NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Report 32-1467

Reliability Modeling and Analysis of a Dynamic TMR System Using Standby Spares

F. P. Mathur

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

November 1, 1969

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Report 32-1467

Reliability Modeling and Analysis of a Dynamic TMR System Using Standby Spares

F. P. Mathur

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

November 1, 1969

Prepared Under Contract No. NAS 7-100
National Aeronautics and Space Administration

Preface

The work described in this report was performed by the Astrionics Division of the Jet Propulsion Laboratory, and was presented originally to the *Seventh Annual Allerton Conference on Circuit and System Theory,* held at the University of Illinois, Urbana, October 8–10, 1969.

Acknowledgment

Especially helpful were Mr. William F. Scott, Mr. John J. Wedel, Jr., and Mr. George R. Hansen for providing the atmosphere conducive to this research and for their encouragement. Special thanks are also due Dr. Ho-sen Lin for his many helpful suggestions regarding the mathematics given here. Particularly, the author is deeply grateful to Professor Algirdas A. Avizienis for introducing him to the subject of fault-tolerance and for the skillful and generous guidance given in negotiating the abundance of literature available in this field.

Contents

Figures

Abstract

A dynamic TMR (triple modularly redundant) system using standby spares, referred to as the TMR/Spares system in this report, is developed, modeled, and analyzed. The characteristic reliability equation of such a system is derived. The behavior of the system reliability as a function of the nonredundant system and normalized time is plotted and comparisons are made with conventional TMR systems. The TMR/Spares model is considered to be a major addition to the redundancy techniques available to the designer of fault-tolerant computers.

Reliability Modeling and Analysis of a Dynamic TMR System Using Standby Spares

I. Introduction

The use of protective redundancy to enhance reliability (Refs. 1 and 2)—once every step has been taken under the limitations of the prevailing state of technology to select, screen, and package highly reliable components—has, as a result of the research conducted and applications made in this field over the last decade (Refs. 3 and 4), found wide acceptance as a fundamental procedure, and is a process that nature in her apparent working sanctions (Ref. 5).

Protective redundancy has been classified as being either massive or selective, and as static or dynamic. The first classification springs from an organizational point of view (Ref. 2), the latter from a functional point of view (Ref. 6). This report presents a system concept that is a hybrid because it uses both static and dynamic redundancy. It is a combination of two well-known techniques, triple modular redundancy (TMR) and replacement system (RS) redundancy.

II. The TMR/Spares System

The simple, TMR types of systems are first reviewed and are illustrated in Fig. 1. A simplex, or nonredundant, system having reliability R or $R(T)$ is shown in Fig. 1a. Throughout this report the term *reliability* means the probability that a system required to perform a certain task will not malfunction prior to its mission time T. The reliability of a simple TMR system as shown in Fig. 1b is given by the following well-known equation:

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

The generalization of the TMR concepts (Ref. 7) to a system using $\eta = 2N + 1$ units and having an $N + 1/\eta$ restoring organ is illustrated in Fig. 1c and is designated as the NMR system; its well-known reliability equation is

$$R_{\text{NMR}} = \sum_{i=0}^{N} \binom{\eta}{i} (1 - R)^i R^{\eta - i} \tag{2}$$

The family of curves illustrating the behavior of the NMR system is shown in Fig. 2, with reliability plotted as a function of normalized time λT.

The underlying failure law will be assumed to be exponential (Ref. 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 TMR/Spares systems, the assumption of statistical independence of failures has been made.

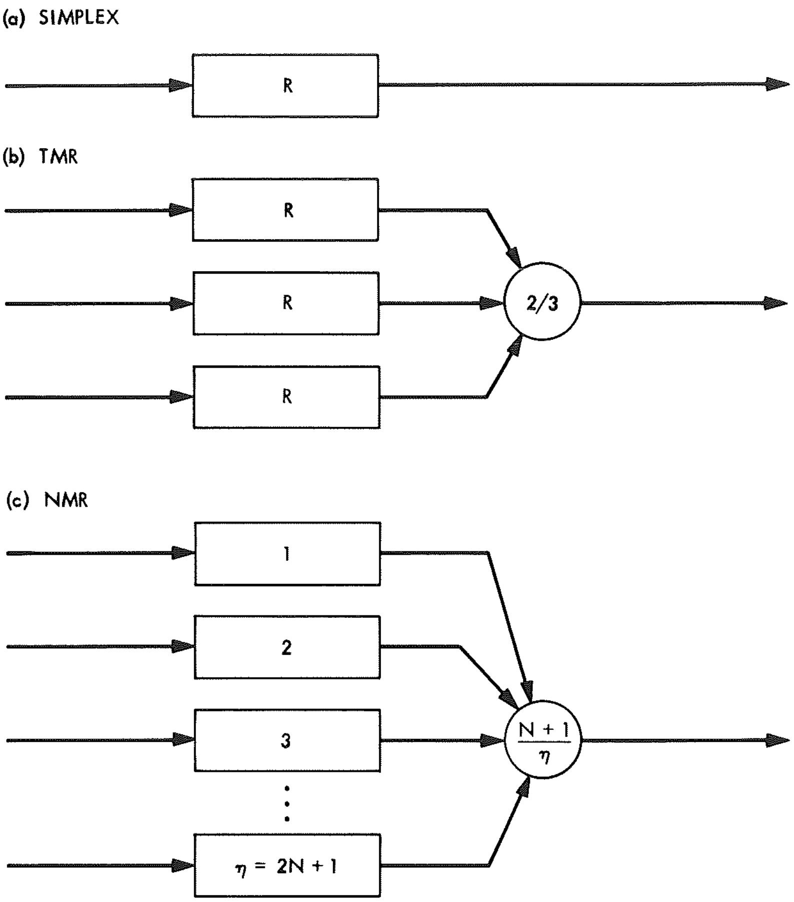


Fig. 1. Simple TMR types of systems

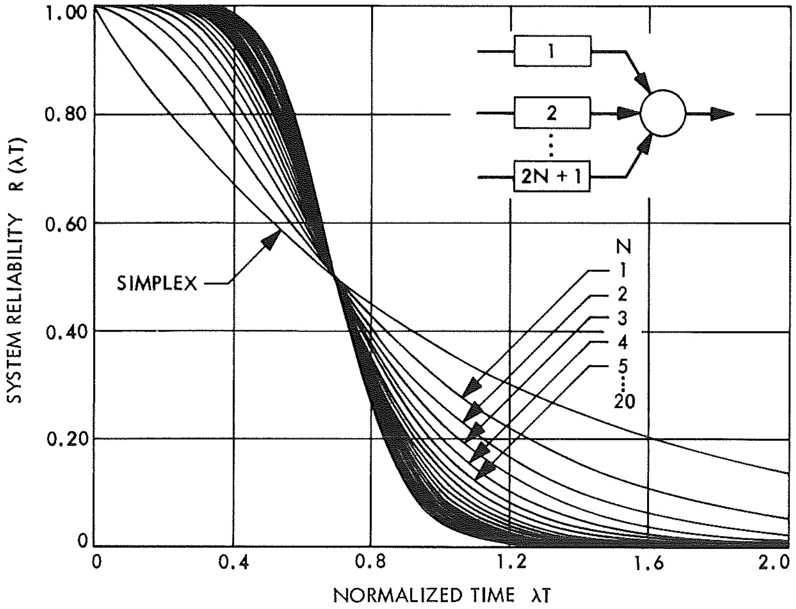


Fig. 2. Reliability of NMR types of systems vs normalized time λT

The TMR/Spares system concept (Fig. 3) consists of a TMR core, with an associated bank of S spare units configured so that when one of the basic TMR units fails the spare unit replaces it and restores the TMR core to the all-perfect state. The active TMR units have a failure rate designated by λ, while the standby spare units, which are said to be in a dormant mode (Ref. 9), have a failure rate designated by μ ($\mu \leqq \lambda$), with the corresponding reliability $R_s = \exp(-\mu T)$. The physical realization of such a system is shown in Fig. 4, where the disagreement detector compares the system output with each one of the basic triplicated units. When a disagreement occurs, a signal is transmitted to the switching unit which replaces the disagreeing unit by switching it out and switching in one of

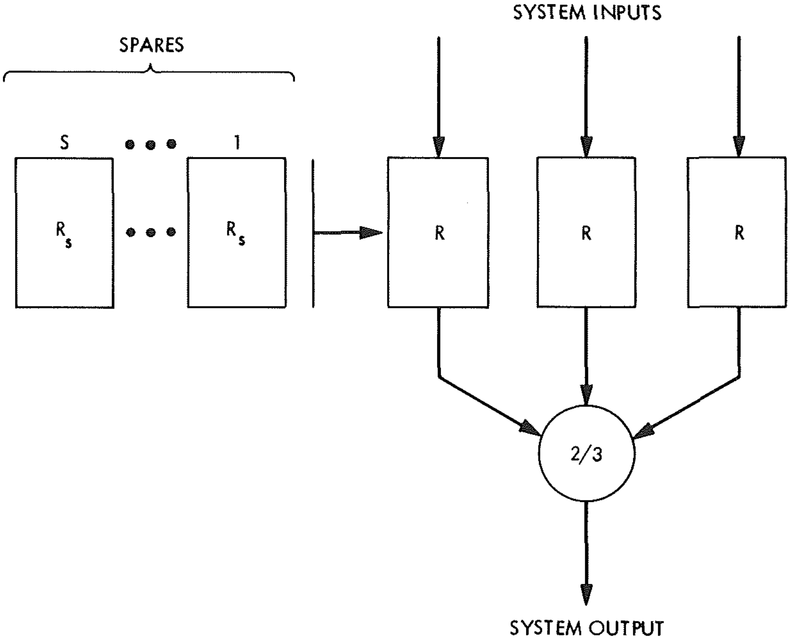


Fig. 3. TMR/Spares system concept

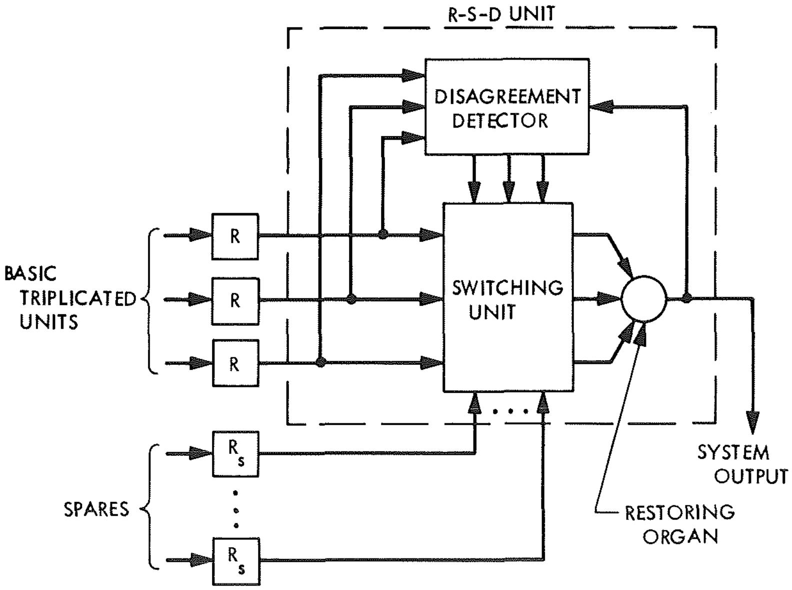


Fig. 4. TMR/Spares system block diagram

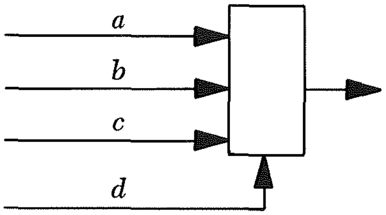
the spares. If the spare fails while in the dormant mode, the disagreement will still exist and the switching unit will replace it with another spare. The TMR/Spares system reduces to a simple TMR system when all the spares have been exhausted, and the whole system fails upon the exhaustion of all the spares and the failure of any two of the basic triplicated units.

The TMR/Spares system concept has been considered in other research from the architectural standpoint (Refs. 10 and 11). A basic derivation (Ref. 12) of the reliability equation when dormancy of the spare units is not considered (i.e., when all the S + 3 units in the system are considered to have identical failure rates) yields

$$R_{\mathrm{TMR/S}} = 1 - (1 - R)^{S+2} \left[1 + R \times (S + 2)\right] \qquad (3)$$

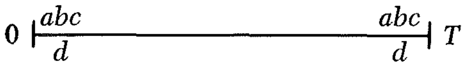
which is simply the probability that at least any two of the total S + 3 units survive the mission duration.

An expression for the reliability of a TMR/1 system (i.e., a TMR/Spares system with one spare) is now derived. Let the three basic triplicated units be designated as a, b, and c, and the spare as d, as follows:



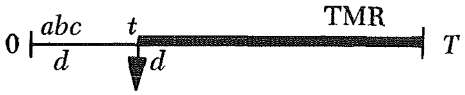
Three cases may be distinguished which yield the success of the system for any mission time T.

Case 1. All units survive time T:



This event has the probability $R^3 R_s$.

Case 2. The spare unit is the first to fail:



At some time t the spare unit d fails, leaving the system in basic TMR for the unelapsed time $[T - t]$. The probability of this event is

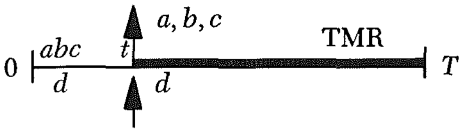
$$\int_0^T e^{-3\lambda t} \mu\, e^{-\mu t} R_{\mathrm{TMR/0}} [T - t]\, dt$$

where

$$R_{\mathrm{TMR/0}} [T - t] = R^3 [T - t] + 3R^2 [T - t] (1 - R [T - t])$$

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

Case 3. An active unit fails before the spare:



At some time t either a or b or c fails and is replaced by the spare d, thus leaving the system in basic TMR for the rest of the time $[T - t]$. The probability of this event is

$$3 \int_0^T \lambda\, e^{-\lambda t} e^{-\mu t} e^{-2\lambda t} R_{\mathrm{TMR/0}} [T - t]\, dt$$

Summing these three cases yields

$$R_{\mathrm{TMR/1}} [T] = R^3 (T) R_s (T) + (3\lambda + \mu) \times \int_0^T e^{-(3\lambda+\mu) t} R_{\mathrm{TMR}} [T - t]\, dt \qquad (4)$$

Similarly, it may be shown that

$$R_{\mathrm{TMR/2}} [T] = R^3 (T) R_s^2 (T) + (3\lambda + 2\mu) \times \int_0^T e^{-(3\lambda+2\mu) t} R_{\mathrm{TMR/1}} [T - t]\, dt \qquad (5)$$

and, in general,

$$R_{\mathrm{TMR/S+1}}\,[T] = R^3(T)\,R_s^{S+1}(T) + [3\lambda + (S+1)\,\mu]\int_0^T e^{-[3\lambda+(S+1)\mu]\,t}\,R_{\mathrm{TMR/S}}\,[T-t]\,dt \tag{6}$$

which may, by making the appropriate substitution, be rewritten as

$$\mathrm{R}_{\mathrm{TMR/S+1}}\,[T] = R^3(T)\,R_s^{S+1}(T)\left\{1 + [3\lambda + (S+1)\,\mu]\int_0^T e^{+[3\lambda+(S+1)\mu]\,\tau}\,R_{\mathrm{TMR/S}}\,[\tau]\,d\tau\right\} \tag{7}$$

The recursive Eq. (7) has the solution

$$R_{\mathrm{TMR/S}} = 3R^2\left\{\prod_{i=0}^{S-1}\left(\frac{3K+S-i}{K+S-i}\right) - \frac{2RK^2}{S!}\left[\prod_{i=0}^{S-1}(3K+S-i)\right]\sum_{i=0}^{S}\binom{S}{i}\frac{(-R_s)^{S-i}}{(K+S-i)\,(3K+S-i)}\right\} \tag{8}$$

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

$$\binom{S}{i} = \frac{S!}{(S-i)!\,i!}$$

For the special situation $K = \infty$, i.e., $\mu = 0$, the solution (8) reduces to

$$R_{\mathrm{TMR/S}} = 3^{S+1}\,e^{-2\lambda T} - e^{-3\lambda T}\left[\sum_{i=0}^{S}\frac{(3\lambda T)^i}{i!}\,(3^{S+1-i} - 1)\right] \tag{9}$$

An alternative way of writing Eq. (8) is

$$R_{\mathrm{TMR/S}} = 3R^2\left[\frac{\binom{3K+S}{3K}}{\binom{K+S}{K}} - 2RK^2\binom{3K+S}{3K}\sum_{i=0}^{S}\binom{S}{i}\frac{(-R_s)^{S-i}}{(K+S-i)\,(3K+S-i)}\right] \tag{10}$$

The proof that Eq. (10) is the solution to the recursive integral Eq. (7) can be verified by inserting Eq. (10) in the right-hand side of Eq. (7).

In the derivation of the system 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. To incorporate the unreliability of these units, a lumped parameter R_v, reflecting their reliability, may be assigned; and with the simplifying assumption that the R-S-D unit has a series reliability relative to the ideal TMR/Spares configuration, the term R_v may be used as a product term to directly modify Eqs. (8), (9), and (10).

The behavior of Eq. (10) is shown graphically in Fig. 5 for the case in which $K = 1$. Reliability is plotted versus the nonredundant unit, i.e., the simplex system having reliability R. A family of curves for the number of spares equal to 6, 4, 2, and 1 is shown; for comparison, the reliability curves of the generalized TMR system (NMR) as given by Eq. (2) are also shown. The same family of curves is also shown in Fig. 6 as a function of normalized time λT.

III. Conclusion

The TMR/Spares system has been developed, and its characteristic reliability equation was derived and analyzed under the assumptions of statistically independent failures and an exponential failure law, and under conditions of dormant failure rates for the spares. The behavior of the equations as a function of the nonredundant system and normalized time has been shown graphically. From these curves, the improvement in reliability resulting from the hybridization of simple TMR with RS redundancy is readily seen. It is to be noted that the well-known crossover point (which in NMR systems occurs at a reliability of 0.5, with the resulting manifold constraints in practical implementation of such systems) in the TMR/Spares system having only one spare is reduced to a maximum value of 0.233, and may be further reduced by allocating more spares. Another major advantage in hardware and cost of the TMR/Spares system over the NMR system is that for an equal number of total units η the NMR system will tolerate failures of only $\eta/2$ units, whereas the TMR/Spares system will tolerate $\eta - 2$ failures.

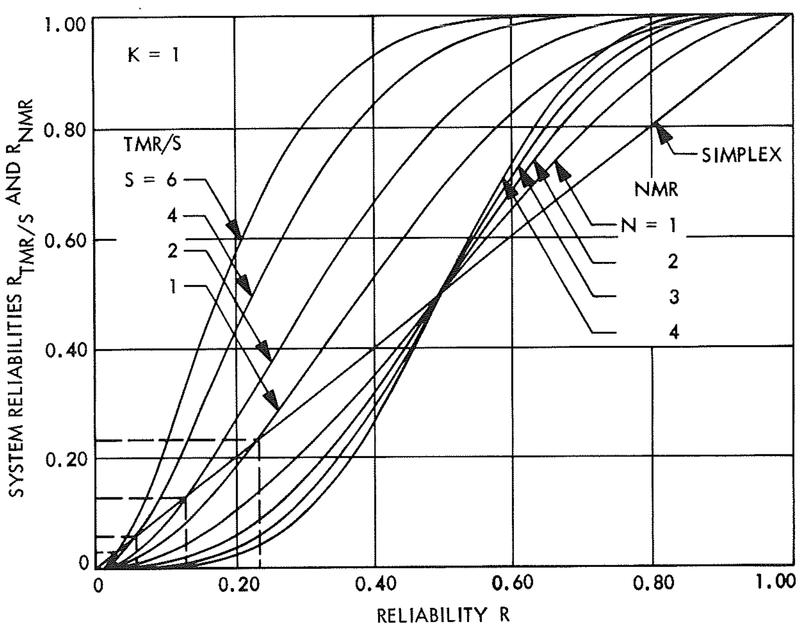


Fig. 5. Comparative reliability curves of TMR/Spares and NMR systems as a function of the simplex reliability *R*

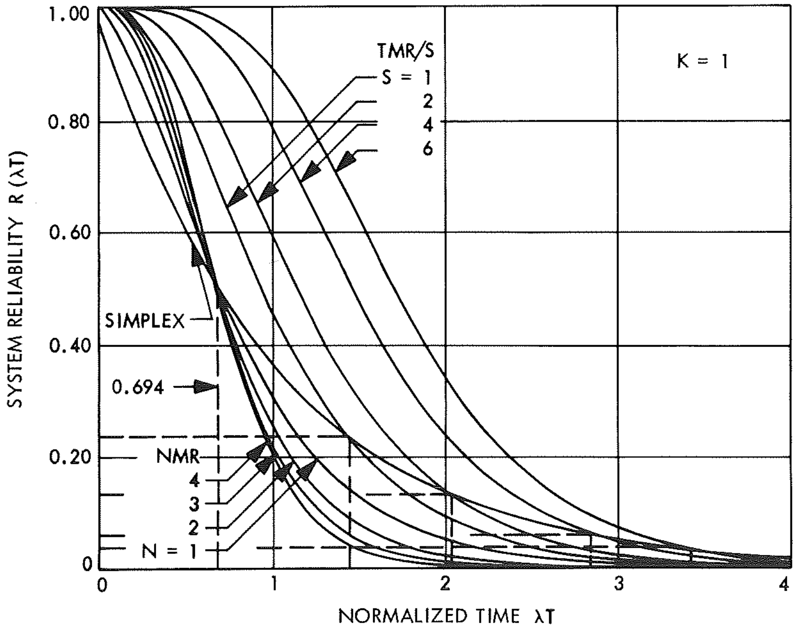


Fig. 6. Comparative reliability curves of TMR/Spares and NMR systems as a function of the normalized time λ*T*

References

1. Moore, E. F., and Shannon, C. E., "Reliable Circuits Using Less Reliable Relays," *J. Franklin Inst.*, Vol. 262, Pt. I, pp. 191–208, and Vol. 262, Pt. II, pp. 281–297, 1956.

2. Avizienis, A. A., "Design of Fault-Tolerant Computers," in *Conference Proceedings of The American Federation of Information Processing Societies,* Vol. 31, proceedings of the Fall Joint Computer Conference, Anaheim, Calif., Nov. 14–16, 1967. Thompson Book Company, Washington, D.C.

3. Avizienis, A. A., Mathur, F. P., Rennels, D., and Rohr, J., "Automatic Maintenance of Aerospace Computers and Spacecraft Information and Control Systems," Paper 69-966, presented at the AIAA Aerospace Computer Systems Conference, Los Angeles, Sept. 8–10, 1969.

4. Anderson, J. E., and Macri, F. J., "Multiple Redundancy Applications in a Computer," in *Proceedings of the 1967 Annual Symposium on Reliability,* Washington, D.C., Jan. 10–12, 1967, pp. 553–562. Institute of Electrical and Electronics Engineers, Inc., New York, N.Y.

5. von Neumann, J., "Probabalistic Logics and the Synthesis of Reliable Organisms From Unreliable Components," in *Automata Studies*, pp. 43–98, Princeton University Press, Princeton, N.J., 1956.

6. Short, R. A., "The Attainment of Reliable Digital Systems Through the Use of Redundancy—a Survey," *Computer Group News,* pp. 2–17, March 1968.

7. Knox-Seith, J. K., "Improving and Reliability of Digital Systems by Redundancy and Restoring Organs," Ph.D. thesis, Department of Electrical Engineering, Stanford University, August 1964.

8. Drenick, R. F., "The Failure Law of Complex Equipment," *J. Soc. Ind. Appl. Math.*, Vol. 8, No. 4, pp. 680–690, December 1960.

9. Mathur, F. P., "Reliability Study of Fault-Tolerant Computers," in *Supporting Research and Advanced Development,* Space Programs Summary 37-58, Vol. III, pp. 106–113. Jet Propulsion Laboratory, Pasadena, Calif., Aug. 31, 1969.

10. Goldberg, J., Levitt, K. N., and Short, R. A., *Techniques for the Realization of Ultrareliable Spaceborne Computers,* Final Report—Phase I, Project 5580, Stanford Research Institute, Menlo Park, Calif., October 1967.

11. Goldberg, J., Green, M. W., Levitt, K. N., and Stone, H. S., *Techniques for the Realization of Ultrareliable Spaceborne Computers,* Interim Scientific Report 2, Project 5580, Stanford Research Institute, Menlo Park, Calif., October 1967.

12. Roth, J. P., Bouricius, W. G., Carter, W. C., and Schneider, P. R., *Phase II of an Architectural Study for a Self-Repairing Computer,* International Business Machines Corporation, Watson Research Center, Watson Heights, N.Y. Report SAMSO TR-67-106, November 1967. Also, AD-825460, Defense Documentation Center, Alexandria, Va.

NASA — JPL — Coml., L.A., Calif.