the Availability Digest

www.availabilitydigest.com

Reliability Diagrams

July 2011

Most highly available systems in use today are complex assemblies of redundant components. We may know the reliability characteristics of each component in the system, but how can we use this information to calculate the availability of the entire system?

The *reliability diagram* is an important tool to achieve this end. In this article, we look at reliability diagrams and give an example of how to use them to calculate the availability of complex systems.

Probability 101

When it comes to availability, we are often concerned about binary states. For instance, we are concerned about whether the state of a system is up (operational) or down (failed). This is a binary system – the statement that the system is up is either true or false.

The value (true or false) of a binary state can be specified as a Boolean function with operators AND, OR, and NOT. For instance, it may be that a certain state is true if *x* AND *y* are true OR if *z* is NOT true. Knowing the probabilities of *x*, *y*, and *z*, what is the probability of the system being in that state?

Let p(*k*) be the probability that *k* is true. These Boolean functions transform into the following probability equations.

AND

The AND operator implies multiplication. The probability that *x* AND *y* are true is

$$p(x \text{ AND } y) = p(x)p(y) \qquad (1)$$

For instance, consider dice. What is the probability of rolling a 2 on the first roll of a dice and then rolling a 4 on the second try? The probability of rolling a 2 is 1/6. The probability of rolling a 4 is 1/6. The probability of rolling a 2 on the first roll AND rolling a 4 on the second roll is

$$p(2 \text{ AND } 4) = p(2)p(4) = (1/6)(1/6) = 1/36$$

The chance of rolling a 2 followed by a 4 is one time in 36 tries.

OR

The OR operator implies addition. The probability that *x* OR *y* is true is

$$p(x\ \text{OR}\ y) = p(x) + p(y) \quad (2)$$

Modifying our above example somewhat, what is the probability of rolling either a 2 or a 4 on the first roll? The probability of rolling either is 1/6. The probability of rolling a 2 OR of rolling a 4 is

$$p(2\ \text{OR}\ 4) = p(2) + p(4) = 1/6 + 1/6 = 1/3$$

The chance of rolling either a 2 or a 4 on a roll of the dice is one time out of every three tries.[1]

<u>NOT</u>

The probability that event *z* is not true is

$$p(z\ \text{NOT true}) = p(\text{NOT}\ z) = 1 – p(z) \quad (3)$$

This is obvious since event *z* is either true or not true. Therefore, the probability that *z* is true OR the probability that *z* is NOT true is one. That is, p(z) + p(NOT z) = p(z) + 1 – p(z) =1.

For instance, if the probability of rolling a 1 is 1/6, the probability of NOT rolling a 1 is

$$p(\text{NOT}\ 1) = (1–1/6) = 5/6$$

<u>Combinations</u>

In our opening paragraph in this section, we asked

> "A certain state is true if *x* AND *y* are true OR if *z* is NOT true. Knowing the probabilities of *x*, *y*, and *z*, what is the probability of the system being in that state?"

We now know that the answer is

$$p(x)p(y) + [1 – p(z)]$$

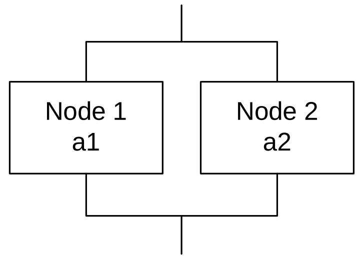
Application to System Availability

Complex systems comprise a wide variety of components, such as processors, storage devices, networks, user terminals, power-distribution systems, and so on. We will call each of these components in a system a *node* of the system.

When considering system availability, there are two major configurations into which the nodes of any system can usually be broken down. They are a parallel (or redundant) configuration and a serial configuration.

[1] For math nuts, the relation for the OR function give in Equation (2) is accurate only if the events are mutually exclusive. However, for our purposes, this is assumed to always be the case.

Redundant Configurations



In a redundant configuration, two (or more) nodes run in parallel. For instance, there may be two processors backing each other up. There may be two networks available for use. Sometimes, the workload is split between them. In other configurations, one acts as a backup to the primary node and can take over should the primary node fail. In any event, the system is up so long as at least one node is operational.

Let us call these nodes *node 1* with an availability of *a1* and *node 2* with an availability of *a2.* Thus,

probability(node 1 is up) = a1
probability(node 2 is up) = a2

Furthermore,

probability(node 1 is down) = probability(node 1 is NOT up) = (1-a1)
probability(node 2 is down) = probability(node 2 is NOT up) = (1-a2)

The probability that the system is down is the probability that node 1 is down AND node 2 is down:

probability(system is down) = (1-a1)(1-a2)

The probability that the system is up is the probability that it is NOT down:

probability(system is up) = 1 – (1-a1)(1-a2) (4)

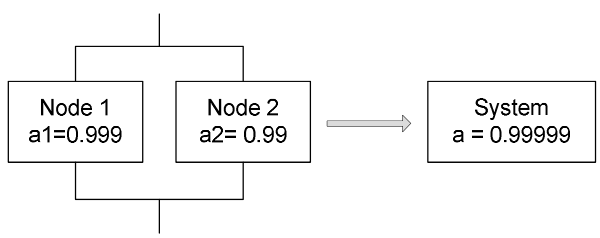
We use Equation (4) to calculate the availability of a redundant pair of components.[2]

For instance, let the availability of node 1 be 0.999 (three 9s) and the probability of node 2 be 0.99 (two 9s). Then the availability of the system is, from Equation (4):

a1 = 0.999
a2 = 0.99

probability(system is up) = 1 – (1-a1)(1-a2)
= 1 – (1 - 0.999)(1 – 0.99) = 1 - 0.001 x 0.01
= 1 – 0.00001 = 0.99999

Pairing a three-9s system with a two-9s system in a redundant configuration yields a system with a much higher availability of five 9s. This leads to a useful rule:



> *The availability of a redundant system is equal to the sum of the 9s of the component nodes.*

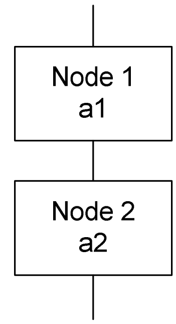
[2] The probability that the system is up could also be stated as the probability that node 1 is up AND node 2 is down OR that node 2 is up AND node 1 is down OR that both nodes 1 and 2 are up. This is a1(1-a2)+a2(1-a1)+a1a2, which can be written as a1 +a2 -a1a2 = 1 + a1 +a2 -a1a2 - 1 = 1 – (1 – a1 – a2 + a1a2) = 1 – (1-a1)(1-a2), which is Equation (4). This is a much more complex analysis leading to the same result.

For instance, if one node has an availability of 0.992, and if its backup node has an availability of 0.95, you can say that the redundant system has an availability of more than three nines (it will, in fact, be 0.9996).

This rule applies to any number of parallel nodes. If three processors are backing each other up with availabilities of 0.9, 0.99, and 0.999 respectively, the resulting processor complex has an availability of six 9s.

Serial Configurations

In a serial configuration, two or more nodes depend upon each other to keep the system operational. If one node fails, the system fails. For instance, a processing node and a storage node must both be up in order for the system to be up.



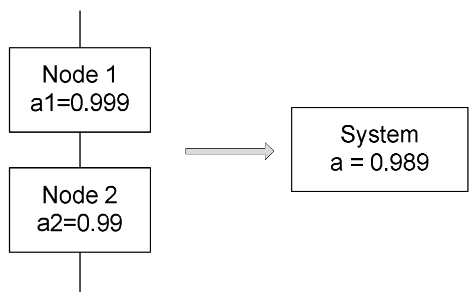
Consider a two-node serial system with node 1 having an availability of a1 and node 2 having an availability of a2:

probability(node 1 is up) = a1
probability(node 2 is up) = a2

The system is up only if both node 1 AND node 2 are operational. Therefore,

$$p(\text{system up}) = a1 \times a2 \qquad (5)$$

Equation (5) applies to any number of nodes in series. If there are *n* nodes, the overall availability of the configuration is the product of all *n* availabilities.



As an example, consider two serial nodes with the availabilities that we used in the redundant example above. Node 1 has an availability of 0.999, and node 2 has an availability of 0.99. The availability of the serial system is, from Equation (5):

$$a1 = 0.999$$
$$a2 = 0.99$$
$$p(\text{system up}) = a1 \times a2 = 0.999 \times 0.99 = 0.989$$

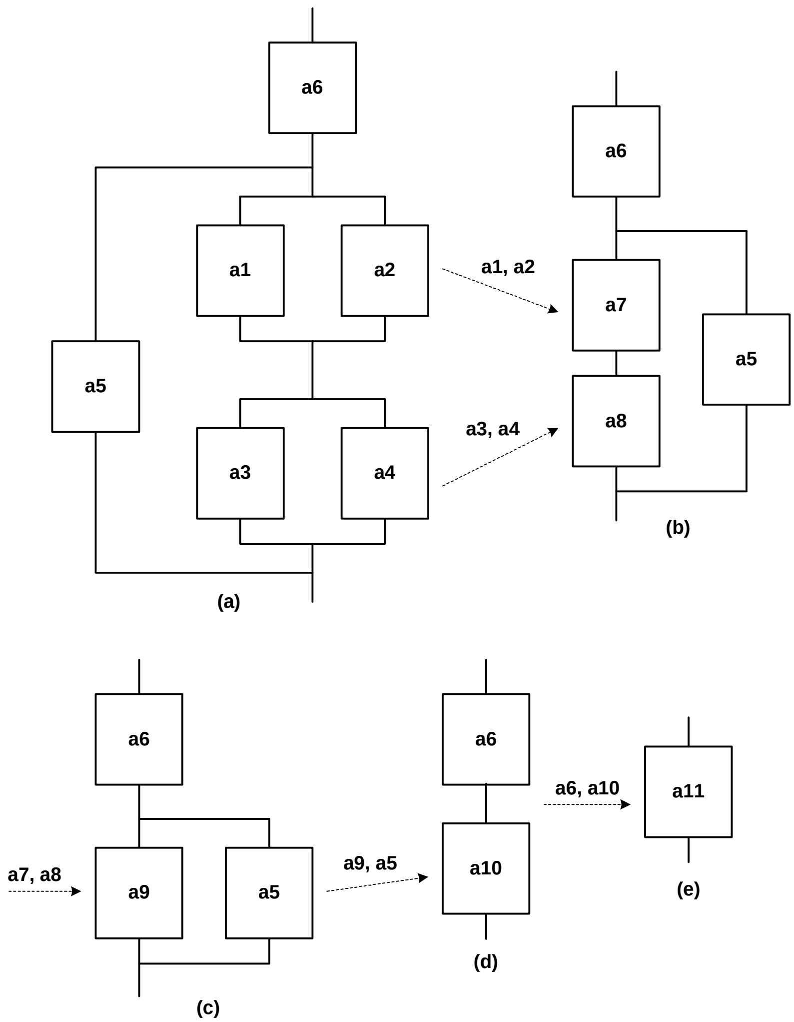
If there were three serial nodes with availabilities of 0.995, 0.998, and 0.9993, the system availability would be 0.995 x 0.998 x 0.9993 = 0.9923.

Notice that the system availability of a serial system is less than any of the nodal availabilities. A system cannot be more reliable than its weakest link.

Complex Systems

Systems can be more complex than the parallel and serial systems considered above. There may be a network of subsystems in a serial/parallel configuration. The first step in analyzing the availability of a complex system is to represent it in a *reliability diagram*, as shown in Figure 1a. This diagram shows the availability interaction of all of the system's nodes expressed as parallel (redundant) and serial architectures.

The availability of a complex system can be analyzed by first calculating the availability of each of the parallel subsystems in the complex and by replacing each with a single node with the equivalent availability. Next, each series of subsystems are replaced with a single node with the equivalent availability. More parallel subsystems may be created and are resolved followed by more serial subsystems. This process continues until the system has been reduced to a single node with its calculated availability, which is the system availability.



A Complex System
Figure 1

For instance, consider the system of Figure 1a. It comprises six nodes with availabilities of a1 through a6. We start by noting that there are two parallel subsystems of two nodes each. The availability of the a1/a2 parallel subsystem is

$$a7 = 1 - (1-a1)(1-a2)$$

The availability of the a3/a4 subsystem is

$$a8 = 1 - (1-a3)(1-a4)$$

We replace these two parallel subsystems with single nodes with availabilities of a7 and a8, as shown in Figure 1b. This now exposes a two-node serial subsystem with availabilities of a7 and a8. Its availability is

$$a9 = a7 \times a8$$

The serial subsystem is replaced with a single node with availability a9, as shown in Figure 1c. This leads to another two-node parallel subsystem with availabilities of a5 and a9. The availability of this parallel subsystem is

$$a10 = 1 – (1\text{-}a5)(1\text{-}a9)$$

Replacing this parallel subsystem with a single node with availability a10 gives the configuration shown in Figure 1d. This again is a two-node serial subsystem, in which the nodes have availabilities of a6 and a10. Its availability is

$$a11 = a6 \times a10$$

We have reduced the complex system to a single node, and a11 is the availability of the entire system of Figure 1a.

An Example

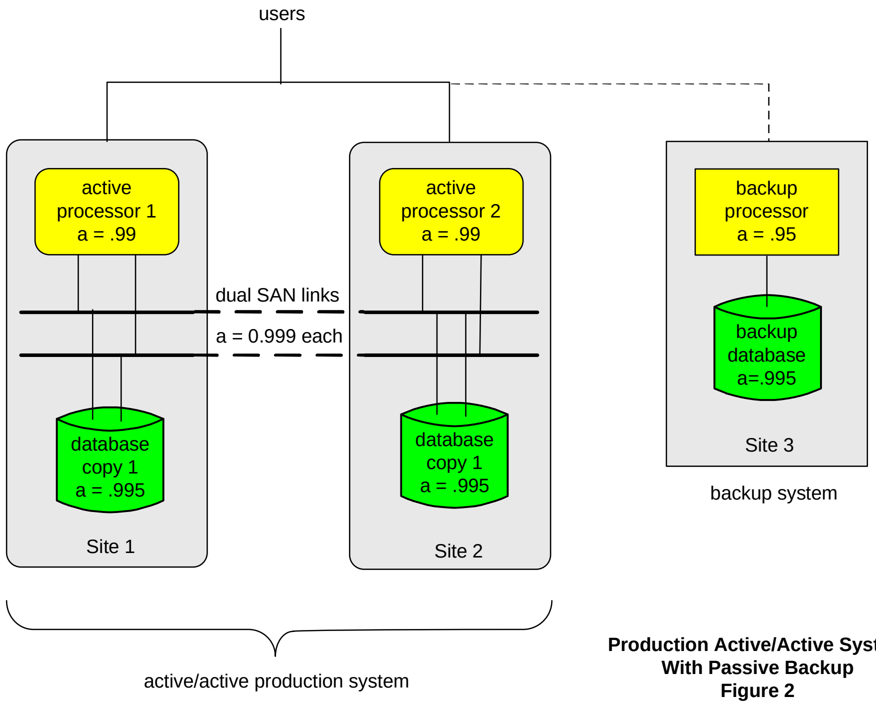
To illustrate the application of these concepts, consider a configuration that is an active/active system backed up by a hot standby system, as shown in Figure 2. The active/active system comprises two processing nodes split across two sites. Each of the processing nodes has access to a redundant Fibre Channel Storage Area Network (SAN) that connects the processing nodes with two identical storage subsystems, one at each site. The storage subsystems use data replication to keep each in synchronization with the other.

The active/active system is up if at least one processor is up as well as one SAN and one storage subsystem. Alternatively, the active/active system is down if the processor pair is down or if the dual SAN is down or if the storage subsystem pair is down.

Should the active/active system fail, the standby system will take over operations for all the users.

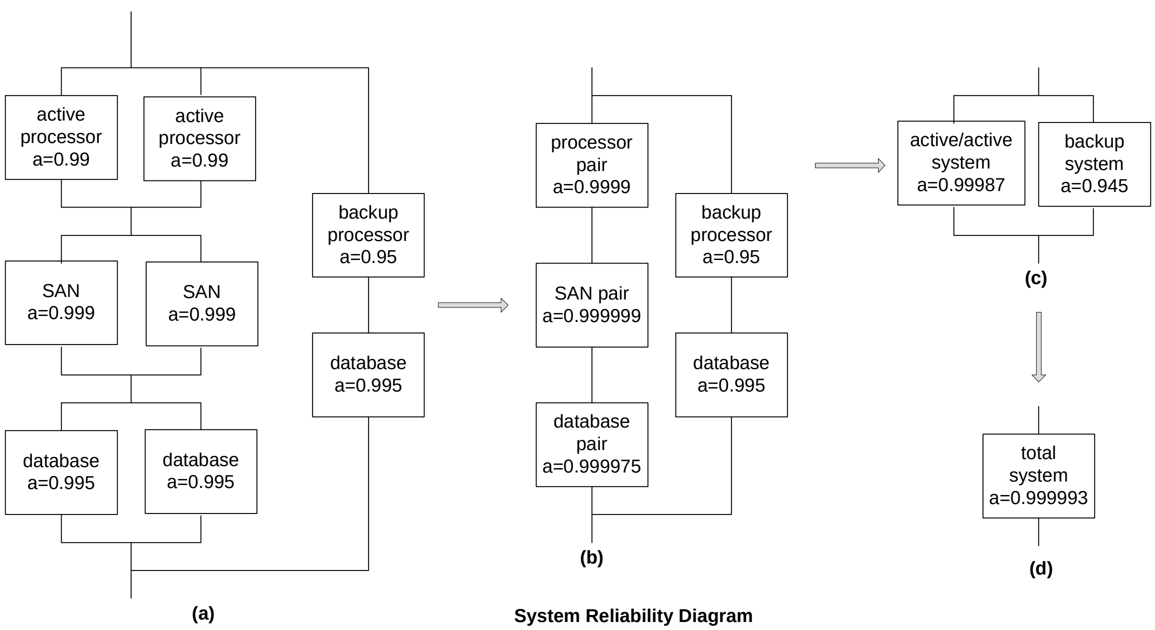
In the active/active system, as shown in Figure 2, the availability of the processors used in the active/active pair is 0.99. The availability of each SAN Fibre Channel network is 0.999. The availability of each storage subsystem (the database) is 0.995.

In the backup system, the processor has an availability of 0.95; and its disk subsystem has an availability of 0.995.



Production Active/Active System
With Passive Backup
Figure 2

To analyze the availability of this system, let us first construct an availability diagram, as shown in Figure 3a.



System Reliability Diagram
Figure 3

This reliability diagram depicts a processor pair, a SAN pair, and a database pair in series. This entire complex is backed up by a backup system comprising a processor and a database in series. The resolution of this diagram to the total system availability proceeds in the following steps:

Step 1 – Resolve parallel components

The availability of the processor pair, from Equation (4), is

[1-(1-0.99)(1-0.99)] = 0.9999 (four 9s)

The availability of the SAN pair is

[1-(1-0.999)(1-0.999)] = 0.999999 (six 9s)

The availability of the database pair is

[1-(1-0.995)(1-0.995] = 0.999975 (over four 9s)

These results are shown in Figure 3b.

Step 2 – Resolve serial components

From Equation (5), the availability of the active/active system is

0.9999 x 0.999999 x 0.999975 = 0.99987 (over three 9s)

The availability of the backup system is

0.95 x 0.995 = 0.945 (over one 9)

These results are shown in Figure 3c.

Step 3 – Resolve parallel components

The system has been resolved down to an active/active node in parallel with a backup node. Thus, the availability of the system is

[1-(1-0.99987)(1-0.945)] = 0.999993 (over five 9s)

This result is shown in Figure 3d.

Summary

Most complex IT systems can be represented as a set of redundant nodes in serial with other nodes. To calculate the availability of such a system, the first step is to draw a reliability diagram of the system. The next step is to resolve each parallel node into a single node using Equation (4). Then each series of serial nodes is resolved into a single node using Equation (5). These two steps are executed iteratively until the system is reduced to a single node giving its availability.

This analysis has focused on system downtime due only to node failures. However, in reality, a redundant system is down if it is in the process of failing over. The extension of reliability diagrams to include failover is discussed in our companion two-part series, Simplifying Failover Analysis, Parts 1 and 2.[3]

[3] http://www.availabilitydigest.com/public_articles/0510/failover_analysis.pdf
http://www.availabilitydigest.com/public_articles/0606/failover_analysis_2.pdf