Analysis of Conditional MTTF of Fault-Tolerant Systems

Hoon Choi\textsuperscript{1}, Wei Wang\textsuperscript{2} and Kishor S. Trivedi\textsuperscript{3}

\textsuperscript{1}Department of Computer Engineering
Chungnam National University
220 Kung-dong, Taejon 305-764, Korea
hchoi@comeng.chungnam.ac.kr

\textsuperscript{2}212 Federal City Road
Lawrenceville, NJ 08648, U.S.A.

\textsuperscript{3}Department of Electrical Engineering
Duke University, Box 90291
Durham, NC 27708-0291, U.S.A.
kst@ee.duke.edu

\textsuperscript{1}This work was supported in part by Korea Telecom Research & Development Group under grant 96-64.
\textsuperscript{2}

\textsuperscript{3}This work was supported in part by the National Science Foundation under grant NSF-EEC-94-18765.
Abstract

Mean time to failure (MTTF) is one of the most frequently used dependability measures in practice. By convention, MTTF is the expected time for a system to reach any one of the failure states. For some systems however, the mean time to absorb to a subset of the failure states is of interest. Therefore, the concept of conditional MTTF may well be useful. In this paper, we formalize the definition of conditional MTTF and cumulative conditional MTTF with an efficient computation method in a finite state space Markov model. Analysis of a fault-tolerant disk array system and a fault-tolerant software structure are given to illustrate application of the conditional MTTF.

1 Introduction

In many practical situations, there are multiple causes of system failure. For instance, failure of a computer system may be due to the failure of processor or memory or disk subsystem. In a disk subsystem, a failure may result in data destruction which is accompanied by a warning. Alternatively data may be corrupted without being detected [11]. The latter event is more serious than the former, so we would like the probability of the latter event to be small and the mean time to the occurrence of the latter event rather long. In fault tolerant software such as a recovery block [6, 12], the acceptance of a module’s erroneous outputs by the acceptance test is more disastrous than a recovery block failure due to exhaustion of alternate modules.

Transient probability of system failure is easily broken down into its constituent causes and has been reported by many existing reliability modeling tools. While these probabilities can be used to estimate the system’s susceptibility to various failure causes, the mean time to failure (MTTF) due to different causes provides more practical information.

There have been some studies about MTTF [3, 9, 10, 13]. The MTTF from a given initial state is one example, and the mean residual life at time $t$ [3] which is the expected time to failure given that the system has been operational up to time $t$, is another. Heidelberger et al. [9] describe an efficient numerical method for computing MTTF in a Markovian dependability model. In [10], the conditional expectation is defined to be the expected time to failure given that the failure occurs within a specific time window. All these studies, however, deal with the MTTF to the group of all failure states. The MTTF due to certain failure causes, or the MTTF to a given subset of failure
states is a relatively unexplored topic. In [5], it is observed that the probability of absorption to a partition of absorbing states from a given initial state may be computed as the accumulated reward until absorption by assigning zero reward rate to the states in the partition and positive reward rate to all the other absorbing states. The possibility of computing the expectation and distribution of time given that the process is absorbed in a state with zero reward is also speculated. In [4], we define the notion of the \( \text{MTTF} \) to a subset of failure states that is named the conditional \( \text{MTTF} \) and show its solution method in a Markov dependability model. Arlat et al. [1] define the term mean safe time or mean time before catastrophic failures for high safety systems. They assume that the system is brought back to operation after a benign (safe) failure and the time to reset the system after such a failure is taken into consideration in their model. The mean safe time is a special case of the cumulative conditional \( \text{MTTF} \) to catastrophic failures which will be defined later in this paper.

The purpose of this paper is to analyze fault-tolerant systems using the concept of the conditional \( \text{MTTF} \) and thus show application area of this concept. The remainder of the paper is organized as follows. The definition and a method of computing conditional \( \text{MTTF} \) are explained in Section 2 for completeness. The concept of cumulative conditional \( \text{MTTF} \) and its computation are discussed in Section 3. In Section 4, analysis of a fault-tolerant disk array system and a fault-tolerant software structure are given to illustrate application of the conditional \( \text{MTTF} \).

2 Conditional Mean Time To Failure

2.1 Definition

The models we consider in this paper are time-homogeneous, finite state, continuous-time Markov chains (CTMC). We will denote such CTMCs by \( \{X(t), t \geq 0\} \). Consider a simple CTMC model of life and death in Figure 1. Suppose that state \( s_0 \) represents man is alive, state \( s_1 \) represents he dies of a disease, and state \( s_2 \) that he dies from an accident. Therefore, \( s_1 \) and \( s_2 \) are two absorbing states representing death. Let \( Y \) be the random variable representing the time for the CTMC to reach the absorbing states. Then \( E[Y] = \text{MTTF} = 1/(\lambda_1 + \lambda_2) \) is the expected length of life.
But very often we are interested in computing the mean time to absorb into a set of specific absorbing states rather than to the whole set of absorbing states. We may want to compute the mean length of life until people die from accident rather than just the mean time until they die of any reason. Insurance companies, for example, need to get the mean length of life (the mean life time) for people to die from a specific reason in order to calculate proper rate of life insurance. They may be interested in how long on the average people survive before they die of cancer (the expected length of life given that people die of cancer), or the expected length of life given that they die of heart attack, or the mean life time till death by traffic accident etc.

In order to obtain these measures, we consider a subset $A$ of absorbing states that correspond to the a specific reason we are interested in. Suppose we are interested in the mean life time to die from accident, hence $A = \{s_2\}$. Then we need to compute the $MTTF$ with a condition that the system absorbs to $A$. The **conditional mean time to failure** to $A$ is defined by:

$$MTTF_{\mathcal{A}} = E[Y \mid X(\infty) \in \mathcal{A}] = E[Y \mid X(\infty) \in \mathcal{A}] / P_{\mathcal{A}}(\infty)$$

which is the expected time until absorption given that the system has absorbed to a set $A$ of states. Here $P_{\mathcal{A}}(\infty) = P\{X(\infty) \in \mathcal{A}\}$, absorption probability. Denote the rest of the absorbing states by set $B$. In case that $X(0) \in B$, $P_{\mathcal{A}}(\infty)$ is simply 0 and if $X(0) \in A$, $P_{\mathcal{A}}(\infty)$ is 1. Therefore, the non-trivial situation of interest is that the system starts in one of the transient states.

We will use the following notation throughout the paper:

- $\{X(t), t \geq 0\}$: a time-homogeneous, finite state, continuous-time Markov chain
- $\Omega$: the state space of the CTMC
- $T$: the set of all transient states, the cardinality of $T$ is represented by $|T|$
- $\Omega_\mathcal{A}$: the set of all the absorbing (failure) states, $\Omega_\mathcal{A} = \Omega - T$
- $A$: a subset of absorbing states satisfying a given failure condition ($A \subseteq \Omega_\mathcal{A}$)
- $B$: the rest of the absorbing states in the reliability model
- $Y$: a random variable representing the time for the CTMC to absorb to $\Omega_\mathcal{A}$
- $E[Y]$ : the expected value of $Y$
- $F_A(t)$ : the distribution of the finite absorption time, $F_A(t) = P\{Y \leq t \text{ and } X(\infty) \in A\}$
- $F(t\vert A)$ : the conditional distribution of absorption time to $A$,
  \[ F(t\vert A) = P\{Y \leq t \mid X(\infty) \in A\} \]
- $P_A(\infty)$ : the probability of absorbing to $A$, $P_A(\infty) = P\{X(\infty) \in A\}$
- $MTTF_{IA}$ : the conditional $MTTF$ to $A$
- $CMTTF_{IA}$ : the cumulative conditional $MTTF$ to $A$
- $1_T$ : a column vector of size $|T|$ with all 1’s
- $0_T$ : a column vector of size $|T|$ with all 0’s.

2.2 Computation of Conditional MTTF

Consider a CTMC with $m \geq 1$ absorbing states as in Figure 2. The set of absorbing states of this CTMC is $\Omega_A = \{r_1, r_2, r_3, \ldots, r_m\}$. Let the infinitesimal generator matrix $Q$ be partitioned so that the transient states appear first followed by states in $A$, and then followed by the remaining absorbing states labeled as $B$. It is clear that $q_{ij} = 0$ ($\forall j \in \Omega$) for a state $i$ in $A$ or $B$.

\[
Q = \begin{bmatrix}
Q_{TT} & Q_{TA} & Q_{TB} \\
& 0 & \\
\end{bmatrix}
\]  

Figure 2: A CTMC with $m$ Absorbing States
Here $Q_{TT}$ is the partition of the generator matrix consisting of the transition rates between the states in $T$, similarly $Q_{TB}$ consists of the transition rates from states in $T$ to states in $B$. $0$ in the $Q$ is the $m \times (|T| + m)$ matrix with zeros. We assume $A$ to have a single state so that $Q_{TA}$ is $|T| \times 1$ matrix. In case that $A$ consists of multiple absorbing states, we can easily lump these states into a single state. Note that this lumping does not imply an approximate solution. Define the state probability vector $P(t) = [P_T(t), P_A(t), P_B(t)]$ where $P_i(t)$ is the partition of the transient state probabilities at time $t$ for states in set $i \in \{T, A, B\}$. Define the integrals of state probabilities, $L_i(t) = \int_0^t P_i(u) du$, and the corresponding vector $L(t) = [L_T(t), L_A(t), L_B(t)]$.

The following proposition can be used to compute the absorption probability to $A$, which is needed in order to obtain conditional MTTF to $A$.

**Proposition 1** The absorption probability to $A$ is given by:

$$P_A(\infty) = \tau_T Q_{TA}$$

where $\tau_T$ is the solution of the linear system:

$$\tau_T Q_{TT} = -P_T(0).$$

*(Proof)*

Let $P^*(s) = \int_0^\infty e^{-st} P(t) dt$ be the Laplace transform (LT) of $P(t)$. Taking LT on both sides of forward Kolmogorov equation,

$$P^*(s)(sI - Q) = P(0).$$

That is,

$$[P_T^*(s), P_A^*(s), P_B^*(s)]
\begin{bmatrix}
  sI_T - Q_{TT} & -Q_{TA} & -Q_{TB} \\
  0 & sI_A & 0 \\
  0 & 0 & sI_B
\end{bmatrix}
= [P_T(0), P_A(0), P_B(0)]$$

where $I_T, I_B$ are identity matrices with dimensions $|T| \times |T|, |B| \times |B|$, respectively. By assumption, $P_A(0) = P_B(0) = 0$, hence:

$$P_T^*(s) = P_T(0)[sI_T - Q_{TT}]^{-1}$$

and

$$P_A^*(s) = \frac{P_T(0)[sI_T - Q_{TT}]^{-1} Q_{TA}}{s}.$$
From the final value theorem of Laplace transform: 
\[ P_A(\infty) = \lim_{t \to \infty} P_A(t) = -P_T(0)[Q_{TT}]^{-1}Q_T. \]
The proof is then completed by denoting \( \tau_T = -P_T(0)[Q_{TT}]^{-1}. \)
\[ \square \]

Note that \( L_T(\infty), \) the integration of state probabilities for the transient states up to time \( \infty, \) is the vector consisting of the expected total time spent by the system in state \( i \) \((i \in T)\) until absorption:
\[ L_T(\infty) = \int_0^\infty P_T(t)dt = P_T^s(0) = -P_T(0)[Q_{TT}]^{-1} = \tau_T. \]
Hence, the (conventional) \( MTTF \) of a system is obtained by summing up the components of the vector \( \tau_T \) [1, 8]:
\[ MTTF = \tau_T 1_T. \] (7)

Next we will present the computational method for conditional \( MTTF \) as Theorem 1. To prove the theorem, we first obtain the conditional distribution of absorption time to \( A \) in the form of Laplace-Stieltjes transform (LST), namely, \( F^\sim(s|A) \). Then we derive conditional \( MTTF \) from the LST of the conditional distribution.

**Theorem 1** The conditional mean time to failure to \( A \) is given by:
\[ MTTF_{IA} = \frac{E[Y \text{ and } Y < \infty]}{P_A(\infty)} = \frac{\theta_T Q_{TA}}{\tau_T Q_{TA}} \] (8)
where \( \theta_T \) is the solution of the linear system:
\[ \theta_T Q_{TT} = -\tau_T. \] (9)

**(Proof)**
Let \( P_A^\sim(s) \) be the LST of \( P_A(t) \) so that:
\[ P_A^\sim(s) = \int_0^\infty e^{-st}dP_A(t) = sP_A^s(s) = P_T(0)[sI_T - Q_{TT}]^{-1}Q_T. \] (10)
We have, for \( t < \infty: \)
\[ F(t|A) = \frac{P\{Y \leq t \text{ and } X(\infty) \in A\}}{P\{X(\infty) \in A\}} = \frac{P_A(t)}{P_A(\infty)} = \frac{F_A(t)}{P_A(\infty)}. \] (11)
Denoting by \( F^\sim(s|A) \), the LST of \( F(t|A) \), we have:
\[ F_A^\sim(s) = P_A^\sim(s) = P_T(0)[sI_T - Q_{TT}]^{-1}Q_T. \]
\[
F^\sim(s|A) = \frac{P_A^\sim(s)}{P_A(\infty)} = \frac{P_T(0)}{P_A(\infty)} \cdot [sI_T - Q_{TT}]^{-1}Q_{TA}.
\] (12)

From the LST of the conditional distribution, we can obtain the conditional \( MTTF \) to \( A \):
\[
MTTF|_A = \lim_{s \to 0} -\frac{dF^\sim(s|A)}{ds} = -\tau_T[Q_{TT}]^{-1}Q_{TA} \cdot \tau_T Q_{TA}.
\]

If we denote \(-\tau_T[Q_{TT}]^{-1} = \theta_T\), we get Equation (8).

Iterative methods such as Gauss-Seidel or SOR (Successive Overrelaxation) may be used for the numerical solution of Equation (4) and (9) [7]. Since \( T \) is a transient subset, it follows that the matrix \( Q_{TT} \) is a non-singular, diagonally dominant matrix. Hence the convergence of an iterative method is guaranteed [15]. The complexity of the method in terms of scalar multiplications to compute the conditional \( MTTF \) is \( O(2(k\sigma + |T|)) \), if we denote the number of non-zero entries in the \( Q_{TT} \) matrix by \( \sigma \) and the number of iterations \( k \) required for the convergence of solutions is determined by the specified tolerance, \( \varepsilon \) [7].

3 The Cumulative Conditional MTTF

One useful extension of the conditional \( MTTF \) is to compute a cumulative measure of time until the occurrence of a specific event. We define cumulative conditional \( MTTF \) as the mean time until failure satisfying a given condition since the system began operation and disregarding other possible system failures that do not satisfy the given condition.

Suppose \( A \subset \Omega_A \) contains one unsafe failure state and \( B = \Omega_A - A \) consists of one safe failure state. If we want the mean time until the unsafe failure occurs, this measure can be obtained by accumulating conditional \( MTTF \) to \( B \) after each time the system absorbs to \( B \), which is the safe failure and assuming the system can be reset to its initial state, until the unsafe failure in \( A \) occurs. For simplicity we assume the time to reset the system from the safe failure state is negligible (This assumption however can be easily removed to include a reset time). The cumulative conditional \( MTTF \) to \( A \) denoted by \( CMTTF|_A \) can then be represented as the random sum of \( R \) copies of \( MTTF|_B \) followed by an \( MTTF|_A \) where \( R \) is a random variable for the number of resets, i.e., the number of occurrences of safe failures before the unsafe failure occurs. \( R \) has a modified geometric distribution with parameter \( P_A(\infty) \) [14]. Hence:
\[
CMTTF|_A = \frac{P_B(\infty)}{1-P_B(\infty)} MTTF|_B + MTTF|_A.
\]
Using Equations (3) and (8):

\[
\text{CMTTF}_{1A} = \frac{\theta_T(Q_{TA} + Q_{TB})}{P_A(\infty)} = \frac{\tau_T \cdot \frac{1}{P_A(\infty)}}{P_A(\infty)} = \frac{MTTF}{P_A(\infty)}.
\]  

(13)

Note that Equation (13) differs from Equation (8) in its numerator. The \( CMTTF_{1A} \) is computed using conventional MTTF whereas \( MTTF_{1A} \) is computed using expected finite absorption time. In this particular example with only one unsafe failure state, the \( CMTTF_{1A} \) simply turns out to be \( \frac{MTTF}{P_A(\infty)} \). This doesn’t hold for the case when multiple unsafe failure states are present and \( A \) consists of a subset of them.

Observe that whenever safe failures occur, the system is reset to its initial state. This behavior can be captured by the modified CTMC obtained from the original CTMC by directing state transitions to the safe failure states (in the original CTMC) to the initial state.

If \( Q' \) is the generator matrix of the modified CTMC, it can be shown that [2]:

\[
Q' = \begin{bmatrix}
Q'_{TT} & Q'_{TA} \\
0 & 0
\end{bmatrix} = \begin{bmatrix}
Q_{TT} + Q_{TB} \cdot \frac{1}{P_T(0)} & Q_{TA} \\
0 & 0
\end{bmatrix}.
\]

The \( Q'_{TT} \) consists of \( Q_{TT} \) of the original CTMC plus the newly added components \( Q_{TB} \cdot \frac{1}{P_T(0)} \). The latter are the rates from \( T \) to \( B \) of the original CTMC which are to be redirected back to \( T \) according to the initial probability distribution of the system. \( 0 \) denotes a submatrix with zero elements. Based on these observations, the following theorem describes the method to compute cumulative conditional MTTF for a general Markov model.

**Theorem 2** Suppose a Markov model has one or more critical failure states and one or more non-critical failure states. The cumulative conditional MTTF to one of the critical failure states in the Markov model is the same as the conditional MTTF to that state in its modified model.

**(Proof)**

Without loss of generality, consider a CTMC, labeled \( Q \), with two critical failure states \( A, A' \) and one non-critical failure state \( B \) as in Figure 3.
The generator matrices of these Markov models are:

\[
Q = \begin{bmatrix}
Q_{TT} & Q_{TA} & Q_{TA}' & Q_{TB} \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}, \quad Q' = \begin{bmatrix}
Q_{TT} + Q_{TB} \cdot P_T(0) & Q_{TA} & Q_{TA}' \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}.
\]

The cumulative conditional MTTF in \( Q \) to \( A \) disregarding the failures to \( B \) is obtained by:

\[
CMTTF_{1A} (Q) = \frac{P_B(\infty)}{1 - P_B(\infty)} \times MTTF_{1B} (Q) + MTTF_{1A} (Q).
\]

Using the results derived earlier, we obtain:

\[
MTTF_{1A} (Q) = \frac{P_T(0)[Q_{TT}]^{-1}[Q_{TT}]^{-1}Q_{TA}}{-P_T(0)[Q_{TT}]^{-1}Q_{TA}}
\]

\[
MTTF_{1B} (Q) = \frac{P_T(0)[Q_{TT}]^{-1}[Q_{TT}]^{-1}Q_{TB}}{-P_T(0)[Q_{TT}]^{-1}Q_{TB}}.
\]

Using the result \( P_B(\infty) = \tau_T Q_{TB} \), we have:

\[
CMTTF_{1A} (Q) = \frac{ku_A s_c + s_A}{u_A}
\]

where \( u_A = -P_T(0)[Q_{TT}]^{-1}Q_{TA} \), \( u_c = -P_T(0)[Q_{TT}]^{-1}Q_{TB} \), \( s_A = P_T(0)[Q_{TT}]^{-1}[Q_{TT}]^{-1}Q_{TA} \), \( s_c = P_T(0)[Q_{TT}]^{-1}[Q_{TT}]^{-1}Q_{TB} \) and \( k = 1/(1 + P_T(0)[Q_{TT}]^{-1}Q_{TB}) \) which are all scalars.

The conditional MTTF to \( A \) in \( Q' \) is computed by:

\[
MTTF_{1A} (Q') = \frac{P_T(0)[Q_{TT} + Q_{TB}P_T(0)]^{-1}[Q_{TT} + Q_{TB}P_T(0)]^{-1}Q_{TA}}{-P_T(0)[Q_{TT} + Q_{TB}P_T(0)]^{-1}Q_{TA}}.
\]

This can be rewritten by using Sherman-Morrison-Woodbury formula [7] as follows:

\[
MTTF_{1A} (Q') = \frac{s_A + ku_A s_c + ku_c s_A + k^2 u_A u_c s_c}{u_A + ku_A u_c}.
\]

It is easy to show that the cross products of the numerators and denominators in Equations (14) and (15) are the same. Therefore, \( CMTTF_{1A} (Q) = MTTF_{1A} (Q') \).

This theorem tells us the computational method for cumulative conditional MTTF can be identified with that for conditional MTTF.
4 Application Examples

The concept of conditional $MTTF$ is useful in many applications, especially fault-tolerant systems. In a fault-tolerant disk array system such as RAID-2 in [11], data will be temporarily unavailable to the users if more than one disk have failed. A more catastrophic failure occurs if a disk failure is undetected by the disk controller since corrupted data is delivered to the users. Therefore, we would like to obtain the conditional mean time to catastrophic failures, as well as the conditional mean time to temporary data loss. These two different measures will help us understand the system’s failure behavior much better. In a fault-tolerant software structure such as recovery blocks (RB), there are several failure modes as we will see later in this section. The conditional $MTTF$ to different failure modes should be of interest to software designers. In this section, we will obtain conditional $MTTF$ measures for both fault-tolerant disk array systems and recovery block scheme.

4.1 Fault-Tolerant Hardware: Disk Array (RAID)

A fault-tolerant disk array is a high performance redundant disk system [11]. It is organized as several groups of disks. Each group consists of $G$ disks, including $D$ data disks and $C$ check disks (i.e., $G = D + C$). All the disks are made by the same manufacturer and are identical. We will apply our computational method for conditional $MTTF$ to one such group of disks.

We assume a single correction and double detection Error Correcting Code (ECC) scheme is used in the disk array. A fault in a disk can be detected with probability $p$. Undetected fault in a disk causes a catastrophic failure since corrupted data is passed to the user. A detected fault of a single disk in a group can be tolerated since data stored on the failed disk can be reconstructed using the data and parity information stored on the $G - 1$ operational disks and written to a spare. Therefore, data is still available to the user after the reconstruction. But if a second disk in the same group fails while the reconstruction is being carried out, data can no longer be reconstructed and therefore a data loss situation occurs. In such a situation, the recovery process involves replacing the failed disks with spares and copying data from backup storage if any. We assume unlimited number of spares are available.

Assume that the time to failure of an individual disk is exponentially distributed with mean $1/\lambda$ and the time to reconstruct the data using parity information is exponentially distributed with mean $1/\mu$. The Markov reliability model for a group of $G$ disks is shown in Figure 4(a). In
state $O$, all the disks in the group are operational. In state 1, a single disk has failed. The data reconstruction takes the systems back to state $O$ at rate $\mu$. When the fault is undetected, the system reaches the catastrophic failure state $CF$. State $DL$ is the data loss state when a second disk fails during the reconstruction.

Figure 4: Reliability Model of a Group of Disks

Suppose we are interested in (i) the conditional $MTTF$ to catastrophic failures, (ii) the conditional $MTTF$ to data loss of the disk group, and (iii) the cumulative conditional $MTTF$ to catastrophic failures. The cumulative conditional $MTTF$ to catastrophic failures tells us the mean duration of safe operation with brief interruptions due to data loss. Applying the computational method for conditional $MTTF$, we get:

$$MTTF_{CF} = \frac{(\lambda - G\lambda - \mu) (\lambda - G\lambda + \lambda p - 2G\lambda p)}{G\lambda (\lambda - G\lambda - \mu + \mu p) (\lambda - G\lambda + \mu p - G\lambda p)} ,$$

$$MTTF_{DL} = \frac{\lambda - 2G\lambda - \mu}{G\lambda (\lambda - G\lambda - \mu + \mu p)} ,$$

and

$$CMTTF_{CF} = \frac{\lambda - G\lambda - \mu - G\lambda p}{G\lambda (1 - p) (\lambda - G\lambda - \mu + \lambda p - G\lambda p)} .$$

The conventional $MTTF$ can also be obtained as:

$$MTTF = \frac{\lambda - G\lambda - \mu - G\lambda p}{G\lambda (\lambda - G\lambda - \mu + \mu p)}$$
Figure 5: Comparison of various MTTFs for a Group of G Disks

In Figure 5, we compare the (conventional) MTTF with MTTF\_{\text{CF}}, MTTF\_{\text{DL}} and CMTTF\_{\text{CF}} as the value of p (fault detection probability) varies. By studying the above formulas, we find the following relationships:

\[
\begin{align*}
\text{MTTF}\_{\text{DL}} & \geq \text{MTTF}, \\
\text{CMTTF}\_{\text{CF}} & \geq \text{MTTF}, \\
\text{MTTF} & \geq \text{MTTF}\_{\text{CF}},
\end{align*}
\]

and

\[
\begin{align*}
\text{CMTTF}\_{\text{CF}} & < \text{MTTF}\_{\text{DL}}, \quad \text{if } p < p^* \\
\text{CMTTF}\_{\text{CF}} & = \text{MTTF}\_{\text{DL}}, \quad \text{if } p = p^* \\
\text{CMTTF}\_{\text{CF}} & > \text{MTTF}\_{\text{DL}}, \quad \text{if } p > p^*
\end{align*}
\]

where \( p^* \) is given by

\[
p^* = \frac{G \lambda - G^2 \lambda - 2 G \mu + \sqrt{(G - 1) G (4 \lambda^2 - 13 G \lambda + 9 G^2 \lambda^2 - 8 \lambda \mu + 12 G \lambda \mu + 4 \mu^2)}}{2 (\lambda - 3 G \lambda + 2 G^2 \lambda - \mu)}.
\]

These relationships are plotted in Figure 5. Note that MTTF\_{\text{CF}} and MTTF are equal if and only if \( p = 0 \). Similarly, CMTTF\_{\text{CF}} and MTTF are identical under the same condition. Therefore, we have

\[
\text{CMTTF}\_{\text{CF}} = \text{MTTF} = \text{MTTF}\_{\text{CF}} = \frac{1}{G \lambda}, \quad \text{if } p = 0.
\]

If instead \( 0 < p < 1 \), the following relationship holds:

\[
\text{CMTTF}\_{\text{CF}} > \text{MTTF} > \text{MTTF}\_{\text{CF}}.
\]

If \( p = 1 \), MTTF\_{\text{CF}} is no longer a meaningful measure because state CF is not reachable and CMTTF\_{\text{CF}} is infinite since it is the sum of an infinite number of MTTF\_{\text{DL}}.

When \( p = 1 \), MTTF\_{\text{DL}} and MTTF become the same, i.e.,

\[
\text{MTTF}\_{\text{DL}} = \text{MTTF} = \frac{\lambda - 2 G \lambda - \mu}{G \lambda (\lambda - G \lambda)}.
\]

Otherwise, MTTF\_{\text{DL}} is strictly larger than MTTF. Analogous to MTTF\_{\text{CF}}, MTTF\_{\text{DL}} is not defined at \( p = 0 \) since state DL can not be reached in this case.
The value of \( CMTTF_{1,CF} \) grows very fast as \( p \) approaches 1. This is because a larger \( p \) means a larger transition rate from state \( O \) to state 1 and a larger rate from state 1 to state DL (Figure 4(a)). Correspondingly, the rates from state \( O \) to state CF and from state 1 to state CF become smaller. Therefore, in case failure occurs, the system is more likely to change to state 1 and then to absorb to state DL rather than to state CF. As a result, the cumulative conditional \( MTTF \) to catastrophic failures is very high and approaches infinity when the value of \( p \) is extremely close to 1.

4.2 Fault-Tolerant Software: Recovery Block (RB)

Recovery block is a software construct that utilizes design diversity to achieve fault-tolerance [12, 6]. It consists of a primary module, one or more alternate modules and an acceptance test (AT). The primary and alternate modules are developed using different algorithms. For a given set of data inputs, the primary module is executed first and the results are checked by the AT. If the AT fails to accept the results, the alternate modules are invoked in succession until one produces results that are accepted by the AT or until all of them fail to satisfy the AT. In the latter case, the RB is said to have failed on this input data set. We will consider a RB scheme with one primary module and one alternate module.

Figure 6: Reliability Model of a RB with One Alternate Module

The primary module and the alternate module are numbered 0 and 1 respectively. The execution time of module \( i \) is exponentially distributed with mean \( 1/\lambda_i \). The execution time of the AT is also assumed to be exponentially distributed with mean \( 1/\lambda_A \). The probability that module \( i \) produces
incorrect (erroneous) output is $\rho_i$. The Markov reliability model for such a RB scheme is shown in Figure 6. In state 0, module 0 (primary) is being executed. State $0_e$ ($0_c$) corresponds to the case when the results produced by module 0 are correct (erroneous). When the results are correct, the AT may reject the results and therefore raise a false alarm. Let the probability that the AT raises a false alarm be $p_f$. If a false alarm is raised, the alternate module needs to be invoked (recovery). The recovery process is not always successful. We denote the probability of a successful recovery following a failure to satisfy the AT by $c$ (the coverage factor). A successful recovery results in the execution of the alternate module (state 1). Otherwise the system reaches the recovery failure state RF. The primary module may also produce incorrect result. Let $p_e$ be the probability that the AT fails to detect erroneous output. A catastrophic failure (state CF) occurs when the erroneous output is accepted by the AT. The results produced by the alternate module are also checked by the AT. Should the AT fail to accept the results produced by the alternate module, the RB is considered failed due to exhaustion of redundancy (state ER). A catastrophic failure can also occur when the erroneous output from the alternate module is accepted by the AT.

Figure 7: Comparison of the $MTTF$ and conditional $MTTF$s of RB

The absorbing states RF and ER are both safe failure states in the sense that no erroneous output is delivered to the user. Therefore, we are interested in obtaining (i) the $MTTF$ given that a catastrophic failure occurs which is $MTTF_{|CF}$ and (ii) the $MTTF$ given that safe failures occur which is $MTTF_{|SF}$, where $SF = \{RF, ER\}$. For the latter case, we lump the two safe absorbing states by summing up the rates to absorb to these two states.

Assume the execution rate of the primary module is $\lambda_0 = 1 \text{ min}^{-1}$, and the execution rate of the alternate module is $\lambda_1 = 0.75 \text{ min}^{-1}$. The execution rate of the AT is $\lambda_t = 100 \text{ min}^{-1}$. Let the
probabilities be: \( \rho_0 = \rho_1 = 0.01 \) and \( p_e = p_f = 0.01 \). We plot the values of \( \text{MTTF}_{\text{CS}} \), \( \text{MTTF}_{\text{SF}} \) and \( \text{MTTF} \) corresponding to high coverage values \( c \) in Figure 7. As we can see from the plot, when the value of the coverage factor is greater than 0.98, \( \text{MTTF} \) is lower than both \( \text{MTTF}_{\text{CS}} \) and \( \text{MTTF}_{\text{SF}} \). The values of \( \text{MTTF}_{\text{CS}} \) and \( \text{MTTF}_{\text{SF}} \) are very close. As the coverage factor \( c \) increases, mean times to failures (both conventional and conditional) increase, which justifies our intuition.

**Acknowledgment**

We like to thank Dr. A. V. Ramesh for informing us of the Sherman-Morrison-Woodbury formula for the proof of Theorem 2.

**References**


