An Engineering Approach to Mathematical Reliability Models

JACK W. NICHOLAS* AND ROBERT K. PRINCE JR.†
Lockheed-California Company, Burbank, Calif.

In the practice of reliability analysis, we frequently encounter systems which cannot be exactly represented by the series-parallel model usually preferred for reliability analysis and display. A technique has been devised for constructing conservative series-parallel engineering approximations to such systems. The technique permits extensive use of current computer technology to minimize clerical error and to facilitate the analysis of the relatively large systems met in practice. In particular, errors of omission will cause a conservative underestimate of reliability.

Introduction

IF a system consists of n statistically independent components, each of which may or may not fail, then the set of mission outcomes (success, failure) for the system can be described as a sample space of n dimensions. If each component has a single failure mode, then each dimension of the sample space must take one of two values, giving 2^n points (combinations of individual success/failure for all the components simultaneously) in the sample space. When components have more than one failure mode, of course, the size of the sample space is increased accordingly.

For simple systems consisting of a relatively small number of components, each point of the sample space (each possible combination of failures/successes) can be examined against a set of success criteria. The probabilities associated with each success point can then be evaluated and summed to determine the probability of mission success. This form of model has been successfully used.

For more complex systems, however, the examination of 2^n sample points is impractical. In one real subsystem on an advanced commercial airplane, the sample space contained over 10^{30} points! An engineering approximation for problems of this magnitude would therefore be extremely useful.

First Approximation

The first step toward such an engineering approximation might be to disregard those points of the sample space which have a negligible effect on system reliability. It is convenient to consider the ways in which the system can fail (failure modes). We let a_i = the occurrence of the ith component failure mode, $i = 1, 2, \ldots, n$. r = the maximum number of simultaneous component failure modes to be considered. ϵ = the upper limit of allowable unconservative error in the evaluation of system reliability. Then if the probabilities $P(a_i)$ are ranked and indexed in order of decreasing magnitude (least reliable first), the minimum value of r can be selected which satisfies the inequality

$$\binom{n}{r+1} \prod_{i=1}^{r+1} P(a_i) < \epsilon \tag{1}$$

where

$\binom{n}{r+1}$ is the $(r+2)$th binomial coefficient of order n.

Equation (1) is based on the conservative assumption that each possible combination of $r+1$ simultaneous occurrences of component failure modes may constitute a system failure. In applications to high-reliability systems, acceptable values of r have ranged from three to four. Even in low-reliability systems, it is doubtful that values of r greater than six would be required.

If N represents the remaining number of points in the sample space, then

$$N = \sum_{j=0}^{r} \binom{n}{j} \tag{2}$$

For example, consider a system of ten components, each with a single failure mode and probability of failure $P(a_i) = 0.01$ and let $= 0.000003$ be the limit of acceptable error. Trying $r = 2$, Eq. (1) yields $120\ (0.01)^3 = 0.00012$, which is not less than 0.000003. Trying $r = 3$, $210\ (0.10)^4 = 0.0000021$, which does meet the criterion. We may thus base our reliability analysis on consideration of at most three simultaneous failures. Of the $2^{10} = 1024$ combinations (sample points) implied by the data, we use only

$$\binom{10}{1} + \binom{10}{2} + \binom{10}{3} = 175 \text{ combinations}$$

Definition of System Success

Equation (2) represents a considerable reduction in the number of sample points to be considered. However, for a complex system, examination of each point and evaluation of the associated probabilities may still be a formidable task. To reduce the magnitude of this task, another approximation, this time conservative, can be made.

As before, let a_i = failure in the ith component failure mode, $i = 1, 2, \ldots, n$. Then, for a system with multiple modes of operation, minimum system successes, S_j, $j = 1, 2, \ldots, m$ can be defined as the logical intersections of nonoccurrences of these failures. Set-theoretic notation will be used for intersection ($\cap$), complementation ($-$), and inclusive union ($\cup$);

$$S_j = \bigcap_{k_j=1}^{l_j} \overline{b_{kj}} \tag{3}$$

where l_j is the number of nonoccurrences of component failure modes in the jth mode of system operation, and k_j is the index of these nonoccurrences. That is,

$$\overline{b_{kj}} = \overline{a_i} \tag{4}$$

for some i and, since the system has multiple operating modes, it is implied that

$$l_j < n \tag{5}$$

The minimum system successes S_j are a normal output of the engineering process, required for the preparation of oper-

Received December 13, 1965; revision received April 12, 1967. [10.01]

* Senior Reliability Specialist, Reliability Engineering.
† Manager, Scientific Computer Techniques Department. Member AIAA.

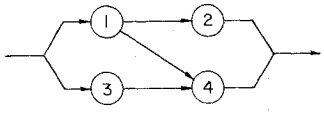

Fig. 1 Schematic flow diagram.

ating and maintenance instructions, etc., and obtainable from the system schematic. They should therefore be readily available to the reliability analyst. They are a conservative basis for reliability analysis, since the omission of an S_j cannot increase the success portion of the sample space.

The event of system success S is an inclusive union of the minimum successes S_j;

$$S = \bigcup_{j=1}^{m} S_j \tag{6}$$

As an illustration, consider the simple system of Fig. 1. Direct evaluation of Eqs. (3) and (6) from the schematic flow diagram yields $S_1 = \bar{a}_1 \cap \bar{a}_2$; $S_2 = \bar{a}_1 \cap \bar{a}_4$; $S_3 = \bar{a}_3 \cap \bar{a}_4$; and $S = S_1 \cup S_2 \cup S_3$.

Boolean Operation in the Reduced Sample Space

Substituting Eqs. (3) and (4) in (6), and defining system failure F as the complement of system success, then

$$F = \bigcap_{j=1}^{m} \bigcup_{k_j=1}^{l_j} b_{kj} \tag{7}$$

where each

$$b_{kj} = a_i \tag{8}$$

for some i. Substituting the equivalent identities of b_{kj} from (8) into (7), the latter can be rearranged as a union of intersections

$$F = \bigcup_{p=1}^{z} F_p \tag{9}$$

where each

$$F_p = \bigcap_{k_p=1}^{y_p} c_{kp} \tag{10}$$

and each

$$c_{kp} = a_i \tag{11}$$

for some i. Further, from the definition of the reduced sample space, the limit of y_p can be constrained by the inequality

$$y_p \leqq r \tag{12}$$

where r satisfies the inequality (1).

The algebraic regrouping involved in converting to Eqs. (9) and (10) result, in general, in Eq. (10) operating on different groups of failure modes (a_i) than does Eq. (3). Further, the number of groups may be different (z need not equal m). In the example,

$$F_1 = a_1 \cap a_3 \qquad F_2 = a_1 \cap a_4$$

$$F_3 = a_2 \cap a_4 \qquad F = F_1 \cup F_2 \cup F_3$$

The events F_p might be called minimum failures of the system. It should be noted that any F_p contained in the intersection of two mutually exclusive failure modes (e.g., a relay cannot fail both open and closed) must be eliminated from the union of Eq. (9).

These operations are tedious. Fortunately, the complementation of Eq. (6) to produce Eq. (7), rearrangement of the latter into the form (9) and the definitions of (10) and (11) can readily be carried out by computer. The Lockheed-California Company has in operation a FORTRAN IV program to do this for systems with up to 200 components and 2000 definitions of minimum system success. It was of course necessary to resort to bit logic in order to fit the program into the core storage limitations of the current generation of computers.

In the program, the minimum system successes S_j are stored as the column vectors of a matrix with the ith element equal to zero if S_j is contained in $\bar{a}_i$ and equal to unity otherwise. If any combination of component failure modes represents a system failure, then the logical intersection of the row vectors corresponding to those failure modes is identically zero, i.e., each of its elements is zero. In the example given previously, this matrix would be

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Evaluation of the Model

Equation (9) can be considered as a model of unreliability. Its associated probabilities of failure can be evaluated by use of the relations

$$P(X \cup Y) = 1 - [1 - P(X)][1 - P(Y)] \tag{13}$$

$$P(X \cap Y) = P(X)P(Y) \tag{14}$$

Alternatively, Eq. (9) can be complimented to give a reliability model

$$S = \bar{F} = \bigcap_{p=1}^{z} \bar{F}_p \tag{15}$$

where each

$$\bar{F}_p = \bigcup_{k_p=1}^{y_p} \bar{c}_{kp} \tag{16}$$

and each

$$\bar{c}_{kp} = \bar{a}_i \tag{17}$$

for some i. Equations (13) and (14) are also used to evaluate the reliability model. These equations assume independence of the events. This assumption is true by hypothesis at the component level. However, it will not always hold true for the intersections F_p of Eq. (9). Before evaluating the model, therefore, it is desirable to reduce or to eliminate the effect of this statistical dependence.

Refinement of the Model

The F_p of Eq. (9) are not always statistically independent. Those with common elements can be collected and combined into more complex expressions. In the example, either

$$F_1 \cup F_2 = a_1 \cap (a_3 \cup a_4)$$

or

$$F_2 \cup F_3 = (a_1 \cup a_2) \cap a_4$$

Then the event F of Eq. (9) could be expressed as

$$F = [a_1 \cap (a_3 \cup a_4)] \cup [a_2 \cap a_4]$$

and the event S would be the complement of F;

$$S = [\bar{a}_1 \cup (\bar{a}_3 \cap \bar{a}_4)] \cap [\bar{a}_2 \cup \bar{a}_4]$$

It will be noted that some statistical dependence still remains in the refined model. However, its effect is both small and conservative. The refined reliability model will always be in the form of an intersection of terms, some of which will

be of the complex form of the bracketed terms given in the example.

Consider any two such terms, symbolized by X and Y. Evaluation of the model uses Eq. (14), repeated here for convenience; $P(X \cap Y) = P(X)\ P(Y)$. More accurate evaluation would be given by

$$P(X \cap Y) = P(X|Y)\ P(Y) \tag{18}$$

The use of Eq. (14) is always conservative, since component successes only are used in the reliability model, and

$$P(X|Y) \geqq P(X) \tag{19}$$

The magnitude of this error can also be approached from the unreliability model. This model includes the effects of certain failure patterns more than once. The patterns so redundantly included, however, are the intersections of more failures than are required to fail the system. With components of reasonable reliability, therefore, the numerical effect is small. The example illustrates this. Let

$$P[a_1] = P[a_2] = P[a_3] = P[a_4] = 0.10$$

Evaluation of the model for this example shows a reliability for the system >0.971 compared to a value of 0.972 from a Bayesian analysis of the system. With higher reliability components, the effect of statistical dependence would be even less noticeable. For example, if

$$P[a_1] = P[a_2] = P[a_3] = P[a_4] = 0.01$$

then the system reliability as given by the model is conservative by an additional increment of only 1.0×10^{-6}.

Summary

The mathematical reliability model is developed from a readily available and philosophically conservative basis. The labor of model generation can be reduced to the preparation of computer input data in standard form. The output is easily interpreted; it can even be displayed as a series-parallel diagram. Evaluation is straightforward, eliminating any Bayesian analysis, and can also readily be performed on the computer. The two errors of approximation are small and tend to cancel each other. The unconservative error can be held below a specified upper bound.

JULY-AUG. 1967 J. AIRCRAFT VOL. 4, NO. 4

Design of a Fairing for the Junction of Two Wings

R. SOPHER*
Canadair Limited, Montreal, Quebec, Canada

A comparatively simple iterative method for the design of bullet-like fairings giving a subsonic, subcritical flow with a desired velocity at the junction of two wings is presented. It differs from published methods because its equations are consistently satisfied by using the calculated shape in the next calculation, until convergence is established. It can yield complete fairings, including sections at right angles to the freestream. The chief result is that further iterations may noticeably improve the shape. However, in all cases except one, convergence is well-advanced on the second iteration. The effect of slenderness on the waisting required is also illustrated. The validity of the method is partially established from independent theoretical and flight-test results. The report should be regarded as providing only part of the results, with further work capable of giving the section of the fairing at right angles to the freestream. This is tentatively assumed to be made up of circular arcs.

Nomenclature

a = x coordinate of the front of the fairing
B = Prandtl-Glauert factor [$= (1 - M^2)^{1/2}$]
b = x coordinate of the rear of the fairing
c = chord length of rectangular wing
$\pm F(x)$ = z coordinate of the surface of the horizontal wing
f = perturbation potential of the horizontal source sheet
$\pm G(x)$ = y coordinate of the surface of the vertical wing
g = perturbation potential of the vertical source sheet
$H(x,\theta)$ = r coordinate of the surface including wings and fairing
$H(x,\theta^*)$ = r coordinate of the design line
H_1 = r coordinate of the design line at initial design point
h = line source perturbation potential
M = freestream Mach number
$q_H(x)$ = reduced line source strength
V = velocity
V_0 = freestream velocity
$V_b(x)$ = velocity increment required on the design line
x_1 = x coordinate of the initial design point
(x, y, z) = Cartesian coordinates
(x, r, θ) = cylindrical coordinates
$\theta^*(x)$ = polar angle of the design line
ϕ = perturbation potential ($= f + g + h$)

Subscripts

x,r,θ = differentiation with respect to x, r, θ

Superscript

$(\ )'$ = running coordinate

Received January 3, 1967; revision received April 17, 1967. [3.01, 3.02]

* Member of Staff; now Senior Research Engineer, Sikorsky Aircraft, Stratford, Conn. Member AIAA.

Introduction

THE use of bullet-like fairings to improve the flow at the junctions of intersecting wings is well-established. In published literature, an early subject is the reduction of the drag of struts.[1] Later, a vortex ring representation was used to design tail-junction fairings for shockless flow at subsonic speed.[2] A few remarks about this method are in order. Although the use of vortex rings is sound, the results obtained are poor, as is established from incompressible flow pressure distribution measurements. This is due chiefly to the use of only a few unknowns and results corresponding to only the first iteration used here. The method does not lend itself