the Availability Digest

Calculating Availability – Failure State Diagrams

September 2007

In the previous articles in our *Calculating Availability* series, we have studied a variety of topics. These have included failure probabilities, repair and recovery strategies, failover and failover faults, environmental faults, and the interdependence of hardware and software faults. In all of this work, we have derived a series of relations based on intuitive reasoning.

However, intuition is not always accurate. How realistic are these relationships? Have we been led astray by inaccurate reasoning? It turns out that there is a very formal way to derive these same relationships. That is through failure state diagrams, which we discuss in this article.[1]

All of the relationships that we have presented in previous Geek Corner articles are based on formal results achieved by analyzing failure state diagrams. Basically, having determined the correct answers through a fairly laborious procedure – the state diagram, we then formulated intuitive approaches to arrive at the same conclusions; and these are what we have been presenting in our Geek Corner articles. Sometimes, we had to stretch a bit to explain intuitively a certain result; and we may have left you feeling a little uneasy with the outcome. We hope that this has been infrequent.

In this article, we explain the use of failure state diagrams. They are actually simple in concept, but sometimes can take some messy algebra to solve. We demonstrate the use of this technique with a trivial example that proves that availability, *A*, is related to system MTBF (mean time before failure) and system MTR (mean time to recover) by

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTR}} \tag{1}$$

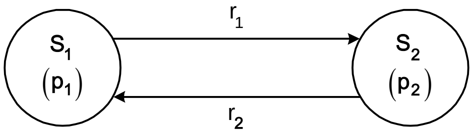
In later articles, we will use failure state diagrams to prove more significant results.

The Failure State Diagram

A failure state diagram is a graph in which the nodes represent the various failure states in which the system can be, and the connectors are the rates at which the system will transition from one state to another. For instance, Figure 1 shows a simple system that can be in two states – S_1 and S_2. The probability that the system is in state S_1 is p_1, and the probability that it is in state S_2 is p_2.

While in state S_1, the system will transition to state S_2 at a rate of r_1 transitions per second. Likewise, while in state S_2, the system will transition to state S_1 with a rate of r_2 transitions per second.

[1] W. H. Highleyman, P. J. Holenstein, B. D. Holenstein, Appendix 3, Failover Fault Models, *Breaking the Availability Barrier: Survivable Systems for Enterprise Computing*, AuthorHouse; 2003.



Simple Failure State Diagram
Figure 1

In the steady state, the outgoing transition rate for a state must equal the incoming transition rate. For instance, consider state S_1. The outgoing transition rate for state S_1 is the probability that the system will be in state S_1, which is p_1, multiplied by the outgoing transition rate from state S_1, which is r_1. Therefore, the outgoing rate from state S_1 is (p_1 r_1). Likewise, its incoming transition rate from state S_2 is the product of the probability that the system is in State S_2, which is p_2, and the transition rate from state S_2, which is r_2. Therefore, the incoming transition rate to state S_1 is (p_2 r_2). Thus, in the steady state,

$$p_1 r_1 = p_2 r_2 \qquad (2)$$

A similar analysis for state S_2 results in

$$p_2 r_2 = p_1 r_1 \qquad (3)$$

Notice that Equations (2) and (3) are two equations with two independent variables, p_1 and p_2. Therefore, in principle, they can be solved to find p_1 and p_2. However, Equations (2) and (3) are identical and therefore do not lend themselves to a solution. This is true of all state diagrams. If there are *n* states, there will be *n* state equations, such as Equations (2) and (3). However, there will be only *n*-1 independent equations since any one of these *n* equations can be derived from the other *n*-1. One more equation is needed to break this impasse, and that is the simple observation that the system must always be in one and only one state at any given time. Therefore, the state probabilities must sum to one:

$$p_1 + p_2 = 1 \qquad (4)$$

Using Equation (4) as the other independent equation, Equations (2) and (4) can now be solved to find the state probabilities. From Equation (2),

$$p_1 = p_2 r_2 / r_1 \qquad (5)$$

From Equation (4),

$$p_2 = 1 – p_1 \qquad (6)$$

Thus, substituting the value for p_2 given in Equation (6) into Equation (5), we have

$$p_1 = (1- p_1) r_2 / r_1$$

or

$$p_1 = r_2 / (r_1 + r_2) \qquad (7)$$

Substituting this value into Equation (2), we have

$$p_2 = r_1 / (r_1 + r_2) \qquad (8)$$

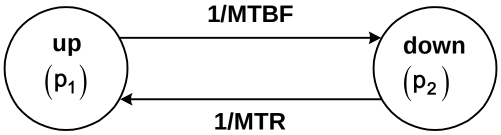
Note that these probabilities add up to one as required by Equation (4).

We now know the probabilities that the system will be in state S_1 or in state S_2 in terms of the transition rates. For instance, if the system will transition from state S_1 to state S_2 once per second when it is in state S_1 ($r_1 = 1$), and if it will transition from state S_2 to state S_1 nine times per second when it is in state S_2 ($r_2 = 9$), then the probability that it will be in state S_1, p_1, is 90%; and the probability that it will be in state S_2, p_2, is 10%.

By the way, note that the transition rate out of a state is the inverse of the amount of time that the system spends in that state. If the transition rate from state S_1, r_1, is once per second, this means that the system will remain in state S_1 for an average of one second. Likewise, if the transition rate from state S_2, r_2, is nine times per second, it will remain in state S_2 for 1/9th of a second.

Single System Failure

So far, failure state diagrams may seem a little abstract. Let us correct that with a simple example. Let us apply Equations (7) and (8) to the trivial case of a single system with a mean time before failure of MTBF and a mean time to recover of MTR. Let state S_1 be the state in which the system is operational and state S_2 be the state in which the system is failed.



Single System Failure State Diagram
Figure 2

Since the transition rates are the inverse of the time spent in a state, the transition rate out of the up state is 1/MTBF; and the transition rate out of the down state is 1/MTR. With respect to Equations (7) and (8), we have

$$r_1 = 1/\text{MTBF}$$

$$r_2 = 1/\text{MTR}$$

Then, from Equations (7) and (8), we have:

$$\text{probability that the system is up } = p_1 = \frac{1/\text{MTR}}{1/\text{MTBF}+1/\text{MTR}} = \frac{\text{MTBF}}{\text{MTBF}+\text{MTR}} \qquad (9)$$

$$\text{probability that the system is down } = p_2 = \frac{1/\text{MTBF}}{1/\text{MTBF}+1/\text{MTR}} = \frac{\text{MTR}}{\text{MTBF}+\text{MTR}} \qquad (10)$$

These are the definitions of availability, *A*, and the probability of failure, *F*. Using the simplifying assumption that MTBF >> MTR (which is certainly the case for the systems in which we are interested), these relations can be written as

$$A = p_1 = \frac{1}{1+\dfrac{\text{MTR}}{\text{MTBF}}} \approx 1 - \frac{\text{MTR}}{\text{MTBF}} \qquad (11)$$

$$F = p_2 \approx \frac{MTR}{MTBF} \qquad (12)$$

Equations (11) and (12) are the simplified forms of the availability equations that we have been using.

Application to Availability Issues

In our next article, we will apply failure state diagrams to the important case of multinode systems with dual redundancy. We will consider two different repair strategies:

- Parallel repair, in which there are multiple repair people available to work simultaneously on all failed nodes in the system.

- Sequential repair, in which there is only one repair person so that only one failed node at a time can be serviced.

In later articles, we will consider systems with a non-zero recovery time and the relative impact of hardware and software failures.