Reliability analysis and architecture of a hybrid-redundant digital system: Generalized triple modular redundancy with self-repair

by FRANCIS P. MATHUR*

Jet Propulsion Laboratory
Pasadena, California

and

ALGIRDAS AVIŽIENIS

University of California
Los Angeles, California

"A random series of inept events
To which reason lends illusive sense, is here,
Or the empiric Lifes instinctive search,
Or a vast ignorant mind's colossal work . . ."
Savitri, B.I.C.2—Sri Aurobindo[1]

INTRODUCTION: FAULT-TOLERANT COMPUTING

The objective to attain fault-tolerant computing has been gaining an increasing amount of attention in the past several years. A digital computer is said to be fault-tolerant when it can carry out its programs correctly in the presence of logic faults, which are defined as any deviations of the logic variables in a computer from the design values. Faults can be either of transient or permanent duration. Their principal causes are: (1) component failures (either permanent or intermitent) in the circuits of the computer, and (2) external interference with the functioning of the computer, such as electric noise or transient variations in power supplies, electromagnetic interference, etc.

Protective redundancy in the computer system provides the means to make its operation fault-tolerant. It consists of additional programs, additional circuits, and additional time of operation that would not be necessary in a perfectly fault-free system. The redundancy is deliberately incorporated into the circuits and/or software of the computer in order to provide either masking of or recovery from the effects of some types of faults which are expected to occur in the computer. Repetition of programs provides time redundancy. Programmed reasonableness checks and diagnostic programs are forms of software redundancy. Finally, monitoring circuits, error-detecting and error-correcting codes, structural redundancy of logic circuits (component quadding, channel triplication with voting, etc.), replication of entire computers, and self-repair by the switching-in of standby spares (replacement systems) are the most common forms of hardware redundancy.

The historical perspective shows that the study and use of hardware redundancy, which began nearly 20 years ago,[2,3] has been steadily increasing in the past decade. A very strong reason for this has been the evolution of integrated circuit technology. The inclusion of redundant circuitry is now economically more feasible. The large cost and size of diagnostic software in today's complex computer systems also motivates the relegation of as much checking as possible to special hardware. This special hardware is required to interact with a supervisory program to provide fault-tolerance and recovery without interaction with the human operator.

The presently existing computer systems with extensive use of hardware redundancy are found in applications with extreme reliability requirements. The

*This work was done in partial fulfillment towards the Ph.D. in the Computer Science Department of the University of California, Los Angeles. A preliminary version of this paper was presented as a working paper at the IEEE Computer Group Workshop on "Reliability and Maintainability of Computing Systems," Lake of the Ozarks, Missouri, October 20–22, 1969.

most interesting illustration is the SATURN V launch vehicle computer which employs triple-modular redundancy (TMR) with voting elements in its central processor and duplication in the main memory.[4] Subsequent studies of fault-tolerance in manually non-accessible computers with life requirements of over 10 years have shown that replacement systems with standby spares of entire computer subsystems offer advantages over complete triplication.[5] These studies have led to the design and construction of an experimental Self-Testing-And-Repairing (STAR) computer.[6] This computer is presently in operation at the Jet Propulsion Laboratory. It is being used as an experimental vehicle to study and refine self-repair techniques which incorporate fault-detection and recovery by repetition of programs and/or by automatic replacement of faulty subsystems.

Many systems with hardware redundancy (including the STAR computer and other replacement-repair systems) share the common problem of a "hard core." This "hard core" consists of logic circuits which must continue to function in real time in order to assure the proper fault detection and recovery of the entire system. The purpose of this paper is to present the results of a general study of the architecture and reliability analysis of a new class of digital systems which are suitable to serve as the "hard core" of fault-tolerant computers. These systems are called *hybrid-redundant* systems and consist of the combination of a multiplexed system with majority voting (providing instant internal fault-masking) and of standby spare units (providing an extended mean life over the purely multiplexed system). The new quantitative results demonstrate that hybrid systems possess advantages over purely multiplexed systems in the relative improvement of reliability and mean life with respect to a nonredundant reference system.

It is also possible that the continuing miniaturization of computers will make hybrid redundancy applicable at the level of an entire computer serving as the non-redundant reference unit. The hybrid-redundant multi-computer system may then serve as the hard core of very large and complex data handling systems, such as those required for spacecraft, automated telephone exchanges, digital communication systems, automated hospital monitoring systems, and time-sharing-utility centers.

TABLE OF SYMBOLS AND NOTATION

λ	Failure rate of a non-redundant active unit, $(\lambda \geq 0)$.
μ	Failure rate of a non-redundant standby-spare unit, $(\mu \leq \lambda)$.
K	Ratio of λ to μ, $(=\lambda/\mu)$, $1 \leq K \leq \infty$.
S	Total number of standby-spare units, $(S \geq 0)$.
N	Total number of active redundant units, $(=2n + 1)$.
n	Degree of active redundancy, $(=(N-1)/2)$.
C	Total number of units in a system, $(=N + S)$.
T	Mission time, (≥ 0).
t or τ	Dummy variables for time, $(0 \leq t \text{ or } \tau \leq T)$.
$\binom{A}{B}$	Combinatorial notation for $\frac{A!}{(A-B)!B!}$.
DD	Disagreement detector.
SU	Switching unit.
R–S–D unit	An abbreviation for the unit which incorporates the restoring organ, switching unit, and the disagreement detector.
Simplex system	A non-redundant unit or system.
TMR system	Triple-modularly redundant system, $(N = 3)$.
NMR system	N-tuple-modularly redundant system.
Hybrid (N, S) system	A hybrid redundant system having a total of $N + S$ units of which N units are active and S units are standby-spares.
$H(N, S)$	An abbreviation for Hybrid (N, S).
$H(N, 0)$	A reduced case of $H(N, S)$ which yields an equivalent system to basic NMR under the assumption of fail-proof R–S–D unit and voter elements.
$H(3, 0)$	A reduced case of $H(N, 0)$ which yields an equivalent system to basic TMR.
R ("System Characterization") ["time"]	The format of a compact notation for simplifying the writing of reliability equations. Here "R" the reliability is followed in parentheses by the "system characterization" such as (N, S), (NMR), (TMR) or (Simplex) and is then succeeded in square brackets by the parameter "time." The parameter "time" is usually the mission time T and this term may be omitted if it is unambiguous to do

so. If the "system characterization" refers to a simplex system, then both the "system characterization" term and the "time" term may be omitted.

Thus,

$R(N, S)[T]$ is the reliability of a hybrid redundant system $H(N, S)$ for a mission time of duration T.

THE N-TUPLY MODULAR REDUNDANT SYSTEM

The basic TMR types of systems are first reviewed and are illustrated in Figure 1. A simplex or nonredundant system having reliability R is shown in Figure 1(a). The reliability of the basic triple-modular or TMR system as shown in Figure 1(b) is given (under the worst-case assumption that no compensating failures occur) by the following well known equation:

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

The generalization of the TMR concepts[7] to an N-tuply modular system utilizing $N = 2n + 1$ units and having a $(n + 1)$ out-of-n-restoring organ is illustrated in Figure 1(c) and is therein designated as the

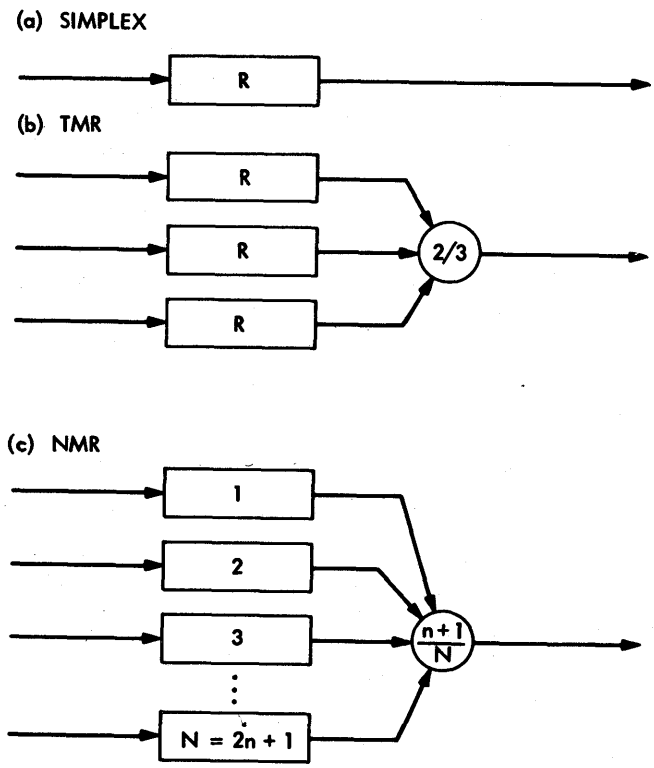


Figure 1—Basic TMR-type systems

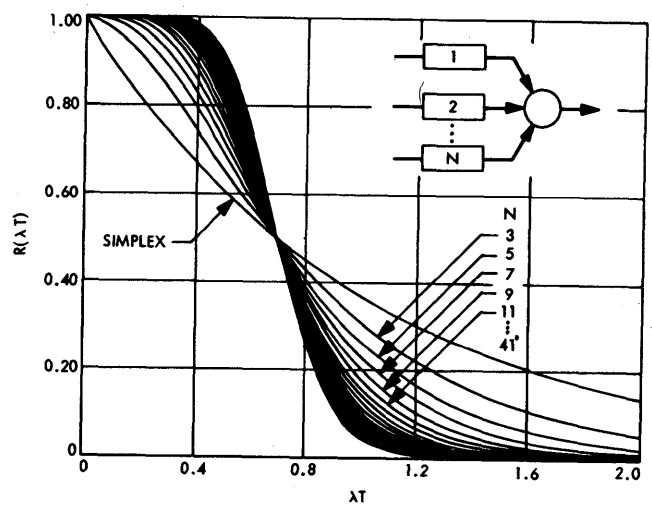


Figure 2—Reliability of NMR-type systems vs normalized time

NMR system; its reliability equation is

$$R(\text{NMR}) = \sum_{i=0}^{n} \binom{N}{i} (1 - R)^i R^{N-i} \qquad (2)$$

where the combinatorial notation $\binom{N}{i} = \dfrac{N!}{(N - i)!\,i!}$

The family of curves illustrating its behavior is shown in Figure 2, with reliability plotted as a function of normalized time λT. The underlying failure law throughout this paper is assumed to be exponential.[8] Thus the simplex reliability R is given by $\exp(-\lambda T)$, where λ is the failure rate of the nonredundant system when it is active. In the ensuing development of the probabilistic model for the Hybrid(N,S) systems, the assumption of statistical independence of failures has been made.

THE HYBRID(N,S) SYSTEM

The Hybrid(N,S) system concept (Figure 3) consists of an NMR core, with an associated bank of S spare units such that when one of the N active units fails, the spare unit replaces it and restores the NMR core to the all-perfect state. The active NMR units have a failure rate designated by λ, while the standby-spare units, which are said to be in a dormant mode,[9] have a failure rate designated by μ $(\mu \leq \lambda)$, with the corresponding reliability $R_s = \exp(-\mu T)$.

The physical realization of such a system is shown in Figure 4, where the disagreement detector (DD) compares the system output from the restoring organ with

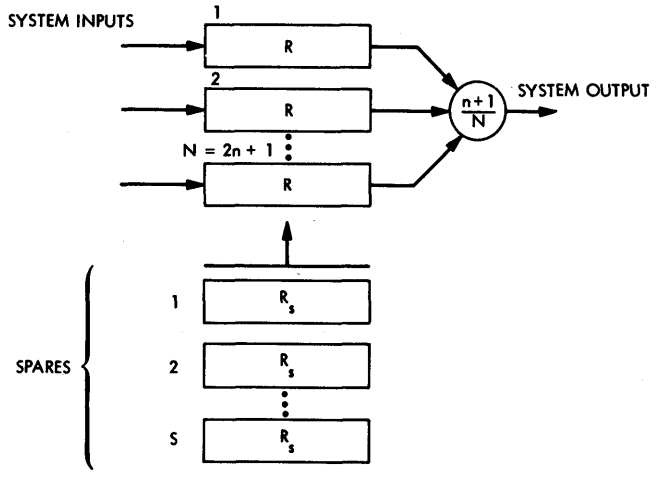


Figure 3—Hybrid (N, S) sytem concept

the outputs of each one of the active $2n + 1$ units. When a disagreement occurs, a signal is transmitted to the switching unit (SU), which replaces the unit that disagreed by switching it out and switching in one of the spares. If the spare were to fail in the dormant mode and was switched in on demand from the DD unit, the disagreement would still exist and the SU would again replace it by one of the spares. The Hybrid(N,S) system reduces to a simple NMR system when all the spares have been exhausted, and the whole system fails upon the exhaustion of all the spares and the failure of any $n + 1$ of the basic $2n + 1$ units. In the special case where $N = 3$ the Hybrid(N,S) system reduces to a Hybrid(3,S) system.[10] In the case of zero spares the Hybrid(3,S) system then reduces to Hybrid(3,0) which is the basic TMR system.

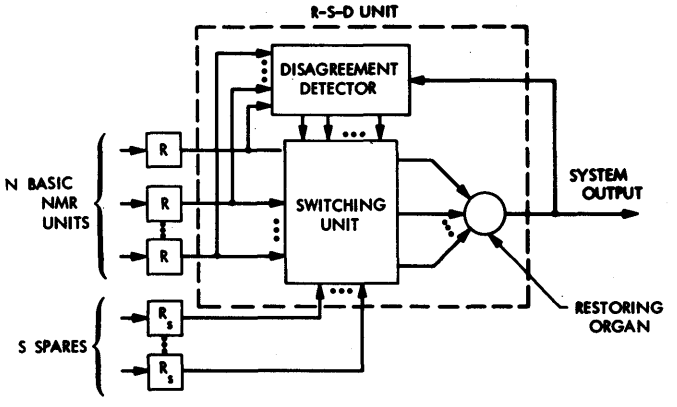


Figure 4—Hybrid (N, S) system block diagram

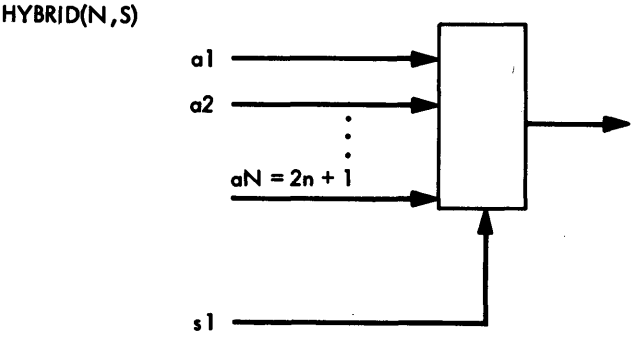
The Hybrid(N,S) system concept has been considered by other researchers from the architectural standpoint.[11,12] A derivation[13] of the reliability equation when dormancy of the S spare units is not considered (i.e., when all the $S + 3$ units in the system are considered to have identical failure rates) yields

$$R(3, S) = 1 - (1 - R)^{S+2}[1 + (R) \cdot (S + 2)]$$

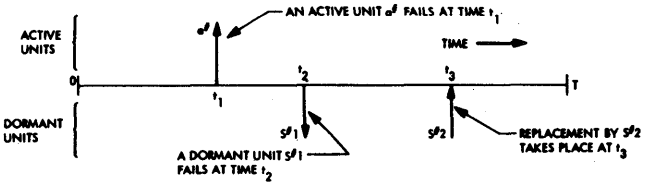
which is simply the probability that at least any two of the total $S + 3$ units survive the mission duration, when assumption is made that the majority organ and associated detection and switching logic are fail-proof.

DERIVATION OF $R(N,S)$, THE CHARACTERISTIC RELIABILITY EQUATION OF THE HYBRID(N,S) SYSTEM

First an expression for the reliability of Hybrid(N,1) system (i.e., $S = 1$) will now be derived. Let the N basic units be designated as $a1$, $a2$, $\cdots aN$, and the spare as $s1$, as follows:



Three cases may be distinguished which yield the success of the system for any mission time T. These three cases are illustrated by means of the line drawings shown in Figure B, Figure C, and Figure D. The notation of these descriptive drawings is explained in Figure A.



The nomenclature in Figure A is the following. The horizontal line represents the time axis from the start of the mission (time = 0) to the end of the mission

(time = T). The region above the lines is the domain of the active units (massively redundant) while the region below the line is the domain of the dormant units (selectively redundant). Arrows leaving the line represent failure of a unit. The direction of the arrow leaving the line towards the active or the dormant domain indicates failure of an active or dormant unit respectively. An arrow going towards the line indicates a replacement action where a dormant unit replaces a failed active unit, thus in Figure A t_3 would equal t_1 since the failure of an active unit demands a replacement from the spare bank.

Case (*i*). All units survive mission time T:

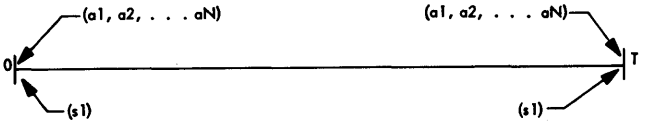
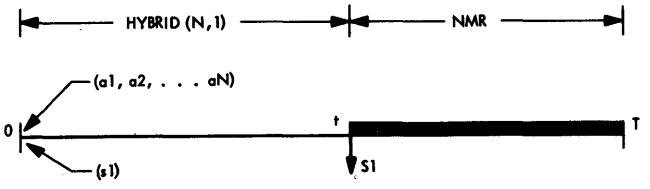


Figure B shows that the active units ($a1$, $a2$, $\cdots$ aN) which were good at time = 0 are still good at time = T and likewise for the dormant unit $s1$. This event has the probability $R^N \cdot R_s$.

Case (*ii*). The spare unit is the first unit to fail:



At some time t ($0 \leq t \leq T$) the spare unit $s1$ fails, leaving the system in basic NMR, i.e., Hybrid(N,0), for the unelapsed time $[T - t]$. The probability of this event is

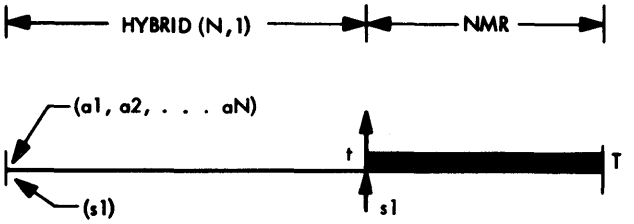
$$\int_0^T e^{-N\lambda t} \cdot \mu e^{-\mu t} \cdot R(N, 0)[T - t]\, dt$$

where

$$R(N, 0)[T - t] = \sum_{i=0}^{n} \binom{N}{i} \cdot (1 - R[T - t])^i \cdot R^{N-i}[T - t]$$

which is the reliability of the basic NMR system for a mission time $[T - t]$.

Case (*iii*). An active unit fails before the spare:



At some time t one of the basic N units fails and is replaced by the spare $s1$, thus leaving the system in basic NMR for the rest of the time $[T - t]$. The probability of this event is:

$$N \int_0^T e^{-\mu t} \cdot \lambda e^{-\lambda t} \cdot e^{-(N-1)\lambda t} \cdot R(N, 0)[T - t]\, dt$$

Summing the above three cases yields

$$R(N, 1)[T] = R^N[T]R_s[T] + (N\lambda + \mu) \int_0^T e^{-(N\lambda+\mu)t} \cdot R(N, 0)[T - t] \cdot dt \quad (3)$$

Similarly it may be shown that for the case of two spares

$$R(N, 2)[T] = R^N[T]R_s^2[T] + (N\lambda + 2\mu) \int_0^T e^{-(N\lambda+2\mu)t} \cdot R(N, 1)[T - t] \cdot dt \quad (4)$$

and, in general, for S spares

$$R(N, S)[T] = R^N[T]R_s^S[T] + (N\lambda + S\mu) \int_0^T e^{-(N\lambda+S\mu)t} \cdot R(N, S - 1)[T - t] \cdot dt \quad (5)$$

which may be rewritten by letting $\tau = T - t$ as

$$= R^N[T]R_s^S[T] \cdot \left\{1 + (N\lambda + S\mu) \int_0^T e^{(N\lambda+S\mu)\tau} \cdot R(N, S - 1)[\tau] \cdot d\tau\right\} \quad (6)$$

The recursive integral equation for the case of one spare ($S = 1$) has the solution

$$R(N, 1)[T] = R^N R_s \left[1 + (NK + 1) \sum_{i=0}^{n} \binom{N}{i} \cdot \sum_{l=0}^{i} \binom{i}{l} \frac{(-1)^{i-l}}{(Kl + 1)} \left(\frac{1}{R_s R^l} - 1\right)\right] \quad (7)$$

and the general solution for $(S > 1)$ is given by

$$R(N, S)[T] = R^N R_s^S \left[1 + \sum_{j=0}^{S-2} \binom{NK+S}{j+1} \cdot \left(\frac{1}{R_s} - 1\right)^{j+1} + \sum_{i=0}^{n} \binom{N}{i} \binom{NK+S}{S} \cdot \sum_{l=0}^{i} \frac{\binom{i}{l}(-1)^{i-l}}{\binom{Kl+S}{S}} \left\{ \left(\frac{1}{R_s^S R^l} - 1\right) - \sum_{j=0}^{S-2} \binom{Kl+S}{j+1} \cdot \left(\frac{1}{R_s} - 1\right)^{j+1} \right\} \right] \quad (8)$$

where $K = \lambda/\mu$; $\mu \leq \lambda$ and $1 \leq K < \infty$.

For the special situation of non-failing spares, we have $K = \infty$, (i.e., $\mu = 0$) and the solutions (7) and (8) reduce to:

(i) for $S = 1$

$$R(N, 1)[T] = R^N \left\{ 1 + \lambda NT(-1)^n \binom{2n}{n} + N \sum_{i=1}^{n} \binom{N}{i} \sum_{j=1}^{i} \binom{i}{j} \frac{(-1)^{i-j}}{j} \left(\frac{1}{R^j} - 1\right) \right\} \quad (7a)$$

(ii) for $S > 1$

$$R(N, S)[T] = R^N \left\{ \sum_{i=0}^{S-1} \frac{(N\lambda T)^i}{i!} + \frac{(N\lambda T)^s (-1)^N}{s!} \cdot \binom{2n}{n} + N^s \sum_{i=1}^{n} \binom{N}{i} \sum_{j=1}^{i} \binom{i}{j} (-1)^{i-j} \cdot \left[\frac{1}{j^s} \left(\frac{1}{R^j} - 1\right) - \sum_{l=1}^{S-1} \frac{(\lambda T)^l}{l!\, j^{s-l}} \right] \right\} \quad (8a)$$

The proof that equations (7) and (8) are the solutions to the recursive integral equation (6) may be verified by inserting them on the righthand side of (6) with parameter equal to $S - 1$. The meanings of all symbols in the above equations are summarized in Table 1.

In the derivation of the above equations it was assumed that the restoring organ, the switching unit, and the disagreement detector (jointly referred to as the R–S–D unit) are fail-proof. In order to incorporate the reliability of these units, they may be assigned a lumped parameter R_v, reflecting their reliability; and with the simplifying assumption that the R–S–D unit has a series reliability relative to the ideal Hybrid (N, S) configuration, the term R_v may be used as a product term to directly modify the reliability equations derived here.

DISCUSSION OF THE MODEL BEHAVIOR

The application of redundancy in general does not necessarily guarantee improvement in reliability. This is especially evident from the characteristic reliability curves of the simple NMR system as shown in Figure 2. It is to be noted that if R (the reliability of the non-redundant unit) is less than 0.5 (i.e., $\lambda T > 0.697$) then the system is worse off with redundancy. Furthermore the application of higher orders of redundancy (larger value of N) makes the system progressively worse. Also one of the characteristics of such a system is that the cross-over point where the redundant system reliability is equal to the non-redundant system reliability does not vary with the order of redundancy N. It sets a large lower bound on the reliability of the original system amenable to improvement by the application of the basic NMR form of redundancy technique.

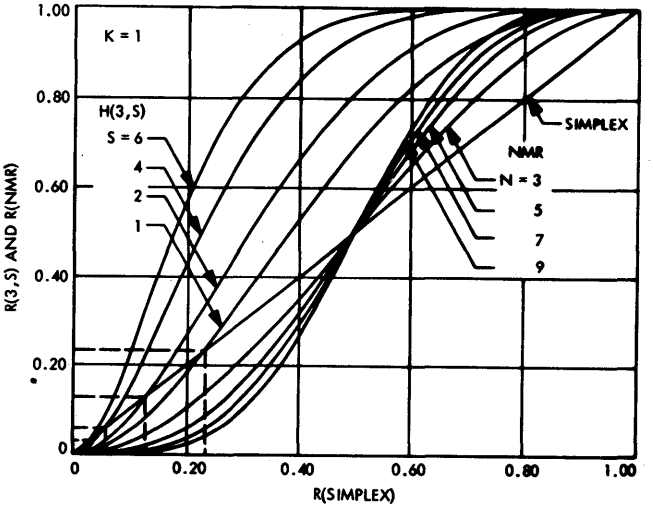


Figure 5—Comparative reliability curves of H (3, S), NMR, and simplex systems

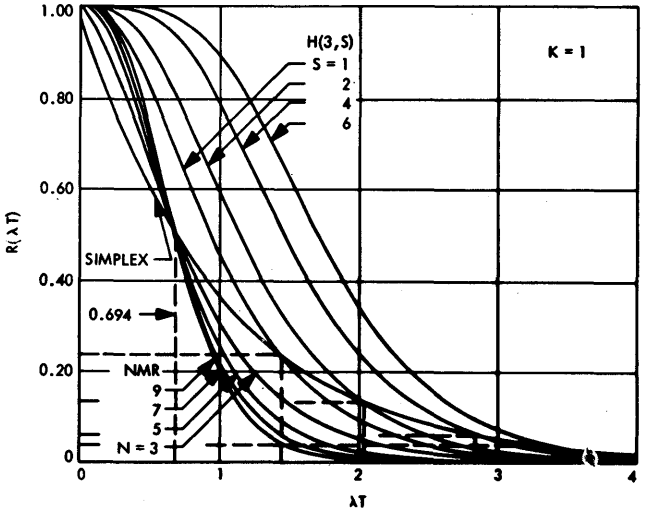


Figure 6—Reliability comparison of a H (3, S) and NMR systems vs normalized time λT

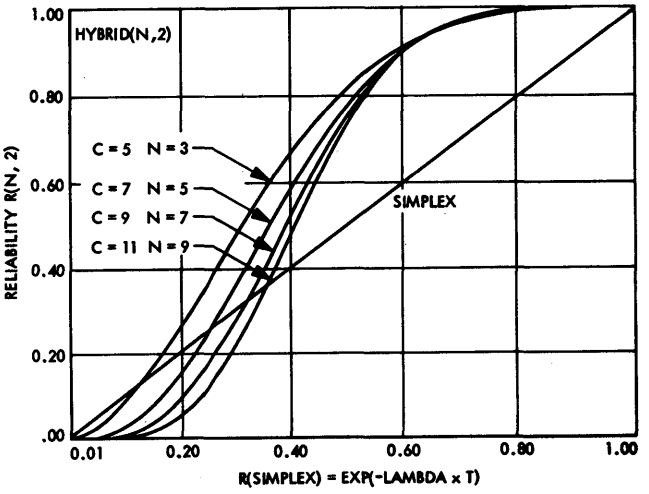


Figure 8—Reliability R (N, 2) vs R (Simplex)

The effects of hybridization (i.e., the addition of standby spares) on the NMR system with the replacement form of redundancy as analytically expressed by equation (8) are shown graphically in Figure 5 through Figure 10. The reliability of the Hybrid(3,S) system for the case of $N = 3$, $K = 1$ and with several values of S (the number of spares) is shown in Figure 5 and Figure 6. Also alongside for comparative purposes the reliability curves of the NMR system and the non-redundant system are also shown. In Figure 7 and Figure 8 are shown the reliability of the Hybrid(N,S) system versus the reliability R of the non-redundant unit for several values of N. They illustrate the effect of the variation of the order of redundancy N in the NMR core. In Figure 9 and Figure 10 are shown reliability curves for $K = 1$ and $K = 10$ respectively for various values of the number of spares S.

The improvement in reliability of the Hybrid(N,S) system over the NMR system is readily seen from the curves. It is to be noted that the well-known crossover point, which in NMR systems occurs at a reliability of 0.5 is significantly reduced in the Hybrid(N,S) system. With $N = 3$ and $S = 1$ the crossover point occurs at $R = 0.233$ for the value of $K = 1$, and rapidly diminishes with higher allocation of the number of spares ($S > 1$). The shift in the crossover point is also

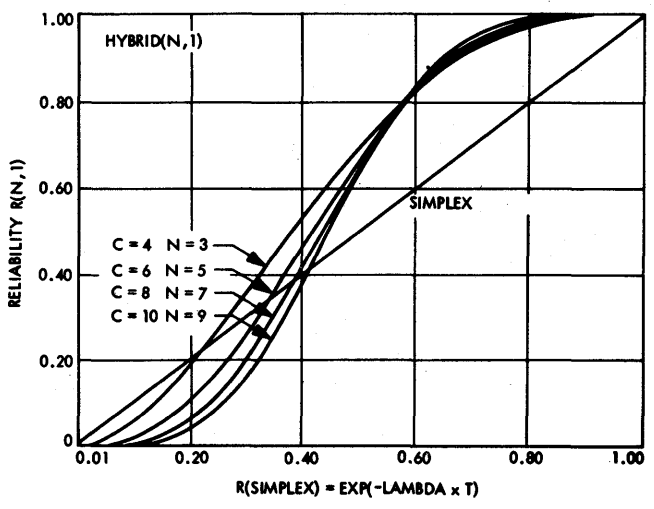


Figure 7—Reliability R (N, 1) vs R (Simplex)

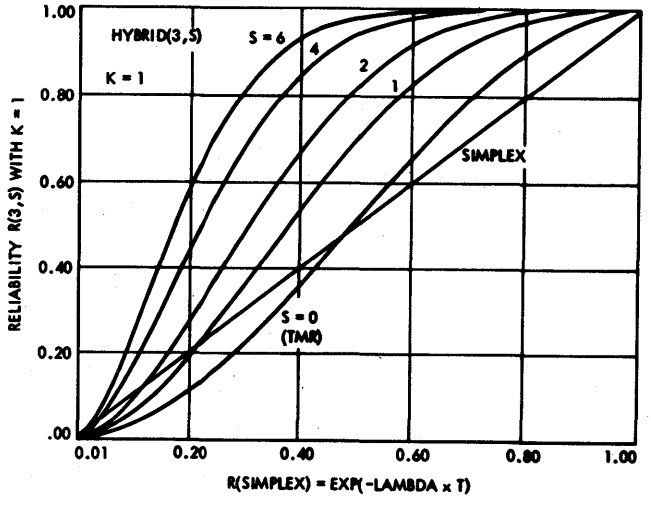


Figure 9—R (3, S) vs R (Simplex) with $K = 1$

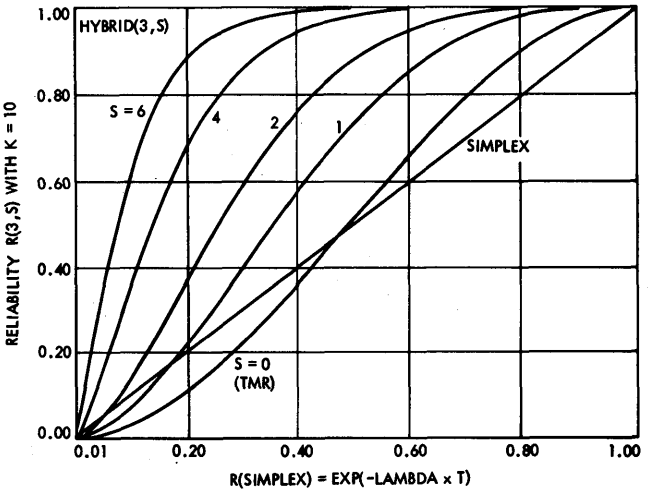


Figure 10—R (3. S) vs R (Simplex) with $K = 10$

sensitive to variations in the value of K. The effect of changes in values of K on the system reliability and the shifts of the crossover point become very slight when K exceeds the value of 10.

The decision as to how to allocate redundancy for a given total number of units $C = N + S$, where N is the number of active redundant units in the NMR core and S is the number of standby spares, is resolved by the curves shown in Figure 7 and Figure 8. Since N is always an odd number it follows that if C is odd then S is even and vice versa. The possible allocation policies are then as tabulated below.

With one spare, $S = 1$, as shown in Figure 7 the improvement in reliability in going to higher order N of active redundancy is restricted to the range $0.58 < R < 1$. When the number of spares is increased to two, $S = 2$, with N as the variable, the range of improved reliability is further restricted to $0.65 < R < 1$. Also, within this shrinking range (as a function of increased S), the improvement in reliability due to larger values of N also tends to become less significant. This indicates that the order of massive redundancy N should be kept at a minimum in the NMR core (i.e., $N = 3$). Maximum redundancy should be inserted in the spares bank, thus in practical implementation N should equal three, with S as variable to suit the desired level of mission reliability.

TABLE II

ALL POSSIBLE ALLOCATION POLICIES OF C

C_0 is odd		C_e is even	
$N = 3$	$S = C_0 - 3$	$N = 3$	$S = C_e - 3$
$N = 5$	$S = C_0 - 5$	$N = 5$	$S = C_e - 5$
.	.	.	.
.	.	.	.
.	.	.	.
$N = N$	$S = C_0 - N$	$N = N$	$S = C_e - N$
.	.	.	.
.	.	.	.
.	.	.	.
$N = C_0 - 2$	$S = 2$	$N = C_e - 3$	$S = 3$
$N = C_0$	$S = 0$	$N = C_e - 1$	$S = 1$

Hardware utilization and hence cost is another major advantage of the Hybrid(N,S) redundant system. Efficient hardware utilization over comparable NMR systems is due to the fact that for an equal number of total N units the NMR system will tolerate failures of only $(N - 1)/2$ units whereas the Hybrid $(3,S)$ system will tolerate as many as $N - 2$ failures. Thus when an NMR system fails it leaves behind n good units while in the Hybrid$(3,S)$ system only one good unit remains upon system failure. In general the Hybrid(N,S) system upon exhaustion of all spares and subsequent failure of the system leaves $(N - 1)/2$ good operating units which is a minimum when $N = 3$. Thus another argument for keeping the parameter N confined to the value three in Hybrid(N,S) system is this of efficient hardware utilization.

ACKNOWLEDGMENTS

The authors wish to thank William F. Scott, John J. Wedel, and George R. Hansen of the Flight Computers and Sequencers Section of the Astrionics Division of the Jet Propulsion Laboratory for their constant encouragement and for providing the atmosphere conducive to this research. Thanks are also due to Prof. Leonard Kleinrock of the University of California, Los Angeles for his advice on the subject of queueing theory; the notation used herein to describe the dynamics of replacement has been adapted from similar notation used to describe the behavior of queues.

This paper represents in part research which has been carried out at the Jet Propulsion Laboratory under NASA Contract NAS7-100.

REFERENCES

1 S AUROBINDO
Savitri—A legend and a symbol
Sri Aurobindo International University Centre Collection
Vol II Pondicherry India 1954

2 J VON NEUMANN
Probabalistic logics and the synthesis of reliable organisms from unreliable components
In Automata Studies p 43–98 Princeton University Press
Princeton New Jersey 1956

3 E F MOORE C E SHANNON
Reliable circuits using less reliable relays
J of the Franklin Institute Vol 262 Pt I pp 191–208 and Vol 262 Pt II p 281–297 1956

4 J E ANDERSON F J MACRI
Multiple redundancy application in a computer
Proc 1967 Annual Symposium on Reliability p 553–562 Washington 1967

5 A A AVIZIENIS
Design of fault-tolerant computers
AFIPS Conference Procedings Vol 31 p 733–743 1967

6 A A AVIZIENIS F P MATHUR D RENNELS J ROHR
Automatic maintenance of aerospace computers and spacecraft information and control systems
Proc of the AIAA Aerospace Computer Systems Conference Paper 69–966
Los Angeles September 8–10 1969

7 J K KNOX-SEITH
Improving the reliability of digital systems by redundancy and restoring organs
PhD thesis Electrical Engineering Stanford University August 1964

8 R F DRENICK
The failure law of complex equipment
J Soc Ind Appl Math Vol 8 No 4 p 680–690 December 1960

9 F P MATHUR
Reliability study of fault-tolerant computers
In Supporting Research and Advanced Development Space Programs Summary 37–58 Vol III p 106–113 Jet Propulsion Laboratory Pasadena California August 31 1969

10 F P MATHUR
Reliability modeling and analysis of a dynamic TMR system utilizing standby spares
Proc of the Seventh Annual Allerton Conference on Circuit and Systems October 20–22 1969

11 J GOLDBERG K N LEVITT R A SHORT
Techniques for the realization of ultrareliable spaceborne computers
Final Report Phase I Project 5580 Stanford Research Institute Menlo Park California October 1967

12 J GOLDBERG M W GREEN K N LEVITT H S STONE
Techniques for the realization of ultrareliable spaceborne computers
Interim Scientific Report 2 Project 5580 Stanford Research Institute Menlo Park California October 1967

13 J P ROTH W G BOURICIUS W C CARTER P R SCHNEIDER
Phase II of an architectural study for a self-repairing computer
International Business Machines Corporation Report SAMSO TR-67-106 November 1967