Abstract

The failure and repair of modules in an N-Modular Redundant (NMR) system are governed by a failure time distribution and repair time distribution, respectively. It is generally reasonable to assume that a module’s failure time distribution is a simple exponential distribution. However, it is not reasonable to assume that the repair time distribution is also exponential. Reliability models with non-exponential repair have a higher computational complexity than a model of the same system with an exponential repair time distribution.

This paper presents the results of a systematic study to determine whether non-exponential repair distributions produce significant differences in calculated NMR system Unreliability, relative to an exponential repair distribution with the same Mean Time to Repair (MTTR). Our approach is to embed Erlang repair distributions in Generalized Stochastic Petri Net (GSPN) models of NMR systems and evaluate the Unreliability. Our results show that for a wide range of system parameters, the choice of a repair time distribution has minimal impact on the calculated Unreliability. Rather, it is the MTTR that is the dominant parameter affecting Unreliability.

1. Introduction

The failure and repair of modules in an N-Modular Redundant (NMR) system are stochastic processes governed by a failure time distribution and a repair time distribution, respectively. System dependability is thus dependent upon these distributions. It is generally reasonable to assume that a module’s failure time distribution is a simple exponential distribution. However, it is not reasonable to assume that the repair time distribution is also exponential. In previous research, the Lognormal, increasing Weibull, and Erlang distributions have been the most popular choices to represent equipment repair time distributions.

Dependability models with non-exponential repair distributions have higher computational complexities than a model of the same system with an exponential repair time distribution. Therefore, we examine whether the repair time distribution makes a significant difference in the calculated Unreliability of an NMR system. Comparisons are made between exponential and representative non-exponential distributions with the same Mean Time To Repair (MTTR).

Our approach follows established methods of using Erlang distributions to approximate non-exponential repair distributions. It has been shown [10] that Erlang distributions can provide extremely accurate approximations of the Lognormal and Weibull distributions. Furthermore, an Erlang distribution can be implemented as a “phase-type” distribution comprising a sequence of exponentially distributed stages. Phase-type distributions can be embedded into Markovian models such as Generalized Stochastic Petri Nets (GSPNs). GSPNs constitute a flexible and powerful modeling methodology that permits a large number of system models to be studied under widely varying system parameters.

---

1. This work was partially funded by NASA via Nebraska Space Grants Consortium grant number NGT5-40037, and by the University of Nebraska Center for Communication and Information Science Research.

2. This work was performed while the author was with the Dept. of Computer Science and Engineering, University of Nebraska – Lincoln, Lincoln, NE 68588 - 0115
Section 2 presents background material on the more commonly used non-exponential repair time distributions. Section 3 is an overview of our methodology for comparing exponential and non-exponential distributions, and Section 4 presents the numerical results of the comparisons. Finally, Section 5 presents our conclusions and suggests directions for future research.

2. Background

2.1 Fault Distribution

In general, it has been shown that the failure rates of electronic components obey the so-called "bathtub" curve consisting of three distinct periods [1, 8]: (1) an initial “Infant Mortality” period, during which a component’s failure rate decreases with time, (2) a “steady state” period, during which the failure rate is constant, so that the failure distribution is exponential, (3) a “wear-out” period, during which the failure rate increases with time. In most applications, it is reasonable to assume a constant failure rate, yielding the exponential failure distribution. The rationale for this assumption is that first, all components are “burned-in”, or tested beyond the end of the infant mortality period, and second, preventive maintenance policies require component replacement before the wear-out period begins.

2.2 Repair Distributions

While it is generally reasonable to assume that failure distributions are exponential, it is not reasonable to assume that repair time distributions are also exponential [1, 12, 13]. In previous research, several distributions have been proposed as reasonable representations of equipment repair time distributions. By far, the most popular repair time distributions in the literature are the Lognormal and increasing Weibull distributions [1, 10, 13, 15]. Other popular repair distributions, like the Gamma, Rayleigh and Erlang [3, 10, 15], closely approximate Lognormal and Weibull distributions, but at a lower computational complexity.

2.2.1 Repair Distribution Shapes

What all of the above distributions have in common is the ability for the Cumulative Distribution Function (CDF) curve to assume a characteristic “S” shape that is representative of actual repair processes. Figure 1 illustrates this fact with the exponential CDF and the Lognormal, Weibull and Erlang CDFs with typical parameters (to be defined later). For purposes of illustration and comparison, all curves shown in Figure 1 have a mean value (MTTR) of unity.

In Figure 1, the time following the failure of a module is partitioned into three phases based on the semantics of a typical repair process. Phase A, immediately after failure, represents delays in beginning repair (e.g., travel, diagnosis, obtaining parts). Thus, during phase A, the probability of completing repair is near zero. During phase B, repair is typically in-progress. In phase C, the probability of repair being completed approaches unity. The “S” shapes of the three non-exponential curves in Figure 1 are good fits to these phenomena, while the exponential distribution offers a poorer fit (especially in phase A). Therefore, distributions that assume this “S” shape have proven to be good fits to empirical repair time data [10, 13, 15].

Fig. 1: Exponential vs. Common Non-exponential Repair CDFs

2.2.2. Overview of Repair Distributions

This subsection summarizes the most popular non-exponential repair distributions. Since space constraints demand brevity, the reader is referred to the literature for more details (e.g. [9, 11]).

A **Weibull distribution** has two parameters, $\lambda$ and $\kappa$, which affect the scale (extent along the time axis) and shape of the CDF curve, respectively. If $\kappa =1$, then the Weibull distribution becomes the exponential distribution. However, if $\kappa >1$, then the Weibull distribution assumes an “S” shape, which becomes more pronounced as the value of $\kappa$ increases. The Rayleigh distribution is simply a Weibull distribution with $\kappa =2$.

A **Lognormal distribution** also has two parameters, $\rho$ and $\alpha$, which likewise affect the scale and shape of the CDF curve, respectively. As with the Weibull
distribution, the parameter of primary interest for this study is \( a \). For values of \( a < 1 \), the Lognormal CDF assumes an “S” shape which becomes more pronounced as the value of \( a \) decreases.

**An Erlang distribution** is a phase-type distribution. Phase-type approximation is a method of representing a non-exponentially distributed function by a series of exponentially distributed stages, \([1, 2, 11]\). The method thus transforms a non-Markov model into an equivalent Markov model, which is generally simpler to solve. Distributions such as the Lognormal and Weibull can be closely approximated by relatively simple stage combinations \([11]\).

The Erlang distribution has two parameters, \( r \) and \( \rho \), which are the number of exponential stages in the series, and the transition rate of each stage, respectively. Clearly a single stage Erlang is just an exponential distribution. However, as the number of stages increases, the Erlang CDF assumes an “S” shape similar to those of the Weibull and Lognormal distributions. In fact, it has been shown that the Erlang distribution can accurately approximate Lognormal and Weibull distributions \([3, 10, 11, 13]\), as illustrated in Figure 1.

### 2.3 Previous Comparison Repair Distributions

Despite the large volume of research conducted on Non-Exponential repair distributions, few publications have compared calculated Unreliability between different distributions \([2, 5, 10]\).

In one study, a comparison of the Lognormal distribution to a Gamma approximation of the Lognormal has shown that the Gamma distribution can be used in lieu of the Lognormal for computing the system Availability. However, no comparison of the Lognormal to the exponential distribution was reported \([2]\). A second study compared the steady-state Availability of redundant computer systems with common-cause failures under exponential repair and Gamma repair, respectively \([5]\). However, the comparison condition did not use the same mean time to repair (MTTR) for both distributions. Another study compared a Lognormal repair distribution to an exponential repair-time distribution with the same MTTR \([10]\). The resulting difference in calculated Unreliability did not exceed 10%. However, that study was limited to a single architecture, a dual redundant system, and only one value for MTTR.

It thus appears that until now, no systematic study has been performed to determine whether non-exponential repair distributions produce significant differences in calculated reliability than exponential repair distributions. The remainder of this paper presents such a study.

### 3. Approach and Methodology

This section describes a study to determine whether non-exponential repair distributions produce significant differences in NMR system Unreliability, relative to an exponential distribution with the same MTTR. The goal is to determine which combinations of system parameters yield significant differences in calculated Unreliability. Based on the previous research cited in subsection 2.2.2, we use Erlang distributions as representative non-exponential distributions.

The constant in each comparison is the MTTR. Our approach is to embed the Erlang repair distributions in Generalized Stochastic Petri Net (GSPN) models of NMR systems and evaluate the Unreliability. In the process, a number of system parameters are systematically varied over a wide range of values. Evaluation of the GSPNs was conducted using the commercially available Stochastic Petri Net Package (SPNP) \([4]\). As a tutorial on Petri Nets is beyond the scope of this paper, the reader is referred to the literature for further background \([9, 11]\).

#### 3.1. GSPN Model of Erlang Distribution

Figure 2 shows the GSPN model of Chen et al \([3]\) for an Erlang distribution with \( \text{MTTR} = 1/\mu \). This model has \( r \) exponential transitions, each with mean transition rate \( \rho = r \cdot \mu \). The place labeled Assure controls the number of modules that may be under repair at one time. The initial number of tokens in place Assure represents the number of repair technicians available.

![Fig. 2: GSPN Model for Erlang Distribution [3]](image)

#### 3.2. System Parameters

This study makes three assumptions, all of which tend to maximize the system’s sensitivity to the repair time distribution. First, if centralized voting is used, the voter does not fail. Thus, system Unreliability depends entirely on module failure and repair. Second, there is only one repair technician. Third, fault coverage (the
probability that a fault is correctly identified once it occurs \([6]\) is 100\%. Thus, all faulty modules are submitted to the repair process.

The key system parameters and their ranges used in the Unreliability evaluations are as follows:

- \(r\) = The number of stages in the Erlang repair distribution. For each system, Unreliability was evaluated for \(r = 1, 2, 3,\) and \(4\), respectively. The significance of these numbers lies in the fact that with \(r =1\), the Erlang distribution degrades to the exponential distribution. At the other extreme, it has been shown that 4 stages are sufficient to yield an extremely accurate approximation of a Weibull distribution \([11\ \text{pp. 22-24}]\).
- \(\lambda\) = The mean module failure rate. Module failure rates can vary widely, from around \(10^{-4}/\text{hr}\) for a typical embedded processor in a harsh environment, down to approximately \(10^{-6}/\text{hr}\) for a single disk drive in a RAID system. However, for our purposes, the actual value of \(\lambda\) is not of particular importance since all other temporal parameters can be scaled to \(\lambda\). In particular, the ratio of mean repair rate to mean module failure rate proved to be of importance. Thus, the value of \(\lambda\) was fixed at \(10^{-4}/\text{hr}\) for all evaluations.
- \(\mu\) = The mean repair rate. It varied from \(10^{-4}/\text{hr}\) to \(10/\text{hr}\), yielding a ratio of \(\mu/\lambda\) varying from 1 to \(10^5\). The upper limit of \(10/\text{hr}\) corresponds to a 6 minute MTTR, as might occur for on-line replacement by an on-site operator (e.g. replacement of a RAID disk drive). The lower limit of \(10^{-4}/\text{hr}\) is equal to the failure rate \(\lambda\). For values of \(\mu < \lambda\), system behavior quickly converged to that of a non-repairable system.
- \(t\) = The system mission time. It was varied from \(10^3\ \text{hr}\) (41 days) to \(10^5\ \text{hr}\) (11.4 years).
- \(N\) = The number of modules in the NMR system. \(N\) varied from 2 to 4, to represent Dual-, Triple-, and Quad-MR. While there are systems for which \(N > 4\), (principally RAIDs), the range was limited to \(N \leq 4\) in order to constrain both the number and complexity of GSPN evaluations to be run. Furthermore, as will be shown in Section 4, \(N \leq 4\) proved sufficient to reveal the sensitivity of system Unreliability to the repair distribution.
- \(K\) = The minimum number of non-faulty modules needed for operation (i.e., each case is modeled as a \(K\)-out-of-\(N\):G system). For each \(N\), the value of \(K\) varied from 1 to \((N-1)\), thereby covering the full range of all possible \(K\) values. These values of \(K\) also map to the behavior of realistic faults. For example, most RAID systems are \((N-1)\)-out-of-\(N\):G systems. In addition, given \(N \leq 4\), each value of \(K\) corresponds to one of the fault modes defined in the Thambidurai and Park Hybrid fault model \([14]\). Specifically:
  - \(K=1\) corresponds to a benign, (self incriminating, manifest, or fail-notify) fault, for which the system can continue to operate as long as any one module remains non-faulty.
  - \(K=2\) (for \(N=3\) and \(N=4\)) corresponds to a symmetric malicious fault, requiring a majority of the modules to be non-faulty.
  - \(K=3\) (for \(N=4\)) corresponds to an asymmetric malicious (Byzantine) fault, for which strictly greater than two-thirds of the modules must be non-faulty.

3.3. System Unreliability Model

For each combination of the above parameters, a GSPN Unreliability model was constructed and evaluated using SPNP \([4]\). Figure 3 shows the GSPN model for a \(K\)-out-of-\(N\):G redundant system incorporating the Erlang repair submodel defined in Figure 2.

![GSPN Model for NMR Systems with Erlang Repair](image)

The number of tokens in place “\(n\_up\)” equals the number of non-faulty modules in the system. Initially, “\(n\_up\)” contains \(N\) tokens. Transition “\(fault\)” fires when a module fails. Its transition rate is thus \(\lambda\) times the number of tokens in “\(n\_up\)”. Place “\(n\_dn1\)” represents the number of faulty modules that have not yet completed repair, while place “\(n\_dn2\)” represents the
number of faulty modules that have not yet started repair. Places “n_dn2” and “outer” are the “input” and “output” places of the Erlang submodel of Figure 2. Upon completion of a repair, instantaneous transition “finish” removes a token from place “n_dn1” and produces one token in place “n_up” (restoring the repaired module to service).

Transition “fail” is enabled when place “n_dn1” has at least $N-K+1$ tokens (since this is a K-out-of-N:G system). If there is one token appearing in place “sys_failed”, the system has failed. In order for “sys_failed” to model absorbing states, there is an inhibitory arc from “sys_failed” to every timed transition in the GSPN, including all $r$ transitions in the Erlang repair submodel.

4. Evaluation Results

Using the SPNP program, the above GSPN model, and system parameters $\lambda$, $\mu$, $t$, $N$, $K$, as defined above, system unreliability at time $t$ was computed as the probability of having a token in place “sys_failed” in interval $[0, t]$. Variations in system parameters yielded 330 cases, each of which was evaluated using all four repair distributions (i.e., all four values of $r$), for a grand total of 1,320 GSPN evaluations. The following results were obtained for each case:

- $Q_r(t)$ ($r=1, 2, 3, 4$) is the Unreliability obtained using an $r$-stage Erlang repair distribution.
- Maximum Unreliability Relative Difference (MURD) is, for a given set of parameters, the worst-case difference between the Unreliability with the exponential distribution, and the unreliability with any other distribution, normalized by the Unreliability obtained with the exponential distribution. MURD is determined by the following pseudocode:

\[
\begin{align*}
\text{Max}_\text{diff} &= \max \{|Q_1(t)-Q_2(t)|, \; Q_1(t)-Q_3(t), \; Q_1(t)-Q_4(t)\}; \\
\text{Min}_\text{diff} &= \min \{|Q_1(t)-Q_2(t)|, \; Q_1(t)-Q_3(t), \; Q_1(t)-Q_4(t)\}; \\
\text{IF} \; [\text{Max}_\text{diff} > |\text{Min}_\text{diff}|] \; \text{THEN} \; \text{MURD} = \text{Max}_\text{diff} / Q_1(t) \\
\text{ELSE} \; \text{MURD} = \text{Min}_\text{diff} / Q_1(t).
\end{align*}
\]

4.1. Representative System Results

The most useful result is MURD, because it reveals the relative Unreliability difference between the exponential distribution and all other repair distributions. Our evaluations revealed that the value of MURD depends on the repair rate $\mu$. (more precisely, on the ratio of $\mu/\lambda$). It also shows a weaker dependence on the mission time $t$. However, the MURD shows little dependence on either $K$ or $N$ independently. Rather, it showed a strong dependence on the fault-tolerance ($N-K$).

It is neither practical nor instructive to discuss here the individual MURDs for all 330 cases. Rather, we note that all systems with a given value of the fault-tolerance ($N-K$) yielded very similar MURD graphs. We therefore present MURD graphs of a representative system for each value of the ($N-K$). The graphs presented plot MURD vs. $\log_{10}(\mu/\lambda)$ – due to the extreme range in $\mu/\lambda$. Each graph presents several curves, one curve for each value of mission time $t$.

4.1.1. Single-Fault-Tolerant (1-FT) Systems

The 1-out-of-2:G system is representative of all Single Fault-Tolerant (1-FT) systems evaluated. Figure 4 shows the MURD curves for this system. Behaviorally, the curve can be partitioned into two regions. The left hand side of the curve ($\mu/\lambda < 10^2$), corresponds to the long repair times representative of remotely located systems (e.g., a satellite requiring a manned space mission to effect repair). In this region, the plot shows a tendency for the exponential distribution to underestimate Unreliability, relative to the other distributions. However, the worst case MURD for any 1-FT system was only -22%. The right hand side of the curve ($\mu/\lambda > 10^2$) corresponds to the shorter repair times representative of the most common systems. In this region, the MURD approaches zero as the repair rate increases. In short, a 1-FT system is extremely insensitive to the repair time distribution, especially for shorter MTTRs.
4.2. Two-Fault-Tolerant (2-FT) Systems

The 1-out-of-3:G system is representative of the behavior of all Two-Fault-Tolerant (2-FT) systems evaluated. Figure 5 shows the MURD curves for this system. The left-hand side of the curve shows the same behavior as the 1-FT system, with a worst-case underestimation of -30%. On the right-hand side of the plot, the MURDs converge to a value of +38%, rather than to zero. While 2-FT systems showed a greater sensitivity to the repair distribution than 1-FT systems, there was still less than 40% difference in the unreliability calculated with the exponential distribution, and that calculated with any of the other repair distributions.

4.1.3. Three-Fault-Tolerant (3-FT) Systems

The 1-out-of-4:G system was the only Three-Fault-Tolerant (3-FT) system evaluated. Figure 6 shows that the 3-FT MURD curves are very similar in shape to the 2-FT MURD curves, although the MURD values were somewhat higher. The worst-case underestimation for the 3-FT system was -33%, while the asymptotic overestimation was 69%.

4.2. Results Summary

Figures 4 through 6 show that the system fault-tolerance (N-K) is the dominant factor in determining the maximum value of MURD. To demonstrate that this behavior is the same for all combinations of K and N, Figure 7 shows the worst-case MURD curve for each (K,N) pair. This figure clearly shows that the asymptotic behavior is controlled by the difference (N-K), rather than either N or K individually.

MURD measures the maximum relative difference in calculated unreliability between the exponential distribution and the 2, 3, and 4 stage Erlang distributions. In every case, the magnitude of the difference increased as more stages were added to the Erlang distribution, i.e.:
\[ |Q_3(t) - Q_d(t)| > |Q_2(t) - Q_d(t)| > |Q_1(t) - Q_d(t)|. \]

However, for every system evaluated, the 2-stage Erlang accounted for at least 60% of the worst-case MURD, and the 3-stage Erlang accounted for over 85% of the worst-case MURD. Thus, as the number of stages increases, the impact of the new stage on MURD decreases. This result makes sense in the context of Figure 1 in that the 2-stage Erlang initiates the “S” shape of the repair time distribution, while adding more stages merely “fine-tunes” the shape of the curve. Therefore, adding still more stages to the Erlang repair distribution, or otherwise fine-tuning the repair distribution will have minimal impact on the calculated Unreliability.

5. Conclusions and Future Work

This paper has presented a systematic study to determine whether non-exponential repair distributions produce significant differences in NMR system Unreliability, relative to an exponential repair distribution with the same MTTR. Based on the previous research, Erlang distributions were employed as representative of non-exponential distributions. The Erlang distributions were embedded into GSPN models of NMR systems and the Unreliability was evaluated. In the process, a number of system parameters were systematically varied over a wide range of values, resulting in a total of 1320 GSPN evaluations.

5.1 Conclusions

The primary result is that there was little difference between Unreliabilities calculated with an exponential repair distribution and those calculated with non-exponential Erlang distributions. For all systems modeled, the worst case MURD was less than 70%. For reasonably rapid repairs, (e.g. MTTR < 100 hr), the MURD value approached a positive constant dependent only on the system fault-tolerance (N-K). Thus, for the most common systems, the exponential distribution produced a small, predictable, conservative overestimate of system Unreliability. We thus conclude that calculated Unreliability for NMR systems is relatively insensitive to the choice of the repair time distribution, i.e., the dominant parameter of the repair time distribution is its first moment (MTTR).

In particular, Figures 4 and 7 show that with relatively short MTTRs (i.e. \( \mu >> \lambda \)), the impact of the repair distribution is negligible for single fault-tolerant (1-FT) systems. This result is of exceptional importance since 1-FT comprises the most common fault-tolerant systems, including Dual- and Triple-Redundant systems, RAID systems, and most practical Byzantine-safe systems.

5.2. Future Work

The system redundancy was limited to \( N \leq 4 \) primarily for reasons of complexity. This value was sufficient to reveal the dependency between MURD and fault-tolerance (N-K). Additional studies with \( N > 4 \) can be performed to model more systems (e.g. RAID systems can have 7 or more disks). Simulations of systems with greater than 3-FT can then be performed. This additional data will allow regressions to be run to quantify the relationship between MURD and fault-tolerance, and permit expressions for correction factors to be derived.

This study assumed that only a single module could be under repair at one time. It is expected that multiple repair capability will further reduce the sensitivity of Unreliability to the repair time distribution. By adding more tokens to the Assure place in Figure 2, multiple repair evaluations can be run to verify and quantify this hypothesis.

This study also considered only homogeneous NMR systems. More complex factors such as heterogeneous systems, imperfect coverage, or hybrid faults can be evaluated by the same methods as those used herein. In addition, the impact of the repair distribution on other objective functions such as Availability and Performability can be similarly evaluated.

References


