n_{1,t}$ systems in the form of the following theorems. These theorems are stated without proof for reason of space limitation.

Theorem 6: If $n \geq t^2-t+1$ then every faulty node in a $C^n_{1,t}$ system is tested by at least one fault-free node.

Corollary 1: If $n \geq t^2-t+1$ and in a $C^n_{1,t}$ system two node u_i and u_j are diagnosed to be faulty such that there are links from u_i to u_k and u_j to u_k for some u_k then u_k is fault-free.

Theorem 7: If $n \geq t^2$ and in a $C^n_{1,t}$ system units u_i and u_{i+j} with $2 \leq j \leq t+1$ are diagnosed to be faulty then units u_{i+k}, $0<k<j$ are also faulty.

Theorem 8: If $n \geq t^2$ and in a $C^n_{1,t}$ system at some stage $k(<t)$ units have been diagnosed to be faulty then it is possible to find a single loop subsystem in the $C^n_{1,t}$ system containing no more than $(t-k)$ faulty units. Furthermore, the number of nodes in such a single loop subsystem is $\geq n-k(t-1)$.

Lemma 3: For $n \geq t^2-2t+4$ and $0 \leq k < t$, $t \geq 3$

$$n-k(t-1) \geq \left\lfloor \frac{t-k}{2} \right\rfloor \left(t-k-\left\lfloor \frac{t-k}{2} \right\rfloor\right) + t-k+2$$

We can now state our final result about 1-CF t-fault one-step diagnosability.

Theorem 9: A $C^n_{1,t}$ system with $n \geq t^2$ is 1-CF t-fault one-step diagnosable for $t \geq 3$.

Proof: Clearly $n \geq t^2 > n_p^t$ for $t \geq 3$. Therefore one fault can be located when no more than t faults are present in a $C^n_{1,t}$ system by considering the single-loop subsystem containing all units and using Algorithm 1.

Now assume at some stage we have located k faulty units. By Theorem 8 we can find a single loop subsystem containing at least $n-k(t-1)$ units and having no more than $t-k$ faults. By Lemma 3 $n-k(t-1) \geq n_p^{t-k}$. Therefore

(i) we can locate one more faulty unit, or
(ii) the single loop so formed contains only fault free units.

If (i) holds we would have located (k+1) faults. In this case we reapply Theorem 8 and Lemma 3.

If (ii) holds we can diagnose the system completely as we would have discovered at least one fault-free unit and we can use Theorems 6 and 7 to find all the faulty and fault-free units.

VVV

It is evident that the structure of a $C^n_{1,t}$ system is relatively simpler than the structure of a D_{1t} system. A $C^n_{1,t}$ system contains only $2n$ links whereas a D_{1t} system contains tn links.

5 CONCLUSION

In this paper we have investigated two diagnosable designs and proposed a 1-CF diagnosable design. It can be shown that general subgraph faults may demand as complex a system structure as required for systems with random fault distribution. However if k is bounded then the structure may be simpler. We have demonstrated that if $k=1$ then the structure is considerably simpler. Study of system structures for other values of k appears to be an interesting problem to investigate.

6 REFERENCES

[1] SALUJA, K.K. (1979). System Level Diagnosis: A Survey. Proc. IREE Intern. Electronics Convention. Sydney. August.

[2] PREPARATA, F.P., METZE, G. and CHIEN, R.T. (1967). On the Connection Assignment Problem of Diagnosable Systems. IEEE Trans. on Computers. EC-16, pp. 848-854. December.

[3] FUJIWARA, H. and KINOSHITA, K. (1978). On the Computational Complexity of System Diagnosis. IEEE Trans. on Computers. C-27, pp. 881-885. October.

[4] SALUJA, K.K. and ANDERSON, E.D.O. (1980). Fault Diagnosis in Loop Connected Systems. Information Sciences. Vol. 21, pp. 75-92.

[5] KARUNANITHI, S. and FRIEDMAN, A.D. (1979) Analysis of Digital Systems Using a New Measure of System Diagnosis. IEEE Trans. on Computers. C-28, pp. 121-133. February.

[6] RUSSELL, J. and KIME, C. (1975). System Fault Diagnosis: Closure and Diagnosability with Repair. IEEE Trans. on Computers. C-24, pp. 1078-1088. November.