IEEE Transactions on Nuclear Science, Vol. NS-26, No. 3, June 1979

FAULT-TOLERANT TECHNIQUES FOR RADIATION ENVIRONMENTS*

Ronald C. DeVries

Abstract

This paper reports on a study made on the use of fault-tolerant systems in radiation environments for radiation hardening and hardness assurance purposes. The fault-tolerant systems studied in depth are TMR, TMR/Simplex, Switching Redundancy, Self-Purging Redundancy, and Radial Logic. Failure distributions were obtained for a number of components and for various radiation environments. These were used to graph radiation related indicators as a function of radiation level. One indicator relates to radiation hardness and a second relates to hardness assurance. The effects of imperfect switches and voters and of system size and system sectioning were considered. Finally, the chosen systems were ranked with respect to radiation hardness and hardness assurance.

Introduction

Present and future military systems are generally required to operate sucessfully in the unique environment generated by a nuclear burst in addition to the conventional environments such as temperature, shock, humidity, etc. The same is true of systems designed for operation in a space environment where radiation is a constant hazard. Electronic components are particularly susceptible to radiation in such environments, radiation which includes neutrons, gamma rays, X-rays, and electromagnetic pulses (EMP). This paper considers a systems approach to radiation hardness and hardness assurance, that of fault-tolerant techniques.

Fault-tolerant techniques use redundancy to mask or otherwise bypass faults in a circuit. The advent of Large Scale Integration (LSI) has made the use of redundancy in military systems feasible. Circuit complexity can be greatly increased without any significant penalty in either power or speed, and this increase in complexity allows the use of fault-tolerant techniques that was only possible before in manned space programs. The fault-tolerant techniques increase reliability and quality assurance for both conventional and radiation environments. Fault-tolerant techniques were studied with the intent of using them in military and space applications requiring tolerance to various radiation environments.[1]

*This work was supported by the Defense Nuclear Agency Subtask TD043 and monitored by the Air Force Weapons Laboratory (ELP), Air Force Systems Command, United States Air Force Kirtland Air Force Base, New Mexico 87117, under contract F29601-75-C-0041 with U.N.M.

The author is with the Department of Electrical Engineering and Computer Science, University of New Mexico, Albuquerque, New Mexico 87131.

Manuscript received August 28, 1978

A circuit designed for a radiation environment must be capable of withstanding a certain level of radiation without failing. The level at which the circuit fails is a measure of its radiation hardness. The task of radiation hardening a circuit is then one of increasing the radiation level at which the circuit fails. Hardness assurance, on the other hand addresses itself to the variability among devices which cause the circuits in which they are used to fail at different levels. The task of providing hardness assurance is one of assuring that the parts actually used will result in circuits surviving to the specified radiation level. In this paper, radiation hardness and hardness assurance will be related to calculable indicators which give a measure of hardness and hardness assurance.

The approach taken in the study was first to determine what fault-tolerant schemes are in use or have been proposed and to determine their applicability to use in a radiation environment. Some schemes were discarded and others were retained for further study. Failure distributions were then obtained for a number of components and for various radiation environments. Computer programs were written to graph radiation for two indicators. Ideal switches and voters were assumed initially, and later the programs were modified to include the non-ideal case. The effects of both system size and system sectioning were considered. Finally, the remaining schemes were compared and ranked with respect to radiation hardness and hardness assurance. A basic assumption made throughout the study is that components do not deteriorate with time or under use and that all deterioration is due solely to the radiation itself. The objective was to analyze the situation in which the dominant cause of failure is the stress due to radiation. Certainly other forms of stress, e.g., time dependent stress, can be included in the model, but this was not done.

Fault-Tolerant Techniques

By fault-tolerance is meant the ability of a system to produce the correct output in the presence of a certain limited set of transient and/or permanent faults. Systems which employ redundancy to provide fault tolerance are referred to as fault-tolerant systems. The fault may be caused by any one of a number of stresses, the particular stresses of interest here being radiation induced. Fault-tolerant systems can be divided up a number of ways into categories. These categories are considered next.

One major way of dividing up fault-tolant systems is into static and reconfigurable systems. A redundancy scheme is called static if its structure does not intentionally change throughout the mission time. All parts or sections actively participate in producing the output of the system. Each part remains powered and no new parts or sections ever

0018-9499/79/0600-4320$00.75 © 1979 IEEE

become activated or prevented from further participation, e.g., by forcing its output to be a constant. (The output might unintentionally become a constant due to a fault, however.) By reconfigurable is meant any system whose structure can be intentionally changed during the course of the mission due to a sensed error. Spare units, either powered or unpowered, can replace faulty units, or units can be prevented from further active participation by turning off the power to the unit or logically nullifying its effect on the result.

The categorization of systems into static and reconfigurable was chosen because of the manner in which transient faults are handled by each. Static systems tend to handle transient faults well; whereas, reconfigurable systems do not. The problem with reconfigurable systems is that transient faults cause restructuring of the system just as do permanent faults. Such reconfiguration due to transient faults is undesirable since it results in the loss of good parts. Therefore, reconfigurable systems are often equipped with retry capabilities in which one or more past operations are performed over again. If the error persists, the fault is assumed to be permanent, and reconfiguration takes place. Otherwise, the fault is assumed to have been temporary and operation is continued without reconfiguration.

Fault-tolerant systems can also be devided into masking and error-evident systems. In masking redundancy, error propagation is limited. The error is either eliminated by a restoring organ or interface of some kind and, at least in static systems, operation continues normally. Error correction can be thought of as instantaneous. In error-evident schemes, an error is detected and acted upon in some way. Most error-evident schemes are reconfigurable ones, and the error generally forces a reconfiguration of the system to take place. About the only way of obtaining error correction in a static system upon detection is through retry, and that is only useful for transient errors. (An exception would be the use of a different algorithm in a computer, for example, where the algorithm does not use the faulty component).

Figure 1 shows most of the fault-tolerant systems that were studied and the categories into which they have been placed. The number of such systems proved to be too great to study all of them in detail. Furthermore, some of the systems are not worth considering in a radiation environment. Therefore, certain of the systems were eliminated from further consideration. The specific systems chosen for further study are TMR (Triple Modular Redundancy), TRM/Simplex, Self-purging, and Switching Redundancy. Radial logic was also retained with the recognition that it is only applicable to a limited set of technologies. A brief discussion of each follows.

Triple Modular Redundancy[2] (TMR) is a static, masking redundancy scheme. In this scheme, the outputs of three identical circuits having identical inputs are applied to a majority gate (voter) and the output is the majority. (Single errors are corrected.) If R is the reliability of one of the units and V is the reliability of the voter, the reliability of the TMR circuit is

$$R_{TMR} = V[3R^2 - 2R^3] \quad (1)$$

The majority circuit is what has been called a restoring organ. In systems with restoring organs it is possible to use more than one restoring organ, in this case one per module, in order to prevent faults in the restoring organ from causing system failure. If the outputs of the units are fed to three majority gates producing three outputs which in turn become inputs to yet other such circuits, the reliability of the voters can be considered as part of the network which it drives. The reliability of a segment consisting of 3 units and 3 voters is

$$R_{TMR3} = 3R^2V^2 - 2R^3V^3 \quad (2)$$

A variation of TMR is TMR/simplex[3] which is a reconfigurable, masking redundancy scheme in which discrepancies in the outputs of the units are detected and cause a reconfiguration of the TMR system. Specifically, when an error is detected, the failed unit and one of the good units are discarded leaving one remaining good unit. The reliability of such a system if voters are ignored is

$$R_{TMR/S} = 1.5R - 0.5R^3 \quad (3)$$

where R is again the reliability of a single unit.

Self-purging[4] is a reconfigurable, masking redundancy scheme. N identical channels with identical inputs operate in parallel and the output of each channel is compared to the system output which is derived from a threshold gate. When a disagreement is found, the channel that disagrees is effectively removed from the system by forcing the output of the channel, as seen by the threshold gate, to 0. The system reliability is dependent upon the chosen threshold. Under the assumption that only one active channel can be faulty at any given time, the optimum threshold is two. The system is operable as long as at least two channels are operative and the monitor is operative. If R is the reliability of a unit and R_M is the reliability of the monitor, the reliability of a self-purging system of N channels is

$$R_S = \left[\sum_{i=2}^{N} \binom{N}{i} R^i (1-R)^{N-i}\right] R_M \quad (4)$$

Since the self-purging monitor is essentially a restoring organ, one restoring organ per unit can be used to ensure that no single fault disables the system.

Switching (or parallel) Redundancy[5] is a reconfigurable, error-evident system. A unit is used in a system until it fails, at which time it is replaced. The emphasis for modern equipment is on automatic detection and switching when the unit goes faulty. Switching redundancy systems are divided into two types, active, in which all units are powered, and standby, in which all spares are unpowered.

In the simplest model, all units whether powered or not are assumed to have the same failure rate. If R is the reliability of the unit and S is that of the switch, a parallel redundancy system has a reliability of

$$R_p = S[1 - (1-R)^N] \quad (5)$$

for the case of N total units in the system initially. Note that if unpowered spares are used, the new spare must be placed in some prefault state or at least an operable state. This restoration of the system is called recovery.

The last fault-tolerant system retained for study is radial logic,[6,7] a static, masking technique. Radial logic makes use of the fault masking properties of the NOR (or NAND) gate with independent duplicated inputs. In radial logic of order 2, each k-input NOR in the prototype is replaced by a pair of 2k-input NOR gates with duplicated inputs. Stuck-at-0 output faults are corrected at the next level.

Stuck-at-1 output faults cannot be corrected. Thus, this technique can only be used with technologies in which stuck-at-1 output faults are extremely rare. The reasons for considering radial logic are first that the reliability improvement can be quite large for a relatively small additional cost and certain kinds of technologies tend to produce one-sided faults in radiation environments, e.g., TTL/NAND gates in a neutron environment.

Radiation Related Indicators

A means of comparing the various schemes must be found. Some classical measures, such as the mean time between failures, are not appropriate. Two indicators were found, one relating to radiation hardness and the other to hardness assurance. Keep in mind that in all of the reliability formulas given above, the reliability of a unit can be a function of any kind of stress, e.g., time, temperature or as is our interest, some form of radiation.

The first of the two indicators is the reliability improvement index[8,9] (RII). The RII is defined by Klaschka as

$$RII = \frac{\ln R}{\ln R_r} \quad (6)$$

where R is the reliability of the prototype and R_r is that of the redundant system. For the usual case in which the reliabilities are close to 1,

$$RII = \frac{\ln R}{\ln R_r} \quad \frac{-(1-R)}{-(1-R_r)} = \frac{F}{F_r} \quad (7)$$

where F and F_r are the failure probabilities of the prototype and redundancy system, respectively. Of course, one can easily define the RII as F/F_r with little change in conclusions drawn from them since both are decreasing functions of R and increasing functions of R_r.

The RII relates to hardness assurance. Hardness assurance was defined earlier as an effort to assure that the parts actually used will result in circuits surviving to the specified radiation level. The lower the probability of failing at the given level, the higher the hardness assurance. The RII in fact gives the ratio of the failure probability of the prototype to the failure probability of the redundant system at a given radiation level, and in that sense is a measure of hardness assurance. The higher the RII, the greater the hardness assurance.

The second indicator is the ratio of the stress of the redundant system to the stress of the prototype for a given reliability and will be called the figure of merit[10] (FM). For example, if a given system has a reliability of 0.99 for a gamma total dose of 3.0×10^4 rads (SI) and a redundant system has that same reliability at 6.0×10^4 rads (SI), the figure of merit is 2. That is, for a given desired reliability of 0.99, the redundant system can tolerate twice the total dose that the unredundant system can tolerate.

This second indicator then relates to hardness. The FM directly indicates for a given desired reliability how much more radiation a redundant system can stand relative to the unredundant prototype.

Failure Distributions

BDM Corporation was engaged in a consulting role to provide failure distributions for electronic components (transistors and logic gates) subject to various forms of radiation. These were to be used in the analysis of the fault-tolerant systems. A representative sample of distributions was chosen to provide a maximum of information. Forms of radiation included neutron fluence, gamma total dose, gamma dose rate, and EMP power. Component types included integrated circuits as well as single transistors. Finally, components exhibiting both normal and log-normal distributions were taken. Preference was given to components that would be used in digital systems and for which sample sizes were large. The six cases chosen for the study are

1. 2N709 Transistor, gamma total dose, log-normal distribution.
2. 2N2222 Transistor, neutron fluence, normal distribution.
3. Commercial 5400 TTL NAND gates, neutron fluence, normal distribution.
4. Commercial 5400 TTL NAND gates, neutron fluence, log-normal distribution.
5. DTL/TTL Integrated Circuits, EMP power overstress, log-normal distribution.
6. RCA T8007 transistor, gamma dose rate, log-normal distribution.

Procedure

Computer programs were written to graph the two radiation related indicators, the RII and FM, against radiation level for the five redundancy schemes and the six distributions. Furthermore, curves for switching redundancy could be obtained for 2,3 or 4 units, and for 3,4, or 5 units for self-purging. Other variables were system size and system sectioning.

System size was varied from small systems of 500 components to large systems of 60,000 components. By system sectioning, we mean the division of the system into parts (equal parts being assumed in the study) with each part using the redundancy technique. Such a division improves reliability over the unsectioned case, but a point of diminishing returns is soon reached. System sectioning was examined for the unsectioned case to up to 40 sections.

The initial part of the analysis of the various fault-tolerant techniques used a simplified model in which all switches and voters were considered ideal. Later the effects of having nonideal switches and voters were considered. Refinements were made in the model of the ideal case to account for the switches and voters. Furthermore, a single output per unit is certainly unrealistic. The model assumed the number of outputs to be a function of the number of components in the system and the number of sections into which the system was divided.

Fig. 2 is typical of the graphs produced by plotting the RII against radiation, in this case a gamma dose rate environment. The particular set of curves is for a TMR redundancy scheme in which the component, the RCA T8007 transistor, exhibits a log-normal failure distribution. The lower curve is for the unsectioned case and the upper curve is for the same system divided into 10 sections, each with a TMRed output. Ideal voters were assumed in creating these curves. Since it was felt that an RII greater than about 1000 becomes somewhat meaningless, curves were limited to the range of 1000 or less on the RII index.

Fig. 3 is typical of the curves produced by plotting the FM against radiation for the same case as the RII graph. Again the lower curve is for the unsectioned case and the upper curve is for the case of 10 sections. For low values of radiation, the reliability of the systems becomes so close to 1 that for all practical purposes it had to be taken as 1. In certain cases, the low values of radiation became a fuzzy area, and the FM was taken as the first at all meaningful value.

A glance at the curves of Figure 3 shows that the curves look very much like exponentials. Indeed, in the ideal case, an exponential curve is a good fit to the graphs. Specifically, the FM can easily be fit to a curve of the form

$$FM = AMP \cdot e^{-\frac{RAD-START}{TAU}} + 1.0 \qquad (8)$$

For the lower curve in Figure 3, AMP = 3.35, START = 8.00×10^4 rads (SI)/sec, TAU = 3.08×10^5 rads (SI)/sec. and RAD is the radiation level at which the FM is desired.

Obtaining a closed form solution for the FM starting from the reliability equations for the unredundant and redundant systems is generally quite difficult. Therefore, a computer program was written which would accept the reliability of the unredundant system at a given radiation level and find by iterative covergence, the radiation level at which the redundant system has the same reliability. The program takes as its starting point the last radiation level found by the program and increases it until the redundant system reliability goes below that of the unredundant system. It then backtracks in smaller increments and eventually converges on the desired radiation level. A simple division gives the FM.

Results

In order to evaluate the effectiveness of the fault-tolerant techniques in the various radiation environments, an RII of 10 was arbitrarily established as a minimum desired improvement. The radiation level at RII=10 was determined for each system in each radiation environment. (At an RII of 10, the redundant system has a reliability of 0.9 or greater). The percentage of the mean radiation level and the reliability of both unredundant and redundant systems were also determined. For example, for the upper graph of Figure 2, RII = 10 at 2.75×10^6 rads (SI)/sec. This value is only 4.3% of the mean of the distribution, but for this radiation value, the unredundant system has a reliability of 0.71, whereas the TMR system has a very respectable reliability of 0.971 at this level. These figures rather dramatically illustrate that the designer of a system intended for a radiation environment cannot expect a system to operate reliably at or near the mean value of the failure distribution. They also show that by using redundancy, a redundant system can be expected to survive where an unredundant system may have a high failure probability.

The study shows that fault-tolerant techniques can be used in hardness assurance for all environments and components studied. They can operate reliably at radiation levels at which the unredundant systems would be expected to fail. Sectioning does help in this respect. As a result of the studies, the fault-tolerant systems in radiation environments were ranked as shown in Table 1 with respect to radiation hardness.

TABLE 1

Ranking of Fault-Tolerant Systems

According to Hardness Assurance

Ranking	System
1	Switching Redundancy, four units
2	Self-Purging, five units
3	Switching Redundancy, three units
4	Self-Purging, four units
5	Switching Redundancy, two units
6	TMR/Simplex
7	TMR and Self-Purging, three units

For a given RII, the relationship between the reliability of the redundant and unredundant systems can easily be determined. Since

$$RII = \frac{1-R}{1-R_r} \qquad (9)$$

$$R_r = \frac{R+(RII-1)}{RII} \qquad (10)$$

For RII = 10, we find

$$R_r = \frac{R+9}{10} \qquad (11)$$

which is why the redundant system has a reliability of at least 0.9 for RII = 10. For a given FM, such a simple relationship is not easily determined. Therefore, a different analysis approach was taken. First, radiation levels were determined that produced reliabilities of 0.9, 0.95, 0.99, and 0.999 for the unredundant system and the various components and distributions under consideration. One can then enter the graph and determine the FM (or RII for that matter) for that component and distribution. Next, an FM of 2 was set as a minimum desired improvement. That is, the redundant system was required to withstand at least twice the radiation level of the unredundant system for the same reliability before the improvement was considered significant. FMs of 2 or better were found to occur only for cases in which the reliability of the unredundant system was high to begin with (0.99 and 0.999) and then only for two environments, gamma dose rate and EMP power overstress.

The study showed that only for switching redundancy and self-purging systems of a sufficient number of units is redundancy very effective in radiation hardening, i.e., in increasing the radiation level at which the redundant system will operate for a given reliability of the unredundant system. Even then, these improvements occur only at levels of reliability at which the unredundant system is already reasonably reliable. Table II gives a ranking of the systems which have an FM of at least 2 in the range of reliabilities of the unredundant system at or below 0.999. The others were not ranked.

TABLE II

Ranking of Fault-Tolerant Systems

According to Radiation Hardness

Ranking	Systems
1	Switching Redundancy, four units
2	Self-Purging, five units
3	Switching Redundancy, three units
4	Self-Purging, four units

Two parameters, system size and system sectioning, were considered in the study. These were studied via the FM graphs and for the nonideal case. The nonideal case was found not to differ appreciably from the ideal case at high radiation levels. Furthermore, they did not differ appreciably from each other if switches and voters were replicated or if the distribution was a normal distribution. However, when the distribution was a log normal distribution and the switches and voters were not replicated (that is, they were modelled as series elements), the FM was considerably reduced at the low radiation levels (high reliability region). System size is considered next.

A somewhat surprising conclusion from examination of the data is that system size does not have a very great effect on radiation hardness, relatively speaking. A variation in system size of 8 to 1 did not cause the FM to have anywhere near an 8 to 1 change. In fact, if a comparison is made at a given unredundant system reliability, radiation hardness is found to be almost independent of system size. For example, curves were run of the FM assuming a 4-unit switching redundancy system in a gamma dot threshold environment. For an unredundant system reliability of 0.9 and an 8 to 1 size differential, the FM varied from 1.8 to 2.2, i.e., inversely with size.

The second parameter is that of system sectioning. Recall that curves for the ideal case gave FM and RII values for the unsectioned case as well as for the 10 section case. Curves for the nonideal case were produced for systems sectioned from 10 to 40 sections in increments of 10. The curves for the 40 section case do not appreciably differ from those of the 10-section case. There is a noticable difference in the curves for the 10-section case as opposed to the unsectioned case. The conclusion is that once past about 10 sections, little improvement results with an increase in the number of sections.

Summary and Conclusions

Fault-tolerant techniques were studied with the intent of using them in military and space applications subject to radiation environments. Representative failure distributions of electronic components in various radiation environments were obtained from available data and were used to obtain grapical data of two radiation related indicators. These indicators were then analyzed to ascertain the performance of a number of fault-tolerant techniques relative to radiation hardness and hardness assurance.

The usefulness of fault-tolerant techniques in a radiation environment depends upon the environment, the shape of the distribution, and the objective. They prove to be of little help in radiation hardening in gamma total dose and neutron environments, they are of some help in gamma dose rate and EMP environments. The techniques are also of some help in hardness assurance, more so in gamma dose rate and EMP environments.

The use of such techniques as triplication of voters and replication of switches was found to be useful at the low radiation levels (high reliability region). When imperfect switches and voters combined with a log normal distribution, reliability was considerably reduced at low radiation levels relative to the ideal case, but little difference was noted at high radiation levels. Finally, sectioning of the system into a number of relatively equal parts is helpful in both radiation hardening and hardening assurance, but continued division into finer and finer sections gives diminishing returns. After a division into about 10 sections, continued division is of little help.

The study was to some extent hampered by the lack of data on failure distributions. The available data in most cases involved components of obsolete technologies. Where data were available, the sample size was not

sufficiently large to define the critical region of the lower tail of the distribution as precisely as we would have liked. Although the assumed distributions, normal and log-normal, were good fits in some cases, this was not always true. It is hoped that in the future, when parts are tested in a radiation environment, some consideration will be given to obtaining not only failure levels, but also failure distributions as well. Enough parts should be tested so that the lower tail of the distribution is well-defined.

Acknowledgment

The author would like to express his appreciation to Pat Vail and Bob Simon, project officers on the contract.

References

1. R. C. DeVries, "Application of Fault-Tolerant Techniques and Differential Logic to Radiation Hardened Circuit and System Design," Air Force Weapons Laboratory, AFWL TR-77-76, November, 1977.

2. J. von Neumann, "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components," Automata Studies, Annals of Math Studies No. 34, Princeton University Press, Princeton, N. J., 1956.

3. F. P. Mathur, "On Reliability Modeling and Analysis of Ultrareliable Fault-Tolerant Digital Systems," IEEE Transactions on Computers, Vol. C-20, No. 11. November 1971, pp. 1376-1382.

4. J. Losq, "A Highly Efficient Redundancy Scheme: Self-Purging Redundancy," IEEE Transactions on Computers, Vol. C-25, No. 6, June 1976, pp. 569-578.

5. R. Teoste, "Digital Circuit Redundancy," IEEE Transactions on Reliability, Vol. R-13, No. 2, June 1964, pp. 42-61.

6. T. F. Klaschka, "Reliability Improvement by Redundancy in Electronic Systems, Part II-An Efficient New Redundancy Scheme-Radial Logic" TR69045, Royal Aircraft Establishment, Farnborough, Hants, England, March 1969.

7. A. Friedman and P. Menon, Fault-Detection in Digital Circuits, Prentice Hall, Englewood Cliffs, N. J., 1971.

8. T. F. Klaschka, "Reliability Improvement by Redundancy in Electronic Systems, Part I-A Method for Analysis and Assessment of Redudancy Schemes," TR68130, Royal Aircraft Establishment, Farnborough, Hants, England, May 1968.

9. T. F. Klaschka, "A Method for Redundancy Performance Assessment," IEEE Transactions on Computers, Vol. C-20 , No. 11, November 1971, pp. 1371-1376.

10. W. G. Bouricius, et. al., "Reliability Modeling for Fault-Tolerant Computers," IEEE Transactions on Computers, Vol. C-20, No. 11, November 1971, pp. 1306-1311.

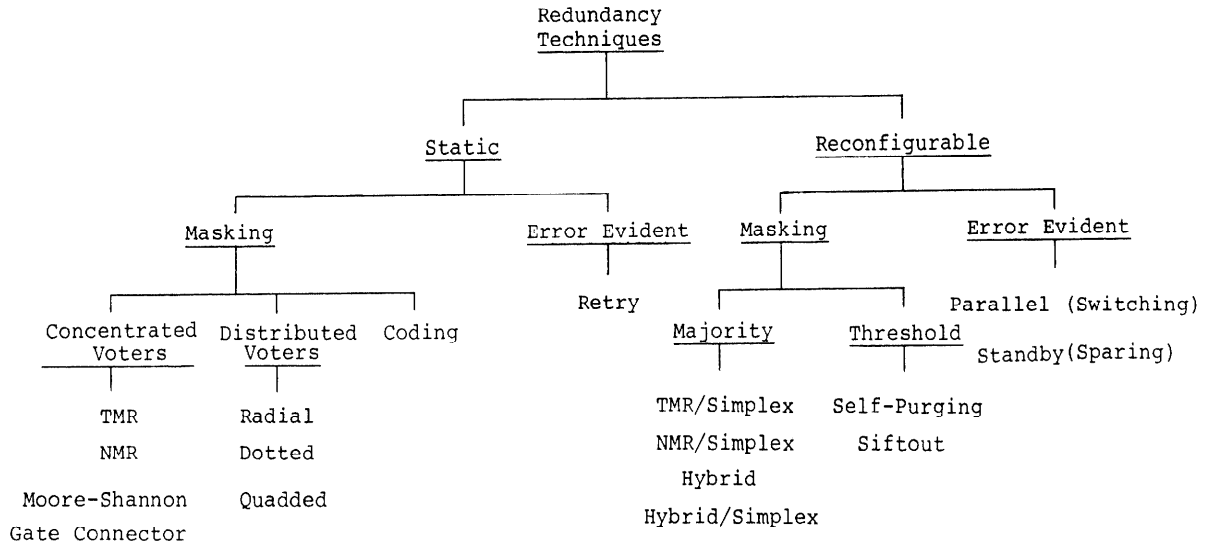

Figure 1. Redundancy Techniques

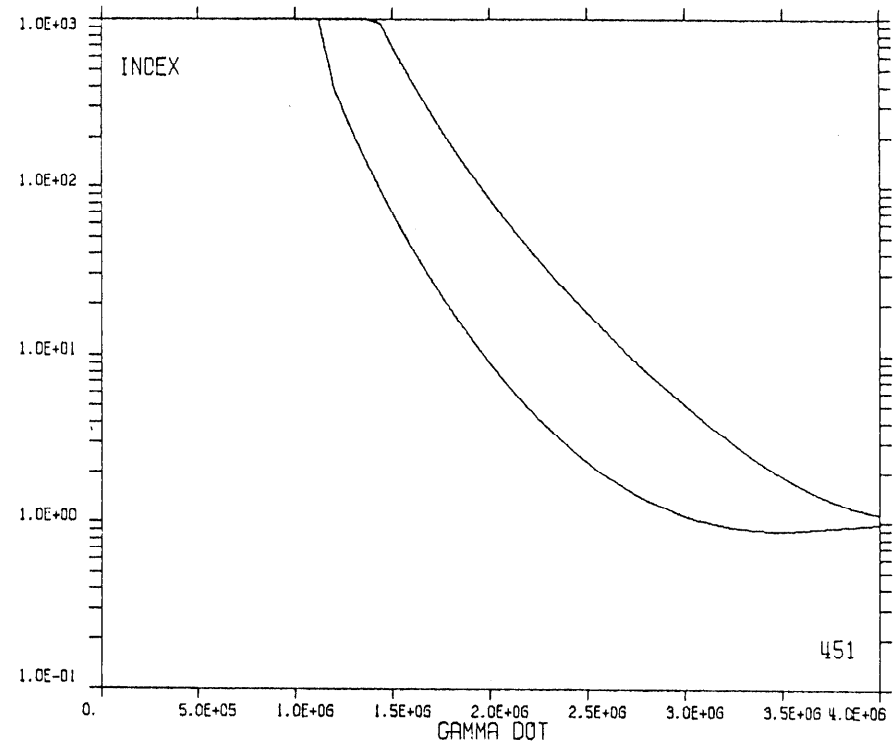

Figure 2. Graph of RII - TMR, Log Normal Distribution, Gamma Dose Rate Environment, RCA T8007 Transistor

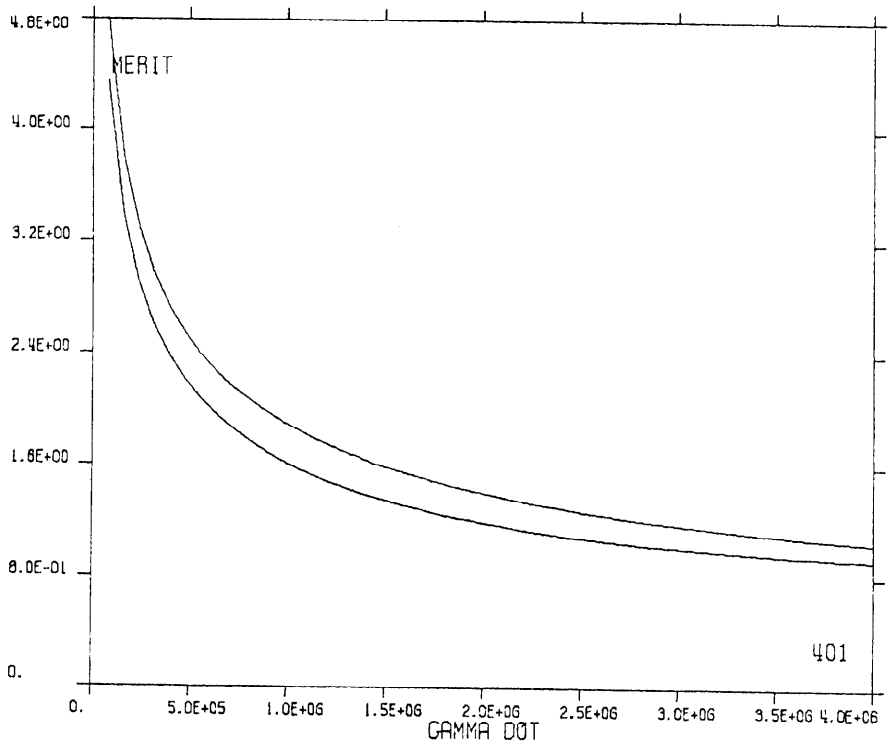

Figure 3. Graph of FM - TMR, Log Normal Distribution, Gamma Dose Rate Environment, RCA T8007 Transistor