Expected Time to Failure of a Parallel System

Bruce Reistle[a] and Colton Brehm[b]
[a]NASA, Johnson Space Center, Houston, Texas, bruce.c.reistle@nasa.gov
[b]NASA, Johnson Space Center, Houston, Texas, colton.d.brehm@nasa.gov

Abstract: Consider a parallel redundant system modeled in a probabilistic risk assessment. The system fails when every unit fails (there is no repair capability). This system is likely to be subject to both independent and common cause failures. The goal of this paper is to find the expected time to failure of the primary parallel system given that the system fails before the mission is complete. That is, suppose there is a parallel system of size two and that there is a cold standby unit ready to be used if the primary system fails. To model the failure probability of the cold standby unit, the failure time of the primary system is required to determine how much mission time is remaining.

Traditionally, the time to failure of the primary system has been taken to be the total mission time divided by two provided the failure rate of the system is low. This paper will explain how to calculate a more accurate failure time of the for a primary system with equations derived for primary systems with two to four redundant units.

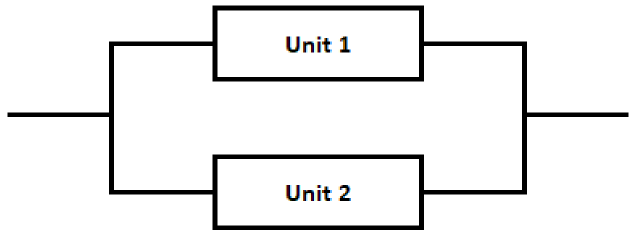
1. INTRODUCTION

Having cold standby units can significantly reduce risk. The advantage of cold standby units is that they are not subject to the entire mission time T, and are only needed to operate successfully for the remainder of the mission when they are needed. Call the remaining required operating time that cold standby units need to operate T_{Cold}. If the system fails at time t^*, then the cold standby time is $T_{Cold} = T - t^*$. Clearly T_{Cold} is greater than zero and less than the mission time, T. However, t^* is not generally known. For this reason, it is common to split the difference and use the mission time divided by two, that is $T_{Cold} = T/2$. The question is whether $T/2$ is the best estimate for T_{Cold}. This paper will demonstrate a way to calculate the **expected value** of t^* and that setting $T_{Cold} = T/2$ is generally (but not always) an overly conservative estimate.

2. EXAMPLE

The simplest redundant system is a system consisting of two units. Assume each has an exponential failure distribution, which is a common assumption. The system fails when both units have failed. The concepts here apply generally to larger sized parallel systems with exponential failure distributions but a system of size two will be used to demonstrate the methodology.

Figure 1: Parallel System of Size Two



For the purposes of this model, the failure *probability* of the redundant system is assumed to be known and is denoted F_{Total}. This probability would most likely come from a fault tree with a known failure rate and a mission time *T*. The failure probability would include both independent and common cause failure scenarios. When modeling independent and common cause failures in a fault tree, the *failure times* are not modeled, only the probability that the failures occur within the mission time *T*.

The following steps are used to obtain the expected value of the time to failure of a parallel system:

3. METHODOLOGY

Step 1
Get F_{Total} from the fault tree model (or other probability model). This total probability of system failure includes all failure contributors (e.g., independent and common cause) over mission time *T*. In all likelihood F_{Total} will be dominated by common cause.

Step 2
Use F_{Total} to obtain a **global exponential failure rate** for the system, λ^G. This will be the failure rate that will result in F_{Total} over the given mission time using the standard exponential model. Essentially, λ^G is the failure rate with common cause included that preserves the total failure mission failure probability with time T.

In general, the failure probability for a single unit with failure rate λ running for time *t* is $F(t) = 1 - e^{-\lambda t}$ and the failure probability of the parallel system of size two, $F_2(t)$ is:

$$F_2(t) = F(t)^2 = \left(1 - e^{-\lambda t}\right)^2$$

In this example let $\lambda = \lambda^G$ and $t = T$ and $F_2(t) = F_{Total}$, so $F_{Total} = \left(1 - e^{-\lambda^G T}\right)^2$.
Solving for λ^G:

$$\lambda^G = -\left(\frac{1}{T}\right) ln\left(1 - F_{Total}^{\frac{1}{2}}\right)$$

In general, given a system of *N* parallel units, the equation for λ^G is:

$$\lambda^G = -\left(\frac{1}{T}\right) ln\left(1 - F_{Total}^{\frac{1}{N}}\right)$$

Step 3
Get the cumulative distribution function $F(t|\lambda^G)$ for the system using the global failure rate, λ^G. This has the same form as in Step 2.

$$F(t|\lambda^G) = \left(1 - e^{-\lambda^G t}\right)^2$$

Step 4
Get the probability density function $f(t|\lambda^G)$ by taking the derivative of $F(f|\lambda^G)$ with respect to t.

$$f(t|\lambda^G) = \frac{d}{dt}F(f|\lambda^G) = \frac{d}{dt}\left(1 - e^{-\lambda^G t}\right)^2$$

$$f(t|\lambda^G) = 2\lambda^G e^{-\lambda^G t} - 2\lambda^G e^{-2\lambda^G t}$$

Step 5
In general, the expected value of a random variable X over time t is $E(X) = \int_0^t xf(x)dx$, where $f(x)$ is the density function. For this step, we want the expected value of t, call it t', from zero to mission time T:

$$t' = \int_{t=0}^{t=T} tf(t|\lambda^G)dt$$

In our example we have:

$$t' = \int_{t=0}^{t=T} t\left(2\lambda^G e^{-\lambda^G t} - 2\lambda^G e^{-2\lambda^G t}\right)dt$$

$$t' = \frac{3}{2\lambda^G} - \frac{2}{\lambda^G}e^{-\lambda^G T} + \frac{1}{2\lambda^G}e^{-2\lambda^G T} - 2Te^{-\lambda^G T} + Te^{-2\lambda^G T}$$

If we are looking for the Mean Time to Failure (MTTF) then let $T \to \infty$ in the above equation and then the $MTTF = \frac{3}{2\lambda^G}$.

To be clear, t' is the expected value of a system failure occurring from time zero to time T. What we want is the expected value of t from time zero to time T *given that the system fails before* time T. Therefore, t' needs to be conditioned on the probability that $t' < T$.

$$P(t' < T) = F(T|\lambda^G) = F_{Total}$$

Let t^* be the expected value of t given that $t < T$. To get the conditional expected value of time t^*, t' simply needs to be divided by F_{Total}:

$$t^* = \frac{1}{F_{Total}}\left(\frac{3}{2\lambda^G} - \frac{2}{\lambda^G}e^{-\lambda T} + \frac{1}{2\lambda^G}e^{-2\lambda^G T} - 2Te^{-\lambda^G T} + Te^{-2\lambda^G T}\right)$$

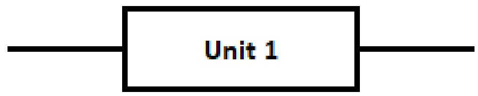
Since t^* is the expected time to failure of the primary system, the standby system would need to function for time $T_{Cold} = T - t^*$.

4. ADDITIONAL CASES

The two-item parallel case has been demonstrated above. The equations for cases of one, three, and four parallel items will be shown below and are derived using the same methodology as the two-item case.

Case: One Unit
Consider a single unit.

Figure 2: Single Unit



In the case of a single unit, the expected time to failure of the system is simply the expected time it takes for a single unit to fail. Also, since there is no redundancy there is no common cause contribution, so λ^G is most likely just the base failure rate. If the failure *probability*, F_{Total}, for the time-based system of size one is provided then:

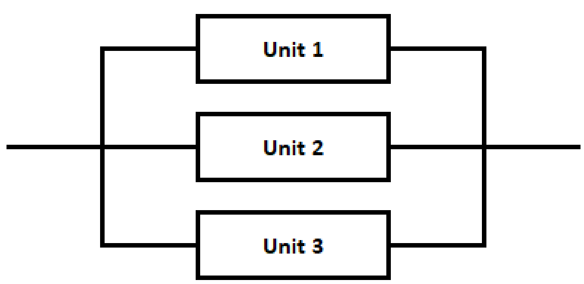
$$\lambda^G = -\left(\frac{1}{T}\right) ln(1 - F_{Total})$$

The equation for t^* is:

$$t^* = \frac{1}{F_{Total}}\left[\frac{1}{\lambda}\left(1 - e^{-\lambda^G T}\right) - Te^{-\lambda^G T}\right]$$

Case: Three Units
Consider a parallel system of size three.

Figure 3: Parallel System of Size Three



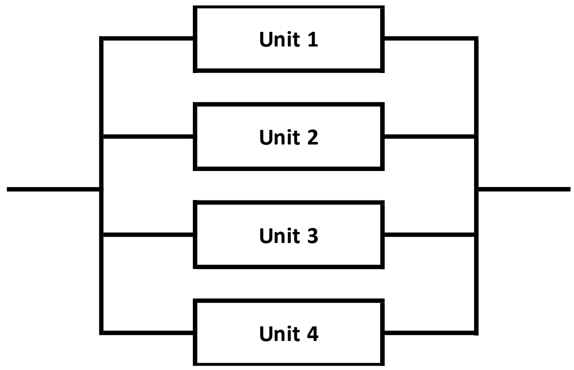
The method for obtaining the equations for a system of size three is the same as for a system of size two.

$$\lambda^G = -\left(\frac{1}{T}\right) ln\left(1 - F_{Total}^{\frac{1}{3}}\right)$$

$$t^* = \frac{1}{F_{Total}}\left(-3Te^{-\lambda^G T} - \frac{3}{\lambda^G}e^{-\lambda^G T} + \frac{3}{\lambda^G} + 3Te^{-2\lambda^G T} + \frac{3}{2\lambda^G}e^{-2\lambda^G T} - \frac{3}{2\lambda^G} - Te^{-3\lambda^G T} - \frac{1}{3\lambda^G}e^{-3\lambda^G T} + \frac{1}{3\lambda^G}\right)$$

Case: Four Units
Consider a parallel system of size four.

Figure 4: Parallel System of Size 4



$$\lambda^G = -\left(\frac{1}{T}\right) ln\left(1 - F_{Total}^{\frac{1}{4}}\right)$$

$$t^* = \frac{-T\left[1-\left(1-e^{-\lambda^G T}\right)^4\right] + \frac{1}{\lambda^G}\left[\left(1-e^{-\lambda^G T}\right) + \frac{1}{2}\left(1-e^{-\lambda^G T}\right)^2 + \frac{1}{3}\left(1-e^{-\lambda^G T}\right)^3 + \frac{1}{4}\left(1-e^{-\lambda^G T}\right)^4\right]}{F_{Total}}$$

5. CHECK

Simulation can be used to check t^* (and $T/2$). Consider a total system failure probability, F_{Total} of 1% and a mission time of $T = 100$. Failure times are randomly sampled from an exponential distribution with rate λ^G. In a given replication the system fails when all failure times are less than the mission time, T. The table below shows the results of simulating the four group sizes and the resulting estimates of the system failure time.

Table 2: Results (100,000 Replications of Each Case)

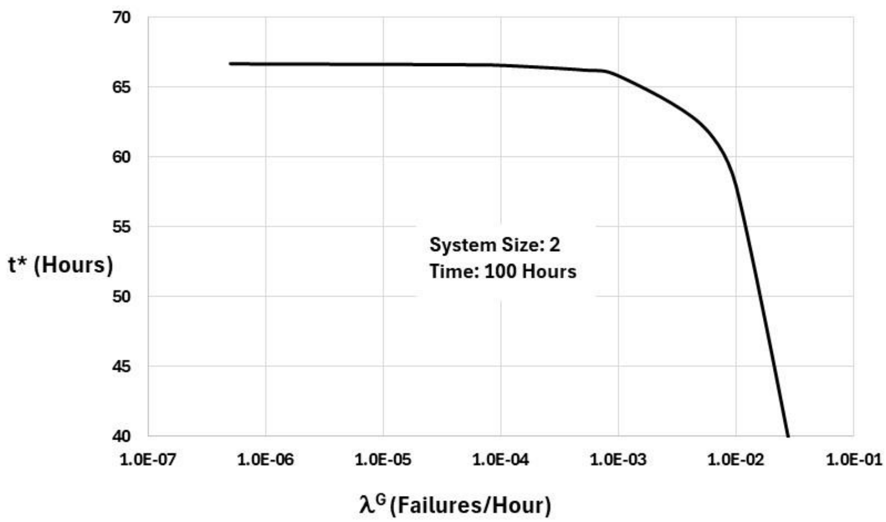
Number of Units	Inputs			Time to Failure Estimates		
	F_{Total}	Mission Time	λ^G	T/2	t*	Simulated
1	0.1	100	1.1E-03	50.0	49.1	49.1
2	0.1	100	3.8E-03	50.0	63.4	63.3
3	0.1	100	6.2E-03	50.0	70.0	70.1
4	0.1	100	8.3E-03	50.0	73.9	73.7

It appears that the $T/2$ method is reasonably close in the single unit case but not in the other three cases. The simulated results match t^* very closely, as expected.

6. RESULTS

Consider a parallel system of size two running for 100 hours. The following plot shows how the values of t^* change with λ^G.

Figure 5: Values of t* for a Parallel System of Size Two



From the figure, most values of λ^G correspond to values of t^* around 67 hours. This would require the cold standby to run for 33 hours, as opposed to 50 if applying the $T/2$ method. If there is a single standby unit, the result is a 33% decrease in risk.

7. CONCLUSION

There are some pros and cons to using this method. On the positive side, you get a more accurate, less conservative answer using the above equations rather than using the generic $T/2$ method. On the negative side, the equations are not generalized for any positive integer N. The equations are unique for each N and get increasingly complex as N gets larger, so if you have a case that is not detailed above then you are forced to solve it, simulate, or use $T/2$.