DUAL VERSUS TRIPLICATION RELIABILITY ESTIMATIONS

Wing N. Toy

Wing N. Toy *is supervisor of the 5E4 Productivity and Functionality Group at AT&T Bell Laboratories at Indian Hill Park, Naperville, Illinois. His responsibilities are managing the 5ESS™ System Laboratory resources for the generic 5E4(2) Integrated Services Digital Network development and improving the productivity of designers of large-scale software for the 5ESS switching system. He received B.S. and M.S. degrees from the University of Illinois and a Ph.D. from the University of Pennsylvania, all in electrical engineering. He joined AT&T in 1952.*

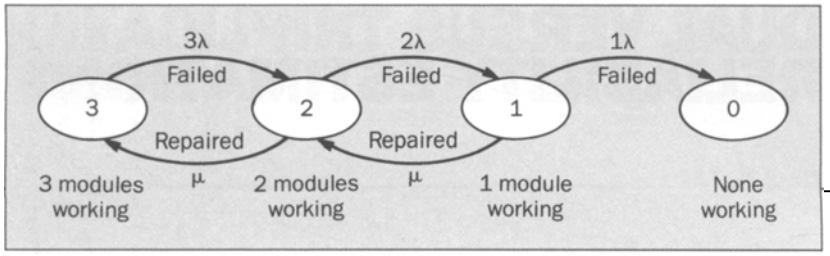
The system mean time to failure (MTTF), a measure of reliability, depends largely on the failure rate, the mean time to repair, and the coverage factor. All contribute to the calculation of MTTF and influence the system design in terms of reliability objectives. In dynamically redundant systems, such as dual systems, coverage plays an extremely important role. It is a probability that the system will recover from a single fault. This involves both hardware and software components to properly detect, isolate, and reconfigure around a faulty module without adversely affecting the system operation. A small reduction in coverage can affect the MTTF dramatically. In a static redundant triple modular redundancy (TMR) system, the inherent error detection and correction property gives a near-perfect coverage for the first detected fault. As a result, the calculated MTTF of a TMR configuration is substantially greater than that of a dual system. This paper discusses and compares the reliability estimation of dual and TMR systems.

Introduction

The failure pattern of in-service equipment can be categorized into three periods of operation, commonly referred to as the bathtub curve.[1] The early failure rate, although relatively high, decreases progressively and eventually levels off to a long, relatively steady period at an approximately constant failure rate. In this period, the failure rate is usually low and the failures are unlikely to be due to any single cause. This means the failures from a wide variety of causes occur at random and at a uniform rate without any obvious pattern. The normal working life of a system occurs during this interval.

In the wear-out period, the components rapidly deteriorate,

Figure 1. Markov model of TMR 3-2-1.



and each component eventually wears out. The failure rate rises again. Wear-out failures can be avoided by replacing components before they reach this period.

The constant failure rate during the normal working life of a system implies that the probability of failure is independent of age. This simply means that old equipment that is still operating is just as good as new stress-tested equipment that has been recently installed. The value of reliability depends only on time. The reliability function that is characterized by a constant failure rate is the negative exponential distribution. The importance of the negative exponential distribution function is that the reliability is independent of where time $t = 0$ is defined. If an item of equipment has a failure rate λ, its reliability for the period time t is $e^{-\lambda t}$. If at the end of this time the item is still in the same operating condition, its reliability for the next time period of equal duration is still $e^{-\lambda t}$.

The negative exponential function is a good representation of the reliability of the equipment. Many reliability analyses of repairable systems are based on this constant failure rate assumption.

The mean time to failure (MTTF) is a quantitative measure of reliability.[2] It gives the average time interval during which equipment is expected to operate without failure. There is no certainty that the item will not break down before the end of this period or, for that matter, that it will not function longer.

Redundant Repairable Systems

In general, fault-tolerant commercial computers are repairable. When one unit in a duplicated system is defective, it depends on the second unit to continue operation. If the defective unit is repaired quickly, the chance of the complete system going down becomes quite small because the second unit will operate in such a manner as to preserve the integrity of the system's operation. Since the system is vulnerable only during the time it takes to repair the defective unit, a short repair time can increase the system reliability tremendously. The system MTTF, a measure of reliability, depends on the failure rate and the repair time.

Another major factor that influences the MTTF is the redundant structure of the system. Its ability to isolate the defective unit and ensure a fault-free operation contributes directly to the coverage factor. It impacts directly on system reliability. This paper compares the dual and the triple modular redundancy (TMR) structure from an architecture viewpoint, assuming a fixed failure rate for a single module and a fixed repair rate.

Dual 2-1 Configuration. The dual redundancy structure is one of the more commonly employed architectures used in providing real-time continuous control. This technique has been used successfully in electronic telephone switching systems for the past 25 years.[3] The important steps in achieving high reliability in a dual configuration are fault detection, fault recovery, and repair. Both units are monitored continuously so that faults in the backup (standby) are found just as quickly as those in the on-line unit. This is accomplished by running the on-line and standby units in the synchronous match mode of operation. Every operation in both units is performed in step and key outputs are compared for error detection. If a mismatch occurs, each unit goes through the fault recognition program to determine which half of the system is faulty. The suspected unit is removed from service and the system continues to function.

Although the system takes only milliseconds to recover from a fault, the resulting errors may have propagated and affected the system outputs, causing a "glitch" to the system operation. Such a glitch may not adversely affect certain applications. In the case of telephone systems, the computer may be in the process of handling one or perhaps several calls during the error interval. The consequence may be that the call is processed incorrectly, resulting in a wrong connection. The users will hang up and redial to correct the problem. However, for other applications, such a glitch may be catastrophic as in the case of safety shutdown systems or expensive process control systems.

The MTTF derived from the Markov model for the dual 2-1 system with repair is given by the following expression.[1]

Table I. MTTF of Simplex, Dual, and TMR Systems

System	MTTF	MTTF, years
Simplex	$1/\lambda$	1
Dual 2-1	$3/2\lambda + \mu/2\lambda^2$	625
TMR 3-2	$5/6\lambda + \mu/6\lambda^2$	208
TMR 3-2-1	$11/6\lambda + 2\mu/3\lambda^2 + \mu^2/6\lambda^3$	260,400

$\mu = 0.125$, $\lambda = 10^{-4}$

$$\text{MTTF} = \frac{3}{2\lambda} + \frac{\mu}{2\lambda^2} \quad (1)$$

where μ is the repair rate or the reciprocal of mean time to repair (MTTR) and λ is the failure rate of one module.

Triple Modular Redundancy 3-2 Configuration. The standard TMR 3-2 configuration[1] operates in the synchronous mode like the dual system. However, the TMR architecture has an inherent fault masking capability. Error detection and correction are done in a single step without any disturbance or glitch in the system operation. This unique property is the strength of TMR structure. Recovery from a fault in one module is automatic. Transient errors are corrected automatically. These attributes are realized by having three modules rather than two.

When one module becomes defective, the remaining two continue to function as in the dual configuration with only error detection capability. The system is completely transparent to a single faulty module. If a second module becomes defective before the first one is completely repaired, the standard practice has been to take the system down since a glitch to the system is unacceptable. The MTTF for the TMR 3-2 configuration from Reference 5 is

$$\text{MTTF} = \frac{5}{6\lambda} + \frac{\mu}{6\lambda^2} \quad (2)$$

Notice that Equations (1) and (2) are similar. Both systems are operated essentially in a dual mode with the system going down when two modules become defective. However, the MTTF is better (greater) for the dual structure because there is one module less than in the TMR. The major advantages of TMR over dual redundancy are the "bumpless" transition and the near perfect coverage from a 3 to 2 configuration.

TMR 3-2-1 Configuration. This configuration combines both the TMR 3-2 and the dual 2-1 operational states into a single system, allowing one module to continue

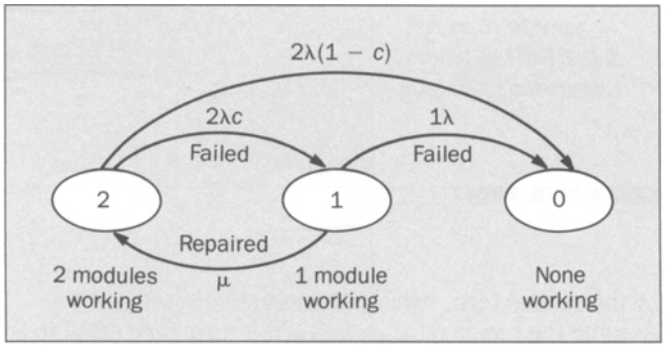


Figure 2. Markov model of dual system including coverage.

operation when the other two become defective. The MTTF can be extended substantially if the application is capable of recovery from a glitch type of transition. The Markov model of the TMR 3-2-1 is shown in Figure 1. In the 3 or normal state, all three modules are fault-free, fully operational. As long as the modules are fault-free, the system stays in this state. Since λ is the failure rate for one module and there are three modules in the system, the probability of transition from 3 to 2 state is 3λ. When one module fails, the system goes to state 2. Upon repair, with the probability of a repair rate μ, it is restored to state 3.

Should another module fail before repair is completed, the system degrades from the 2 to the 1 state. The transition back to the previous state is by repairing defective modules one by one. The trapping state or the 0 state is when the last module fails, bringing the system down completely. Notice that the number of λ decreases by one with each state. This corresponds to the number of working modules. The MTTF calculation is the time that the system takes to reach the 0 state. If the repair time is short, the possibility of moving out of 2 into 1 state is very small and smaller yet from the 1 to the 0 state. The solution to this MTTF follows a similar procedure as outlined in Reference 2 in solving the TMR 3-2 case except that it is considerably more complex in the calculation involving many more terms. The result is:

$$\text{MTTF} = \frac{11}{6\lambda} + \frac{2\mu}{3\lambda^2} + \frac{\mu^2}{6\lambda^3} \quad (3)$$

MTTF Comparisons. Table I shows the MTTF calculations for the various configurations. The λ is the failure rate of a single module.[6] It is assumed to have a value of 10^{-4}, one failure in 10^{-4} hours. The MTTF for a nonredundant system is then $1/\lambda$, 10^4 hours, or approximately 1 year. In the dual 2-1 configuration, the MTTF is dominated

by the second term, which varies inversely with λ^2. Assume the repair rate, μ, is 0.125 (repair time equal to 8 hours). The MTTF is calculated to be 625 years, a substantial increase in reliability as compared with a nonredundant simplex system. However, this is an upper bound and it decreases substantially by imperfect coverage in the 2 to 1 transition. This problem is discussed in the next section.

In the TMR 3-2 configuration, system operation continues as long as two of the three modules are working properly. A second module failure takes the system down. This is basically the same modeling as the dual system, except that there is one additional module. As a result, the MTTF is reduced approximately by a factor of 3 to a value of 208 years as compared with a perfect dual system. However, the transition from a 3 to 2 state is bumpless and perfect in coverage. This is a unique characteristic of the static type of redundancy in which a fault is automatically masked. As a result, the MTTF is not reduced drastically as in the case of the dual system because of imperfect coverage.

If the TMR is permitted to function with a single module, the MTTF is increased to a phenomenal value of 260,400 years. The TMR 3-2-1 is a combination of the standard TMR and the dual arrangement from the modeling and operational viewpoint. Although the transition from the 3 to 2 state is a bumpless one with perfect coverage, the 2 to 1 transition is similar to the dual configuration with possible glitches and imperfect coverage. Again, as in the case of the dual 2-1, the MTTF will be reduced considerably because of imperfect coverage. The impact of a glitch is dependent upon application. The MTTF value is very impressive.

Table II. MTTF of Dual and TMR Systems with Coverage

System	MTTF, years			
	$c = 1$	$c = 0.99$	$c = 0.95$	$c = 0$
Dual 2-1	625	50	10	0.5
TMR 3-2	208			
TMR 3-2-1	260,400	20,833	4167	208

$\mu = 0.125$, $\lambda = 10^{-4}$

Effect of Coverage

The basic hardware redundancy structures can be classified as static redundancy and dynamic redundancy. Both of these may play a role in the same system. The first is also known as fault masking; error correction is done automatically, making the error transparent to the system. The common form is the TMR structure. The dynamic technique generally requires two sequential steps: detection and correction. A fault is first detected, then recovery action corrects the error. Dual redundancy is a form of dynamic structure. The important factor in dynamic redundancy is the concept of coverage, the ability to recover successfully from a fault.[7]

In the TMR case, the inherent fault masking property gives a complete coverage of 100 percent. This of course may not be quite realizable in practice but it is capable of achieving the highest possible coverage. For all practical purposes, we can assume it has the value of 1. This is the strength of TMR structure.

In the dual system, the ability to isolate the faulty unit depends heavily on both hardware and software support in diagnosing and pinpointing the defective module. The inadequacy of the recovery program to configure a working system around the faulty unit reduces the coverage factor.

The coverage factor can be included in the reliability modeling as shown in Figure 2 for the dual configuration. It is assumed that not all faults are recoverable and c is the coverage factor denoting the conditional probability that the system will recover, given that a fault has occurred. The transition rate is $2\lambda c$ from the 2 to 1 state and it is $2\lambda(1 - c)$ to the 0 state. A fault occurring in the normal working state can take the system down depending upon the coverage factor. The calculation based upon the Markov model as shown in Figure 2 for the dual

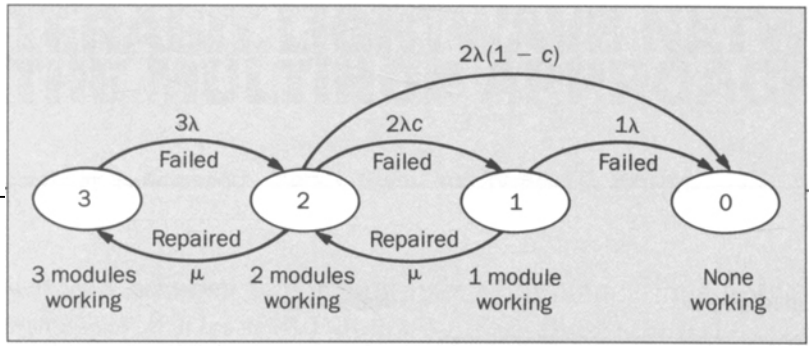


Figure 3. Markov model of TMR 3-2-1 including coverage.

2-1 structure from Reference 8 is:

$$\text{MTTF} = \frac{\lambda(1 + 2c) + \mu}{2\lambda[\lambda + \mu(1 - c)]} \qquad (4)$$

Notice the factor of $(1 - c)$ in the denominator has great influence in the value of MTTF. Table II shows that if c has the value of 0.99 or 99 percent, the MTTF is reduced from 625 years ($c = 1$) to 50 years. This is a substantial reduction in reliability. If c equal 0.95, the MTTF is further reduced to 10 years. Consequently, coverage factor is very important in reliability calculations. When it is included, the TMR structure ($c = 1$) is far better than the dual system, where c falls between 0.95 and 0.99. When c equals 1, Equation (4) becomes Equation (1).

Figure 3 shows the Markov reliability model of the TMR 3-2-1 configuration with coverage included for the transition from the 2 to 1 state. The MTTF equation is similarly evaluated by the procedure outlined in Reference 5, except that the expression is considerably more complex. The result is:

$$\begin{aligned}\text{MTTF} = {} & \{\mu^2\lambda^2(7 + 2c^2 - 8c) + \mu\lambda^3 \\ & (17 - 13c) + \mu^3\lambda(1 - c) + 5\lambda^4 \\ & - \mu\lambda^3(6 - 12c + 6c^2) + 6\lambda^4 c\} \\ & \div 6\lambda^3[\lambda + \mu(1 - c)]^2\end{aligned} \qquad (5)$$

If c equals 0.99, the MTTF is reduced from 260,400 years to 20,833 years. Again, it is a substantial reduction. If c equals 0.95, the MTTF becomes 4,167 years. If c equals 0, Equation (5) becomes Equation (2) for the TMR 3-2 configuration. This means that MTTF ranges from 260,400 years to 208 years for c equal to 1 and 0, respectively.

Clearly, the TMR 3-2 is a high-quality system in a category by itself, as indicated by its bumpless transition and full coverage in transition from the 3 to 2 state. The dual system, on the other hand, is degraded substantially with imperfect coverage. It can be compared with the TMR 3-2-1 system assuming the coverage factor ranges from 0.95 to 0.99. The MTTF result is shown in Table III. A tremendous increase in MTTF is realized with the 3-2-1 concept, if a glitch transition from the 2 to 1 state is acceptable in the application.

Comments on TMR 3-2 and TMR 3-2-1 Configurations

The reliability requirements are strongly dependent upon the intended applications. It may mean merely establishing a working hardware system configuration (such as telephone switching processors) or it may mean that no data are lost or corrupted (such as in transaction processing computers, used in banks) or it may demand flawless real-time control operation (such as in safety shutdown controllers for nuclear plants).

The TMR 3-2-1 competes directly with the dual 2-1 market. At a 50 percent increase in hardware, the MTTF is increased by a factor of 400 over the dual system. As in any system, the computer control usually represents only a very small percentage of the total system cost, but its influence in system operation is dramatic. A failure of the control section affects the system totally. Therefore, additional hardware to achieve a substantial improvement in availability is a good trade-off.

The TMR 3-2 is a near-flawless control system directed toward critical applications, wherein a false operation is usually very costly to the applications, perhaps endangering the product, the process, the environment, or even human safety. For these applications, it is better for the control to execute an orderly safe shutdown sequence and wait for repair rather than continue with one module when others are defective. The sequence is deterministic and is specified by the application. Otherwise, a single functional module, without any concurrent error detection capability, exposes the system to potential costly false

Table III. Results of MTTF Calculations

System	MTTF, years	
	$c = 0.95$	$c = 0.99$
Dual 2-1	10	50
TMR 3-2-1	4167	20,833

operations. A shorter MTTF for a more safe operation is the trade-off between the two. A market niche exists for this new TMR technology that the current dual systems cannot meet in terms of extended reliability and bumpless transition when the first module fails.

Summary

The static redundant TMR structure provides error detection and correction automatically and is transparent to system operation. This results in a bumpless transition in going from three to two working modules. The important coverage factor is considered to be perfect. Should another module fail, the remaining good module takes the system down in a deterministic and orderly manner to prevent any possible malfunction of the system. This structure is termed the TMR 3-2 configuration. It meets the application needs that require absolute error-free operation. The MTTF is calculated to be 208 years.

As compared with the dual 2-1 configuration with a realistic coverage of 0.95 to 0.99, the MTTFs are calculated to be 10 and 50 years, respectively. However, the transition from the 2 to 1 state may cause a glitch to the system operation.

By combining the TMR 3-2 and the dual 2-1 mode of operation, the resulting structure is the TMR 3-2-1 configuration. The coverage factor is near perfect for the 3-2 transition and imperfect for the 2-1 transition (the same as the dual 2-1 configuration). The MTTF calculations are 4167 and 20,833 years for coverages of 0.95 and 0.99, respectively. The MTTF comparison between the TMR 3-2-1 and the dual 2-1 is improved by a factor of 400.

References

1. G. D. Kraft and W. N. Toy, *Microprogrammed Control and Reliable Design of Small Computers*, Prentice-Hall, Englewood Cliffs, N.J., 1981.
2. J. E. Arsenault and J. A. Roberts, *Reliability and Maintainability of Electronic Systems*, Computer Science Press, Rockville, Md., 1980.
3. W. N. Toy, "Fault-Tolerant Design of Local ESS Processors," *Proceedings of IEEE*, pp. 1126-1145, October 1978.
4. R. E. Lyons and W. Vanderkulk, "The Use of Triple-Modular Redundancy to Improve Computer Reliability," *IBM Journal of Research and Development*, Vol. 6, pp. 200-209, April 1962.
5. D. P. Siewiorek and R. S. Swarz, *The Theory and Practice of Reliable System Design*, Digital Press, Bedford, Mass., 1982.
6. Department of Defense, "Reliability Prediction of Electronic Equipment," Military Handbook, MIL-HDBK-217D, 15 January 1982.
7. T. F. Arnold, "The Concept of Coverage and Its Effect on the Reliability Model of a Repairable System," *IEEE Transactions on Computers*, Vol. 22, pp. 251-254, March 1973.
8. K. S. Trivedi, *Probability and Statistics with Reliability Queuing, and Computer Science Applications*, Prentice-Hall, Englewood Cliffs, N.J., 1982.

(Manuscript received March 10, 1987)