Probability and Statistics Notes

Note 4

Determination of System Probability of Failure from Subsystem Probabilities of Failure

by
Sgt M. A. Skinner

26 January 1972

Air Force Weapons Laboratory

Abstract

This note presents a method for determining a system probability of failure when the probabilities of failure of individual subsystems are known. The note shows how to obtain upper and lower bounds on the system probability of failure when the means by which subsystem failures combine to produce a system failure are not known. The note also develops a "nominal" probability of failure for the case where the individual subsystems operate independently to produce a system failure.

INTRODUCTION

A general, complex system may have many fault modes (i.e. modes of failure). These fault modes may be associated with the failures of several independent or interacting subsystems. This note presents a method for determining a system probability of failure when the probabilities of failure of individual subsystems are know. It is also assumed that the system contains no redundant subsystems, that is, failure of any subsystem will result in a system failure.

The note shows how to obtain upper and lower bounds on the system probability of failure when the means by which subsystem failures combine to produce a system failure are not known. The note also develops a "nominal" probability of failure for the case where the individual subsystems operate independently to produce a system failure.

DISCUSSION

It will be assumed in this note that probabilities of failure of the subsystems are known. It should be noted that usually, only estimates of these probability of failure curves are available, i.e. only a finite number of tests have been performed to determine the subsystem probability of failure. This more realistic case will be treated in a later note.

The subsystem probability of failure curves are assumed to be of the form of figure 1.

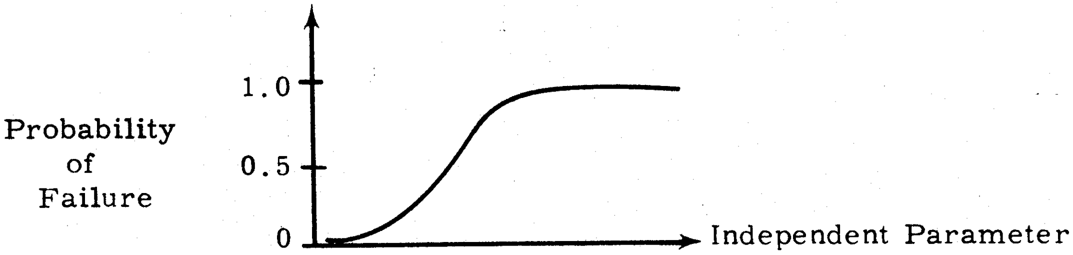

Figure 1 - Probability of Failure Curve (General)

Examples of figure 1 might be the probability that a certain size of steel cable will break where the independent parameter is the tension in the cable. For this example, the cable is one of the subsystems in an overall system that might be a suspension bridge.

Another example might be the probability that a logic circuit will be upset where the independent parameter is the noise voltage applied to the circuit input terminals. For this example the circuit is one of the subsystems in an overall system that might be a digital computer.

As a first example of computing the system probability of failure, a system consisting of only two subsystems will be considered. Three different means by which subsystem failures cause system failure will be considered; these will be the upper bound, lower bound, and nominal value of the probability of system failure.

The system of interest is shown in figure 2.

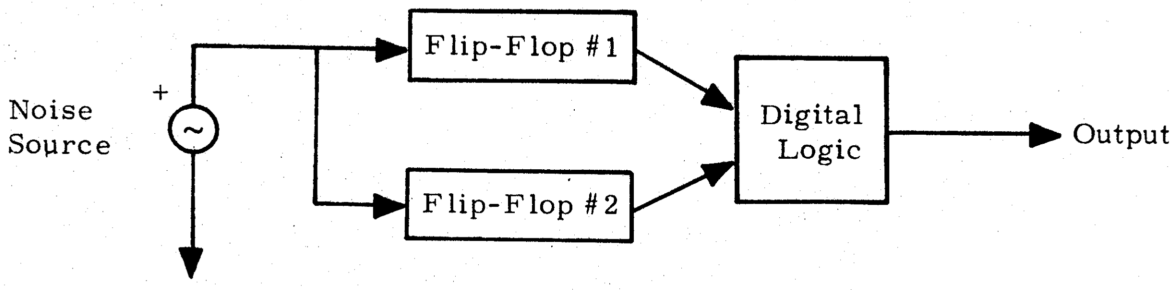

Figure 2 - System Composed of Two Subsystems

The two subsystems are the flip-flops #1 and #2. They are being upset by a noise voltage source. Their outputs are combined by the digital logic to produce an output that may or may not produce a system failure.

The probabilities of failure of the two subsystems can be calculated versus the noise voltage level from the known, subsystem probability of failure curves. The probabilities of failure of the two flip-flops are shown in figure 3.

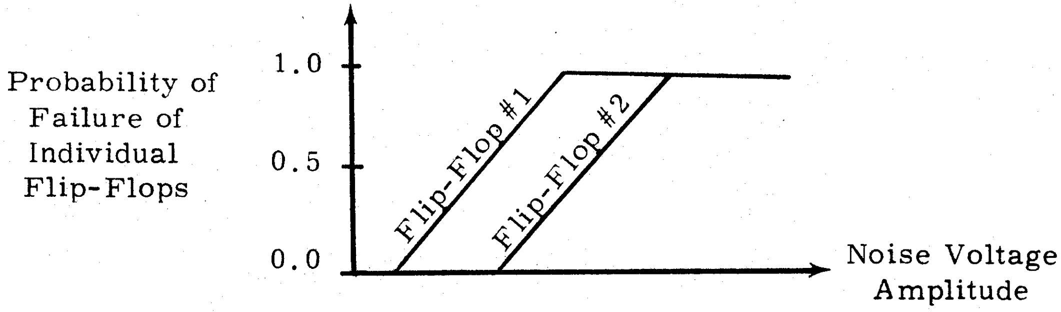

Figure 3 - Probabilities of Failure for Individual Flip-Flops

It is desired to combine the individual probability of failure curves of figure 3 to obtain one system probability of failure curve.

CASE 1: INDEPENDENT SUBSYSTEMS

It is assumed that a failure of either subsystem 1 or subsystem 2 or both subsystems 1 and 2 will cause a system failure. Then the event that the system fails is the event that subsystem 1 fails or subsystem 2 fails or that both subsystems 1 and 2 fail.

Let A = the event that subsystem #1 fails, B = the event that subsystem #2 fails, and C = the event that the system fails.

The region of system failure can be shown with the Venn diagram of figure 4.

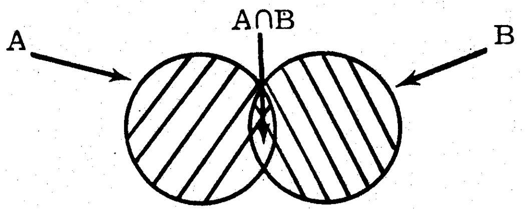

Figure 4 - Venn Diagram Showing Independent Subsystem Failures

From figure 4 it is seen that

$$C = A + B - (A \cap B) \tag{1.}$$

From equation 1 it is possible to write the probability of failure of the system as

$$P_F = P_{F_1} + P_{F_2} - P_{F_1 \cap F_2} \tag{2.}$$

where

P_F = probability of system failure,

P_{F_1} = probability of failure of subsystem 1,

P_{F_2} = probability of failure of subsystem 2,

and

$P_{F_1 \cap F_2}$ = probability of failure of subsystem 1 and subsystem 2.

Rewriting the last term of equation 2 gives

$$P_{F_1 \cap F_2} = P_{F_1 | F_2} \cdot P_{F_2} = P_{F_2 | F_1} \cdot P_{F_1} \qquad (3.)$$

where

$P_{F_1 | F_2}$ = probability of failure of subsystem 1 given that subsystem 2 has failed.

For case 1 it is assumed that subsystem 1 and subsystem 2 fail independently, i.e. that

$$P_{F_1 | F_2} = P_{F_1} \quad \text{and} \quad P_{F_2 | F_1} = P_{F_2} \qquad (4.)$$

Combining equations 2, 3, and 4 yields

$$\boxed{P_F = P_{F_1} + P_{F_2} - P_{F_1} \cdot P_{F_2}} \qquad (5.)$$

for independent subsystem failures.

An example of a system failure caused by two, independent subsystem failures might be a suspension bridge supported by 2 steel cables. If either or both of the cables fail, the bridge will collapse. Each cable could fail independently of the other cable.

Figure 5 shows the system probability of failure curve for Case 1 given the individual probability of failure curves of figure 3.

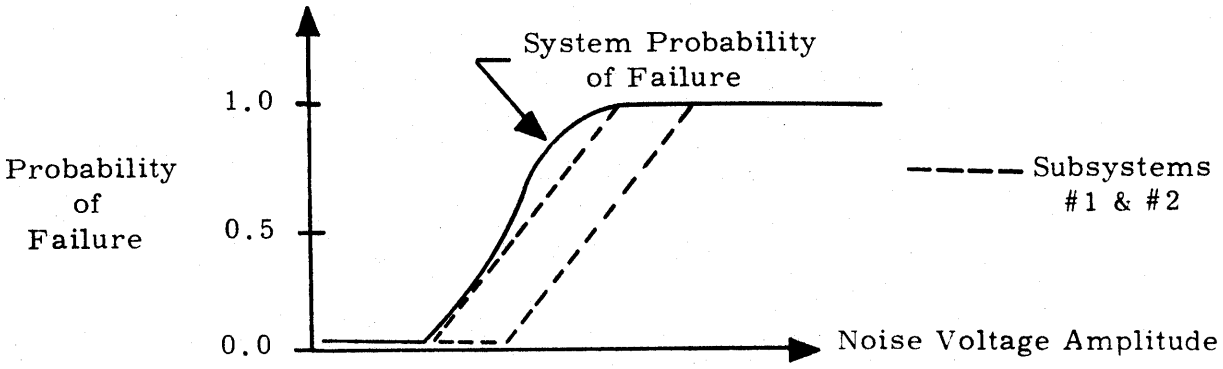

Figure 5 - System Probability of Failure From Subsystem Probability of Failure--Independent Subsystem Failures

CASE 2: MUTUALLY EXCLUSIVE SUBSYSTEMS

For Case 2 the events A and B are mutually exclusive, i.e. they contain no common elements. As for Case 1 let A = the event that subsystem #1 fails, B = the event that subsystem #2 fails, and C = the event that the system fails.

The Venn diagram for Case 2 is shown in figure 6.

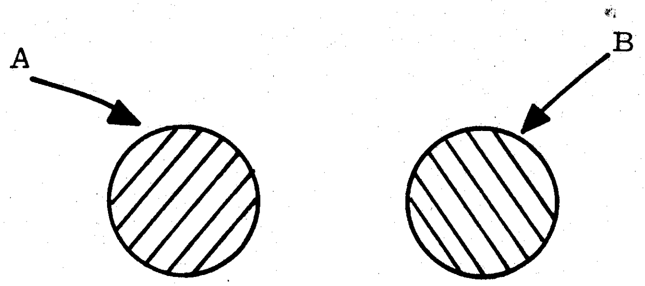

Figure 6 - Venn Diagram for Mutually Exclusive Subsystem Failures

From figure 6 it is seen that

$$C = A + B \qquad (6.)$$

$$A \cap B = \phi, \text{ the null set.} \qquad (7.)$$

From equation 6 it is possible to write the probability of failure of the system as

$$\boxed{P_F = P_{F_1} + P_{F_2}} \qquad (8.)$$

for mutually exclusive failures.

In terms of equation 1 it can also be stated that

$$P_{F_1 \cap F_2} = 0 \; ; \qquad (9.)$$

that is, the probability that both events A and B occur is zero. The events are mutually exclusive; the occurrence of one event prevents the other event from happening.

In terms of equation 3 it can be stated that

$$P_{F_1|F_2} = 0 \quad \text{and} \quad P_{F_2|F_1} = 0 \ . \tag{10.}$$

An example of a system failure caused by two, mutually exclusive subsystem failures might be a digital computer that fails if an input logic circuit sends it the input sequences (0,0) or (1,1). The logic circuit can cause computer failure by generating either of these sequences.

The two failure events are mutually exclusive; if either sequence occurs, the other sequence cannot occur simultaneously.

Figure 7 shows the system probability of failure curve for Case 2 given the individual probability of failure curves of figure 3.

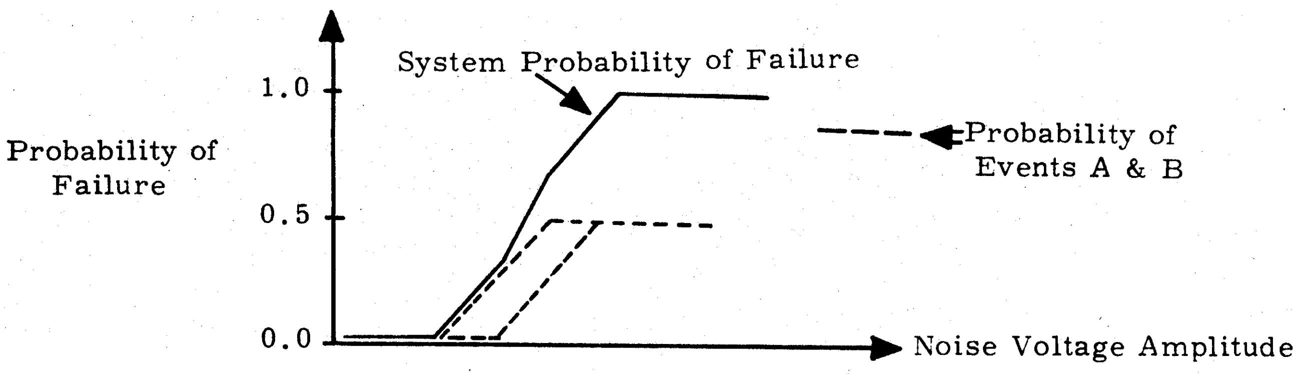

Figure 7 - System Probability of Fail From Subsystem Probability of Failure--Mutually Exclusive Subsystem Failures

CASE 3: TOTALLY DEPENDENT SUBSYSTEMS

It is assumed that a failure of either subsystem 1 or subsystem 2 or both subsystems 1 and 2 will cause a system failure. For Case 3 the event that subsystem 2 fails is a subset of the event that subsystem fails; that is, every time that subsystem 2 fails, subsystem 1 fails also.

As for Cases 1 and 2 let A = the event that subsystem #1 fails, B = the event that subsystem #2 fails, and C = the event that the system fails.

The Venn diagram for Case 3 is shown in figure 8.

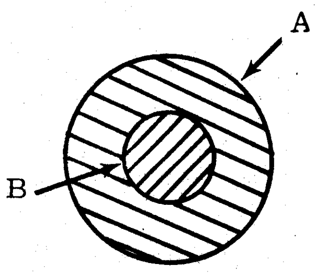

Figure 8

From figure 8 it can be seen that

$$C = A + B - (A \cap B) \qquad (11.)$$

The event B is a subset of the event A; then

$$A \cap B = B \qquad (12.)$$

and equation 11 becomes

$$C = A \qquad (13.)$$

From equation 13 it is possible to write the probability of failure of the system as

$$\boxed{P_F = P_{F_1}} \qquad (14.)$$

for subsystem 2 failure totally dependent on subsystem 1.

In terms of equation 2 it can also be stated that

$$P_{F_1 \cap F_2} = P_{F_2} \; ; \qquad (15.)$$

that is, the probability that both event A and event B occur is the probability that event B occurs.

In terms of equation 3 it can be stated that

$$P_{F_1 | F_2} = 1.0 \qquad (16.)$$

An example of a system with a failure mode exhibiting total dependence is shown in figure 9.

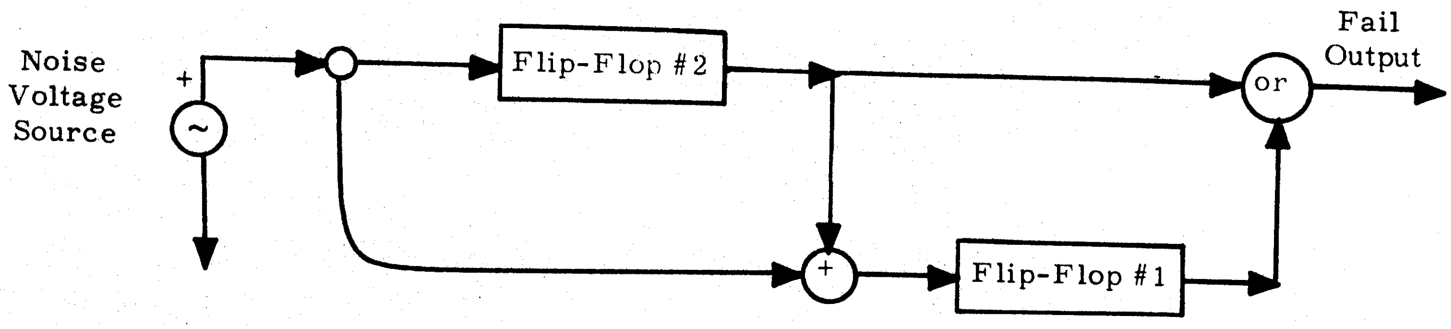

Figure 9 - System with Totally Dependent Failure Mode

For this system each time flip-flop #2 is upset, it also upsets flip-flop #1 and initiates a "FAIL" output.

Assume it is possible to observe the probability of upset of both flip-flops versus the noise voltage level. This allows probability of failure curves of figure 3 to be drawn for upset of flip-flops #1 and #2.

The analysis shows that the probability of failure for the system is just the probability of failure of flip-flop #1.

Figure 10 shows the probability of failure curve for the Case 3 given the individual, probability of failure curves of figure 3.

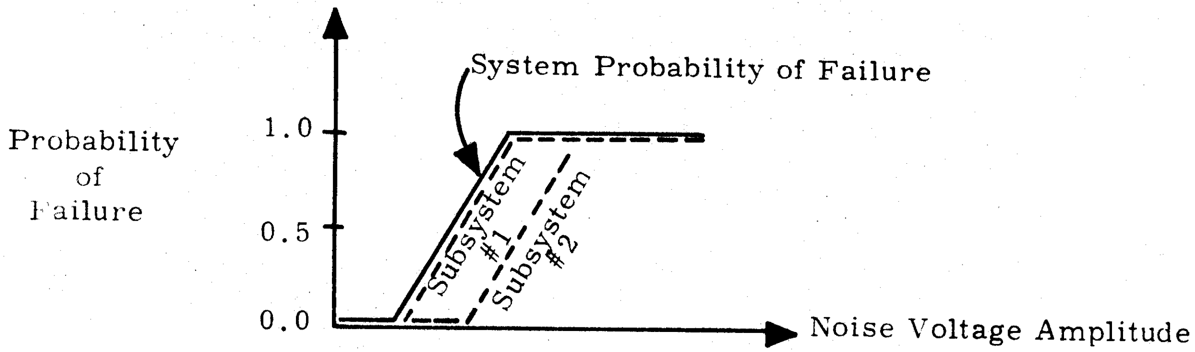

Figure 10 - System Probability of Failure From Subsystem Probability of Failure--Totally Dependent Subsystem Failures

A degenerate example of Case 3 occurs when subsystem #1 always causes subsystem #2 to fail and subsystem #2 always causes subsystem #1 to fail. Then event A = event B and $P_F = P_A = P_B$.

UPPER AND LOWER BOUNDS FOR SYSTEM PROBABILITY OF FAILURE

Suppose that the probability of failure curves of figure 3 are given, but the relationship of the subsystems in producing system failure is not known. It is possible to assume that each of the three cases so far studied will apply and use the results to obtain upper and lower bounds on the system probability of failure.

It will be assumed first that the probability of failure curves of figure 3 are known. Suppose that a particular noise voltage level is chosen and the probabilities of failure of the subsystems at the noise level are known, i.e. P_{F1} and P_{F2}.

1. Assume independent events. Then from equation 5

$$P_F = P_{F_1} + P_{F_2} - P_{F_1} \cdot P_{F_2} \tag{5.}$$

Both P_{F1} and P_{F2} are in the interval zero to one. Then the result of equation 5 will also be in the interval zero to one.

2. Assume mutually exclusive events. Then from equation 8

$$P_F = P_{F_1} + P_{F_2} \tag{8.}$$

If this yields a P_F greater than one, then the events cannot be mutually exclusive. This case is not valid for the events observed.

3. Assume totally dependent events. From equation 14

$$P_F = \max\{P_{F_1}, P_{F_2}\} \tag{14.}$$

That is, choose the larger of the probabilities. This is the same as assuming that one subsystem fails each time the other subsystem fails, or event A is a subset of event B or vice-versa.

Equations 8 and 14 can be then used to place upper and lower bounds on the system probability of failure.

From equations 5 and 8 it can be seen that

$$P_{F,\text{independent}} \le P_{F,\text{ mutually exclusive}} \tag{17.}$$

This can be proven as follows:

$$P_{F_1} + P_{F_2} - P_{F_1} \cdot P_{F_2} \overset{?}{\leq} P_{F_1} + P_{F_2}$$

$$- P_{F_1} \cdot P_{F_2} \leq 0$$

and

$$P_{F_1} \cdot P_{F_2} \geq 0$$

From equations 8 and 14 it can be seen that

$$P_{F,\text{totally dependent}} \leq P_{F,\text{mutually exclusive}} \qquad (18.)$$

This can be proven as follows:

$$\max\{P_{F_1}, P_{F_2}\} \overset{?}{\leq} P_{F_1} + P_{F_2}$$

This is true because both P_{F_1} and P_{F_2} are between 0 and 1. From equations 5 and 14 it can be seen that

$$P_{F,\text{totally dependent}} \leq P_{F,\text{independent}} \qquad (19.)$$

This can be proved as follows:

$$\max\{P_{F_1}, P_{F_2}\} \overset{?}{\leq} P_{F_1} + P_{F_2} - P_{F_1} \cdot P_{F_2}$$

Suppose that $\max\{P_{F_1}, P_{F_2}\} = P_{F_1}$; then

$$P_{F_1} \overset{?}{\leq} P_{F_1} + P_{F_2} - P_{F_1} \cdot P_{F_2}$$

$$0 \overset{?}{\leq} P_{F_2} - P_{F_1} \cdot P_{F_2}$$

$$0 \overset{?}{\leq} P_{F_2}(1 - P_{F_1})$$

Both P_{F_2} and $(1 - P_{F_1})$ are non-negative and the inequality holds.

Using equations 17, 18, and 19 yields

$$\boxed{P_{F,\text{totally dependent}} \leq P_{F,\text{independent}} \leq \min\{P_{F,\text{mutually exclusive}}, 1.0\}} \qquad (20.)$$

Equation 20 can be used to obtain upper and lower bounds on the system probability of failure when the subsystem probabilities of failure are known, but the dependence of subsystem failures in producing a system failure is not known.

For example suppose that $P_{F1} = 0.6$, $P_{F2} = 0.4$. Then

$$P_{F,\text{mutually exclusive}} = 1.00$$

$$P_{F,\text{independent}} = 0.76$$

$$P_{F,\text{totally dependent}} = 0.60 \ .$$

N - INTERACTING SUBSYSTEMS

This analysis can be extended to the case of any number, N, of interacting subsystems to provide upper and lower bounds on the probability of failure curves.

The resulting formulas are

UPPER BOUND (MUTUALLY EXCLUSIVE FAILURES)

$$\boxed{P_F = \min\{P_{F_1} + P_{F_2} + \cdots + P_{F_N}, 1.0\}} \qquad (21.)$$

LOWER BOUND (TOTALLY DEPENDENT FAILURES)

$$\boxed{P_F = \max\{P_{F_I}\}, \quad (I = 1, 2, \cdots, N)} \qquad (22.)$$

"NOMINAL" CASE (INDEPENDENT FAILURES) *

$$\boxed{P_F = 1.0 - (1.0 - P_{F_1}) \cdot (1.0 - P_{F_2}) \cdots (1.0 - P_{F_N})} \qquad (23.)$$

Equations 21 and 22 can be used to calculate upper and lower bounds on the system failure threshold curves when the individual failure threshold curves are known. Equation 23 can be used when the subsystems are known to operate independently. In general the interactions of the subsystem and the precise failure mechanisms are not known; for this case equations 21, 22, and 23 can be used as upper bounds, lower bounds, and nominal values of the system failure thresholds.

*Equation 23 is derived in Appendix I of this note.

APPENDIX I: AN INTERESTING RELATION FOR INDEPENDENT SUBSYSTEMS

An interesting relation exists for the probabilities of survival for the independent case. (Case 1.)

Let

$$P_{S_1} = 1.0 - P_{F_1}$$

$$P_{S_2} = 1.0 - P_{F_2} \qquad \text{(A.1)}$$

where

P_{S_1} = probability of survival of the system when subsystem 1 when it is driven.

and

P_{S_2} = probability of survival of the system when subsystem 2 when it is driven.

Also

$$P_{S,IND} = 1 - P_{F,IND} \qquad \text{(A.2)}$$

where

$P_{F,IND}$ = probability of failure of the system for independent failures,

and

$P_{S,IND}$ = probability of survival of the system for independent failures.

Then

$$P_{S,IND} = 1.0 - P_{F,IND}$$

$$= 1.0 - (P_{F1} + P_{F2} - P_{F1} \cdot P_{F2})$$

$$P_{S,IND} = 1.0 - P_{F1} - P_{F2} + P_{F1} \cdot P_{F2} \qquad \text{(A.3)}$$

This may be factored to yield

$$P_{S,IND} = (1.0 - P_{F1})(1.0 - P_{F2}) \tag{A.4}$$

or

$$P_{S,IND} = P_{S1,IND} \cdot P_{S2,IND} \tag{A.5}$$

From equation A.5 the probability of survival of a system composed of 2 independent subsystems is just the product of the probabilities of survival of the two subsystems. This makes sense since the event that the entire system survives is the event that both subsystems survive, i.e. subsystem 1 survives <u>and</u> subsystem 2 survives.