

Failure State Diagrams – Recovery Following Repair

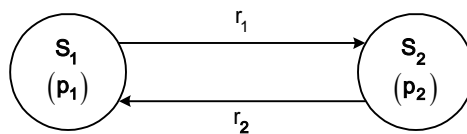
December 2007

Failure State Diagrams Reviewed

In our September, 2007, Geek Corner article, [Calculating Availability – Failure State Diagrams](#), we introduced failure state diagrams as a formal way to derive availability relationships. A failure state diagram contains nodes that represent various states of failure of a system and connectors that indicate ways in which one state may transition to another.

Each connector is characterized by the rate at which its source state will transition to its target state. In the steady state, the transition rates exiting a state must equal the transition rates entering a state.

For instance, Figure 1 shows a system with two states, S_1 and S_2 . The system will be in state S_1 with a probability of p_1 , and it will be in state S_2 with a probability of p_2 . When in state S_1 , the system will transition to state S_2 at a rate of r_1 . Likewise, when the system is in state S_2 , it will transition to state S_1 at a rate of r_2 . Therefore, the total transition rate from state S_1 to S_2 is p_1r_1 ; and the total transition rate from state S_2 to S_1 is p_2r_2 .



**Simple Failure State Diagram
Figure 1**

What are the probabilities that the system will be in either state?

Since the exiting transition rate from a state must be equal to its entering transition rate in the steady-state condition, then

$$\begin{aligned} p_1r_1 &= p_2r_2 && \text{for state } S_1 \\ p_2r_2 &= p_1r_1 && \text{for state } S_2 \end{aligned}$$

Note that for these two nodes, there are two equations; but they are not independent (in this trivial case, they are, in fact, the same). In general, for an n -node system, there will be n equations; but only $n-1$ of them will be independent (that is, any one of the equations can be derived from the others). Since we want to solve for n variables (the n probabilities), we need one more equation. This equation is simply the observation that the probabilities must add up to one since the system will always be in one and only one state. Thus,

$$p_1 + p_2 = 1$$

These equations can now be solved for the probabilities that the system will be in state S_1 or in state S_2 :

$$\text{probability that the system will be in state } S_1 = p_1 = \frac{r_2}{r_1 + r_2}$$

$$\text{probability that the system will be in state } S_2 = p_2 = \frac{r_1}{r_1 + r_2}$$

In our October article, [Failure State Diagrams – Repair Strategies](#), we applied failure state diagrams to sequential and parallel repair strategies to derive the relationships that we had earlier informally derived for these strategies. We now apply this technique to formalize our intuitive look at systems that need to be recovered once they are repaired.

Application of the Failure State Diagram to Recovery

Intuitive Analyses

In our December, 2006, article entitled [Calculating Availability – The Three Rs](#), we informally derived the availability of a system that required recovery following a repair. In these systems, should one node fail, the system continues in operation in simplex mode until the failed node is returned to service. The failure is transparent to the user. However, if both nodes fail, the system is down until at least one node is repaired. Before returning it to service, however, the system must be *recovered*. Recovery might include, for instance, rebuilding the database, starting applications, and testing the system.

Our analysis led to the relations:

$$A = 1 - F \tag{1}$$

$$F = \frac{n(n-1)}{2} \frac{r/2 + R}{r/2} (1-a)^2 \quad \text{for parallel repair and one spare node} \tag{2}$$

$$F = n(n-1) \frac{r+R}{r} (1-a)^2 \quad \text{for sequential repair and one spare node} \tag{3}$$

where

- A = system availability (the probability that the system will be up)
- F = probability of system failure (the probability that the system will be down)
- r = repair time
- R = recovery time
- n = number of nodes in the system
- a = nodal availability

This relationship was based on a loose statement that since the return-to-service time had to be increased from r to $r + R$, we had to increase the failure probability by a factor of $r / (r + R)$. We now confirm this intuitive insight formally with failure state diagrams for the case of parallel repair. The derivation for the case of sequential repair is similar.

Repair Followed by Recovery

The failure state diagram for a system that must be recovered following its repair is shown in Figure 2. The system comprises n nodes. There is one spare node in the system. Therefore, the system will survive the failure of any one node. Should any two nodes fail, the system is down.

Once a node is repaired, the system must be recovered before it can be returned to service (rebuild the database, load applications, test the system, etc.).

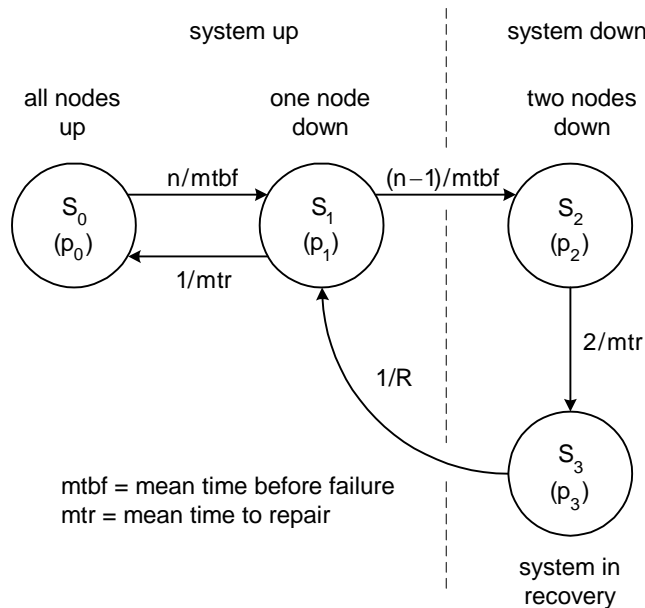
There are four states in this system. In state S_0 , all nodes are operational. In state S_1 , one node has failed; but the system continues in operation. In state S_2 , two nodes have failed; and the system is down. In state S_3 , one of the two downed nodes has been repaired; and the system is undergoing recovery.

A node failure in state S_0 will cause a transition to state S_1 . Each node fails at the rate of $1/mtbf$, where $mtbf$ is the mean time between failure for a node (i.e., if the nodal $mtbf$ is 1,000 hours, each node will fail once every 1,000 hours, or 0.001 failures per hour). Therefore, in state S_0 , in which n nodes are operational, the nodal failure rate will be $n/mtbf$. This is the rate at which the system will transition from state S_0 to state S_1 .

When in state S_1 , it will take a repair time of mtr (mean time to repair) to repair the node. Thus, the system will transition from state S_1 back to state S_0 at a rate of $1/mtr$.

Alternatively, while in state S_1 , a second node could fail. In this case, the system will enter state S_2 , at which point the system is down. Since there are $n-1$ nodes operational in state S_1 , the transition rate to state S_2 is $(n-1)/mtbf$.

While in state S_2 , one of the two downed nodes will be repaired and the system will move to state S_3 , where it will undergo recovery. Since there are two nodes in state S_2 being repaired in parallel, the average repair time is $mtr/2$. Transitions from state S_2 to state S_3 will therefore occur at a rate of $2/mtr$. Recovery takes a time R . Therefore, at a rate of $1/R$, the system will enter state S_1 , where it will once again be operational, albeit with one node down.



Recovery Failure State Diagram
Figure 2

In the steady state, the transitions into and out of each state must be equal. This leads to the following state transition probabilities:

State Transition Equations

State 0	$p_0 n / mtr = p_1 / mtr$
State 1	$p_1 [1 / mtr + (n - 1) / mtr] = p_0 n / mtr + p_3 / R$
State 2	$2p_2 / mtr = p_1 (n - 1) / mtr$
State 3	$p_3 / R = 2p_2 / mtr$

Solving for the state probabilities in terms of p_0 , we have

State Probabilities (in terms of p_0)

$$p_0 = p_0$$

$$p_1 = \frac{n(mtr)}{mtr} p_0 = n \frac{(1-a)}{a} p_0$$

$$p_2 = \frac{n(n-1)}{2} \frac{mtr^2}{mtr^2} p_0 = \frac{n(n-1)}{2} \frac{(1-a)^2}{a^2} p_0$$

$$p_3 = \frac{R}{mtr} n(n-1) \frac{(1-a)^2}{a^2}$$

where we have used the fact that

$$\frac{mtr}{mtr} = \frac{1 - \frac{mtr}{mtr + mtr}}{\frac{mtr}{mtr + mtr}} = \frac{1-a}{a}$$

To solve for the state probabilities, we must now make use of the fact that the sum of the probabilities must be 1:

$$p_0 + p_1 + p_2 + p_3 = 1$$

This lets us solve for the state probabilities as a function of nodal availability, a :

State Probabilities (in terms of a)

$$p_0 = a^2 / D$$

$$p_1 = na(1-a) / D$$

$$p_2 = \frac{n(n-1)}{2} (1-a)^2 / D$$

$$p_3 = \frac{R}{mtr} n(n-1)(1-a)^2 / D$$

where

$$D = a^2 + na(1-a) + \frac{n(n-1)}{2} (1-a)^2 + \frac{R}{mtr} n(n-1)(1-a)^2$$

$$= a^2 + na(1-a) + \frac{n(n-1)}{2} \frac{mtr/2 + R}{mtr/2} (1-a)^2 \tag{4}$$

The system is down if it is in state S_2 or state S_3 . Thus, the probability of failure of the system, F , is the probability that the system will be in state S_2 or state S_3 :

$$F = p_2 + p_3 = \frac{n(n-1)}{2}(1-a)^2/D + \frac{R}{mtr}n(n-1)(1-a)^2/D$$

or

$$F = \frac{n(n-1)}{2} \frac{r/2 + R}{r/2} (1-a)^2/D \quad (5)$$

where we have substituted r for mtr for ease of notation.

Equation (5) is the true expression for the availability of a single-spared n -node system that requires recovery after a parallel repair. It is equivalent to our intuitive Equation (2) except for the denominator D . To the extent that the value of D departs from one, D represents the error in our intuitive approach.

D can be written as

$$\begin{aligned} D &= a^2 + na(1-a) + \frac{n(n-1)}{2} \frac{r/2 + R}{r/2} (1-a)^2 \\ &= [a^2 + 2a(1-a) + (1-a)^2] + (n-2)a(1-a) + \left[\frac{n(n-1)}{2} \frac{r/2 + R}{r/2} - 1 \right] (1-a)^2 \\ &= [a + (1-a)]^2 + \text{func}(1-a) \\ &= 1 + \text{func}(1-a) \\ &\approx 1 \end{aligned}$$

D is equal to 1 plus some function of $(1-a)$. If $(1-a)$ is small, $\text{func}(1-a)$ can be ignored; and D is approximately equal to one. Thus, we find that the accuracy of the intuitive approach of Equation (2) depends upon the nodal availability a being very close to one and therefore $(1-a)$ being very small. It also depends upon there being a modest number of nodes in the system. (More specifically, it depends upon the quantity $(n-2)a(1-a)$ being very small.) This is certainly the case for the high-availability systems in which we are interested. Under these assumptions, D is approximately one; and the intuitive relationship holds.

If nodal availability is not close to one (say less than two 9s), or if there are hundreds of nodes in the system, the more accurate Equation (5) should be used.

Summary

Our intuitive expressions for system availability for a system requiring recovery after a parallel repair are valid provided that the nodal availability is high and that the number of nodes in the system is modest. This is certainly the case for the redundant systems with which we are concerned.

Should these approximations not be valid, Equation (5) should be used to calculate the availability of a single-spared system that is under parallel repair and that needs recovery.

A similar analysis will verify the accuracy of Equation (3) for recovery following sequential repair. The only differences are that the transition rate from state S_2 to state S_3 is $1/mtr$ and that there is no factor of 2 in Equation (4). That is

$$D = a^2 + na(1-a) + n(n-1) \frac{mtr + R}{mtr} (1-a)^2 \quad (6)$$

for sequential repair.