Reliability Analysis of Systems with Concurrent Error Detection

C. V. RAMAMOORTHY, MEMBER, IEEE, AND YIH-WU HAN, STUDENT MEMBER, IEEE

Abstract—**There is an increasing use of error detectors and correctors in computer subsystems, such as parity detectors in memory modules and residue checkers in arithmetic units. Their fault tolerant characteristics are studied through the model of detector redundant systems. Their reliabilities and availabilities are analyzed and compared with those which do not have any such error detectors. The design of fault isolating and reconfiguring networks used in the implementation of such systems are developed.**

Index Terms—**Availability, critical reliability of detector, detector redundant system, hybrid (N, S), N-tuple modular redundant system, reconfiguration switch, subsystem, triple modular redundant system, validating gate.**

INTRODUCTION

THE DEMAND for fast error-free computation over large intervals of time and the availability of relatively inexpensive large-scale integration (LSI) circuits have increasingly emphasized the use of the fault-masking redundancy in computer architecture.

Hardware redundancy takes many forms, some of which include component level replication, use of error-detecting or error-correcting circuits, and structurally redundant logic circuits, etc. Reliability enhancement at the level of functional modules, such as triplication and N-tuplication with majority voting [triple-modular redundant system (TMR) and N-tuple modular redundant system (NMR)] and the dynamic switching-in of spare units in case of failures, can extend the mean life time of fault-free operation [1], [2]. A scheme based on the above principles was employed in the implementation of the hard core of the JPL-STAR computer [3]. It can be shown that such schemes can be sensitive to simultaneous faults in multiple units. A scheme known as the self-purging system was proposed to overcome certain of these faults in a hybrid system [4]. In this paper we shall consider a class of redundant systems which use error detectors. We shall call them detector redundant systems. We shall present a reliability analysis of such systems and show necessary and sufficient conditions under which they can provide higher reliability and longer mission times over NMR and NMR hybrid systems.

Manuscript received June 5, 1973; revised March 21, 1975. This work was supported in part by the Office of Naval Research under Contract N00014-59-A-0200-1064.

The authors are with the Department of Electrical Engineering and Computer Sciences and the Electronics Research Laboratory, University of California, Berkeley, Calif. 94720.

INADEQUACY OF HYBRID REDUNDANT SYSTEM

A hybrid redundant (3,2) system as shown in Fig. 1 consists of three active units and two spares. A majority voter generates an output which is the same as that generated by a majority of its active units. When an active unit disagrees with the majority, it will be replaced by a spare. When the number of simultaneously failed active units is less than the majority and if the voter is fault-free, this system will operate correctly. Correct operation will be sustained until all the spares are used up and a majority of active units have failed. When a majority of active units fails simultaneously and when each failed unit generates the same erroneous output, the voter will generate an incorrect output which would initiate the replacement of good active units with spare units. Since the majority of active modules is still malfunctioning, the system will reject all the good spare units until all of them are used up and the system will crash [4]. Even though the probability of failure of a majority of active units in one instant is small, the consequence is catastrophic. The detector redundant system overcomes some of these problems and provides a longer and safer fault-free mission life time.

DETECTOR REDUNDANT SYSTEMS (DR)

In these systems a number of identical modules (units) operate simultaneously using identical inputs. An error detector is associated with each module. If it agrees that the output of the module is correct, a signal is generated by the detector validating the output. Otherwise, a disagreement signal is produced. The network which receives the output of the module and the validation signal of its detector decides whether to accept or ignore the module output. In general, the outputs of those modules whose detectors generate proper validation signals are used. A wide variety of detectors are currently in use in many computing systems. Memory modules use parity checkers, multierror detecting codes, etc. [5]. Arithmetic units use residue codes, etc., for error detection [6], [7]. Thus it is feasible to develop detectors to validate the operation of any functional unit in a computing system at all times. It is also highly desirable to check the operation of the detectors periodically using known input-output patterns and simulating errors in the module outputs.

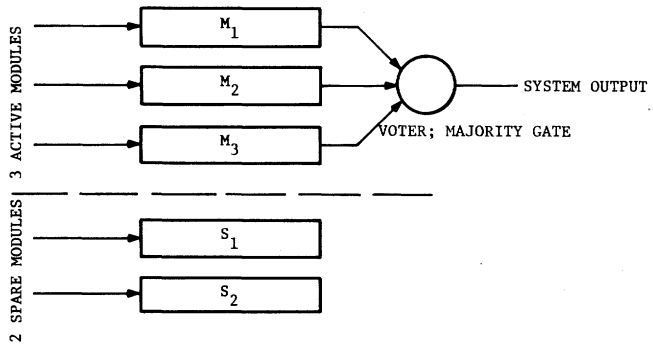


Fig. 1. Hybrid (3,2) system.

Table of Symbols and Notation

TMR	Triple-modular redundant system.
NMR	N-tuple modular redundant system, where $N = 2n + 1$.
$H(N,S)$	Abbreviation for hybrid (N,S), where $N = 2n + 1$.
DR	Detector redundant system.
$DR(2)$	Duplex detector redundant system.
$DR(N)$	N-tuple detector redundant system.
$DR(N,S)$	Hybrid N-tuple detector redundant system with S spares, as usual $N = 1$ or 2.
R	Reliability of the single module.
R_D	Reliability of the detector, generally $R_D > R$.
$\tilde{P}_u$	Probability of the occurrence of undetected errors in the module output by the detector algorithm.
R_c	$1 - \tilde{P}_u$, the probability that the detector algorithm of the detector is capable of validating its associated module output.
R_H	Reliability of the hardware parts of the detector.
$R^*(H(N,S))$	Reliability of $H(N,S)$ with R as its simple module reliability.
$R^*(DR(N,S))$	Reliability of $DR(N,S)$.
$R^*(DR(N,S),R_D)$	Reliability of $DR(N,S)$ with R_D as the original reliability of its detector.
Critical $R_D(N,S,N',S')$	R_D to make $DR(N,S)$ have equal reliability to $H(N',S')$. In other words, it is the minimal R_D to make $R^*(DR(N,S)) \geq R^*(H(N',S'))$.
D	Output of the detector. If $D = 1$, the detector agrees with the output of the module; otherwise $D = 0$.
D_i	Output of the ith detector.
M_i	Output of the ith module.
V	Validating gate output for $DR(N)$ system.
T_i	Power switch of the ith module, where $T_i = 1$ means power is on, otherwise $T_i = 0$.
S_i	ith spare unit.
$\binom{A}{B}$	Combinatorial notation for $(A!)/((A - B)!B!)$.

CONVENTIONS

Before our discussion, we shall clarify the conventions that will be used in the figures. Every module, as shown in Fig. 2(a), has a set of inputs and a set of outputs. For simplicity, only a single line is drawn to represent a set of lines as shown in Fig. 2(b). The interconnection between a detector and its associated module is shown in Fig. 2(c). Similarly, the detector redundant systems are represented using conventions as shown in Fig. 2(d).

MODEL OF DETECTOR REDUNDANT SYSTEMS, *DR*

The basic characteristics of the simplex DR system $DR(1)$, the duplex system $DR(2)$ and the hybrid DR system $DR(N,S)$ as shown in Fig. 2(d)–(f), respectively, are introduced here.

$DR(1)$: The $DR(1)$ system consists of a module whose output is checked by a detector. If the detector agrees with the module output, the output of the detector is a binary one; otherwise it is zero and the total system which contains the module enters the critical mode. The critical mode is the state in which a module of a system is detected to be faulty but there are no spare units to replace it, where the unit is defined as the module and its associated detector. In this mode, either an indicator displays this condition to the outside world requesting repair or replacement or a preprogrammed reconfiguration of the system proceeds to prepare for graceful degradation. Meanwhile, the unit may provide fail-safe outputs. The purpose of associating a detector with a module is for reducing the propagation and the contamination of errors and also for easing the maintenance, since the faulty modules are located automatically by themselves. Therefore the repair time is reduced.

$DR(2)$: This detector redundant system consists of two active units, a checker for the detectors and a validating gate. Every unit consists of a module and its associated detector. The checker, which will be discussed in detail later, is the checking circuit for the module detectors, and the validating gate is the circuit that generates the system output.

If more than one unit is used on-line, then the detectors detect the errors of their associated modules; then, by comparing the module outputs and the detector outputs, the checker checks the correctness of the detectors. A $DR(2)$ system and the checker for its detectors are shown in Fig. 2(e).

We shall describe the functional operation of this system by means of Table I, wherein M_i and D_i represent the outputs of the ith module and its detector, respectively. An element of K, the first column, is a "1" whenever

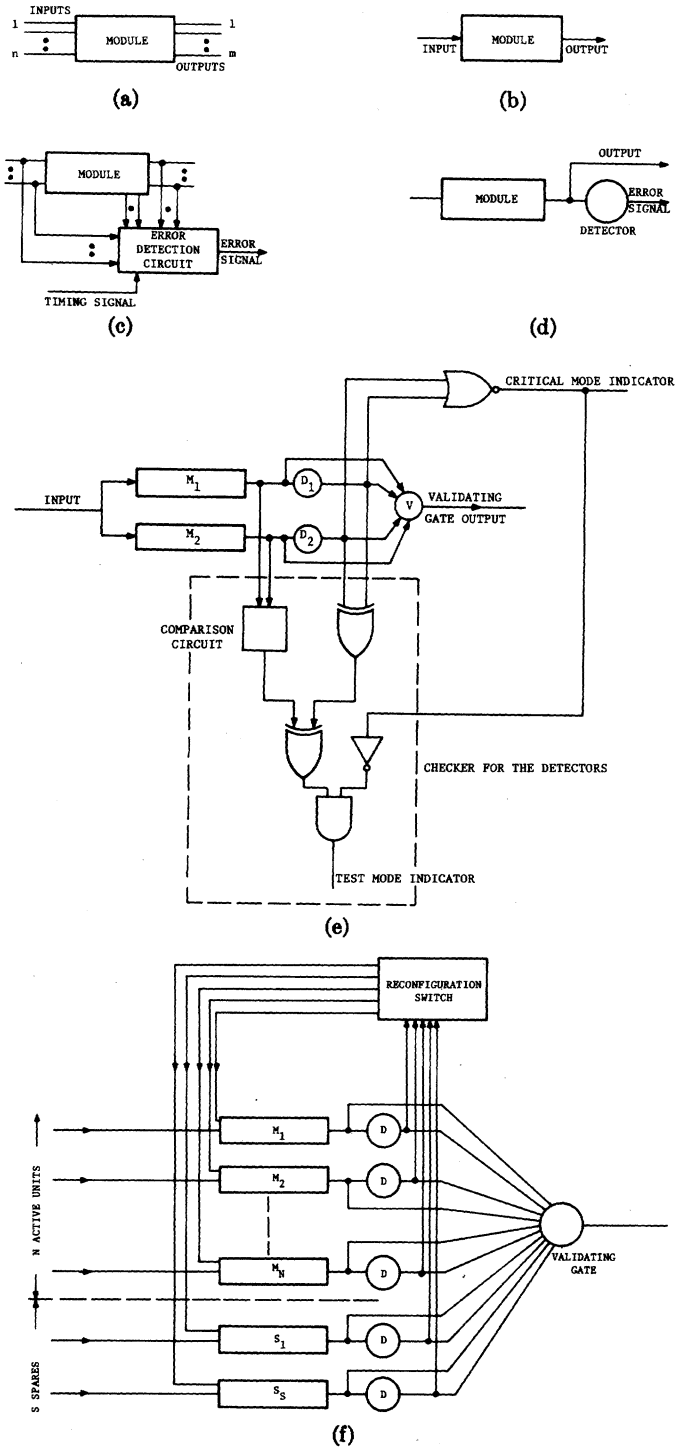


Fig. 2. (a)–(e) $DR(2)$, where the comparison circuit outputs 1 if there are any differences between the module outputs; otherwise it outputs 0. The 1 output of a mode indicator indicates that the system is in that mode. (f) Block diagram of $DR(N,S)$ system.

$M_1 = M_2$; otherwise it is "0." The elements of the last column (V) represent the system output, which could be a value output M_1 (or M_2), an indication to perform a further test (test mode) or an indication that the system has failed (critical mode). "Test mode" occurs when the checker detects some error in a detector. The error may be due to a fault in the hardware parts of a detector or a faulty module output which is not detectable by its detector, because the detector algorithm may not cover this fault of the module. Then a special diagnostic test on the system is required to locate the faulty detector or the faulty module. After performing the test, the validating gate produces a system output. This is the module output that is agreeable to its associated detector whose operation has been verified to be correct by the checker and the test. The critical mode occurs when both the detectors disagree

TABLE I
THE SYSTEM OUTPUT OF THE $DR(2)$ SYSTEM

K	D_1	D_2	system output, V
0	0	0	system in critical mode
0	0	1	M_2
0	1	0	M_1
0	1	1	system in test mode
1	0	0	system in critical mode
1	0	1	system in test mode
1	1	0	system in test mode
1	1	1	M_1 or M_2

with their associated modules. If the system is neither in critical mode nor in test mode, the system output is the one generated by the validating gate.

$DR(N,S)$: This detector redundant system consists of N active units, S spare units, a checker for the detectors, a validating gate, and a reconfiguration switch, where every unit consists of a module and its associated detector. The checker and the validating gate can be defined similarly as in the $DR(2)$ system. The reconfiguration switch enables the system to be dynamically reconfigurable by switching out the faulty units and switching in the spare units to replace them.

As in the $DR(2)$ system, the checker verifies the correctness of the detectors which are considered correct if and only if $M_i = M_j$ and $D_i = D_j = 1$ or $M_i \neq M_j$ and $D_i \neq D_j$ for all pairs of active units; otherwise a special test should be performed and the system is in test mode. If the undetectable errors by the detector are very scarce, it may be enough to take the majority of the outputs of the modules which are agreeable to their detectors as the validated outputs, if such majority exists. When all available detectors disagree with their modules, the system is in critical mode.

If the system is neither in the critical mode nor in the test mode, the validating gate generates the system output that conforms to the output of the module whose detector has been properly checked out by the checker and provides a 1 output.

The first function of the reconfiguration switch is to identify units with faulty modules (by their associated detectors) and/or faulty detectors (using the checker and some special tests if needed). Then the reconfiguration switch switches out faulty units one at a time and replaces them by spare units whose detectors agree with their module outputs.

The logical design of the switch will be discussed in detail later.

RELIABILITY OF THE DETECTOR, R_D

The inherent reliability of a detector, R_D, depends on R_C, the probability that the detector algorithm of the detector is capable of validating its associated module outputs, and R_H, the reliability of its hardware parts. If $\bar{P}_u$ is the probability of the occurrence of undetected errors in the module outputs, then $R_C = 1 - \bar{P}_u$ and $R_D = R_C \cdot R_H$. In general, R_C is a monotonically increasing function of R, the reliability of the module with which the detector is associated. This is because if a more reliable module is used, the probability of the occurrence of undetected errors decreases since the fault incidence is decreased. For example, the parity checker of the contents of a register with N bits can only detect errors odd in number, then

$$R_C = 1 - \bar{P}_u = 1 - \sum_{i=1}^{i=\lfloor N/2 \rfloor} \binom{N}{2i} R_1^{N-2i}(1 - R_1)^{2i}$$

$$\cong 1 - \binom{N}{2} R_1^{N-2}(1 - R_1)^2$$

where $\lfloor N/2 \rfloor$ is the greatest integer less than or equal to $N/2$, R_1 is the reliability of each bit stage and R_1^N is the reliability of this register. It is obvious that the higher R_1^N is the higher R_C. For a module with a fixed reliability R, by combining in some way several different kinds of detectors which cover various types of errors, we can get a composite detector with a higher R_C than any one of those detectors acting alone.

In a $DR(1,S)$ system, if both the active module and its associated detector fail simultaneously, then the failed active module may be considered operational by its associated detector and the outputs of the module are accepted as the outputs of the system. Thus, the system generates incorrect outputs, although the spares are good and have not been used. To overcome this problem due to undetected errors, $DR(N,S)$ systems, $N \geq 2$, are suggested. When $N \geq 2$, the checker whose reliability can be enhanced by applying some fault tolerant schemes checks the correctness of the detectors. Then, the probability that the system fails at any instant due to undetected errors is reduced to the probability that all active modules and their associated detectors fail simultaneously and in the same mode.

In general, the choice of the detectors and the number of active units N of the $DR(N,S)$ systems depends on the reliabilities and the costs of available subsystems, detectors and the requirements of the design goals.

After choosing a suitable detector, it is still possible to apply TMR or NMR schemes at the detector level to improve the R_H of the detector. However, sometimes it might be difficult to find a suitable detector of a module other than by duplication of the module. Then the output of module is validated by comparing outputs of both

TABLE II
UNDETECTED ERROR-RATE ESTIMATES FOR A SAMPLE COLLECTION OF CODES

$n = 8$		$n = 15$		$n = 17$		$n = 21$		$n = 23$		$n = 31$	
k	$\bar{P}u$	k	$\bar{P}u$	k	$\bar{P}u$	k	$\bar{P}u$	k	$\bar{P}u$	k	$\bar{P}u$
*	1.7×10^{-5}	11	2.6×10^{-6}	9	9.4×10^{-8}	15	6.4×10^{-7}	12	1.0×10^{-8}	21	2.8×10^{-8}
7	3.1×10^{-5}	10	1.0×10^{-6}	8	4.1×10^{-8}	12	4.9×10^{-7}	11	4.6×10^{-9}	21	3.0×10^{-8}
4	1.1×10^{-6}	7	8.4×10^{-8}			11	2.5×10^{-8}			20	1.2×10^{-8}
		6	3.7×10^{-8}			9	4.2×10^{-9}			20	1.1×10^{-8}
		6	3.5×10^{-8}			5	2.0×10^{-10}			16	8.2×10^{-10}
		5	1.2×10^{-8}							15	3.9×10^{-10}
		4	5.3×10^{-9}							15	3.5×10^{-10}
		2	1.7×10^{-9}							11	1.4×10^{-11}
										10	7.4×10^{-12}

* The 4-out-of-8 code.

modules. In this case, every module and the comparison circuit is a detector of the other. Its R_H is the hardware reliability of the comparison circuit which compares the outputs of the modules; and its R_C is the probability that these two modules do not have the same fault simultaneously.

UNDETECTED ERRORS

The probability of undetected errors was evaluated for a large number of useful codes, e.g., parity check, *B-C-H*, etc., experimentally in data transmission and memory storage applications and these are summarized in Table II. Here n is the number of bits in the transmitted block, k is the dimension of codes, and $\bar{P}_u = 1 - R_C$ is the average probability of undetected error [8]. The codes in that collection present a wide range available for detector implementation and indicate it would not be difficult to select appropriate codes and their detectors for specific data transmission and storage applications in a computer system. Similar comments apply to arithmetic error detection and control processor error detection [10]–[12].

RELIABILITY ANALYSIS AND EVALUATION

A fundamental aspect of the $DR(N)$ system and the $DR(N,S)$ system is that the survival of a single module ensures the reliable operation of the entire system, if we have a near perfect reconfiguration switch for the $DR(N,S)$ system and near perfect detectors.

We shall use the notation described earlier for evaluating various reliability parameters, in which TMR stands for triple modular redundant system, NMR for N-tuple modular redundant system, $DR(N,S)$ for hybrid N-tuple detector redundant system with S spares, R for the reliability of the module, $R^*(X)$ for the reliability of the system where X is the applied fault tolerant scheme, and R is the reliability of the simple module.

Then, it is well known that

$$R^*(\text{TMR}) = R^3 + 3R^2(1 - R) \tag{1}$$

$$R^*(\text{NMR}) = \sum_{i=0}^{n} \binom{N}{i} (1 - R)^i R^{N-i}, \quad \text{where } N = 2n + 1. \tag{2}$$

For systems with stand-by spares, even though $R_S \geq R$, let us assume $R_S = R$ and the reconfiguration switch, the voters and the validating gates are perfect for simplicity. Then

$$R^*(H(3,S)) = 1 - (1 - R)^{S+2}(1 + R(S + 2)) \tag{3}$$

$$R^*(H(N,S)) = \sum_{i=0}^{i=n+S} \binom{N + S}{i} (1 - R)^i R^{N+S-i}. \tag{4}$$

(Assuming no more than n units fail simultaneously.)

Although some detectors may have the capability to correct errors in their associated modules, the error correcting capability should be used cautiously. For data transmission in noise channels, error correcting capability is very useful to correct transmission errors due to noise interference. For arithmetic and storage functions in digital systems, error correcting capability is helpful in correcting errors due to transient faults. If errors are due to permanent faults, the utilization of the error correcting capability can only provide temporarily correct outputs. However, faults could accumulate and thus make the system produce erroneous outputs. For example, a detector utilizing a Hamming code with a distance of $2d + 1$ can detect $2d$ or fewer errors or correct d or fewer errors. If the first permanent fault causes d or fewer errors, at this moment by the error correcting capability the unit which includes the detector and its associated module would still be operational. However, if other faults occur before the removal of the first fault and if the number of errors generated is greater than $d + 1$, then, this unit will produce erroneous outputs. For this reason and for simplicity, the error correcting capability is not assumed in the subsequent discussion.

$$R^*(DR(1)) = R \cdot R_D \cong R \text{ if } R_D \cong 1 \tag{5}$$

$$R^*(DR(2)) = 2R \cdot R_D - (R \cdot R_D)^2 \cong 2R - R^2 \text{ if } R_D' \cong 1. \tag{6}$$

Assuming all active modules and their associated detectors do not fail simultaneously, we obtain

$$R^*(DR(N,S)) = 1 - (1 - R \cdot R_D)^{N+S} \cong 1 - (1 - R)^{N+S} \text{ if } R_D \cong 1. \tag{7}$$

R,$R^*(\text{TMR})$, and $R^*(DR(N,S))$, with the assumption

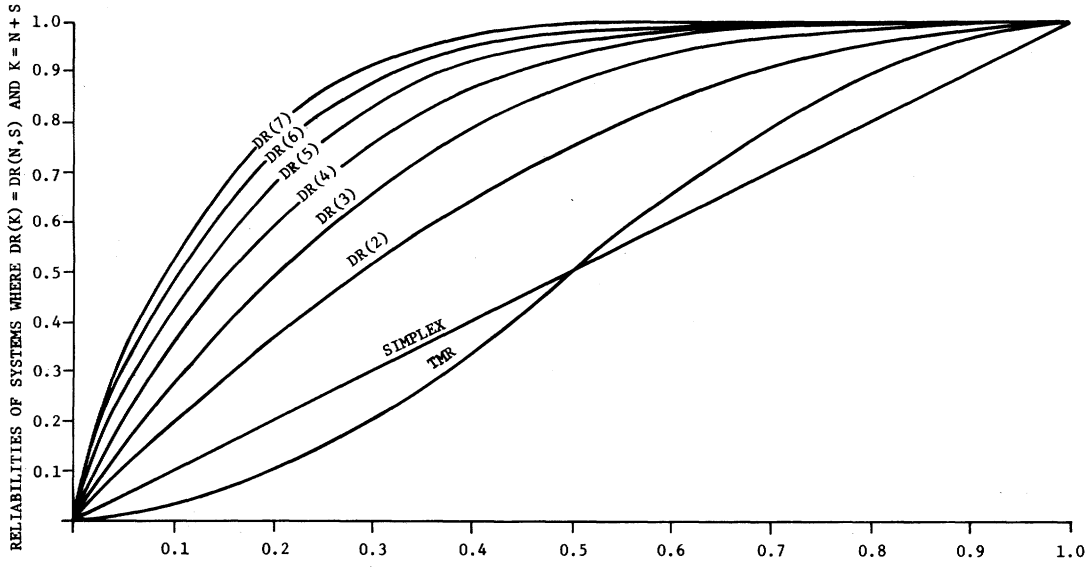


Fig. 3. Reliabilities of DR, TMR, and simplex systems.

$R_D \cong 1$, are shown in Fig. 3. It is instructive to take this extreme case of assuming $R_D \cong 1$ and compare the reliabilities of DR systems with the reliabilities of systems with other schemes. We shall later remove this restriction and find the exact value of R_D for which the DR system still has a higher reliability than those compared.

Let us consider

$$\begin{aligned} &R^*[DR(2)] - R^*(\text{TMR}) \\ &\quad = 2R - R^2 - R^3 - 3R^2(1-R) \\ &\quad = 2R(1-R)^2 \end{aligned}$$

$2R(1-R)^2$ is always positive and therefore,

$$R^*[DR(2)] \geq R^*(\text{TMR}), \qquad \text{for any } R(0 \leq R \leq 1).$$

This implies that even though $DR(2)$ requires only two modules, it has a higher reliability than a TMR system with three modules under the above mentioned assumptions. Generalizing, we see that from (6)

$$\begin{aligned} R^*[DR(N,0)] = R^*[DR(N)] &= 1-(1-R)^N \\ &= \sum_{i=0}^{N-1} \binom{N}{i} (1-R)^i R^{N-i} \end{aligned} \tag{8}$$

and using (2) with the result above, then

$$\begin{aligned} &R^*[DR(N)] - R^*(\text{NMR}) \\ &\quad = \sum_{i=n+1}^{N-1} \binom{N}{i} (1-R)^i R^{N-i} > 0 \end{aligned} \tag{9}$$

where $N = 2n + 1$.

Similarly, we write (6) as

$$R^*[DR(N,S)] = \sum_{i=0}^{N+S-1} \binom{N+S}{i} (1-R)^i R^{N+S-i}. \tag{10}$$

From (10) and (4)

$$\begin{aligned} &R^*[DR(N,S)] - R^*[H(N,S)] \\ &\quad = \sum_{i=n+S+1}^{N+S-1} \binom{N+S}{i} (1-R)^i R^{N+S-i} > 0. \end{aligned} \tag{11}$$

CRITICAL RELIABILITY OF THE DETECTOR R_D

So far we have assumed that $R_D \cong 1$; we shall now determine the minimum values of R_D for which the conclusions reached earlier about the inherent superior reliability of the detector redundant systems over others would still be valid.

1) Let $R^*[DR(2)] \geq R^*(\text{TMR})$ from (1) and (5)

$$2RR_D - R^2R_D^2 \geq 3R^2 - 2R^3$$

$$R^2R_D^2 - 2RR_D + R(3R - 2R^2) \leq 0$$

$$RR_D^2 - 2R_D + 3R - 2R^2 \leq 0.$$

Then the necessary and sufficient condition for $R^*[DR(2)] \geq R^*(\text{TMR})$ is

$$\frac{1-(2R+1)^{1/2}(1-R)}{R} \leq R_D \leq 1.$$

Let us define critical $R_D(N,S,N',S')$ to be the R_D for which $R^*(DR(N,S)) = R^*(H(N',S'))$. In other words, it is the minimum reliability of the detector that makes $R^*(DR(N,S)) \geq R^*(H(N'\,S'))$.

$$\text{The critical } R_D(2,0,3,0) = \frac{1-(2R+1)^{1/2}(1-R)}{R}. \tag{12}$$

2) Similarly, the necessary and sufficient condition for $R^*[DR(2)] \geq R^*(\text{simplex}) = R$ is

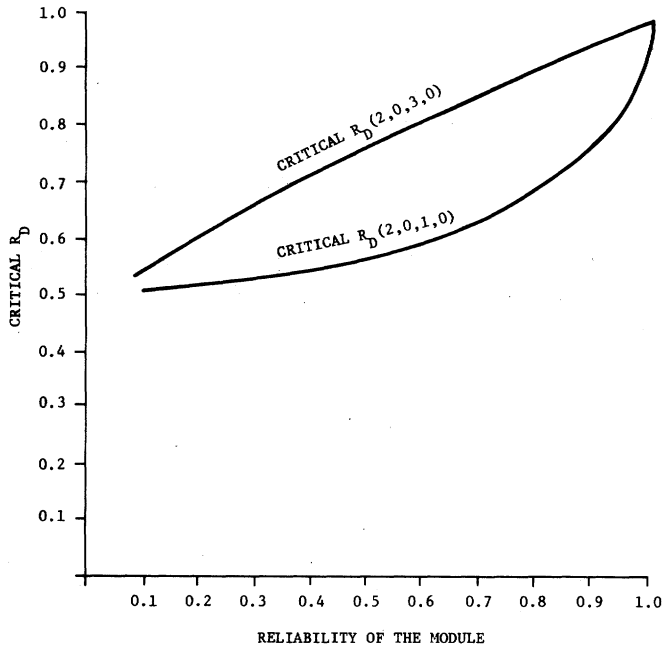


Fig. 4. Critical R_D.

$$\frac{1-(1-R)^{1/2}}{R} \leq R_D \leq 1.$$

$$\text{The critical } R_D(2,0,1,0) = \frac{1-(1-R)^{1/2}}{R}. \quad (13)$$

The critical R_D for 1) and 2) as a function of R are shown in Fig. 4.

3) To determine the critical R_D of the detector such that $R^*[DR(N,S)] \geq R^*[H(N',S')]$ we proceed as follows.

From the definition, it is known that critical $R_D(N,S,N',S')$ is the R_D that makes

$$R^*(DR(N,S),R_D) = R^*(H(N',S')) \quad (14)$$

where $R^*(DR(N,S),R_D)$ and R_D are the reliability of $DR(N,S)$ and its detectors, respectively. It can be easily proved that only one value of critical R_D exists.

RECONFIGURATION SWITCH AND VALIDATING GATE

Siewiorek and McCluskey [9] have suggested a reconfiguration switch for the $H(N,S)$ system and two switching schemes. Both of these switching schemes appear to be applicable in the reconfiguration process for the $DR(N,S)$ system. In the first scheme, a power switch can turn on the power on a selected spare unit and allow the output to be used. In the second scheme, the spare units have their power always on but the outputs are not gated until needed. Both the switching schemes as adapted to the detector redundant systems are shown in Fig. 5. When the above schemes are used, appropriate failure rates must be used in the analysis since the failure rate of the powered unit may be different from the failure rate of the unpowered one. The logic diagram for reconfiguration

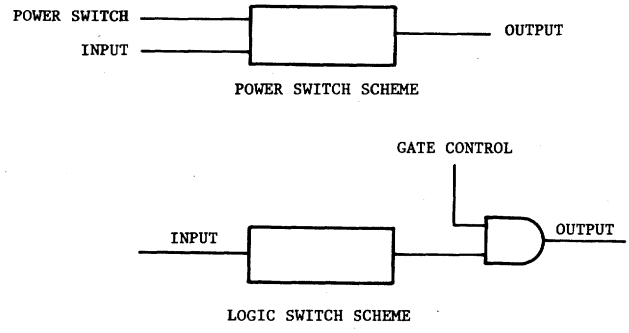


Fig. 5. Power switch and logic switch schemes.

for the $DR(3,2)$ system with the power switch scheme is shown in Fig. 6. If a module is turned off, its output is supposed to be zero. The use of detectors helps not only in fault location but also in simplifying the reconfiguration process in which the malfunctioning units are replaced by good spares. The asynchronous pulse generator shown in Fig. 6, generates a pulse when one output of the detector of an active unit changes from one to zero. If some (more than one) detectors disagree with their module outputs simultaneously, the number of pulses generated by the pulse generator will be equal to the number of failed modules. During every pulse, one reconfiguration process proceeds, i.e., switching out a faulty active unit and replacing it with a spare unit, until all the failed units have been replaced.

In the "reconfiguration switch" and the "validating gate" shown in Fig. 6, it is assumed that the priorities of spare units to be switched on follow their numerical order, that is, the ith spare S_i has a higher priority than S_{i+1}. The spare unit S_i whose output is agreeable to its detector will be switched on to replace any failed active unit, if all the other spares with higher priorities have been activated or failed. Fig. 7 indicates the S_i part of the reconfiguration switch.

On the busses between the detectors and the pulse generator, there are switches which are designed to avoid switching out modules with transient faults. To distinguish between permanent and transient faults in the system, the system does the following. If a fault is detected by a detector and it persists beyond a specified interval of time, then a permanent fault is assumed and the switch generates a 0 at the end of the interval. However, during this interval, it sustains a 1 output, assuming that the fault is nonpermanent. At the same time, the validating gate masks out the transient fault provided $N \geq 2$ in the $DR(N)$ system. Please note that the reconfiguration switch as shown is of a simplex design to demonstrate its structure. It may be desirable to enhance its reliability by applying a suitable fault tolerant scheme on it.

AVAILABILITY ANALYSIS

When a system fails totally, no matter what redundant schemes have been utilized, it will be either thrown away

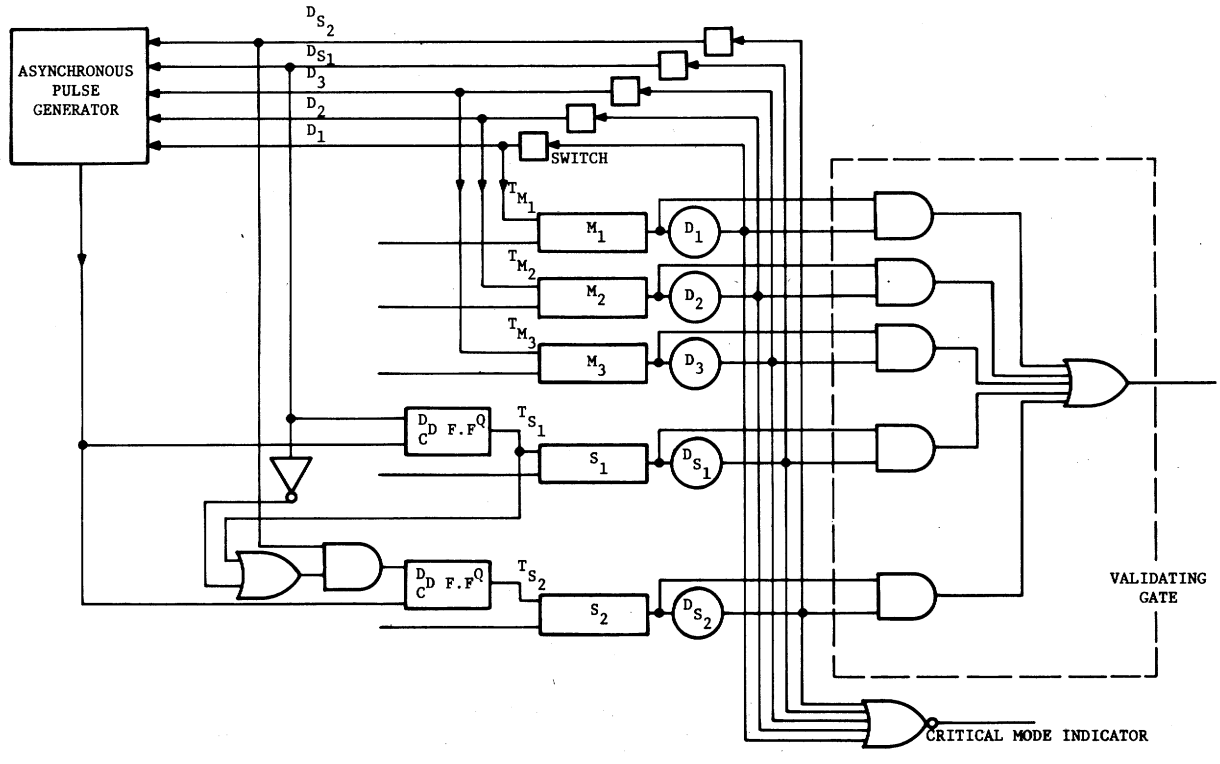


Fig. 6. Logic circuits for reconfiguration switch and validating gate of *DR* (3,2). (*Remark:* Where flip-flop is a falling edge triggered. The checker for detector is not shown. Every detector of the spare unit outputs 1 before it is switched on.)

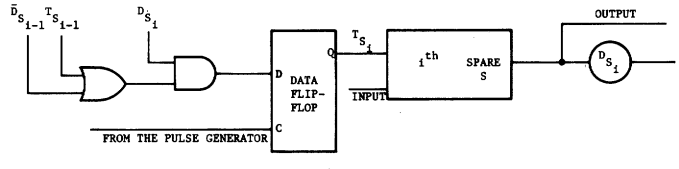


Fig. 7. Reconfiguration switch for S.

or will be repaired for reuse. When the system has to be repaired for reuse, then the repair time of a faulty system becomes a critical parameter for the availability of the system. A reliable system may not provide a satisfactory availability, if a time-consuming testing, fault-locating and repair is needed whenever the system fails. The reconfiguration switch discussed earlier improves the availability by switching in a fault-free spare unit and permitting the repair of the faulty unit off-line. The fault location and repair will be reduced sharply by utilizing the *DR* schemes discussed earlier. To illustrate how to reach a required system availability by applying various redundant schemes, and to show how *DR* systems provide availabilities superior to their unchecked counterparts, we shall discuss a memory system design having the same availability specifications as the Bell Telephone Laboratory's ESS system [12], [13]. The ESS system memory consists of a number of subsystems which must all be operational in order to keep the total system operational, i.e., any subsystem malfunction will bring down the total system.

Let A be the system availability which is the fraction of total time during which the system is available for computation. Let the system consist of n subsystems whose individual availabilities are given by $A_1, A_2, \cdots, A_n$.

Then $A = A_1, A_2, \cdots, A_n$, and

$$\text{unavailability } U = 1 - A$$
$$= 1 - (1 - U_1)(1 - U_2)\cdots(1 - U_n)$$
$$\cong U_1 + U_2 \cdots + U_n,$$

where the approximation is valid for $U \ll 1$.

We shall next use the same quantitative parameters and assumptions as those used in the ESS systems.

1) The required unavailability of the memory system should be less than 2 hours in 40 years, i.e., $U < 10^{-5}$.
2) The mean repair time $R = 2$ h.
3) The mean time between failure $F = 10^4$ h.

Let us now consider the techniques of improving the availability of the system through redundancy to meet the required unavailability.

a) Basic System [Fig. 8(a)]: The basic system consists of eight unduplicated memory modules (stores). Then the availability of each store

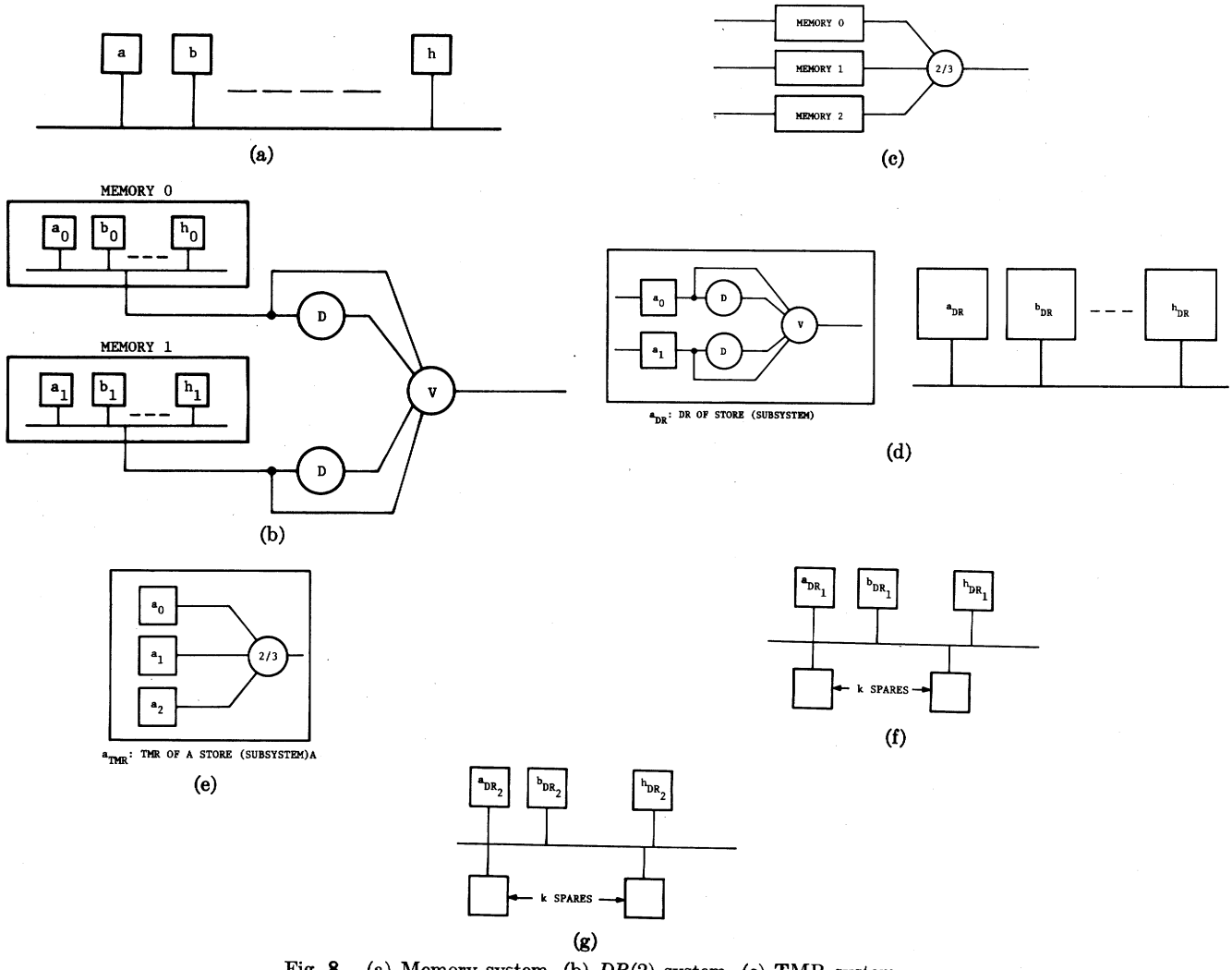


Fig. 8. (a) Memory system. (b) $DR(2)$ system. (c) TMR system. (d) $DR(2)$ stores; store level duplication with detectors. (e) TMR at store level. (f) N stores with k spares. (g) N DR stores with k DR spare.

$$A_i = \frac{F}{F+R}$$

$$U_i = \frac{R}{F+R} \cong \frac{R}{F}.$$

Corresponding to a 40 year down time of 4200 minutes with assumed values of $F = 10^4$ h., $R = 2$ h.,

$$A = A_a A_b \cdots A_h,$$

$$U \cong U_a + U_b \cdots + U_h$$

$$\cong \frac{8R}{F} = 33600 \text{ min for 40 years.}$$

The 40 year down time is 33600 min and so the unavailability is far in excess of the required 2 h.

Although the DR schemes reduce the repair time sharply by locating faults at its module level the added circuitry required in these schemes may increase the failure rate. We shall assume in the foregoing discussion that the failure rate and the repair time have not been affected by the specific scheme used, and that the off-line faulty units will not be repaired until the total system fails.

b) DR at System Level: This is indicated in Fig. 8(b). We shall call the upper system memory 0 and the lower one memory 1. Then the memory system is down if any store in memory 0 is down *and* any store in memory 1 is down. The detectors are used to check the outputs of the subsystems. This is the $DR(2)$ system discussed earlier.

$$U = U_0 U_1 = (U_{a0} + U_{b0} \cdots + U_{h0})$$

$$\cdot (U_{a1} + U_{b1} \cdots + U_{h1})$$

$$\cong \left(\frac{8R}{F}\right)^2 = 64\left(\frac{R}{F}\right)^2.$$

This implies a down time of 54 min over a 40 year period. Such a reduction in down time is achieved by the addition of 8 additional stores.

c) TMR at System Level [Fig. 8(c)]: If TMR is used at system level then the unavailability of the system U_s will be

$$U_S = U_0U_1U_2 + U_0U_1A_2 + U_0A_1U_2 + A_0U_1U_2$$
$$= 8^3\left(\frac{R}{F}\right)^3 + 3 \times 8^2\left(\frac{R}{F}\right)^2\frac{F}{R+F}$$
$$\cong 3 \times 8^2\left(\frac{R}{F}\right)^2 = 162 \text{ min in 40 years.}$$

d) DR at Store Level (Subsystem Level) [Fig. 8(d)]: Here the duplication is on the store basis and each pair of stores constitute a subsystem with unavailability

$$U_a = U_{a0}U_{a1} = \left(\frac{R}{F}\right)^2 = 0.84 \text{ min/40 years.}$$

For the whole system requiring eight stores

$$U_S = U_a + U_b \cdots U_n$$
$$= 8\left(\frac{R}{F}\right)^2 = 6.7 \text{ min/40 years.}$$

e) TMR Store Level (Subsystem Level) [Fig. 8(e)]: Here

$$U_a = U_{a0}U_{a1}U_{a2} + U_{a0}U_{a1}A_{a2}$$
$$+ U_{a0}A_{a1}U_{a2} + A_{a0}U_{a1}U_{a2}$$
$$= \left(\frac{R}{F}\right)^3 + 3\left(\frac{R}{F}\right)^2\frac{F}{R+F} \cong 3\left(\frac{R}{F}\right)^2$$

$$U_S \cong 8 \times 3\left(\frac{R}{F}\right)^2 = 20.1 \text{ min/40 years.}$$

f) DR(1) at Store Level with K Spares [Fig. 8(f)]: Here we assume that $n + K$ stores are available, of which n stores are needed and k stores are spares. When a malfunctioning store is detected, it is replaced by a spare module. The disadvantage of this scheme is that if a faulty store is lost, it may result in an interruption to the processing capability. It is good for applications where loss in process data is less important than the recovery of service after a fault.

An $(n + K)$ system is available whenever there are at least n good stores among $(n + K)$ stores.

Subsystem availability for $j (j \leq K)$ faulty stores

$$A_S = \sum_{j=0}^{K}\binom{n+K}{j}\left(\frac{R}{F}\right)^j\left(1 - \frac{R}{F}\right)^{n+K-j}$$

$$U_S = \sum_{j=K+L}^{n+K}\binom{n+K}{j}\left(\frac{R}{F}\right)^j\left(1 - \frac{R}{F}\right)^{n+K-j}$$

when $n = 8$, $F = 10^4$ h, and $R = 2$ h.

$U_S = 30.3$ min for $K = 1$; 0.02 min for $k = 2$.

g) DR(2) at Store Level with K Spares [Fig. 8(g)]: Here the individual unavailability of each store $= U_i = (R/F)^2$

$$U_S = \sum_{j=K+1}^{n+K}\binom{n+K}{j}\left(\frac{R^2}{F^2}\right)^j\left(1 - \frac{R^2}{F^2}\right)^{n+K-j}, \quad j > K$$

for $n = 8$, $F = 10^4$ h, $R = 2$ h, and $K = 1$.

$$U_S \cong 36\left(\frac{R^2}{F^2}\right)^2 = 1.2 \ \mu\text{s/40 years.}$$

The unavailabilities of different store configurations are summarized as follows:

Basic system	U_S = 33600 min/40 years.
TMR at system level	U_S = 162 min/40 years.
$DR(2)$ at system level	U_S = 54 min/40 years.
$DR(2)$ at store level (subsystem level)	U_S = 6.7 min/40 years.
TMR at store level	U_S = 20.1 min/40 years.
$DR(1)$ at store level with 1 spare	U_S = 30.3 min/40 years.
$DR(1)$ at store level with 2 spares	U_S = 0.02 min/40 years.
$DR(2)$ at store level with 1 spare	U_S = 1.2 μs/ years.

From the foregoing results, it is clear that the detector redundant scheme applied at the subsystem level (store level) provides a higher availability than that applied at the system level in this example. If the scheme is applied at gate level, the added interconnections which were neglected before, may reduce the reliability of the system. Also we may not find a suitable detector at the gate level except by duplicating and output comparison.

CONCLUSION

In our discussion of the $DR(N,S)$ systems, we have made some simplifications and assumptions which can be removed by further analysis. For instance, we have assumed that the reconfiguration switch and the validating gate of the $DR(N,S)$ systems are perfect in the calculations of their reliabilities. However, in the real case, although they are part of the hardcore, their reliabilities should be taken into account.

The complexity of the switch and the validating gate grows with the number of modules. Then the reliability of the switch and the validating gate decreases with the number of modules. From Fig. 6 and Fig. 7, regardless of the fan-in and fan-out limit on the components in the validating gate and the switch, the increased hardware, due to the addition of one unit, for the validating gate is one AND gate, for the reconfiguration switch is one AND gate, one OR gate and a flip-flop. Compared with the complexity of the module, the increased hardware is quite negligible. Therefore, we believe that the present analysis provides sufficient insight into the characteristics of the *DR* systems.

In summary, provided suitable detectors and reconfiguration switches for a system are available, *DR* schemes have some special advantages over other fault masking schemes:

1) They have higher reliabilities over the other schemes.
2) They have higher availabilities over the other schemes.
3) The handling of transient faults becomes simpler since most faults are detected immediately whenever they happen.
4) The maintenance is easier, since faults can be located easily.

We believe that since *DR* schemes provide another important strategy to improve fault tolerance of computers, additional techniques must be developed particularly at the levels of microprocessor operations and I-O controller operations.

REFERENCES

[1] F. P. Mathur and A. A. Avižienis, "Reliability analysis and architecture of a hybrid-redundant digit system: Generalized triple modular redundancy with self-repair," in *1970 Spring Joint Computer Conf., AFIPS Conf. Proc.*, vol. 36. Montvale, N. J.: AFIPS Press, 1970, pp. 375–383.

[2] W. G. Bouricius, W. C. Carter, and P. R. Schneider, "Reliability modeling techniques for self-repairing computer systems," in *Proc. 1969 Ann. Ass. Comput. Mach. Conf.*, p. 69, pp. 295–309.

[3] A. A. Avižienis, "Design of fault-tolerant computers," in *1967 Fall Joint Computer Conf., AFIPS Conf. Proc.*, vol. 31. Washington, D. C.: Thompson, 1967, pp. 733–743.

[4] K. M. Chandy, C. V. Ramamoorthy, and A. Cowan, "A framework for hardware-software tradeoffs in the design of fault-tolerant computers," in *1972 Fall Joint Computer Conf., AFIPS Conf. Proc.*, vol. 41. Montvale, N. J.: AFIPS Press, 1972, pp. 55–63.

[5] A. M. Patel and M. Y. Hsiao, "An adaptive error correction scheme for computer memory system," in *1972 Fall Joint Computer Conf., AFIPS Conf. Proc.*, vol. 41. Montvale, N. J.: AFIPS Press, 1972, pp. 83–87.

[6] A. Avižienis, "Arithmetic error codes: Cost and effectiveness studies for application in digital system design," *IEEE Trans. Comput.*, vol. C-20, pp. 1322–1331, Nov. 1971.

[7] T. R. N. Rao and O. N. Garcia, "Cyclic and multiresidue codes for arithmetic operations," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 85–91, Jan. 1971.

[8] E. O. Elliot, "Estimates of error rates for codes on burst-noise channels," *Bell Syst. Tech. J.*, pp. 1977–1997, Sept. 1963.

[9] D. P. Siewiorek and E. J. McCluskey, "An iterative cell switch design for hybrid redundancy," *IEEE Trans. Comput.*, vol. C-22, pp. 290–297, Mar. 1973.

[10] R. W. Cook, W. H. Sisson, T. F. Storey, and W. N. Toy, "Design of a self-checking microprogram control," *IEEE Trans. Comput.*, vol. C-22, pp. 255–262, Mar. 1973.

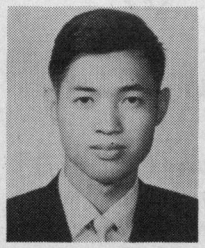
[11] H. Y.-P. Chang, R. C. Dorr, and D. J. Senese, "The design of a microprogrammed self-checking processor of an electronic switching system," *IEEE Trans. Comput.*, vol. C-22, pp. 489–500, May 1973.

[12] H. Y.-P. Chang and J. Scanlon, "Design principles for processor maintainability in real time systems," in *1969 Fall Joint Computer Conf., AFIPS Conf. Proc.*, vol. 35. Montvale, N. J.: AFIPS Press, 1969, pp. 329–337.

[13] J. L. Brewster and W. A. Liss, "Design of reliable peripheral equipment," presented at the Nat. Electron. Conf., 1972.

C. V. Ramamoorthy (M'57) received the undergraduate degree in physics and technology from the University of Madras, Madras, India, the M.S. degree and the professional degree of Mechanical Engineer, both from the University of California, Berkeley, and the M.A. and Ph.D. degrees in applied mathematics and computer theory from Harvard University, Cambridge, Mass.

He was associated with Honeywell's Electronic Data Processing Division, Waltham, Mass. He was Professor in the Departments of Computer Science and Electrical Engineering at the the University of Texas, Austin. He is currently a Professor in the Department of Electrical Engineering and Computer Science at the University of California, Berkeley.



Yih-Wu Han (S'73) was born in Nanking, China, on May 1, 1948. He received the B.S. degree in electrical engineering from the National Taiwan University, Taiwan, China in 1969 and the M.S. degree in electrical engineering from the University of Waterloo, Waterloo, Ont., Canada, in 1972.

He is completing his Ph.D. degree at the University of California at Berkeley where he has been a Research Assistant and Teaching Assistant. His current interests include computer architecture, reliability and performance measurement, operating systems and program methodology.

Mr. Han is a member of the Association for Computing Machinery