NASA TECHNICAL NOTE

NASA TN D-7938 c.1

NASA TN D-7938

2. u/4

IMPACT OF COVERAGE ON THE RELIABILITY OF A FAULT TOLERANT COMPUTER

Salvatore J. Bavuso

Langley Research Center
Hampton, Va. 23665

3. 5.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION • WASHINGTON, D. C. • SEPTEMBER 1975

1. Report No. NASA TN D-7938	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle IMPACT OF COVERAGE ON THE RELIABILITY OF A FAULT TOLERANT COMPUTER		5. Report Date September 1975 6. Performing Organization Code
7. Author(s) Salvatore J. Bavuso		8. Performing Organization Report No. L-10050
9. Performing Organization Name and Address NASA Langley Research Center Hampton, Va. 23665		10. Work Unit No. 505-07-31-01 11. Contract or Grant No.
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration Washington, D.C. 20546		13. Type of Report and Period Covered Technical Note 14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

A mathematical reliability model is established for a reconfigurable fault tolerant avionic computer system utilizing state-of-the-art computers. System reliability is studied in light of the coverage probabilities associated with the first and second independent hardware failures. Coverage models are presented as a function of detection, isolation, and recovery probabilities. Upper and lower bounds are established for the coverage probabilities and the method for computing values for the coverage probabilities is investigated. Further, an architectural variation is proposed which is shown to enhance coverage.

17. Key Words (Suggested by Author(s)) Reliability Coverage Fault tolerant computer Reconfigurable computer	18. Distribution Statement Unclassified – Unlimited Subject Category 66		
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 24	22. Price* $3.25

*For sale by the National Technical Information Service, Springfield, Virginia 22161

IMPACT OF COVERAGE ON THE RELIABILITY OF A FAULT TOLERANT COMPUTER

Salvatore J. Bavuso
Langley Research Center

SUMMARY

A mathematical reliability model is established for a reconfigurable fault tolerant avionic computer system utilizing state-of-the-art computers. System reliability is studied in light of the coverage probabilities associated with the first and second independent hardware failures. Coverage models are presented as a function of detection, isolation, and recovery probabilities. Upper and lower bounds are established for the coverage probabilities and the method for computing values for the coverage probabilities is investigated. Further, an architectural variation is proposed which is shown to enhance coverage.

INTRODUCTION

In recent years, the literature has contained numerous fault tolerant computer architectural designs which are enumerated in reference 1. What is strikingly apparent from the majority of those reported is the usual presentation of a cursory reliability assessment with comparable heuristic justification, if any assessment at all is present.

Early attempts to arrive at realistic reliability estimates for computer systems appear to be due to Roth and Bouricius, et al. (ref. 2). With their presentation of the probabilistic concept of coverage, it was shown that coverage, defined as the conditional probability that a proper recovery occurs if a fault exists, must approach 100 percent to gain the potential reliability attainable by modular replacement systems (ref. 3). Prior to this time, reliability analyses have assumed a coverage of unity upon omission of this concept in reliability equations.

The application of the coverage concept to contemporary computer systems was reported by Sklaroff et al. (ref. 4). They express coverage for a two-fault tolerant triplex configuration as two components, a coverage component for the first failure and a coverage component for the second failure. A reliability comparison between three triplex systems with different failure coverage components is presented. Triplex system A is assigned a first failure coverage of unity and a second failure coverage of $X \ni 0.5 \leqq X \leqq 1$. Triplex system C is assigned the coverage probability of $X \ni 0.5 \leqq X \leqq 1$ for both first and second failures. Systems A and C are master slave architectures; and system B, which assumes a first failure coverage of unity and a second failure coverage $X \ni 0.5 \leqq X \leqq 1$, is a configuration in which all computers issue outputs to an external unit. The work presented in this paper addresses the latter system similarly to the analysis that was performed for triplex system C, with the addition of establishing upper and lower bounds on the first and second failure coverages, C_1 and C_2, and a method for computing values for C_1 and C_2 is investigated. In order to make the results realistic, the fault tolerant avionic flight control computer system utilized for this study is composed of three identical contemporary simplex computers.

SYMBOLS

A	event, A channel is operational
$^{d}A_{o}$	event, channel A detects a fault in the other channel (B)
$^{d}A_{s}$	event, channel A detects a fault in itself
B	event, B channel is operational
$^{d}B_{o}$	event, channel B detects a fault in the other channel (A)
$^{d}B_{s}$	event, channel B detects a fault in itself
C_j	probability of the system defined in figure 2 entering state S_j given that the system was previously in state S_{j-1} and that an unrepairable fault occurred in a channel where $1 \leqq j \leqq 2$; failure coverage
D	fault detection event
$\bar{D}_f$	event, no detection of a fault
$^{c}_{j}D_f$	event, correct detection of a fault for subset j; j = 1, single failure simplex isolating; j = 2, single failure cross isolating
$^{I}D_f$	event, incorrect detection of a fault
F	fault event
I	fault isolation event

$\tilde{I}$	input unit composed of ADC's
i,j	integers
O	output unit composed of DAC's
$P(\ )$	probability of event $(\ )$ occurring
$P_j(t)$	probability of the system being in state j at time t
$P_j\left(D,I,R_c \middle| F\right) \triangleq C_j$	conditional probability the system will detect, isolate, and reconfigure and recover given that the jth fault occurred
${}^{d}P_j \triangleq P_j\left(D \middle| F\right)$	conditional probability the system will detect a fault given that the jth fault occurred
${}^{i}P_j \triangleq P_j\left(I \middle| D,F\right)$	conditional probability the system will isolate (to a channel) a fault given that the jth fault was detected and the fault occurred
${}^{i_k}P_j$	isolation probability in channel k in state j
${}^{r}P_j \triangleq P_j\left(R_c \middle| D,I,F\right)$	conditional probability the system will reconfigure and recover given that the jth fault was detected and isolated and the fault occurred
${}^{\tilde{i}}P_2$	isolation probability which is identical for both duplex channels
P_{sf}	probability of system failure
Q	unreliability given by $1 - R$
Q_A	unreliability of channel A, $1 - R_A$
Q_B	unreliability of channel B, $1 - R_B$
R	reliability given by $\exp(-\lambda t)$
R_A	reliability of channel A
R_B	reliability of channel B

R_c reconfiguration event

${}_{j-1}^{j}\overline{R}$ event, the system fails to recover upon channel failure while attempting to reconfigure from j channels to $j-1$ channels

S_j jth state of the triplex system

t time

X coverage probability defined in reference 4

X_i ith operational channel

$\overline{X}_i$ ith malfunctioned channel

λ constant hardware failure rate of simplex computer

$\triangleq$ defined as

$\ni$ such that

$\overline{}$ complementary event, for example, the complement of event A is $\overline{A}$

$|$ conditional event

$\oplus$ exclusive "or" operation

$+$ inclusive "or" operation

$\cap$ Boolean "and" operation

$\cup$ Boolean "or" operation

$>>$ much greater than

Abbreviations:

ADC analog-to digital converter

BITE built-in test equipment

CSC	contemporary simplex computer
DAC	digital-to-analog converter
MTTF	mean time to failure
RCS	reconfigurable computer system

FLIGHT CONTROL COMPUTER RELIABILITY MODEL

The computer architecture selected for this study appears in figure 1 as a triplex reconfigurable computer system (RCS) composed of three identical computer channels. The contemporary simplex computer (CSC) contained within each channel is a typical aerospace class machine with a 16 000 word memory and a memory add time of 2 μs. In an aircraft environment, the CSC mean time to failure (MTTF) is predicted to be 3275 hr. The $\tilde{I}$ unit is composed of 20 analog-to-digital converters (ADC's) with a combined MTTF of 4000 hr and the O unit is composed of 20 digital-to-analog converters (DAC's) with a combined MTTF of 5500 hr. A channel composed of a CSC, an $\tilde{I}$ unit, and an O unit is assigned a predicted MTTF of 1357 hr which reflects the environmental effects of an operational aircraft. A mission time of 10 hr is assumed; also channel voting/comparing is performed by software via an interprocessor bus.

The Markov state space modeling technique was selected to represent a mathematical reliability model for the described system. Reference 5 describes the theoretical basis for this technique. A Markov state space model of the triplex channel computer system with coverage factors for both first and second channel failures was developed and is presented in figure 2. The figure defines four system states of interest, states S_0 to S_3, where event X_i is defined as the ith operational channel and event $\overline{X}_i$ is the ith malfunctioned channel, $1 \leqq i \leqq 3$. State S_0 is the condition where all channels are operational and is expressed as the Boolean product of three events, $S_0 = X_1X_2X_3$. State S_3 is the system-failure state and occurs when the system does not recover upon a channel failure while attempting to reconfigure from 3 channels to 2 channels $\left(\text{event } {}^{3}_{2}\overline{R}\right)$ or similarly does not recover upon a channel failure while in the dual state $\left({}^{2}_{1}\overline{R}\right)$ or all channels fail. The figures between state nodes are transitional probabilities composed of coverage components C_1 and C_2, λ, Δt, and a constant. The parameters C_1 and C_2 are defined as the probability of the system entering state S_1 and S_2 given that the system was previously in state S_0 and S_1, respectively, and that an unrepairable fault occurred in a channel. Repairable faults, such as benign electrical transient faults, do not cause a change of system state, since this class of faults can be mitigated by machine state vector transfer or software rollback. Unrepairable transients, such as intermittent and long duration faults, do cause a change of system state. Their effects can be incorporated by summing the unrepairable transient fault rate (assumed constant with time) with the channel hardware failure rate. The parameter λ is the channel hardware failure rate and is assumed to be constant for this model. It is related to the reciprocal of the MTTF, by $\lambda = 1/\mathrm{MTTF}$. The constant multiplier in the transitional probability term relates to the number of operational channels prior to failure and Δt is an increment of time.

The RCS model can be expressed as a system of first-order ordinary differential equations (discrete state, continuous time)

$$\frac{dP_0(t)}{dt} = -3\lambda P_0(t)$$

$$\frac{dP_1(t)}{dt} = 3\lambda C_1 P_0(t) - 2\lambda P_1(t)$$

$$\frac{dP_2(t)}{dt} = 2\lambda C_2 P_1(t) - \lambda P_2(t)$$

$$\frac{dP_3(t)}{dt} = 3\lambda(1 - C_1)P_0(t) + 2\lambda(1 - C_2)P_1(t) + \lambda P_2(t)$$

where P_0 is the probability of the system being in state S_0, that is

$$P_0 = P(S_0) \qquad P_1 = P(S_1)\ P_2 = P(S_2)\ P_3 = P(S_3)$$

and the initial conditions are

$$P_0(0) = 1 \qquad P_1(0) = P_2(0) = P_3(0) = 0$$

The derivation of these equations can be found by inspection of the graph in figure 2 by utilizing the following analog: From signal flow graph theory, the probability of the system being in state S_j is the analog of a signal source and the transition probability is the analog of a transmission gain. The probability of the system being in state S_j at time $t + \Delta t$ is the sum of all signals arriving at the S_j node. The other nodes behave as probability sources at time t. For example, the ordinary differential equation associated with state zero is given by

$$P_0(t + \Delta t) = P_0(t) - 3\lambda C_1 \Delta t P_0(t) - 3\lambda(1 - C_1)\Delta t P_0(t)$$

Rearranging terms and taking a limit gives

$$\lim_{\Delta t \to 0} \frac{P_0(t + \Delta t) - P_0(t)}{\Delta t} = \frac{dP_0(t)}{dt} = -3\lambda P_0(t)$$

The solution to the system of differential equations was derived analytically and is presented as follows:

$$P_0(t) = e^{-3\lambda t}$$

$$P_1(t) = 3C_1\left(e^{-2\lambda t} - e^{-3\lambda t}\right)$$

$$P_2(t) = 3C_1C_2\left(e^{-\lambda t} - 2e^{-2\lambda t} + e^{-3\lambda t}\right)$$

$$P_3(t) = 1 - \left[P_0(t) + P_1(t) + P_2(t)\right]$$

The results of the probability of system failure P_{sf} at 10 hr of mission time as a function of C_1 and C_2 are plotted in figure 3 for P_3. In the best case when $C_1 = C_2 = 1$, the P_{sf} is predicted at 3.96×10^{-7} at 10 hr of mission time. For C_1 and C_2 less than unity, P_{sf} increases exponentially with C_2.

Intuitively, it is obvious that prior to fault recovery via reconfiguration, a fault must be detected and located by the computer system. It will be seen later that both of these factors can be incorporated in the computation of C_1 and C_2. During initial operation, however, three computers are available for fault detection and isolation and, therefore, it is expected that C_1 will be very nearly unity; whereas, after the first channel failure, fault isolation must be accomplished without a majority vote and is expected to cause C_2 to be much less than unity. The literature is extremely sparse in predicting values for C_1; however, reference 4 indicates $C_2 \leqq 0.95$ at the present state of the art (assuming perfect recovery from transient faults and perfect software in a correctly designed system).

When $C_1 \leqq 0.999$, an interesting phenomenon occurs. The data (observed in fig. 3) indicate that P_{sf} becomes insensitive to C_2, that is, for some $C_1 < 0.999$, P_{sf} becomes insensitive to changes in C_2. The implication is that if C_1 is not sufficiently greater than 0.999, the achievement of high C_2 is unimportant; hence $C_1 = 0.999$ is assigned as a reasonable lower bound for this computer architecture. In view of the fact that hitherto C_1 has been essentially ignored by the usual assumption of $C_1 = 1$, it appears that attention should be focused on determining realistic values of C_1. Alternately, when $C_1 > 0.999$, the data show that high gains in system reliability can be approached only if $C_2 > 0.94$; hence, $C_2 = 0.94$ is assigned as a lower bound. The data depicted in figure 3 show that for $C_2 \leqq 0.996$, little gain in reliability occurs for $C_1 > 0.99999$ (note superposition of such curves). The coverage value, $C_1 = 0.99999$, may be assigned to this model as a reasonable upper bound, that is, the achievement of coverages greater than 0.99999 contributes little for this contemporary system since it is unlikely that values of $C_2 \gg 0.996$ can be achieved as is shown later.

C_j COMPUTATION

In the previous discussion, a mathematical relationship between RCS P_{sf} and coverage components was developed. Theoretical coverage bounds were established for system first and second failure coverage components. This section investigates the coverage contribution of simplex computer channels to the first and second failure coverage components.

The jth failure coverage C_j may be defined as

$$C_j \triangleq P_j\left(D,I,R_c \middle| F\right)$$

that is, the jth failure coverage is the probability that the system will detect a fault, isolate the fault to a channel, and reconfigure and recover given that a fault occurred. Since R_c is dependent on D, I, and F; I is dependent on D and F; and D is dependent on F, C_j may be further defined as the product of conditional probabilities. (See appendix A for derivation.)

$$C_j = P_j\left(R_c \middle| D,I,F\right) \cdot P_j\left(I \middle| D,F\right) \cdot P_j\left(D \middle| F\right)$$

Further

$$C_j \triangleq {}^rP_j \cdot {}^iP_j \cdot {}^dP_j$$

where

$${}^rP_j = P_j\left(R_c \middle| D,I,F\right)$$

$${}^iP_j = P_j\left(I \middle| D,F\right)$$

$${}^dP_j = P_j\left(D \middle| F\right)$$

For the first failure coverage

$$C_1 = {}^{d}P_1 \cdot {}^{i}P_1 \cdot {}^{r}P_1$$

This equation expresses the events and their occurrence probabilities associated with the computer system's ability to traverse from the triplex state S_0 to the duplex state S_1 as a result of a permanent channel failure. Failure detection and isolation can be accomplished by channel majority voting. After this process, accomplished primarily by software, is completed, the values of ${}^{d}P_1$, ${}^{i}P_1$, and ${}^{r}P_1$ are determined essentially by the correctness of the system hardware and software design and the correctness of the software code. The utility of software self-testing or BITE (built-in test equipment) is lessened by the massive hardware channel redundancy. However, since 100-percent hardware and software design verification and code correctness verification are still unachievable, C_1 is most likely less than unity. A simple example to demonstrate this point regards the common practice of inserting identical copies of software into each CSC. In most cases, operational software contains latent software errors, errors not discovered during the software debugging and testing process. Such errors will never be detected by the majority voting process. The consequences of this type of error occurrence can be devastating to an aircraft which utilizes this computer system as the sole flight control system computer.

The availability of massive channel redundancy, however, does not obviate the need for BITE and software self-test in the triplex state S_0 since BITE is a hardware design implementation and, as such, is somewhat independent of software design. For instance, a latent software error although not detected by majority voting may trigger a BITE detector indicating, for example, an overflow condition. Similarly, software self-testing should not be abandoned either since latent hardware faults and transient-caused faults (permanently altered unprotected memory) can be detected and perhaps corrected prior to the execution of certain critical applications programs such as end of mission (autoland) programs. Thus, when hardware and software design and software coding are considered correct, it is reasonable to assume that

$${}^{d}P_1 \approx {}^{i}P_1 \approx {}^{r}P_1 \approx 1$$

and

$$C_1 \approx 1$$

Of greater interest is the case where $j = 2$, and the second failure coverage is given by

$$C_2 = {}^{d}P_2 \cdot {}^{i}P_2 \cdot {}^{r}P_2$$

For this case the probability of isolation becomes a predominant factor for C_2 since intuitively one recognizes that there is a high probability of detection by comparison; and if a fault could be isolated to a simplex computer, it is reasonable to believe there is a high probability of the system affecting a proper recovery. Assuming in the best case that ${}^{d}P_2 = {}^{r}P_2 = 1$, C_2 can be studied in light of ${}^{i}P_2$.

For $j = 2$, the second failure coverage is expressed by

$$C_2 = {}^{d}P_2 \cdot {}^{i}P_2 \cdot {}^{r}P_2$$

where

$$ {}^{d}P_2 = 1 \qquad {}^{i}P_2 \leqq 1 \qquad {}^{r}P_2 = 1$$

In the duplex mode, ${}^{i}P_2$ is based on the simplex computer failure detection probability which is a function of the isolation test thoroughness, testing time, and BITE detecting effectiveness.

A system architecture that restricts software testing to a single simplex computer such that each simplex machine is capable of determining its own health is defined as a simplex isolating architecture. With this type of architecture configured in the duplex mode, the probability of isolation is identical to the probability of detection in a simplex computer. This conclusion is demonstrated in appendix B. Utilizing the state-of-the-art value for fault detection in a simplex computer which is given in reference 4 as 0.95, ${}^{i}P_3 = 0.95$ and, therefore, $C_2 = 0.95$. For $C_1 = 0.9999$ and $C_2 = 0.95$, figure 3 indicates a P_{sf} of 1.2×10^{-5} as a reasonable state-of-the-art goal. This value for P_{sf} contrasts against the theoretical minimum of 3.96×10^{-7}. An interesting variation on determining the system isolation probability, which to this author's knowledge has not been discussed in the literature, is to remove the restriction of self-testing to a single simplex computer. By allowing each simplex computer access to the other's registers, each machine can test itself as well as the other (cross isolating architecture). In this case, each machine can be conceptually considered as a fault detector searching for a fault in the union of the two simplex computer fault sets. The union of the fault sets becomes the universal fault set; and since the isolation events are independent

$${}^{i}P_2 = {}^{i_1}P_2 + {}^{i_2}P_2 - {}^{i_1}P_2 \cdot {}^{i_2}P_2$$

where ${}^{i_k}P_2$ is the isolation probability in machine number k for $1 \leqq k \leqq 2$. The rationale for this conclusion is presented in appendix B. On letting

$${}^{i_1}P_2 = {}^{i_2}P_2 \triangleq {}^{\tilde{i}}P_2$$

then

$$C_2 = \left(2\,{}^{\tilde{i}}P_2 - {}^{\tilde{i}}P_2^{\,2}\right) \cdot {}^{d}P_2 \cdot {}^{r}P_2$$

and

$$C_2 = \left(2\,{}^{\tilde{i}}P_2 - {}^{\tilde{i}}P_2^{\,2}\right)$$

since

$${}^{d}P_2 = {}^{r}P_2 = 1$$

by assumption. For

$${}^{\tilde{i}}P_2 = 0.95 \qquad C_2 = 0.998$$

Using $C_1 = 0.9999$ and $C_2 = 0.998$, the probability of system failure approaches 2.8×10^{-6} at 10 hr of mission time which is contrasted against the theoretical minimum of 3.96×10^{-7} at 10 hr when $C_1 = C_2 = 1$.

On observing figure 3, the upper bound for C_1 in a simplex isolating architecture is 0.99999, since for $C_2 \approx 0.95$, all the curves for $C_1 \geqq 0.99999$ are superimposed. For cross isolating architectures by contrast, the upper bound for C_1 is 0.999999 since C_2 is likely to approach 0.998.

When ${}^{r}P_2$ is assumed as a variable in a cross isolating architecture

$$C_2 = \left(2\,{}^{\tilde{i}}P_2 - {}^{\tilde{i}}P_2^{\,2}\right) \cdot {}^{r}P_2$$

Figure 4 depicts the sensitivity of C_2 to ${}^{r}P_2$ and ${}^{i}P_2$. The data show that C_2 is considerably more sensitive to changes in ${}^{r}P_2$ than to ${}^{i}P_2$; in fact, for reasonably obtainable values of ${}^{i}P_2$ $\left(0.9 < {}^{i}P_2 < 0.95\right)$, C_2 is nearly completely determined by ${}^{r}P_2$. This observation suggests that considerable effort be devoted toward improving ${}^{r}P_2$ rather than ${}^{i}P_2$ when ${}^{i}P_2 > 0.95$ and the computer architecture is a cross isolating architecture.

CONCLUDING REMARKS

A mathematical model was established for the reliability of a reconfigurable fault tolerant avionic computer system utilizing contemporary simplex computers. The system reliability was computed as a function of a particular system configuration, mean time to failure for a contemporary simplex computer, mission time, and two coverage parameters, one associated with the first independent hardware failure C_1 and the other with the second failure C_2.

Two variations of a duplex configuration were addressed and termed, simplex isolating architecture and cross isolating architecture. The former system architecture restricts software testing to a single simplex computer such that each simplex machine is capable of determining its own health. The latter architecture proposed by the author removes the restriction regarding software testing to a single simplex computer such that it allows each simplex computer access to the other's registers, enabling each machine to test itself as well as the other.

A lower bound for the first failure coverage C_1 was established at 0.999. When $C_1 \leqq 0.999$, the system probability of failure becomes independent of the second failure coverage C_2 so that if C_1 is not sufficiently greater than 0.999, the achievement of C_2 is unimportant. This result suggests that more attention be focused on determining values of C_1.

For a simplex isolating architecture, where values of C_2 will probably be less than or equal to 0.95, an upper bound for C_1 of 0.99999 was established. For cross isolating architectures where C_2 approaches 0.998, the upper bound for C_1 appears to be 0.999999. When $C_1 > 0.999$, the model data predict that high gains in system reliability can be approached only if second failure coverage values are much larger than 0.94; therefore, $C_2 = 0.94$ is assigned as a reasonable lower bound for C_2. The upper bound for C_2 for the described triplex system is 0.998.

A model for computing C_1 and C_2 was proposed for a cross isolating architecture, and an estimate for C_2 was calculated to be 0.998 when perfect detection and recovery in the duplex configuration is assumed and the probability of isolating a fault ${}^iP_2$ is given as 0.95. Assuming $C_1 = 0.9999$ and $C_2 = 0.998$, the probability of system failure approaches 2.8×10^{-6} at 10 hr which is contrasted against the theoretical minimum of 3.96×10^{-7} at 10 hr when $C_1 = C_2 = 1$. The coverage estimates, primarily attributed to $C_2 < 1$, appear to increase the probability of system failure by an order of magnitude. Further, it was shown that the major contributor to C_2, for a cross isolating architecture, is the probability of reconfiguring and recovery ${}^rP_2$ in lieu of the failure isolation probability ${}^{i}P_2$ and suggests that considerable effort be devoted toward improving ${}^{r}P_2$ rather than ${}^{i}P_2$ $\left(\text{for } {}^{i}P_2 > 0.95\right)$.

Finally, it should be noted that the modeling techniques developed in this paper are easily modified to study the case of three failures or greater tolerant systems and may be utilized to predict reliabilities for higher order systems.

Langley Research Center
National Aeronautics and Space Administration
Hampton, Va. 23665
June 9, 1975

APPENDIX A

C_j DERIVATION

The following derivation is a straightforward application of conditional probabilities.

$$C_j = P_j\left(D,I,R_c|F\right) = P_j\left(R_c,D,I|F\right), \quad D\cap I\cap R_c = R_c\cap D\cap I$$

by commutivity.

$$C_j = P_j\left(R_c,D,I|F\right) = P_j\left(R_c,D,I,F\right)|P_j(F)$$

$$P_j\left(R_c,D,I,F\right) = P_j\left(R_c|D,I,F\right)P_j(D,I,F)$$

$$P_j(D,I,F) = P_j(I,D,F) = P_j(I|D,F)P_j(D,F)$$

$$P_j(D,F) = P_j(D|F)P_j(F)$$

$$P_j\left(R_c,D,I,F\right) = P_j\left(R_c|D,I,F\right)P_j(I|D,F)P_j(D|F)P_j(F)$$

$$C_j = \frac{P_j\left(R_c|D,I,F\right)P_j(I|D,F)P_j(D|F)P_j(F)}{P_j(F)}$$

$$C_j = P_j\left(R_c|D,I,F\right)P_j\left(I|D,F\right)P_j(D|F)$$

APPENDIX B

PROBABILITY OF ISOLATION DERIVATION

In the duplex mode, ${}^{i}P_{2}$ is a function of the health of each machine, A and B, which can be modeled by the Poisson reliability model, $R = e^{-\lambda t}$, the ability of each machine to detect a fault in itself, ${}^{d}A_{s}$ and ${}^{d}B_{s}$, and the ability of each machine to detect a fault in the other machine, ${}^{d}A_{o}$ and ${}^{d}B_{o}$. By allowing each event to be a binary event, there are $2^{6} = 64$ possible combination system states depicted in table 1 which represent the universal sample space. By definition, the duplex system probability of fault detection is assigned unity; therefore, the subset of sample points which contains one or more failures (fault subset) is used to determine the probability of isolation. The fault subset may be partitioned to form 12 subsets of interest which are depicted as follows:

	Event	Subset for –	
		Simplex isolating	Cross isolating
Single failure	${}^{c}D_{f} \vert A \oplus B$	1	2
	${}^{I}D_{f} \vert A \oplus B$	3	4
	$\bar{D}_{f} \vert A \oplus B$	5	6
Double failure	${}^{c}D_{f} \vert A \oplus B$	7	8
	${}^{I}D_{f} \vert A \oplus B$	9	10
	$\bar{D}_{f} \vert A \oplus B$	11	12

The heading, simplex isolating, defines the dual architecture with respect to detection, in that each machine cannot detect a fault in the other machine. The heading, cross isolating, removes this restriction. System detection of faults can be either correct, incorrect, or no detection may occur at all. The system could experience a single unrepairable channel fault or a double fault either simultaneously or nearly so.

Subsets 1 and 2 are of particular interest since they represent the case in which the machine fault detectors are so designed that if they announce the detection of a fault, then the fault physically exists. It is postulated that if a processor is capable of announcing the existence of a fault then the fault is real. Subsets 3 and 4 for single failures cover the cases where phantom faults are announced. Only subsets 1 and 2 are considered in this paper.

The sample points for ${}^{c}D_f$ appear in table 1 as S_5, S_{10}, S_{18}, S_{26}, S_{33}, and S_{37}. These events are represented by the following equations:

$$S_5 = A\ \bar{B}\ {}^{d}A_s\ {}^{d}\bar{A}_o\ {}^{d}\bar{B}_s\ {}^{d}\bar{B}_o$$

$$S_{10} = \bar{A}\ B\ {}^{d}\bar{A}_s\ {}^{d}A_o\ {}^{d}\bar{B}_s\ {}^{d}\bar{B}_o$$

$$S_{18} = \bar{A}\ B\ {}^{d}\bar{A}_s\ {}^{d}\bar{A}_o\ {}^{d}B_s\ {}^{d}\bar{B}_o$$

$$S_{26} = \bar{A}\ B\ {}^{d}\bar{A}_s\ {}^{d}A_o\ {}^{d}B_s\ {}^{d}\bar{B}_o$$

$$S_{33} = A\ \bar{B}\ {}^{d}\bar{A}_s\ {}^{d}\bar{A}_o\ {}^{d}\bar{B}_s\ {}^{d}B_o$$

$$S_{37} = A\ \bar{B}\ {}^{d}A_s\ {}^{d}\bar{A}_o\ {}^{d}\bar{B}_s\ {}^{d}B_o$$

where the 1 indicates for A and B that the event failed and for ${}^{d}A_s$, ${}^{d}A_o$, ${}^{d}B_s$, and ${}^{d}B_o$ that the event occurred. The 0 indicates for A and B that the event did not fail and for the others that the event did not occur.

The conditional event ${}^{c}D_f|A\oplus B$ is functionally related to the union of sample points S_5, S_{10}, S_{18}, S_{26}, S_{33}, and S_{37}. By straightforward application of conditional probabilities

$$P\left({}^{c}D_f \middle| A\oplus B\right) = \frac{P\left({}^{c}D_f \cap A\right) + P\left({}^{c}D_f \cap B\right)}{P(A\oplus B)}$$

$$P\left({}^{c}D_f \middle| A\oplus B\right) = \frac{P\left(S_5 \cup S_{33} \cup S_{37}\right) + P\left(S_{10} \cup S_{18} \cup S_{26}\right)}{P(A\oplus B)}$$

$$P\left({}^{c}D_f \middle| A\oplus B\right) = \frac{P(S_5) + P(S_{33}) + P(S_{37}) + P(S_{10}) + P(S_{18}) + P(S_{26})}{P(A\oplus B)}$$

For subset 1, ${}^{c}D_f|A\oplus B$ is denoted ${}^{c}_{1}D_f|A\oplus B$ and is functionally related to the union of sample points S_5 and S_{18} as follows:

$$P\left(S_5\right) = P(A)\ P\left(\overline{B}\right) P\left({}^{d}A_s\right)\ P\left({}^{d}\overline{A}_o\right)\ P\left({}^{d}\overline{B}_s\right)\ P\left({}^{d}\overline{B}_o\right)$$

and since subset 1 precludes cross detection,

$$P\left({}^{d}\overline{A}_o\right) = P\left({}^{d}\overline{B}_o\right) = 1$$

So

$$P\left(S_5\right) = P(A)\ P\left(\overline{B}\right) P\left({}^{d}A_s\right)\ P\left({}^{d}\overline{B}_s\right)$$

Further

$$P\left(S_{10}\right) = 0$$

since

$$P\left({}^{d}A_o\right) = 0$$

Then

$$P\left(S_{18}\right) = P\left(\overline{A}\right) P(B)\ P\left({}^{d}\overline{A}_s\right)\ P\left({}^{d}B_s\right)$$

since

$$P\left({}^{d}\overline{A}_o\right) = P\left({}^{d}\overline{B}_o\right) = 1$$

Additionally,

$$P\left(S_{26}\right) = 0$$

$$P\left(S_{33}\right) = 0$$

$$P\left(S_{37}\right) = 0$$

since

$$P\left({}^{d}A_o\right) = P\left({}^{d}B_o\right) = 0$$

Therefore,

$$P\left({}_{1}^{c}D_f \middle| A \oplus B\right) = \frac{P\left(S_5\right) + P\left(S_{18}\right)}{P(A \oplus B)}$$

or

$$P\left({}_{1}^{c}D_f \middle| A \oplus B\right) = \frac{Q_A R_B\ P\left({}^{d}A_s\right)\ P\left({}^{d}\overline{B}_s\right) + Q_B R_A\ P\left({}^{d}\overline{A}_s\right)\ P\left({}^{d}B_s\right)}{Q_A R_B + Q_B R_A}$$

where $Q_A \triangleq P(A)$, the unreliability of A; and $R_B \triangleq P\left(\overline{B}\right)$, the reliability of B.

When both machines are identical,

$$Q_A = Q_B \triangleq Q \qquad\qquad R_A = R_B \triangleq R$$

Since the first term in the numerator is the condition where A failed, $P\left({}^{d}\overline{B}_s\right) = 1$; likewise in the second term, $P\left({}^{d}\overline{A}_s\right) = 1$, since B failed, and

$$P\left({}_1^{c}D_f \middle| A \oplus B\right) = \frac{1}{2}\left[P\left({}^{d}A_s\right) + P\left({}^{d}B_s\right)\right]$$

If both detection mechanisms are identical,

$$P\left({}_1^{c}D_f \middle| A \oplus B\right) = P\left({}^{d}A_s\right) = P\left({}^{d}B_s\right)$$

The result concludes that the probability of isolation for the duplex system is identical to that of a simplex machine, that is, ${}^{i}P_2 = {}^{i}P_3$.

A more interesting case which appears to have the potential of increasing system probability of isolation is subset 2. A cross isolating architecture can be physically affected by allowing each machine access to the other machine's registers, in which case it is feasible for one machine to diagnose faults in the other. Recalling the assumption that when a processor announces the detection of a fault, the fault physically exists, the following conditions occur for cross isolation:

$$\begin{array}{lll}
P\left({}^{d}\overline{A}_o\right) = P\left({}^{d}\overline{B}_s\right) = 1 & & \left(S_5\right) \\
P\left({}^{d}\overline{A}_s\right) = P\left({}^{d}\overline{B}_o\right) = 1 & P\left({}^{d}A_o\right) \neq 0 & \left(S_{10}\right) \\
P\left({}^{d}\overline{A}_s\right) = P\left({}^{d}\overline{B}_o\right) = 1 & & \left(S_{18}\right) \\
P\left({}^{d}\overline{A}_s\right) = P\left({}^{d}\overline{B}_o\right) = 1 & P\left({}^{d}A_o\right) \neq 0 & \left(S_{26}\right) \\
P\left({}^{d}\overline{A}_o\right) = P\left({}^{d}\overline{B}_s\right) = 1 & P\left({}^{d}B_o\right) \neq 0 & \left(S_{33}\right) \\
P\left({}^{d}\overline{A}_o\right) = P\left({}^{d}\overline{B}_s\right) = 1 & P\left({}^{d}B_o\right) \neq 0 & \left(S_{37}\right)
\end{array}$$

On applying these conditions for subset 2

$$P\left({}_2^{c}D_f \middle| A \oplus B\right) = \frac{P\left(S_5 \cup S_{10} \cup S_{18}\right) + P\left(S_{26} \cup S_{33} \cup S_{37}\right)}{Q_A R_B + Q_B R_A}$$

the numerator becomes

$$Q_A R_B\, P\left({}^{d}A_{s}\right) P\left({}^{d}\overline{B}_{o}\right) + R_A Q_B\, P\left({}^{d}A_{o}\right) P\left({}^{d}\overline{B}_{s}\right) + R_A Q_B\, P\left({}^{d}\overline{A}_{o}\right) P\left({}^{d}B_{s}\right)$$

$$+ R_A Q_B\, P\left({}^{d}A_{o}\right) P\left({}^{d}B_{s}\right) + Q_A R_B\, P\left({}^{d}\overline{A}_{s}\right) P\left({}^{d}B_{o}\right) + Q_A R_B\, P\left({}^{d}A_{s}\right) P\left({}^{d}B_{o}\right)$$

Allowing both machines to be identical hardware gives

$$P\left({}^{c}_{2}D_{f} \middle| A \oplus B\right) = \frac{1}{2} P\left({}^{d}A_{s}\, {}^{d}\overline{B}_{o} + {}^{d}A_{o}\, {}^{d}\overline{B}_{s} + {}^{d}\overline{A}_{o}\, {}^{d}B_{s} + {}^{d}A_{o}\, {}^{d}B_{s} + {}^{d}\overline{A}_{s}\, {}^{d}B_{o} + {}^{d}A_{s}\, {}^{d}B_{o}\right)$$

and assuming all detectors have equal detection probabilities gives

$$P\left({}^{d}A_{o}\right) = P\left({}^{d}A_{s}\right) \qquad P\left({}^{d}B_{o}\right) = P\left({}^{d}B_{s}\right)$$

Therefore,

$$P\left({}^{c}_{2}D_{f} \middle| A \oplus B\right) = P\left(A_{s}\right) + P\left(B_{s}\right) - P\left(A_{s}\right) P\left(B_{s}\right)$$

This result is identical except in notation to the text equation

$${}^{i}P_{2} = {}^{i_1}P_{2} + {}^{i_2}P_{2} - {}^{i_1}P_{2} \cdot {}^{i_2}P_{2}$$

Further, when $P\left(A_{s}\right) = P\left(B_{s}\right) \triangleq P$

$$P\left({}^{c}_{2}D_{f} \middle| A \oplus B\right) = 2P - P^{2}$$

This result is identical to that contained in the text given as

$$2\, {}^{\tilde{i}}P_{2} - {}^{\tilde{i}}P_{2}{}^{2}$$

REFERENCES

1. Goldberg, Jack; Neumann, Peter G.; and Wensley, John H.: Survey of Fault-Tolerant Computing Systems (Revised). Contract No. N00014-72-C-0254, Stanford Res. Inst., Aug. 1972.

2. Roth, J. P.; Bouricius, W. G.; Carter, W. C.; and Schneider, P. R.: Phase II of an Architectural Study for a Self-Repairing Computer. SAMSO TR-67-106, U.S. Air Force, Nov. 1967. (Available from DDC as AD 825 460.)

3. Bouricius, W. G.; Carter, W. C.; and Schneider, P. R.: Reliability Modeling Techniques and Trade-Off Studies for Self-Repairing Computers. RC 2378, Res. Div., IBM Corp., Feb. 14, 1969.

4. Sklaroff, J. R.; Kilmer, F. G.; and Padinha, H. A.: Redundant System Design for Advanced Digital Flight Control. AIAA Paper No. 73-846, Aug. 1973.

5. Shooman, Martin L.: Probabilistic Reliability: An Engineering Approach. McGraw-Hill Book Co., Inc., c.1968.

TABLE 1.- ALL POSSIBLE SAMPLE POINTS

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
A	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
B	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
d_{A_s}	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
d_{A_o}	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
d_{B_s}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
d_{B_o}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
A	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
B	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
d_{A_s}	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
d_{A_o}	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
d_{B_s}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
d_{B_o}	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

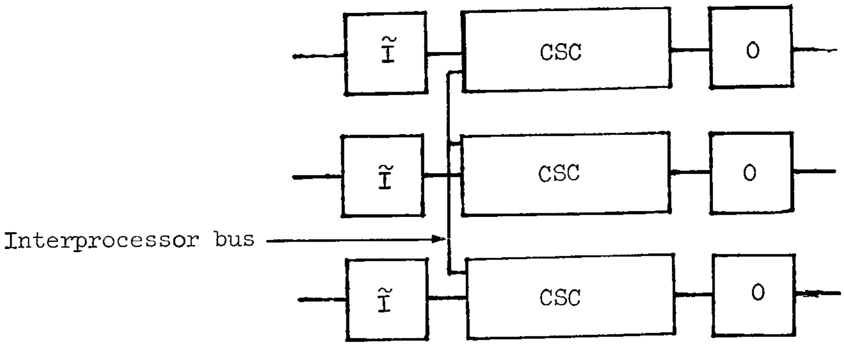

Figure 1.- Triplex computer architecture.

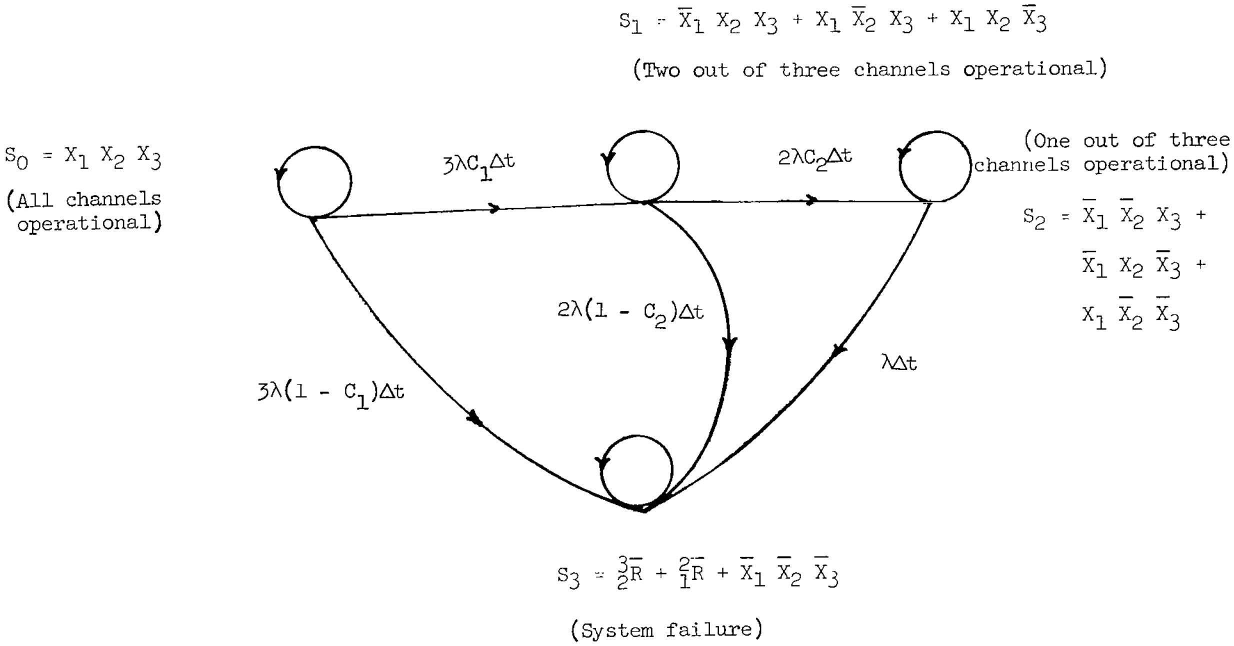
$S_1 = \bar{X}_1 X_2 X_3 + X_1 \bar{X}_2 X_3 + X_1 X_2 \bar{X}_3$
(Two out of three channels operational)
$S_0 = X_1 X_2 X_3$
(All channels operational)
$3\lambda C_1 \Delta t$
$2\lambda C_2 \Delta t$
(One out of three channels operational)
$S_2 = \bar{X}_1 \bar{X}_2 X_3 +$
$\bar{X}_1 X_2 \bar{X}_3 +$
$X_1 \bar{X}_2 \bar{X}_3$
$2\lambda(1 - C_2)\Delta t$
$\lambda \Delta t$
$3\lambda(1 - C_1)\Delta t$
$S_3 = {}^3_2\bar{R} + {}^2_1\bar{R} + \bar{X}_1 \bar{X}_2 \bar{X}_3$
(System failure)

Figure 2.- Markov state space model of triplex channel RCS.

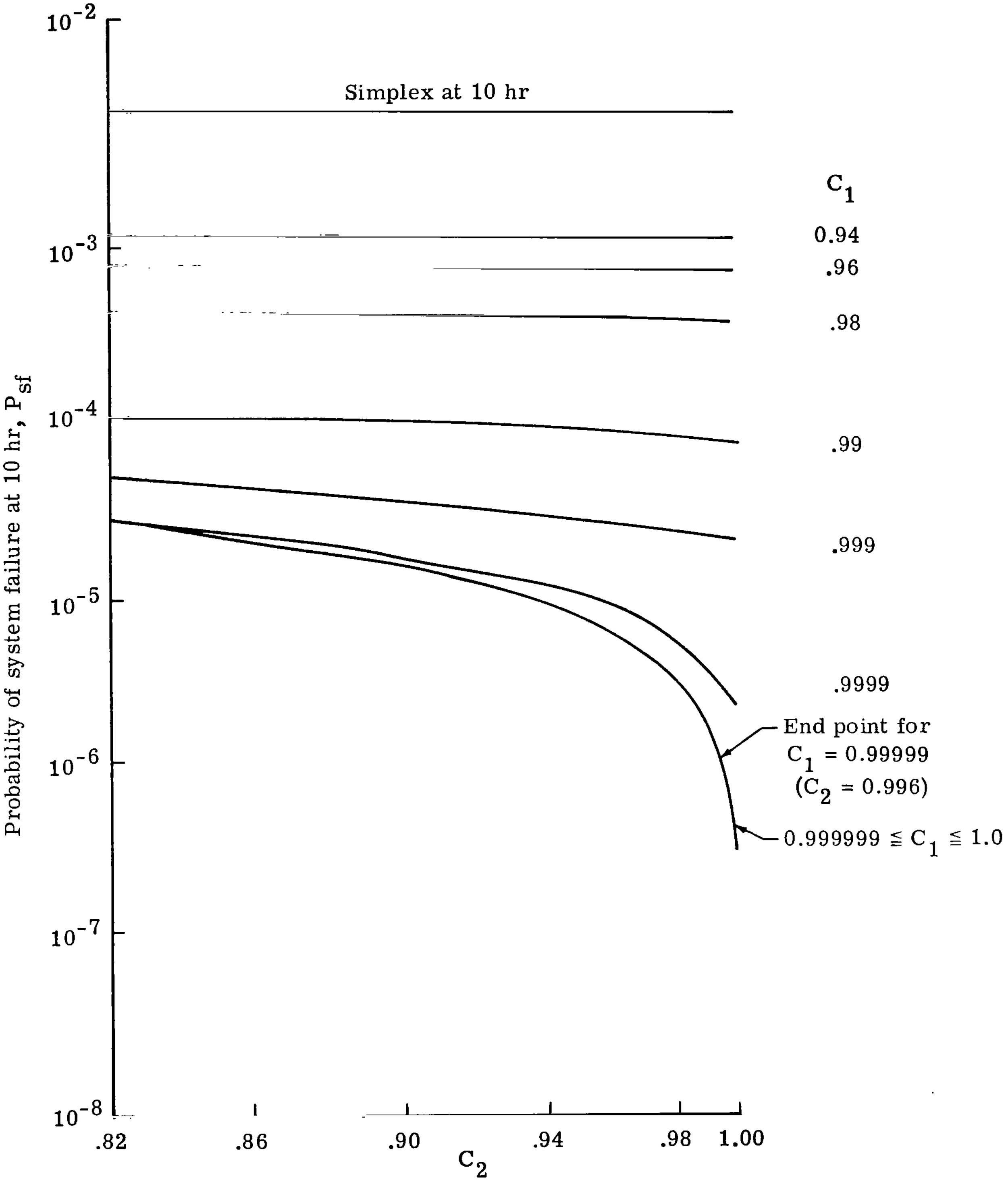

Figure 3.- Probability of system failure as a function of coverage.

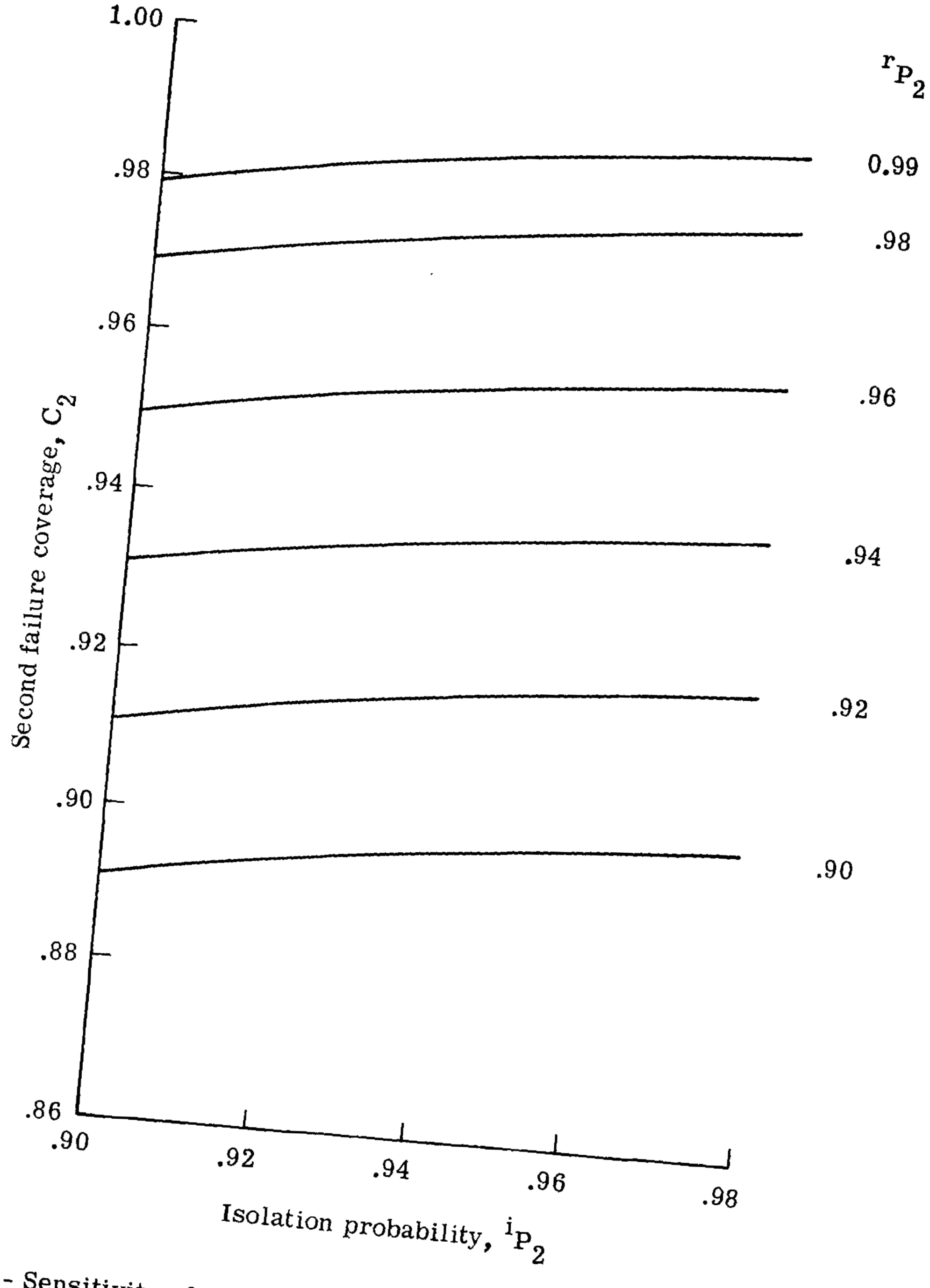

Figure 4.- Sensitivity of second failure coverage to $^{r}P_2$ and $^{i}P_2$. $^{d}P_2 = 1$.

NASA-Langley, 1975 L-10050

> *"The aeronautical and space activities of the United States shall be conducted so as to contribute . . . to the expansion of human knowledge of phenomena in the atmosphere and space. The Administration shall provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."*
>
> —NATIONAL AERONAUTICS AND SPACE ACT OF 1958

NASA SCIENTIFIC AND TECHNICAL PUBLICATIONS

TECHNICAL REPORTS: Scientific and technical information considered important, complete, and a lasting contribution to existing knowledge.

TECHNICAL NOTES: Information less broad in scope but nevertheless of importance as a contribution to existing knowledge.

TECHNICAL MEMORANDUMS: Information receiving limited distribution because of preliminary data, security classification, or other reasons. Also includes conference proceedings with either limited or unlimited distribution.

CONTRACTOR REPORTS: Scientific and technical information generated under a NASA contract or grant and considered an important contribution to existing knowledge.

TECHNICAL TRANSLATIONS: Information published in a foreign language considered to merit NASA distribution in English.

SPECIAL PUBLICATIONS: Information derived from or of value to NASA activities. Publications include final reports of major projects, monographs, data compilations, handbooks, sourcebooks, and special bibliographies.

TECHNOLOGY UTILIZATION PUBLICATIONS: Information on technology used by NASA that may be of particular interest in commercial and other non-aerospace applications. Publications include Tech Briefs, Technology Utilization Reports and Technology Surveys.

Details on the availability of these publications may be obtained from:

SCIENTIFIC AND TECHNICAL INFORMATION OFFICE

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Washington, D.C. 20546