**REPORT DOCUMENTATION PAGE**

<table>
<thead>
<tr>
<th>1. REPORT NUMBER</th>
<th>2. GOVT ACCESSION NO.</th>
<th>3. RECIPIENT'S CATALOG NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>NRL Memorandum Report 4934</td>
<td>A0-A121-2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE (and Subtitle)</th>
<th>5. TYPE OF REPORT &amp; PERIOD COVERED</th>
<th>6. PERFORMING ORG. REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>A SIMULATOR FOR RELIABILITY PREDICTIONS OF FAULT-TOLERANT SYSTEM ARCHITECTURES</td>
<td>Interim report on a continuing NRL problem.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. AUTHOR(s)</th>
<th>8. CONTRACT OR GRANT NUMBER(s):</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.N. Marinos (Consultant)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. PERFORMING ORGANIZATION NAME AND ADDRESS</th>
<th>10. PROGRAM ELEMENT PROJECT, TASK AREA &amp; WORK UNIT NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naval Research Laboratory</td>
<td>62712N; SF-12-131-691; 53-0615-0-0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11. CONTROLLING OFFICE NAME AND ADDRESS</th>
<th>12. REPORT DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>September 30, 1982</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. MONITORING AGENCY NAME &amp; ADDRESS IF DIFFERENT FROM CONTROLLING OFFICE</th>
<th>15. SECURITY CLASS. (OF THIS REPORT)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UNCLASSIFIED</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16. DISTRIBUTION STATEMENT (OF THIS REPORT)</th>
<th>17. DISTRIBUTION STATEMENT (OF THE ABSTRACT ENTERED IN BLOCK 20, IF DIFFERENT FROM REPORT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release; distribution unlimited.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19. KEYWORDS (CONTINUE ON REVERSE SIDE IF NECESSARY AND IDENTIFY BY BLOCK NUMBER)</th>
<th>20. ABSTRACT (CONTINUE ON REVERSE SIDE IF NECESSARY AND IDENTIFY BY BLOCK NUMBER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability simulator</td>
<td>This study is concerned with a simulation technique suitable for predicting the</td>
</tr>
<tr>
<td>Reliable radar design</td>
<td>reliability of fault-tolerant system architectures.</td>
</tr>
<tr>
<td>Reliability</td>
<td>General fault-occurrence probability density functions are introduced, and techniques</td>
</tr>
<tr>
<td></td>
<td>for generating postulated fault environments using these functions are presented.</td>
</tr>
<tr>
<td></td>
<td>Methods for assigning faults to subsystems of a system exposed to a given</td>
</tr>
<tr>
<td></td>
<td>(Continues)</td>
</tr>
</tbody>
</table>
fault-environment are discussed and the utility of these methods for making reliability predictions is illustrated with a specific example derived from the radar field.

The simulator which has been written in FORTRAN-77 is highly interactive and user oriented, and provides in addition to system reliability estimates, system MTBF and availability estimates under various repair strategies and degrees of fault-coverage.
CONTENTS

INTRODUCTION .................................................. 1

FAULT-TOLERANT SYSTEMS ...................................... 1

THE RELIABILITY ESTIMATION SIMULATOR ...................... 3

FAULT-PATTERN SIMULATION .................................. 6

MATHEMATICAL BACKGROUND .................................. 6

FAULT DISTRIBUTION FUNCTIONS .............................. 7

REDUNDANCY MODELING ...................................... 10

MATHEMATICAL BACKGROUND .................................. 10

REDUNDANCY MODES .......................................... 14

SIMULATION EXAMPLES ........................................ 15

CONCLUSIONS .................................................. 25

ACKNOWLEDGEMENTS .......................................... 25

REFERENCES .................................................... 25
A SIMULATOR FOR RELIABILITY PREDICTIONS OF
FAULT-TOLERANT SYSTEM ARCHITECTURES

INTRODUCTION

Very reliable systems are required in many critical applications, such as flight control, radar systems, process control, etc., and in order to meet their high reliability requirements, redundancy techniques must be employed in their implementation. However, the diversity and sophisticated usage of redundant structures has made the problem of reliability prediction so difficult that search for efficient methods for predicting system reliability in a timely and cost-effective manner is presently a matter of great practical interest.

The prime objective of a reliability prediction method is to provide evidence to both the designer and the user that the system will perform its intended function satisfactorily under the environmental and operating conditions present at the time of actual use.

Accurate descriptions of different reliability modes, the manner in which they are incorporated in system design, and the method used for generating the appropriate fault environment constitute the basis of the proposed simulation technique.

The goal of the work reported here has been to develop a general method for predicting system reliability, but in a way which allows evaluation also of systems operating in a fault environment which is different from that implied by their assumed failure modes. In short, this study presents a general viewpoint of reliability models for redundant structures and a technique for exposing fault-tolerant systems to simulated fault environments for the purpose of making system reliability predictions.

FAULT-TOLERANT SYSTEMS

A Fault-Tolerant System is one which is designed to continue performing correctly even in the presence of a fault; reliability is a measure of how well this design objective is met. A fault can be defined as a deviation from normal operation, and it may be either transient or permanent in nature. Transient faults are typically caused by interference, power supply fluctuations, failure to meet temperature or humidity specifications, etc. Permanent faults, on the other hand, are caused by hardware failures, usually of a permanent nature.

Protective redundancy provides a means by which fault-tolerance can be achieved; it consists of additional hardware, software or computation time.
that would not be necessary if the system were fault free. Redundancy in time
is achieved by performing a task many times; redundancy in hardware is realized
by replicating components; and redundancy in software is achieved by writing
more than one program for the same task. These methods require an appropriate
algorithm for choosing the correct result from among the many replications.
The most common such algorithm is the one based on the so-called Majority
Voting Scheme. Systems operating in this manner need no repair mechanism
until a majority of the active units fail. When a fault occurs, the affected
unit is not removed; thus, systems using a voting mechanism are useful in
situations where the vast majority of faults are transient. Other techniques
used to mask faults include error detecting and correcting codes and quadded
logic. For a more detailed discussion of redundancy schemes and fault masking,
the reader is referred to [1-5, 10].

There are many other situations, however, in which it is necessary for a
system to perform self-diagnosis and repair, and thus have the capability of
automatic reconfiguration. That is, the system must be able to detect faulty
output, locate its source, and remove the failed component. The offending
component is replaced by a standby spare, that is, a redundant component
which remains inoperative until needed. Detection and recovery from all
failures is not perfect. There are, in general, a small number of faults from
which a system cannot recover automatically. The fault coverage of a system
is defined as that fraction of faults for which a system recovery strategy
exists. Systems utilizing automatic reconfiguration techniques are inherently
complex; a fairly sophisticated monitoring mechanism is necessary, as well as
a means to switch alternate units into operation.

Various analytical approaches have been used to study the reliability of
fault-tolerant systems. The major drawback of these approaches is the rate
at which computational complexity increases as system complexity increases.
In fact, for many redundant systems, there is no closed form solution, and
alternative approaches must be utilized in order to evaluate their performance
characteristics.

In this study we develop an interactive software package for evaluating
the reliability of fault-tolerant systems. The major difference between this
package and others that have been developed is the basic approach used to
estimate reliability. Most automated reliability estimation packages consist
of a collection of mathematical equations defining the various redundancy
schemes, which are then used to generate a mathematical model for the system
under study [7,12,15]. The system parameters are input to the program, and
the reliability is calculated from these equations. The major shortcoming of
this approach arises from the many simplifying assumptions which are made in
the derivation of the mathematical equations defining the redundancy schemes.

In contrast, the package developed in this study simulates the system
directly. A complete description of the system to be studied is input to the
program interactively, and a varied menu of choices for both redundancy mode
and fault distributions are available. It is not assumed that the failure
rates for the active units and standby spares are identical; neither is the
switch mechanism assumed to be fault-free. The possibility for self-recovery
and manual repair are considered, as is the notion of fault coverage. The
operation of the system with respect to the incidence of faults is simulated
for a specified period of time, and the simulation is repeated several times. The number of repetitions of the simulation depends upon the accuracy which the user requires. The reliability of the system is then estimated as the percentage of the simulation trials in which the system survived to mission end. Comparisons of the simulation results with analytical expressions for simple systems are discussed in a subsequent section.

THE RELIABILITY ESTIMATION SIMULATOR

The Reliability Estimation Simulator predicts the reliability of a fault-tolerant system design by observing its reaction to the specified fault environment. The system being simulated is assumed to consist of a serial connection of \( N \) subsystems as in Fig. 1; functional integrity is assured only if all \( N \) subsystems are operational.

![Fig. 1 - A Serial Connection of N Subsystems](image)

The description of the system is interactively input to the simulator; a complete description of each of the \( N \) subsystems is required. Information is requested concerning the fault arrival pattern, redundancy mode, number of spares, fault coverage and repair mechanism for each of the subsystems. Different fault distributions, coverage and repair parameters are permitted for active and dormant units. The mechanism used to switch in spare units is not assumed to be perfect. The user is then queried as to the length of the mission to be simulated, and the simulation begins.

A list of times at which a fault will occur is generated for each subsystem, according to the specified fault distribution. This list is then sorted for ascending time, and comprises the queue of events to occur. Another type of event is the completion of the recovery procedure invoked on behalf of a faulty component.

The simulator is event-driven: an event occurs, and is processed. Simulated time is then advanced to the next event. Events are considered as long as the system is operational; if the system fails, the simulation ends.

Suppose the event being processed is a fault affecting an active unit, then a random number determines whether the fault is covered. If the fault is covered, the length of the recovery operation is simulated by generating a deviate of the recovery distribution. This deviate, when added to the current time, represents the time at which the failed unit again becomes operational.
If the fault is not covered, the unit has experienced a catastrophic failure and is removed from further consideration for that run.

Fig. 2 - Top level flow of the Reliability Estimation Simulator
If a spare exists in the affected subsystem, it is switched into operation upon the failure of an active unit. From this time, any future faults associated with this unit must follow the distribution of its active status. When the failed unit recovers, it is then placed on the list of spare units, and its faults behave accordingly.

Suppose the event being processed is a fault affecting a spare unit, then it is simply removed from the list of available spares. If the fault is covered, simulated recovery begins as discussed previously. When a fault affects the switching mechanism, the system fails catastrophically.

Suppose the event being processed is the completion of the recovery of a previously faulted unit, then one of two things can happen. If the recovered unit was previously replaced by a spare, it becomes upon recovery a spare unit itself. If it were not replaced by a spare, it is upon recovery switched back into active operation.

After each event is processed, if the system is still operational, the next event is considered. When the system fails, or the mission length is completed, the simulation ends.

The simulation is initially repeated 100 times; the reliability is then viewed as the success ratio [proportion] in a number of Bernoulli trials. The user is advised of the failure ratio/proportion, and is queried as to the absolute error and level of confidence required. The number of additional trials is then calculated by the following formula:[13]

\[ N = \left(\frac{Z_c}{E}\right)^2 \times p \times q - 100 \]

where:
- \( N \) is the number of additional trials to run
- \( E \) is the bound on the error of estimation
- \( p \) is the estimated success ratio (or proportion)
- \( q \) is the estimated failure ratio (or proportion)
- \( Z_c \) is the value such that the probability of making an error of estimation greater than \( E \) is less than \((1 - \text{the level of confidence})\)

The user is then advised as to the number of additional trials necessary to meet the specifications; these specifications can be altered, if necessary. The simulation continues until the specifications are met.

At the completion of the simulation, information is output concerning the overall system reliability (or success rate). Also output is the percentage of catastrophic failures caused by each subsystem, so that the "weakest link" in the system can be identified.

The Reliability Estimation Simulator was written in Fortran-77 (AOS/VS F77) and runs on a Data General MV/8000 System. A program listing is available from the Naval Research Laboratory, Code 5340.
The flexibility of the Reliability Estimation Simulator may be attributed, in part, to the wide variety of fault distributions included. A brief mathematical background is provided here along with a discussion of each of the pertinent distributions.

1. MATHEMATICAL BACKGROUND

Lifetime -- Let $X$ be a random variable which represents the lifetime, or time-to-failure, of a component. Then the cumulative distribution function, $F_X(t)$, is defined as the probability that the lifetime, $X$, is less than or equal to $t$.

$$F_X(t) = \text{Prob} (X \leq t)$$

Reliability function -- The Reliability function, $R_X(t)$, is defined as the probability that the lifetime $X$ is greater than $t$, and thus is the complementary function to $F_X(t)$.

$$R_X(t) = 1 - F_X(t)$$

If $X$ is a discrete random variable, then the distribution function, and as a consequence the reliability function, are step functions. If $X$ is a continuous random variable, its distribution and reliability functions are continuous for all $t$. Also, $F_X(t)$ and $R(t)$ admit a derivative in the interval where they are defined, if $X$ is absolutely continuous, as usually assumed.

Density function -- Consider the distribution function $F_X(t)$ such that $X$ is a continuous random variable. Then $f_X(t)$, the time derivative of the distribution function, is called the lifetime probability density function.

$$f_X(t) = \frac{dF_X(t)}{dt} = -\frac{dR_X(t)}{dt}$$

The quantity $f_X(t)\,dt$ represents the probability that a component experiences a failure in the interval $(t,t+dt)$. We are often more interested in the conditional probability that a component suffers a failure in the interval $(t,t+dt)$, given that the component has survived until time $t$.

Hazard Rate -- The conditional probability of an event $A$, given that event $B$ has occurred, is equal to

$$\text{Prob}(A|B) = \frac{\text{Prob}(A \text{ and } B)}{\text{Prob}(B)}.$$  

If we let event $A$ be "the component suffers a failure in the time interval $(t,t+dt)$" and event $B$ be "the unit has survived until time $t,"$ the above equation becomes

$$f_X(t)\,dt / R(t)$$

We can then define a hazard rate, $h_X(t)$, such that the quantity $h_X(t)\,dt$ is the conditional probability that a component suffers a failure in the interval $(t,t+dt)$, given that the component has survived until time $t$. 


The hazard rate directly determines the reliability of the component:

\[ h(t) = \frac{(-dR(t)/dt)}{R(t)} \]

\[ R(t) = \exp\left\{ \int_0^t h(x) \, dx \right\} \]

Deviate Generation -- One of the tools necessary for successful simulation of component lifetimes is the ability to generate a series of times at which faults will occur, such that the resulting lifetime mimics the desired distribution function. These fault times are called deviates of the distribution, and are formed by an appropriate transformation of a "random number."

In general, a random number uniformly distributed in the interval [0,1] is generated. (This capability is usually a built-in feature of the computer on which the simulation is run.) This random number, call it \( U \), is then associated with a probability,

\[ U = \text{Prob}(X < t) = F_X(t) \quad (1) \]

and the equation is solved for \( t \).

If the inverse of the cumulative distribution function exists, the transformation is analytically tractable. If the inverse does not exist, many well-known approximation techniques are available [14].

2. FAULT DISTRIBUTION FUNCTIONS

Uniform Distribution -- The Uniform distribution is the simplest of the continuous distributions. It is characterized by two parameters, \( a \) and \( b \); events within the interval \([a,b]\) are equally likely to occur, events outside that interval occur with probability zero. The density and distribution functions for the Uniform distribution are:

\[ f(t) = \begin{cases} 1/(b-a) & \text{for } t \in [a,b] \\ 0 & \text{for } t \notin [a,b] \end{cases} \]

\[ F(t) = \begin{cases} 0 & \text{for } t < a \\ (t-a)/(b-a) & \text{for } t \in [a,b] \\ 1 & \text{for } t > b \end{cases} \]
Deviates of a general uniform distribution are obtained by first generating a random number $U$, which is itself uniformly distributed between 0 and 1, and transforming it according to Eq. (1). This yields,

\[ \text{Deviate} = U \cdot (b-a) + a \]

**Exponential Distribution** -- The Exponential distribution is characterized by its constant hazard rate, $K$. This constant failure rate implies that the failure probability remains constant throughout the item's lifetime. This distribution is the most common one used to model time to failure of electronic components. The hazard, density and distribution functions of the Exponential distribution are [17]:

\[
\begin{align*}
    h(t) & = K \\
    f(t) & = Ke^{-Kt} \\
    F(t) & = 1 - e^{-Kt}
\end{align*}
\]

Deviates of the Exponential distribution are generated by the simple transformation:

\[ \text{Deviate} = (-1/K) \cdot \ln(1-U) \]

**Rayleigh Distribution** -- The Rayleigh distribution is characterized by a linearly increasing hazard rate. This model is useful when wear out or deterioration is present in the component. The hazard, density and distribution functions for the Rayleigh distribution are [17]:

\[
\begin{align*}
    h(t) & = Kt \\
    f(t) & = Kte^{-Kt^2/2} \\
    F(t) & = 1 - e^{-Kt^2/2}
\end{align*}
\]

Deviates of the Rayleigh distribution are generated as in Equation (1), by the transformation:

\[ \text{Deviate} = \sqrt{(-2/K) \cdot \ln(1-U)} \]

**Weibull Distribution** -- The Weibull distribution is used to model various hazard rate curves. The hazard, density and distribution functions are given by [17]:

\[
\begin{align*}
    h(t) & = \frac{Kt^{K-1}}{2} \\
    f(t) & = Kte^{-Kt^2/2} \\
    F(t) & = 1 - e^{-Kt^2/2}
\end{align*}
\]
\[ h(t) = Kt^m, \quad m > -1 \]

\[ f(t) = Kt^m \cdot e^{-Kt^{m+1}/m+1} \]

\[ F(t) = 1 - e^{-Kt^{m+1}/m+1} \]

By appropriate choice of the two parameters \( K \) and \( m \), a wide range of hazard curves can be approximated. The parameter \( m \) determines the shape of the distribution, and parameter \( K \) is a scale change parameter.

Deviates of the Weibull distribution are generated, as in Eq. (1), by the transformation of \( U \):

\[ \text{Deviate} = ((-(m+1)/K) \cdot \ln(1-U))^{(1/m+1)} \]

Normal Distribution -- Perhaps the most widely recognized two parameter distribution is the Normal distribution. This distribution is often a good fit for the size of manufactured parts or the magnitude of certain electrical signals. The density and distribution functions of the Normal distribution, where \( M \) is the mean, and \( S \) is the standard deviation are [13]:

\[ f(t) = \frac{1}{S \sqrt{2\pi}} \cdot e^{-\frac{(t-M)^2}{2S^2}} \]

\[ F(t) = \frac{1}{S \sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{(y-M)^2}{2S^2}} \, dy \]

The distribution function is left in integral form since the result cannot be expressed in closed form. This poses no great difficulty since \( F(t) \) has been extensively tabulated; a table look up method is used to generate deviates of the Normal distribution [14]. Negative deviates are disregarded (and new ones calculated) when generating fault times; the accepted deviates more accurately belong to the Truncated Normal Distribution.

Log-Normal Distribution -- The Log-Normal distribution is characterized by the fact that the natural logarithm of deviates of this distribution follow the Normal distribution. The Log-Normal distribution is often used to model skewed data; another important feature of this distribution is that it is a non-negative distribution.

Deviates of the Log-Normal distribution are generated by first generating a deviate, \( X \), of the Normal distribution with mean \( M \) and standard deviation \( S \). Then the Log-Normal deviate is equal to [6].

\[ \text{Deviate} = \exp(X) \]
Chi-Squared Distribution -- The Chi-Squared distribution is characterized by its degrees of freedom, \( N \). The simplest approach to generating deviates of the Chi-Squared distribution is to generate \( N \) deviates of the Normal distribution (\( \mu = 0, \sigma = 1 \)): \( X_1, X_2, \ldots, X_N \), and sum their squares [6].

\[
\text{Deviate} = \sum_{j=1}^{N} x_j^2
\]

REDUNDANCY MODELING

The flexibility of the Reliability Estimation Simulator can also be attributed to the complexity of the model available for each subsystem. This model includes not only structural parameters such as the number of active and dormant units, but also provides for fault coverage, switch reliability and self-repair strategies. Background information for each of the model parameters is presented here, followed by a discussion of each of the redundancy modes included in the simulator.

1. MATHEMATICAL BACKGROUND

Static Redundancy --- Consider a system in which an active component is replicated \( N \) times; system integrity is assured if any \( M \) or more components are operating correctly. We assume that each component has only two possible states, fault-free and failed, and once a fault has occurred, the component remains in the failed state. We further assume that the components fail independently; a failure in one component does not affect the operation of any other component. The system is operational until the \( n \)th failure, where \( n = (N-M+1) \).

The reliability of the system at time \( t \), \( R_s(t) \), may be viewed as the probability that \( n \) or more of the component lifetimes are greater than \( t \). Recall that \( R(t) \) is the probability that the lifetime of a component is greater than \( t \). Then the reliability of the system may be considered as a sequence of \( M \) Bernoulli trials, where the probability of success, \( p \), is precisely the reliability of an individual component.

\[
R_s(t) = \sum_{i=M}^{N} \binom{N}{i} R(t)^i (1-R(t))^{N-i} \tag{2}
\]

The most popular static redundancy scheme consists of three copies of the active component and a majority voting element, and is thus called Triple Modular Redundancy (TMR).

Each of the components receives an identical set of inputs; the three output lines are input to the voter element, which in turn generates the system output. The system output will be correct during the occurrence of any single fault; the system fails if any two or more subsystems fail. The reliability of the TMR system may be calculated by Eq. (2), which reduces to

\[
R_s(t) = 3R(t)^2 - 2R(t)^3 \tag{3}
\]
The concept of TMR can be generalized to N-Modular Redundancy (NMR), in which there are $N$ identical copies of the unit, where $N = 2^n - 1$. The system fails when $n$ or more failures have occurred.

Fig. 3 - Triple Modular Redundancy

Fig. 4 - An NMR type system
Automatic Reconfiguration — Consider a system consisting of \( N \) active units and a bank of \( S \) spare units such that when one of the active units fails, a spare unit replaces it.

![Diagram of an Automatically Reconfigurable System]

The switching mechanism contains a disagreement detector which compares the system output from the voter with the outputs of each of the active units. When a disagreement occurs, the switching unit replaces the offending unit with one of the spares. This system usually reduces to a simple NMR system when all the spares have been exhausted. The correct operation of the switching mechanism is vital to the system: if it fails, the system fails.

The reliability of an automatically reconfigurable system, with \( N \) active and \( S \) spare units, in which the faults for both the active and spare units are exponentially distributed (with parameters \( r \) and \( m \), respectively) is given by the Eq. (11).

\[
R(t) = R_a(t)^N * R_s(t)^S + (N*r + S*m) \int_0^t e^{-(N*r + S*m)x} R\#(x) \, dx
\]
where  
\( Ra(t) \) = reliability of an active unit  
\( Rs(t) \) = reliability of a spare unit  
\( R^s(t) \) = reliability of the system with \( N \) active units  
and \( S-1 \) spare units

The solution for the case of one spare is given in Eq. (11).

**Coverage and Self-Repair** -- Fault Coverage may be also defined as the conditional probability that, given the existence of a failure in the operational system, the system is able to recover, and continue processing with no loss of essential information [16].

\[
\text{Coverage} = \text{Prob} \left[ \text{system recovers} \mid \text{system fails} \right]
\]

The notion of recovery varies with the particular design of a system. In some cases, recovery simply means to retry an operation; in others, it involves detection, location and automatic repair of the hardware involved.

Systems involving automatic recovery mechanisms are most easily analyzed by using Markov chain models. Consider a system composed of one active unit and one spare unit. The time to failure for each component, as well as the time to repair a component are all exponentially distributed. This system may be modeled by a Markov process with three states [1].

![Markov Process Diagram](image)

\[
\lambda = \text{failure rate} \\
\mu = \text{repair rate} \\
P = \text{Prob} \left[ \text{fault covered} \right]
\]

**Fig. 6 - Markov Process**

The system is in state-1 when both units are operational. Covered faults cause a transition to state-2, which represents the condition with one unit operational and one unit under repair. As long as one unit is functional, the system will return to state-1 when repair is completed. A non-covered fault in state-1 causes a transition to state-3, system failed. A transition from state-2 to state-3 occurs if the second unit fails before the first is repaired.

As systems become more complex, the number of states in such a Markovian model increases dramatically. The analysis of such a system becomes very
difficult, even under the assumption that all random variables are exponentially distributed.

2. **REDUNDANCY MODES**

**Simplex Mode** — A system in which only one unit is active is said to operate in the Simplex mode.

Spare units can be switched into active mode in the event of a failure, if the system has fault-diagnosis capabilities and an appropriate switching mechanism. Such a system survives until the last spare unit fails, or until the switching unit fails.

**Duplex Mode** — A Duplex system is comprised of two identical active units performing the same task. The outputs of these units are compared; a fault manifests itself as a disagreement at the comparator.

If the system has on-line fault detection and location capabilities, the faulty unit can be diagnosed and removed from operation. The system then continues functioning in the Simplex mode. If the system does not have these capabilities, the disagreement is interpreted as system failure. In either case, spare units can be switched into operation via the appropriate switching mechanism, until the disagreement disappears.

**TMR Mode** — The Reliability Estimation Simulator models three types of TMR systems: Simple TMR, TMR/Simplex, and Hybrid TMR. Simple TMR consists of three identical active units; the system fails when the second unit fails. TMR/Simplex systems degrade to Simplex mode upon detection and location of the
second fault. Hybrid TMR systems have self-diagnosis capabilities and an appropriate network for replacing a faulted unit with a spare.

**NMR Mode** -- The classical N-Modular Redundant mode is a generalization of TMR mode consisting of N identical active units. The outputs of at least n units must agree \((N = 2n - 1)\). As with other modes, NMR systems with self-diagnosis abilities may contain spare units.

The NMR model can be further generalized to model any K-out-of-N redundant system; as long as K units are operating, the functional integrity of the system is assured.

**SIMULATION EXAMPLES**

In this section, a few fault tolerant designs are presented, and their reliability is estimated by analysis and simulation.
Example 1 -- Consider a TMR system with components having constant failure rate $K = 0.02$ failures per hour. We wish to know the reliability of this system for a mission length of 25 hours. The reliability of a single component can be calculated as

$$F(t) = 1 - e^{-kt} = 0.3935$$

$$R(t) = 1 - F(t) = 0.6065$$

The reliability of the system can be calculated from Eq. (3). That is,

$$R_{sys}(T) = 3R(T)^2 - 2R(T)^3 = 0.6574$$

The simulation output follows:

SYSTEM BEING SIMULATED

NUMBER OF SUBSYSTEMS: 1

SUBSYSTEM NUMBER: 1

REDUNDANCY MODE: TMR

NUMBER NEEDED FOR INTEGRITY: 2

NUMBER OF ACTIVES: 3

NUMBER OF SPARES: 0

FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP .020000000 .000000000

PROBABILITY OF FAULT RECOVERY: .00000

---------END OF SYSTEM DESCRIPTION---------

MISSION LENGTH: 25

SIMULATION COMPLETE.... 3303.0 TRIALS

RELIABILITY: .6566758
SUCCESSES: 2169.0
FAILURES: 1134.0

PERCENTAGE OF SYSTEM FAILURES CAUSED BY:

<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th>PERCENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100.000</td>
</tr>
</tbody>
</table>

16
Consider the same TMR system with the addition of two spare units. The spare units are assumed to fail at the same rate as the active units. The reliability of this system is given in [11] as:

\[ R = 1 - (1 - R)^4 (1 + 4R) \]

which reduces to:

\[ R = 10R^2 - 20R^3 + 15R^4 - 4R^5 = 0.917881 \]

The simulator estimates the reliability to be 0.90232, given that the switch fails only once in 4000 trials. This was accomplished by assuming that the faults for the switch are uniformly distributed between 0 and 100000.

If the failure rate of the spare units is assumed to be half that of the active units, the reliability estimate rises to 0.922821. If half of the faults are assumed to be covered, and the recovery time is normally distributed (mean = 4, st. dev. = 1), the reliability is estimated to be 0.964285. With coverage of 0.9, the estimated reliability becomes 0.9950. Each of these simulations requested a confidence level of 80%, and maximum error of estimation less than 0.01. It took less than one half hour to run these simulations while the Data General MV-8000 machine was moderately loaded.

Example 2 -- Consider the switch circuit shown in Fig. 9. The components and their corresponding total failure rates are given in Fig. 10.

---

**Fig. 9 - Switch Schematic**
This system was modeled first as a serial connection of seven components, then as a simplex system with failure rate = 0.1342E-6 failures per hour. This figure represents the sum of the individual failure rates. The comparison of those simulations with the analytical calculations appears in Fig. 11, for mission times in increments of one million hours. The confidence level for the simulations was 80%, with absolute error less than 0.01.

<table>
<thead>
<tr>
<th>Component</th>
<th>Count</th>
<th>Failures per hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Clock logic</td>
<td>1</td>
<td>0.029E-6</td>
</tr>
<tr>
<td>2 Buffer</td>
<td>1</td>
<td>0.0025E-6</td>
</tr>
<tr>
<td>3 Resistor</td>
<td>2</td>
<td>0.0007E-6</td>
</tr>
<tr>
<td>4 Diode</td>
<td>1</td>
<td>0.075E-6</td>
</tr>
<tr>
<td>5 Capacitor</td>
<td>3</td>
<td>0.001E-6</td>
</tr>
<tr>
<td>6 Filter</td>
<td>2</td>
<td>0.001E-6</td>
</tr>
<tr>
<td>7 RF Connector</td>
<td>2</td>
<td>0.025E-6</td>
</tr>
</tbody>
</table>

Fig. 10 - Component Failure Rates

<table>
<thead>
<tr>
<th>Mission Time in million hours</th>
<th>Simulated</th>
<th>Simulated Simplex System</th>
<th>Simplex Analytical Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.87263</td>
<td>0.85763</td>
<td>0.87442</td>
</tr>
<tr>
<td>2</td>
<td>0.75882</td>
<td>0.75649</td>
<td>0.76460</td>
</tr>
<tr>
<td>3</td>
<td>0.65133</td>
<td>0.64938</td>
<td>0.66858</td>
</tr>
<tr>
<td>4</td>
<td>0.56865</td>
<td>0.57053</td>
<td>0.58462</td>
</tr>
<tr>
<td>5</td>
<td>0.49971</td>
<td>0.50778</td>
<td>0.51120</td>
</tr>
<tr>
<td>6</td>
<td>0.43495</td>
<td>0.43155</td>
<td>0.44700</td>
</tr>
<tr>
<td>7</td>
<td>0.38098</td>
<td>0.37428</td>
<td>0.39086</td>
</tr>
<tr>
<td>8</td>
<td>0.33593</td>
<td>0.31508</td>
<td>0.34178</td>
</tr>
<tr>
<td>9</td>
<td>0.30416</td>
<td>0.26757</td>
<td>0.29885</td>
</tr>
<tr>
<td>10</td>
<td>0.25515</td>
<td>0.22549</td>
<td>0.26132</td>
</tr>
</tbody>
</table>

Fig. 11 - Comparison of Simulation and Analytic Results
Example 3 -- Consider the following RADAR receiving system:

--- > RF Module | --> | Elevation Switch | --> | Receiver | ---

| --- | Data Processor | <-- | Synchronizer | <-- | Driver | ---

| --- | Signal Processor | --> | Power Dist. | ---

<--- | Display | <-- | Interconnections | ---

Fig. 12 - A Radar Receiving System

A detailed description of each subsystem is given in the simulation output, and the constant failure rates are given in the following table:

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Mode</th>
<th>Failures/hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 RF Module</td>
<td>NMR</td>
<td>0.0119E-3</td>
</tr>
<tr>
<td>2 Elevation Sw</td>
<td>NMR</td>
<td>0.0083E-3</td>
</tr>
<tr>
<td>3 Receiver</td>
<td>TMR</td>
<td>0.0257E-3</td>
</tr>
<tr>
<td>4 Driver</td>
<td>Duplex</td>
<td>0.0192E-3</td>
</tr>
<tr>
<td>5 Synch.</td>
<td>Duplex</td>
<td>0.0548E-3</td>
</tr>
<tr>
<td>6 Data Proc.</td>
<td>TMR</td>
<td>0.0215E-3</td>
</tr>
<tr>
<td>7 Signal Proc.</td>
<td>NMR</td>
<td>0.0308E-3</td>
</tr>
<tr>
<td>8 Power Dist.</td>
<td>Simplex</td>
<td>0.005E-3</td>
</tr>
<tr>
<td>9 Interconnect</td>
<td>Simplex</td>
<td>0.005E-3</td>
</tr>
<tr>
<td>10 Display</td>
<td>Simplex</td>
<td>0.006E-3</td>
</tr>
</tbody>
</table>
The reliability of the system for a mission of six months (4320 hours) was calculated and simulated (confidence = 90%, error = 0.01). The comparison of these results follows:

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Module</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Analytic</td>
</tr>
<tr>
<td>1</td>
<td>RF Module</td>
<td>0.78349</td>
</tr>
<tr>
<td>2</td>
<td>Elevation Sw</td>
<td>0.99461</td>
</tr>
<tr>
<td>3</td>
<td>Receiver</td>
<td>0.96919</td>
</tr>
<tr>
<td>4</td>
<td>Driver</td>
<td>0.99674</td>
</tr>
<tr>
<td>5</td>
<td>Synch.</td>
<td>0.97603</td>
</tr>
<tr>
<td>6</td>
<td>Data Proc.</td>
<td>0.98474</td>
</tr>
<tr>
<td>7</td>
<td>Signal Proc.</td>
<td>0.95938</td>
</tr>
<tr>
<td>8</td>
<td>Power Dist.</td>
<td>0.97863</td>
</tr>
<tr>
<td>9</td>
<td>Interconnect</td>
<td>0.97863</td>
</tr>
<tr>
<td>10</td>
<td>Display</td>
<td>0.97441</td>
</tr>
<tr>
<td></td>
<td>Entire System</td>
<td>0.64778</td>
</tr>
</tbody>
</table>

The output for the simulation which was run on the entire system appears on the next four pages.
SYSTEM BEING SIMULATED

NUMBER OF SUBSYSTEMS: 10

SUBSYSTEM NUMBER: 1

REDUNDANCY MODE: NMR
NUMBER NEEDED FOR INTEGRITY: 241
NUMBER OF ACTIVES: 256
NUMBER OF SPARES: 0

FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP \(0.0000119\) \(0.0000000\)

PROBABILITY OF FAULT RECOVERY: \(0.0000\)

SUBSYSTEM NUMBER: 2

REDUNDANCY MODE: NMR
NUMBER NEEDED FOR INTEGRITY: 3
NUMBER OF ACTIVES: 3
NUMBER OF SPARES: 1

FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP \(0.0000083\) \(0.0000000\)
SPARES: EXP \(0.0000001\) \(0.0000000\)
SWITCH : UNIF \(0.0000000\) \(10000000.0000000\)

PROBABILITY OF FAULT RECOVERY: \(0.0000\)

SUBSYSTEM NUMBER: 3

REDUNDANCY MODE: TMR
NUMBER NEEDED FOR INTEGRITY: 2
NUMBER OF ACTIVES: 3
NUMBER OF SPARES: 0

FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP \(0.0000257\) \(0.0000000\)

PROBABILITY OF FAULT RECOVERY: \(0.0000\)

SUBSYSTEM NUMBER: 4
SUBSYSTEM NUMBER: 5
REDUNDANCY MODE: SIM
NUMBER NEEDED FOR INTEGRITY: 1
NUMBER OF ACTIVES: 1
NUMBER OF SPARES: 1

FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP .000054800  .000000000
SPARES: EXP .000001000  .000000000
SWITCH :UNIF .000000000 10000000.000000000

PROBABILITY OF FAULT RECOVERY: .00000

SUBSYSTEM NUMBER: 6
REDUNDANCY MODE: DUP
NUMBER NEEDED FOR INTEGRITY: 2
NUMBER OF ACTIVES: 2
NUMBER OF SPARES: 1

FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP .000021500  .000000000
SPARES: EXP .000001000  .000000000
SWITCH :UNIF .000000000 10000000.000000000

PROBABILITY OF FAULT RECOVERY: .00000

SUBSYSTEM NUMBER: 7
REDUNDANCY MODE: NMR
NUMBER NEEDED FOR INTEGRITY: 5
NUMBER OF ACTIVES: 6
NUMBER OF SPARES: 1

FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP .000030800 .000000000
SPARES: EXP .000001000 .000000000
SWITCH: UNIF .000000000 1.000000000 .000000000

PROBABILITY OF FAULT RECOVERY: .00000

SUBSYSTEM NUMBER: 8
REDUNDANCY MODE: SIM
NUMBER NEEDED FOR INTEGRITY: 1
NUMBER OF ACTIVES: 1
NUMBER OF SPARES: 0
FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP .000005000 .000000000

PROBABILITY OF FAULT RECOVERY: .00000

SUBSYSTEM NUMBER: 9
REDUNDANCY MODE: SIM
NUMBER NEEDED FOR INTEGRITY: 1
NUMBER OF ACTIVES: 1
NUMBER OF SPARES: 0
FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP .000005000 .000000000

PROBABILITY OF FAULT RECOVERY: .00000

SUBSYSTEM NUMBER: 10
REDUNDANCY MODE: SIM
NUMBER NEEDED FOR INTEGRITY: 1
NUMBER OF ACTIVES: 1
NUMBER OF SPARES: 0
FAULT DISTRIBUTION, PARAMETERS:
ACTIVE: EXP .000006000 .000000000

PROBABILITY OF FAULT RECOVERY: .00000

--------- END OF SYSTEM DESCRIPTION ---------

MISSION LENGTH: 4320
SIMULATION COMPLETE.... 6667.0 TRIALS

RELIABILITY: .64841
SUCCESSES: 4323.0
FAILURES: 2344.0

PERCENTAGE OF SYSTEM FAILURES CAUSED BY:

<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th>PERCENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>51.195</td>
</tr>
<tr>
<td>2</td>
<td>1.621</td>
</tr>
<tr>
<td>3</td>
<td>8.447</td>
</tr>
<tr>
<td>4</td>
<td>1.493</td>
</tr>
<tr>
<td>5</td>
<td>6.527</td>
</tr>
<tr>
<td>6</td>
<td>4.096</td>
</tr>
<tr>
<td>7</td>
<td>9.087</td>
</tr>
<tr>
<td>8</td>
<td>3.797</td>
</tr>
<tr>
<td>9</td>
<td>5.205</td>
</tr>
<tr>
<td>10</td>
<td>8.532</td>
</tr>
</tbody>
</table>
CONCLUSIONS

If the interactions between the various parameters in a fault-tolerant system are to be studied, more complex models must be developed to analyze system reliability. Wherever possible, an analytical model should be sought, since it can evaluate the performance with minimal effort and cost over a wide range of choices in the system parameters and configurations. Even with simplifying assumptions and decompositions, however, the resultant analytical model is often not mathematically tractable [9]. Then the only alternative for predicting the performance of a nonexistent system is simulation.

The simulator described in this report is a useful tool for evaluating the reliability of systems utilizing a variety of redundancy modes and fault distribution functions. The system may be provided to the simulator at any level of detail desired.

ACKNOWLEDGEMENTS

The author wishes to acknowledge the efforts of Mrs. Joanne Dugan who wrote the code for this simulator in partial fulfillment of her Master's degree under my supervision.

REFERENCES


